BOOLEAN RELATION THEORY AND INCOMPLETENESS

Harvey M. Friedman
Distinguished University Professor of Mathematics, Philosophy, and Computer Science
The Ohio State University
June 13, 2011 version

TABLE OF CONTENTS

DEDICATION

To my mother, Beatrice Friedman,
and the memory of my father, Allan Friedman

ACKNOWLEDGEMENTS

I have interacted with many scholars over the years concerning Boolean Relation Theory and Concrete Mathematical Incompleteness. These interactions have encouraged me to intensify my efforts. But they also have also made me realize just how much greater are the challenges that lie ahead, if Concrete Mathematical Incompleteness is to be inexorably woven into the mathematical culture.

I want to first thank the three anonymous referees for corrections and comments, as well as advice that was largely adopted.

Special thanks are due to Andrey Bovykin, who organized a one week meeting at Bristol in December, 2009, during which Andrey was accompanied by Lorenzo Carlucci and Andreas Weierman, together with four Ph.D. students Stuart King, Florian Pelupessy, Sam Sanders, and Michiel De Smet, endured about 50 hours(!) of my lectures on Chapter 5, with the expressed goal of finding bugs.

This team of seven divided the checking equally. I am glad to report that they found hundreds of typos, but only a mite (defined as 10% of a bug), all of which have been fixed.

Special thanks are also due to Gregory Cherlin, Peter Koellner, and again to Andrey Bovykin, Lorenzo Carlucci, and Andreas Weierman, for providing detailed corrections and suggestions concerning the lengthy Introduction.

Next, I want to thank several local scholars at The Ohio State University in Columbus, Ohio, USA, who had to listen to me talk their ears off, at all hours of the day and night, in their offices and at their homes, about the singular virtues of Boolean Relation Theory and Concrete Mathematical Incompleteness. These are Ovidiu Costin, David Goss, Christopher Miller, Stephen Milne, Neil Robertson, and Akos Seress of the Mathematics Department; Salvatore Florio, Stewart Shapiro, and Neil Tennant of the Philosophy Department; and Bill Ogden and Bruce Weide of the Computer Science Department.

I want to thank the Editorial Board of the FOM email list, http://www.cs.nyu.edu/mailman/listinfo/fom/, who allowed me to make literally hundreds of FOM postings concerning Concrete Mathematical Incompleteness. I have received special feedback from the Moderator, Martin Davis.

I am grateful for valuable interaction concerning Concrete Mathematical Incompleteness from a great number of mathematical logicians, including Jeremy Avigad, Lenore Blum, Lou van den Dries, Leo Harrington, Denis Hirschfeldt, Jeffrey Hirst, Ehud Hrushovski, Aki Kanamori, Jerry Keisler, Victor Marek, Dave Marker, Donald Martin, Adrian Matthias, Antonio Montalban, Itay Neeman, Anil Nerode, Michael Rathjen, Jeffrey Remmel, Andre Scedrov, Richard Shore, Theodore Slaman, Robert Solovay, Bill Tait, Simon Thomas, and Hugh Woodin.

I have received crucial feedback concerning Concrete Mathematical Incompleteness from many important mathematicians whose area of expertise does not include mathematical logic, including Alain Connes, John Conway, Charles Fefferman, Hilel Furstenburg, Tim Gowers, Ronald Graham, Mikhail Gromov, David Kazhdan, Simon Kochen, Richard Lyons, Yuri Manin, Barry Mazur, David Mumford, Ed Nelson, Paul Sally, Paul Seymour, Joel Spencer, Dan Stroock, Don Zagier, and Doron Zeilberger,

I have also received valuable feedback concerning Concrete Mathematical Incompleteness from many important philosophers, including Andy Arana, Paul Benacerraf, Alan Berger, John Burgess, Mic Detlefsen, Hartry Field, Kit Fine, Warren Goldfarb, Geoffrey Hellman, Juliette Kennedy, Peter Koellner, Saul Kripke, Pen Maddy, Vann McGee, Hilary Putnam, Gideon Rosen, Patrick Suppes, and Jouko Väänänen.

Finally, I would like to acknowledge the tender loving care of my wife, Judith Schwartz, who was so shocked by the length of the Introduction.

PREFACE

The standard axiomatization of mathematics is given by the formal system ZFC, which is read "Zermelo Frankel set theory with the axiom of choice".

The vast majority of mathematical proofs fit easily into the ZFC formalism. ZFC has stood the test of time.

However, a long list of mathematically natural statements of an abstract set theoretic nature have been shown to be undecided (neither provable nor refutable) in ZFC, starting with the pioneering work of Kurt Gödel and Paul J. Cohen concerning Cantor's continuum hypothesis.

Yet these statements involve general notions that are uncharacteristic of normal mathematical statements. The unprovability and unrefutability from ZFC depends on this uncharacteristic generality. For example, if we remove this uncharacteristic generality from Cantor's continuum hypothesis, we obtain a well known theorem of Aleksandrov and Hausdorff (see [Al16] and [Hau16]).

Already as a student at MIT in the mid 1960s, I recognized the critical issue of whether ZFC suffices to prove or refute all concrete mathematically natural statements. Here concreteness refers to the lack of involvement of objects of a distinctly pathological nature. In particular, the finite, the discrete, and the continuous (on nice spaces) are generally considered concrete - although, generally speaking, only the finite is beyond reproach.

From my discussions then with faculty and fellow students, it became clear that according to conventional wisdom, the Incompleteness Phenomena was confined to questions of an inherently set theoretic nature. The incompleteness would not appear if this uncharacteristic generality is removed.

According to conventional wisdom, reasonably well motivated problems in relatively concrete standard mathematical settings can be settled with the usual axioms for mathematics (as formalized by ZFC). The difficulties associated with such problems are inherently mathematical and not "logical" or "foundational".

It was already clear to me at that time that despite the great depth and beauty of the ongoing breakthroughs in set theory regarding the continuum hypothesis and many other tantalizing set theoretic problems, the long range impact and significance of ongoing investigations in the foundations of mathematics is going to depend greatly on the extent to which the Incompleteness Phenomena touches normal concrete mathematics. This perception was confirmed in my first few years out of school at Stanford University with further discussions with mathematics faculty, including Paul J. Cohen.

Yet I was confronted with a major strategic decision early in my career concerning how, or even whether, to investigate this issue of Concrete Mathematical Incompleteness.

The famous incompleteness results of Gödel and Cohen involving the Axiom of Choice (over ZF) and the Continuum Hypothesis (over ZFC), involved problems that had previously been formulated. In fact, the Axiom of Choice and the Continuum Hypothesis were widely offered up as candidates for Incompleteness.

Yet there were no candidates for Concrete Mathematical Incompleteness from ZFC being offered. In fact, to this day, no candidates for Concrete Mathematical Incompleteness have arisen from the natural course of mathematics.

In fact, it still seems rather likely that all concrete problems that have arisen thus far from the natural course of mathematics can be proved or refuted within ZFC.

So what can be the rationale for pursuing a search for Concrete Mathematical Incompleteness?

We offer two rationales for pursuing Concrete Mathematical Incompleteness. One is the presence of Concrete Mathematical Incompleteness in the weaker sense of being independent of significant fragments of ZFC. Since the vast bulk of mathematical activity involves insignificant fragments of ZFC, examples where significant fragments of ZFC are required is significant from the point of view of the foundations of mathematics.

In fact, we do have a rather convincing example of Concrete Mathematical Incompleteness arising from an existing - in fact celebrated - mathematical theorem. This is the theorem of J.B. Kruskal about finite trees. See the detailed discussion in section 0.9B of the Introduction. The story continues with the also celebrated Graph Minor Theorem, as discussed in section 0.10B of the Introduction.

Once the ice is broken with the Concrete Mathematical Incompleteness of existing celebrated theorems, it appears inevitable to consider examples of Concrete Mathematical Incompleteness from significant fragments of ZFC that are in various senses "almost existing mathematical theorems" or "close to existing mathematical theorems" or "simple modifications of existing mathematical theorems". Most of the Introduction is devoted to a detailed discussion of such examples.

The second rationale for pursuing Concrete Mathematical Incompleteness preserves ZFC as the ambitious target. The idea is that normal mathematical activity up to now represents only an infinitesimal portion of eventual mathematical activity. Even if current mathematical activity does not give rise to Concrete Mathematical Incompleteness from ZFC, this is a very poor indication of whether this will continue to be the case, particularly far out into the future.

These considerations give rise to the prospect of uncovering mathematical areas of the future, destined to arise along many avenues, that are replete with Concrete Mathematical Incompleteness from ZFC.

We believe that Boolean Relation Theory is such a field from the future. Most of this book is devoted to Concrete Mathematical Incompleteness from ZFC that arises in Boolean Relation Theory.

We anticipate that further development of BRT will uncover additional connections with concrete mathematical activity - strengthening the argument that it is a field from the future - as well as additional Concrete Mathematical Incompleteness from ZFC.

While completing this book, we have continued the search for additional Concrete Mathematical Incompleteness that opens up new connections with normal mathematics. These new developments - which have yet to be prepared for publication - are discussed in sections 0.14D - 0.14I. They suggest a general structure theory for maximal objects which can, and can only be carried out with the use of large cardinal hypotheses (or their consistency with ZFC).

The extent to which these new developments invade mathematics remains to be seen.

INTRODUCTION
CONCRETE MATHEMATICAL INCOMPLETENESS

This Introduction sets the stage for the new advances in Concrete Mathematical Incompleteness presented in this book.

The remainder of this book can be read without relying on this Introduction. However, we advise the reader to peruse this Introduction in order to gain familiarity with the larger context.

Readers can proceed immediately to the overview of the contents of the book by first reading the brief account in section 0.14C, and then the fully detailed overview in section 0.15. These are self contained and do not rely on the rest of the Introduction.

In this Introduction, we give a general overview of what is known concerning Incompleteness, with particular emphasis on Concrete Mathematical Incompleteness. The emphasis will be on the discussion of examples of concrete mathematical theorems - in the sense discussed in section 0.3 - which can be proved only by using unexpectedly strong axioms.

The incompleteness phenomenon, in the sense understood today, was initiated by Kurt Gödel with his first incompleteness theorem, where he essentially established that there are sentences which cannot be proved or refuted using the usual axioms and rules of inference for mathematics, ZFC (assuming ZFC is free of contradiction). See [Go31], and [Go86-03], volume 1.

Gödel also established in [Go31] that this gap is not repairable, in the sense that if ZFC is extended by finitely many new axioms (or axiom schemes), then the same gap remains (assuming the extended system is free of contradiction).

With his second incompleteness theorem, Gödel gave a critical example of this incompleteness. He showed that the statement

Con(ZFC) = "ZFC is free of contradiction"

is neither provable nor refutable in ZFC (assuming ZFC is legitimate in the sense that it proves only true statements in the ring of integers). Again, see [Go31], and [Go86-03], volume 1.

Although Con(ZFC) is a natural statement concerning the axiomatization of abstract set theory, it does not represent a natural statement in the standard subject matter of mathematics.

While it is true that Con(ZFC) can be stated entirely in terms of finite strings of symbols from a finite alphabet, when stated in this way, it is no longer natural in any mathematical sense.

These considerations led to the informal working distinction between "mathematically natural" and "metamathematically natural".

After the two incompleteness theorems, there remained the crucial question of whether there is a mathematically natural statement which is neither provable nor refutable in ZFC.

This question had a potentially practical consequence. If the answer is no, then there is a clear sense in which mathematicians can forever be content to ignore the incompleteness phenomenon. However, if the answer is yes, then there is a clear sense in which the incompleteness phenomenon can impact their work.

Gödel addressed this question through his pioneering work on Cantor's Continuum Hypothesis (CH). CH states that every infinite set of real numbers is in one-one correspondence with either the integers or the real numbers.

Gödel proved that ZFC does not suffice to refute CH. See [Go38], and [Go86-03], volume 2. That ZFC does not suffice to prove CH had to wait for the pioneering work of Paul J. Cohen, [Co63,64]. Also see [Je78,06].

Thus by the mid 1960s, a mathematically natural statement - the continuum hypothesis - was shown to be neither provable nor refutable in ZFC. Mathematical Incompleteness from ZFC was born.

Yet mathematicians generally did not feel that CH was relevant to their work. This feeling of irrelevance went much deeper than just their particular research interests.

There is a fundamental alienation of "questions like CH" from mathematical culture. Specifically, CH fundamentally involves a level and kind of generality that is entirely uncharacteristic of important and fruitful mathematical questions.

Mathematicians will normally use general abstract machinery - when convenient - in the course of treating a relatively concrete problem. Witness the extensive use of general abstract machinery in Wiles' proof of Fermat's Last Theorem, and how much of this machinery can be removed (see [Mc10]).

The general abstract machinery will be tamed if it causes its own difficulties or ceases to be convenient for various reasons. But the standards for objects of primary investigation of major interest are quite different.

Sets of real numbers that play a role in mathematics as objects of primary investigation, are constructed in some fashion that is related to clear mathematical purposes. In virtually all cases, sets of real numbers appearing as objects of primary investigation, are Borel measurable (i.e., lie in the σ sigma generated by the open sets), and usually very low in the standard hierarchy of Borel measurable sets.

For Borel measurable sets of real numbers, the continuum hypothesis is a theorem, even in the following strong form:

every infinite Borel measurable set of reals is in one-one correspondence with the integers, or in Borel one-one correspondence with the reals.

See [Al16], [Hau16], and [Ke94], p. 83.

This situation is typical of so many statements involving sets and functions in complete separable metric spaces. The Borel measurable forms are theorems, and have nothing to do with incompleteness.

Furthermore, the great generality present in so many such statements is rather empty from the point of view of mathematical culture: there are virtually no mathematically interesting examples beyond Borel sets.

There have been subsequent examples of ZFC incompleteness of less generality than arbitrary sets of reals. Most notably, involving the projective hierarchy of sets of reals, which is obtained by starting with Borel sets in several dimensions, and applying the operations of projection and complementation.

Yet again, we see that the statements are decided in ZFC for Borel sets, and there are virtually no mathematically interesting examples that come under this generality beyond Borel sets.

We take the view that Concrete Mathematical Incompleteness begins at the level of Borel measurable sets and functions on complete separable metric spaces. In section 0.3, we refine this to

Mathematical statements concerning Borel measurable sets and functions of finite rank in and between complete separable metric spaces.

We take the position that once we are discussing possibly very discontinuous functions between complete separable metric spaces, the Borel sets and functions of finite rank are not overly general - there are sufficient mathematically interesting examples of such reaching out to at least the first few finite levels.

In sections 0.11 - 0.13, incompleteness ranging from fragments of ZFC through ZFC and more are discussed in the setting of finite rank Borel sets and functions. In most cases, the incompleteness already starts kicking in at the first few finite ranks of the Borel hierarchy.

However, Borel measurable sets and functions in complete separable metric spaces - even of low finite rank - is still substantially beyond what is considered normal for significant mathematical questions in the present mathematical culture.

Incompleteness begins to become potentially noticeable when the examples live in discrete structures. Here by discrete structures, we mean finitely generated systems such as the ordered ring of integers, and the ordered field of rationals. We work with sets in and functions between discrete structures.

Examples of incompleteness ranging from fragments of ZFC, to ZFC and beyond, are discussed in sections 0.5 - 0.10, and section 0.14.

Boolean Relation Theory, the subject of this book, involves sets in and functions on the nonnegative integers. There is a brief account in section 0.14, and a detailed account in section 0.15.

Some new developments that push Concrete Mathematical Incompleteness even further into the more immediately accessible and perfectly natural, are presented in section 0.14 without proof. The relevant manuscripts are under preparation.

This Introduction concludes with a discussion of Concreteness in the realm of the Hilbert 1900 Problem List. This illustrates how the usual classification of mathematical statements used in mathematical logic (see the four displayed lists in section 0.3) relates to many contexts in core mathematics.

The reader of this Introduction will see rather explicitly how the use of stronger and stronger fragments of ZFC, all the way through ZFC and extensions thereof by so called large cardinal hypotheses, supports proofs of more and more mathematically natural concrete statements.

In other words, this growing body of results shows rather explicitly what is to be gained by strengthening axiom systems for mathematics.

Of course, there is an even greater loss realized by strengthening a consistent axiom system to an inconsistent one. The issue of why we believe, or why we should believe, that the relevant axiom systems used in this book are consistent - or, more strongly, that they prove only true arithmetic sentences - is an important one, but lies beyond the scope of this book.

Since this Introduction is to be viewed as clarifying background material for the six Chapters, many of the proofs are briefly sketched. We also include folklore, results that can be easily gleaned from the literature, and results, without proof, that we intend to publish elsewhere. We provide an adequate, but by no means complete, list of references.

We close these introductory remarks with a topic for specialists.

We use the system EFA (exponential function arithmetic) as a base theory for most of the arithmetical claims. Sometimes SEFA (superexponential function arithmetic) is needed. EFA and SEFA are already presented and used in section 0.1 for a different purpose.

A typical situation is the conservativity of $I\Sigma_1$ (one quantifier induction) over PRA (primitive recursive arithmetic). Perhaps the simplest proof of this result is by a very natural model theoretic argument (see, e.g., [Si99,09], Theorem IX.3.16). SEFA arises because of the need for cut elimination (to which it is equivalent over EFA). Model theoretic proofs in such contexts are often simpler and well known, but cannot be formalized as given in SEFA, or in even stronger systems. A general method for augmenting the model theoretic arguments with additional ideas to get proofs in SEFA is given in [Fr99c]. Proof theoretic approaches to these results and many other such results are known, and originated much earlier. E.g., see [Min73], [Pa70], and [Tak90]. Careful formalizations of these proof theoretic arguments, here and in many other contexts, can also be made in SEFA.

0.1. General Incompleteness.

General Incompleteness was initiated by Gödel's landmark First and Second Incompleteness Theorems, which apply to very general formal systems. The original reference is [Go31].

Throughout this Introduction, we will use the following setup for logic.

MSL (many sorted logic) is many sorted first order predicate calculus with equality. Here we have countably many sorts, countably infinitely many sorted constant, relation, and function symbols, and equality in each sort.

Let T be a set of formulas in MSL. L(T) is the language of T, which consists of the sorts and symbols that appear in T. In particular, L(T) may not have equality in all of the sorts that appear in T.

We say that φ is provable in T (provable from T, T implies φ), if and only if φ is a formula in L(T) which is provable from (the universal closures of elements of) T using the usual Hilbert style axioms and rules of inference for L(T). By the Gödel Completeness Theorem, this is the same as: T semantically implies φ.

0.1A. Gödel's First Incompleteness Theorem.

The powerful recursion theoretic approach to Gödel's First Incompleteness Theorem first appears in [Ro52] and [TMR53], through the use of the formal system Q.

Q is a set of formulas in one sort and 0,S,+,•,≤,=. It consists of the following eight formulas.

1. $Sx \neq 0$.
2. $Sx = Sy \rightarrow x = y$.
3. $x \neq 0 \rightarrow (\exists y)(x = Sy)$.

4. x + 0 = x.
5. x + Sy = S(x + y).
6. x • 0 = 0.
7. x • Sy = (x • y) + x.
8. x ≤ y ↔ (∃z)(z + x = y).

The last axiom is purely definitional. An alternative is to discard axiom 8 and remove ≤ from the language. However, use of ≤ facilitates the statement of the following theorem.

A bounded formula in L(Q) is a formula in L(Q) whose quantifiers are bounded, in the following way.

$$(\forall n \leq t)$$
$$(\exists n \leq t)$$

where t is a term in L(Q) in which n does not appear.

A Π^0_1 (Σ^0_1) formula in L(Q) is a formula in L(Q) that begins with zero or more universal (existential) quantifiers, followed by a bounded formula.

The following is well known and easy to prove.

THEOREM 0.1A.1. A Σ^0_1 sentence in L(Q) is true if and only if it is provable in Q. Let T be a consistent extension of Q in MSL. Every Π^0_1 sentence in L(Q) that is provable in T, is true. (Note that the second part follows from the first).

THEOREM 0.1A.2. Let T be a consistent extension of Q in MSL. The set of all Π^0_1 sentences in L(Q) that are i) provable in T, ii) refutable in T, iii) provable or refutable in T, is not recursive.

Proof: This appears in [Ro52] and [TMR53]. It is proved using the construction of recursively inseparable recursively enumerable sets; e.g., $\{n: \varphi_n(n) = 0\}$ and $\{n: \varphi_n(n) = 1\}$. QED

We can obtain the following strong form of Gödel's First Incompleteness Theorem as an immediate corollary.

THEOREM 0.1A.3. Gödel's First Incompleteness Theorem for Extensions of Q (strong Gödel-Rosser form in [Ross36]). Let T be a consistent recursively enumerable extension of Q in MSL. There is a true Π^0_1 sentence in L(Q) that is neither provable nor refutable in T.

Proof: By Theorem 0.1A.1, we can, without loss of generality, remove "true". If this is false, we obtain a decision procedure for the Π^0_1 sentences in L(Q) that are provable in T, by searching for proofs in T. This contradicts Theorem 0.1A.2. QED

We can use the negative solution to Hilbert’s Tenth Problem in order to obtain other forms of Gödel's First Incompleteness Theorem that are stronger in certain respects, such as Theorem 0.1A.4.

Hilbert's 10th problem asks for a decision procedure for determining whether a given polynomial with integer coefficients in several integer variables has a zero.

The problem was solved negatively in 1970 by Y. Matiyasevich, building heavily on earlier work of J. Robinson, M. Davis, and H. Putnam. In its strong form, the MRDP theorem (in reverse historical order) asserts that every r.e. subset of N^k is Diophantine, in the sense that it is of the form

$$\{x \in N^k: (\exists y \in N^r)(P(x,y) = 0)\}$$

where r,P depend only on k, and P is a polynomial of k+r variables with integer coefficients. (There are stronger forms of this theorem, where r is an absolute number, and involving only one polynomial P). See [Da73], [Mat93].

The MRDP theorem has been shown to be provable in a certain weak fragment of arithmetic which we call EFA = exponential function arithmetic. See section 0.5 for the axioms of EFA. The proof of MRDP in EFA appears in [DG82].

A Diophantine sentence in L(Q) is a sentence in L(Q) of the form

$$(\forall x_1,\ldots,x_n)(s \neq t)$$

where s,t are terms in L(Q). We use the term "Diophantine" because $(\forall x_1,\ldots,x_n)(s \neq t)$ expresses the nonexistence in the nonnegative integers of a zero of the polynomial s-t.

THEOREM 0.1A.4. Gödel's First Incompleteness Theorem for Diophantine Sentences (using [MRDP], [DG82]). Let T be a consistent recursively enumerable extension of EFA in MSL. There is a Diophantine sentence in L(Q) that is neither provable nor refutable in T.

Proof: Since EFA proves MRDP, we see that every Π^0_1 sentence in L(Q) is provably equivalent to a Diophantine sentence, over T. Now apply Theorem 0.1A.3. QED

It is not clear whether EFA can be replaced by a weaker system in Theorem 0.1A.4, such as Q. For then the theory T may not prove MRDP.

An important issue is whether there is a "reasonable" Diophantine sentence $(\forall x_1,\ldots,x_n)(s \neq t)$ that can be used in Theorem 0.1A.4 for, say, T = PA or T = ZFC.

We briefly jump to the use of PA = Peano Arithmetic. The axioms of PA are presented in section 0.5.

Let us call a polynomial P a Gödel polynomial if

i. P is a polynomial in several variables with integer coefficients.
ii. The question of whether P has a solution in nonnegative integers is neither provable nor refutable in PA.

We can also use formal systems other than PA here - for example, ZFC. The ZFC axioms are presented in section 0.11.

A truly spectacular possibility is that there might be an "intellectually digestible" Gödel polynomial.

However, we are many many leaps away from being able to address this question. For the present state of the art upper bound on the size of a Gödel polynomial, see [CM07].

One interesting theoretical issue is whether we can establish any relationship between the least "size" of a Gödel polynomial using PA and the least "size" of a Gödel polynomial using ZFC.

0.1B. Two Roles of Gödel's Second Incompleteness Theorem.

Gödel's Second Incompleteness Theorem has played two quite distinct roles in mathematical logic.

Firstly, it is the source of the first intelligible statements that are neither provable nor refutable. E.g., Con(PA) is neither provable nor refutable in PA, and

Con(ZFC) is neither provable nor refutable in ZFC. (We use the notation Con(T) for "T is consistent", or "T is free of contradiction").

Incompleteness from ZFC, involving mathematical statements - in the sense discussed in section 0.3 - came later. Most notably, the continuum hypothesis - a fundamental problem in set theory - was shown to be neither provable nor refutable in ZFC in, respectively, [Co63,64] and [Go38]. The Concrete Mathematical Incompleteness of ZFC came much later - see sections 0.13, 0.14.

Secondly, the Second Incompleteness Theorem is used as a tool for establishing other incompleteness results. In fact, it is used in an essential way here in this book.

Suppose we want to show that ZFC does not prove or refute a statement φ.

i. First we show that φ is provable in an extension T of ZFC that we "trust". In this book, we use an extension of ZFC by a certain large cardinal axiom - strongly Mahlo cardinals of finite order. See section 0.13.

ii. Then we build a model of ZFC using only φ and a fragment K of ZFC. We will assume that K implies EFA, so that K is strong enough to support Gödel's Second Incompleteness Theorem. In this book, we use K = ACA', a very weak fragment of ZFC, which implies EFA. See Definition 1.4.1.

From i, we have established the consistency of ZFC + φ from the consistency of T.

From ii, we have ZFC + φ proves Con(ZFC). So if ZFC proves φ, then ZFC proves Con(ZFC), violating Gödel's Second Incompleteness Theorem (assuming ZFC is consistent).

Note that we have assumed that ZFC is consistent in order to show the unprovability of φ in ZFC. This is necessary, because if ZFC is inconsistent then φ (and every sentence in the language of ZFC) is provable in ZFC.

There is a way of stating the unprovability of φ in a way that does not rely on the consistency of ZFC.

THEOREM 0.1B.1. Let K be a fragment of ZFC, which is strong enough to support the Gödel Second Incompleteness Theorem.

Suppose K + φ proves Con(ZFC). Then φ is unprovable in every consistent fragment of ZFC that proves K.

Proof: To see this, let S be a consistent fragment of ZFC that proves K. We can assume that S is finitely axiomatized. If S proves φ then by the hypotheses, S proves Con(ZFC). In particular, S proves Con(S). Since S extends K, S is subject to Gödel's Second Incompleteness Theorem. Hence S is inconsistent. This is a contradiction. QED

We use the following variant of Theorem 0.1B.1 in section 5.9. For the definition of SMAH, see section 0.13.

THEOREM 0.1B.2. Suppose ACA' + φ proves Con(SMAH). Then φ is unprovable in every consistent fragment of SMAH that logically implies ACA'.

Informal statements of Gödel's Second Incompleteness Theorem are simple and dramatic. However, current fully rigorous statements of the Gödel Second Incompleteness are complicated and awkward. This is because the actual construction of the consistency statement - as a formal sentence in the language of the theory - is rather complicated, and no two scholars would come up with the same sentence.

Although this is a significant issue surrounding the first use of the Gödel Second Incompleteness Theorem as a foundationally meaningful example of incompleteness, this does not affect the applicability of Gödel's Second Incompleteness Theorem for obtaining incompleteness results.

But the fact that we can so confidently use Gödel's Second Incompleteness Theorem without getting bogged down in the construction of actual formalizations of consistency, does strongly suggest that there is a robust formulation of Gödel's Second Incompleteness Theorem.

It is possible to isolate syntactic properties of a formal consistency statement that are sufficient for Gödel's Second Incompleteness Theorem, and which are independent of the construction of any particular formal consistency statement. In this way, we can remove the ad hoc features in a rigorous formulation of Gödel's Second Incompleteness Theorem.

In [Fe60], [Fe82], sufficiency conditions for formalized consistency in predicate calculus are reached by a step by step analysis of the construction of the formalization. However, this leads to a very complicated and lengthy list of conditions. There may be room for future considerable simplification.

Another approach to presenting sufficiency conditions for formalized consistency in predicate calculus is found in the Hilbert Bernays derivability conditions. See [HB34,39], [Fr10]. These are simpler than the conditions that arise from the preceding approach, although they are rather subtle. They also add clarity to the proof of Gödel's Second Incompleteness Theorem.

We present a third kind of sufficiency condition for formalized consistency in predicate calculus. This is through the Gödel Completeness Theorem. The proofs of our results will appear elsewhere in [Fr∞].

We also refer the reader to [Fr07b] and [Vi09], which are also concerned with novel formulations of Gödel's Second Incompleteness Theorem.

0.1C. Adequacy Conditions for Formalized Consistency.

Here is the key idea:

For Gödel's Second Incompleteness Theorem, it is sufficient that the formalization of consistency used support the Gödel Completeness Theorem.

We will use MSL = many sorted first order predicate calculus with equality. Infinitely many constant, relation, and function symbols are available.

Let S be a set of sentences in MSL, and let σ be a sentence in MSL. We define the notion

φ is an S sufficient formalization of Con(σ).

Here Con(σ) refers to consistency in MSL.

This means that φ is a sentence in L(S) such that there is a structure M in L(σ), whose components (domains, constants, relations, and functions) are given by definitions in L(S), such that S proves

$$\varphi \rightarrow \text{M satisfies } \sigma.$$

Here the consequent is a sentence of L(S) that is defined straightforwardly by relativization. Note that this definition is quite easy to make fully rigorous - by direct combinatorial construction, or by induction on formulas of MSL. The intensionality issues that plague the usual statements of Gödel's Second Incompleteness Theorem are not present here.

The most natural system of arithmetic to use for S is EFA (see section 0.5). This system corresponds to the $I\Sigma_0(\exp)$ of [HP93]. Note that the notion

the usual formalizations of Con(σ)

makes good sense. We can take these to mean those that have been constructed - or are intended - by actual practitioners. Note that such formalizations are rarely given in complete detail, and even more rarely, been thoroughly debugged. EFA is finitely axiomatizable (see [DG82] and [HP93], Theorem 5.6, p. 366).

THEOREM 0.1C.1. Let σ be a sentence in MSL. Every usual formalization of Con(σ) in L(EFA) is an EFA sufficient formalization of Con(σ).

Proof: Let Con(σ)* be a usual formalization of Con(σ) in L(EFA). We show that Con(σ)* is a sufficient formalization of Con(σ) in EFA. We adapt a common proof of the Gödel completeness theorem to EFA. We effectively build a labeled 0,1 tree T whose paths define models of a consistent σ. We then show that if T has finitely many vertices, then T can be converted to a proof in MSL of ¬σ. Otherwise, T has an infinite path, and any infinite path yields a model of σ.

The conversion to a proof in MSL of ¬σ goes through in EFA. So assume T has infinitely many vertices. We define the following property P(v) on vertices v in T. P(v) if and only if

i. There are arbitrarily high vertices extending v.
ii. There exists n such that the following holds. There are at most n vertices extending any vertex to the strict left of v.

It is clear, in EFA, that

iii. Any two vertices obeying P are comparable.
iv. There is no highest vertex obeying P.

If there are arbitrarily high vertices obeying P, then we define a model of σ as usual. Otherwise, we have a "cut" in T. We can use standard cut shortening, if necessary, to form a "cut" in T that can be used to define a model of σ. QED

THEOREM 0.1C.2. Let σ be a sentence in MSL. Every EFA sufficient formalization of Con(σ) implies every usual formalization of Con(σ) in L(EFA), over EFA + Con(EFA). (Here Con(EFA) is any usual formalization of Con(EFA) in L(EFA).)

Proof: Let φ be an EFA sufficient formalization of Con(σ). Let M witness this assumption. We argue in EFA + Con(EFA) + φ that σ is consistent in MSL. Let π be a proof of ¬σ in MSL. By relativizing π to M, we obtain a proof in EFA of $\neg\sigma^M$. But we already have a proof in EFA of σ^M. Hence EFA is inconsistent. Therefore π does not exist. Hence σ is consistent. QED

We remind the reader that the usual formalizations of Con(σ) in arithmetic involves arithmetizing finite sequences of nonnegative integers. Accordingly, we define SEFA (super exponential function arithmetic) to be

EFA + "for all n, there is a sequence of integers of length n starting with 2, where each non initial term is the base 2 exponential of the previous term".

SEFA corresponds to the system $I\Sigma_0$ + Superexp in [HP93], p. 376. It is well known that SEFA proves the cut elimination (see [HP93], Theorem 5.17). From this, it is easy to show that SEFA proves the 1-consistency of EFA.

The following combines Theorems 0.1C.1, 0.1C.2.

THEOREM 0.1C.3. Let σ be a sentence in MSL. The usual formalizations of Con(σ) in L(EFA) are characterized, up to provable equivalence in SEFA, as the weakest EFA sufficient formalizations of Con(σ) (weakest in the sense of SEFA). We can replace SEFA here by EFA + Con(EFA). (Here Con(EFA) is any usual formalization of Con(EFA) in L(EFA).)

The proofs can be refined to replace EFA, SEFA by PFA, EFA. Here PFA is "polynomial function arithmetic". The more standard notation is "bounded arithmetic" or $I\Sigma_0$. This extends Q, within the language of Q, by adding the induction scheme for all bounded formulas (i.e., formulas with bounded quantifiers only). See [HP93].

For this purpose, we need to consider WCon(σ), or "weak consistency of σ in MSL". This means that there is no cut free proof of σ in MSL. WCon(σ) is provably equivalent, over SEFA, to Con(σ). However, this is not the case in EFA.

THEOREM 0.1C.4. Let σ be a sentence in MSL. The expert formalizations of WCon(σ) in L(PFA) are characterized, up to provable equivalence in EFA, as the weakest PFA sufficient formalizations of Con(σ) (weakest in the sense of EFA).

We do not use "usual formalizations of Con(σ) in PFA", but instead "expert formalizations of Con(σ) in PFA". This is because such formalizations in PFA are normally done only by experts in weak systems of arithmetic, because of the limited facility for finite sequence coding.

We extend sufficiency to sets of sentences in MSL. Let S,T be sets of sentences in MSL. We define

φ is an S sufficient formalization of Con(T)

if and only if for every conjunction σ of finitely many sentences in T, φ is an S sufficient formalization of Con(σ).

THEOREM 0.1C.5. Let T be a set of sentences in MSL. Every EFA sufficient formalization of Con(T) proves, over SEFA, the usual formalizations of the consistency of each finite fragment of T. If T is recursively enumerable, then the usual formalizations of Con(T) in L(EFA), based on any algorithm for generating T, are EFA sufficient formalizations of Con(T). We can replace SEFA here by EFA + Con(EFA). (Here Con(EFA) is any usual formalization of Con(EFA) in L(EFA).)

THEOREM 0.1C.6. Let T be a set of sentences in MSL. Every PFA sufficient formalization of Con(T) proves, over EFA, the usual formalizations of the weak consistency of each finite fragment of T. If T is recursively enumerable, then the expert formalizations of Con(T) in L(PFA), based on any algorithm for generating T, are PFA sufficient formalizations of Con(T).

We should mention that in many cases, the usual formalizations use "natural" algorithms for generating the elements of T, rather than arbitrary ones. This would be the case for systems axiomatized by finitely many schemes. However, this interesting issue need not concern us here.

0.1D. Gödel's Second Incompleteness Theorem for Arithmetized Consistency.

The following is obtained from Theorem 0.1C.5.

THEOREM 0.1D.1. Gödel's Second Incompleteness Theorem for Consistency Formalized in EFA. Let T be a consistent set of sentences in MSL that implies SEFA. T does not prove any EFA sufficient formalization of Con(T).

The usual statement of Gödel's Second Incompleteness Theorem for arithmetized consistency, is covered here by taking T to be recursively enumerable, using any usual formalization of Con(T) in EFA, and applying Theorem 0.1C.5.

The following is obtained from Theorem 0.1C.6.

THEOREM 0.1D.2. Gödel's Second Incompleteness Theorem for Consistency Formalized in PFA. Let T be a consistent set of sentences in MSL that implies EFA. T does not prove any PFA sufficient formalization of Con(T).

The usual statement of Gödel's Second Incompleteness Theorem for arithmetized consistency (using expert formalizations of consistency), is covered here by taking T to be recursively enumerable, using any expert formalization of Con(T) in PFA, and applying Theorem 0.1C.6.

0.1E. Gödel's Second Incompleteness Theorem for Sequential Consistency.

Gödel used arithmetized consistency statements. Subsequent developments have revealed that it is more natural and direct to use sequence theoretic consistency statements.

We will use a particularly natural and convenient system for the formalization of syntax of L. We will call it SEQSYN (for sequential syntax).

SEQSYN is a two sorted system with equality for each sort. It is convenient (although not necessary) to use undefined terms. There is a very good and standard way of dealing with logic with undefined terms. This is called free logic, and it is discussed, with references to the literature, in [Fr09], p. 135-138.

In summary, two terms are equal (written =) if and only if they are both defined and have the same value. Two terms are partially equal (written ≅) if and only if either they are equal or both are undefined. If a term is defined then all of its subterms are defined.

The two sorts in SEQSYN are Z (for integers, including positive and negative integers and 0), and FSEQ (for finite sequences of integers, including the empty sequence). We have variables over Z and variables over FSEQ (we use Greek letters). We use ring operations 0,1,+,-,•, and ≤,= between integers. We use lth (for length of a finite sequence, which returns a nonnegative integer), val(α,n) (for the n-th term of the finite sequence α, which may be undefined), and = between finite sequences. The nonlogical axioms of SEQSYN are

i. The discrete ordered commutative ring axioms.
ii. Every α has a largest term.
iii. lth(α) ≥ 0.
iv. val(α,n) is defined if and only if 1 ≤ n ≤ lth(α).
v. α = β if and only if for all n, (val(α,n) ≅ val(β,n)).
vi. Induction on the nonnegative integers for all bounded formulas.
vii. Let n ≥ 0 be given and assume that for all 1 ≤ i ≤ n, there is a unique m such that φ(i,m). There exists a sequence alpha of length n such that for all 1 ≤ i ≤ n, val(α,i) = m ↔ φ(i,m). Here φ is a bounded formula in L(SEQSYN) in which α does not appear.

It remains to define the bounded formulas. We require that the integer quantifiers be bounded in this way:

(∀n)(|n| < t →
(∃n)(|n| < t ∧

where t is an integer term in which n does not appear. Here | | indicates absolute value.

We also require that the sequence quantifiers be bounded in this way:

$(\forall\alpha)(\mathrm{lth}(\alpha) \leq t \wedge (\forall i)(1 \leq i \leq \mathrm{lth}(\alpha) \rightarrow |\mathrm{val}(\alpha,i)| \leq t) \rightarrow$
$(\exists\alpha)(\mathrm{lth}(\alpha) \leq t \wedge (\forall i)(1 \leq i \leq \mathrm{lth}(\alpha) \rightarrow |\mathrm{val}(\alpha,i)| \leq t) \wedge$

where t is an integer term in which α does not appear.

Note that SEQSYN does not have exponentiation, yet SEQSYN clearly supports the usual sequence (string) theoretic formalization of consistency.

THEOREM 0.1E.1. SEQSYN is mutually interpretable with Q and with PFA. SEQSYN is interpretable in EFA but not vice versa.

From the above, we see that the **usual** sequence (string) theoretic formalizations of consistency carry a weaker commitment than the **usual** (not the expert) arithmetic formalizations of consistency (which require finite sequence coding in EFA).

We take EXP to be the following sentence in L(SEQSYN).

There exists a sequence α of length $n \geq 1$ whose first term is 2, where every non initial term is twice the previous term.

THEOREM 0.1E.2. Let σ be a sentence in MSL. The usual formalizations of WCon(σ) in L(SEQSYN) are characterized, up to provable equivalence in SEQSYN + EXP, as the weakest SEQSYN sufficient formalizations of Con(σ) (weakest in the sense of SEQSYN + EXP).

THEOREM 0.1E.3. Let T be a set of sentences in MSL. Every SEQSYN sufficient formalization of Con(T) proves, over SEQSYN + EXP, the usual formalizations of the weak consistency of each finite fragment of T. If T is recursively enumerable, then the usual formalizations of Con(T) in L(SEQSYN), based on any algorithm for generating T, are SEQSYN sufficient formalizations of Con(T).

THEOREM 0.1E.3. SEQSYN + EXP and EFA are mutually interpretable. They are both finitely axiomatizable.

Proof: As remarked earlier, EFA is finitely axiomatizable (see [DG82] and [HP93], Theorem 5.6, p. 366). Now we cannot conclude from the mutual interpretability that SEQSYN + EXP is also finitely axiomatizable. As an instructive example, it is well known that Q and bounded arithmetic are mutually interpretable ([HP93], Theorem 5.7, p. 367), but it is a well known open problem whether bounded arithmetic is finitely axiomatizable. But in this case, we have a synonymy of the strongest kind, and that preserves finite axiomatizability. QED

THEOREM 0.1E.4. Gödel's Second Incompleteness Theorem for Consistency Formalized in SEQSYN. Let T be a consistent set of sentences in MSL that implies SEQSYN + EXP. T does not prove any SEQSYN sufficient formalization of Con(T).

0.1F. Gödel's Second Incompleteness Theorem for Set Theoretic Satisfiability.

Let T be a finite set of sentences in ∈,=. By the Set Theoretic Satisfiability of T, we mean the following sentence in set theory (∈,=):

> there exists D,R, where R is a set of ordered pairs from D, such that (D,R) satisfies each element of T.

Let RST (rudimentary set theory) be the following convenient set theory in ∈,=.

a. Extensionality.
b. Pairing.
c. Union.
d. Cartesian product.
e. Separation for bounded formulas.

It can be shown that RST is finitely axiomatizable.

THEOREM 0.1F.1. Gödel's Second Incompleteness Theorem for Set Theoretic Satisfiability. Let T be a consistent finite set of sentences in ∈,= which implies RST. T does not prove the Set Theoretic Satisfiability of T.

COROLLARY. Let T be a consistent set of sentences in ∈,=, which implies RST. Let φ be a sentence in ∈,= such that T + φ proves the set theoretic satisfiability of each finite subset of T. Then T does not prove φ.

It does not appear that we can obtain Gödel's Second Incompleteness Theorem for PA and fragments, in any reasonable form, readily from Gödel's Second Incompleteness Theorem for Set Theoretic Satisfiability.

0.1G. Gödel's Incompleteness Theorems and Interpretability.

The notion of Interpretation between theories is due to Alfred Tarski in [TMR53], and has generated an extensive literature. See [Fr07], lecture 1 for a guide to many highlights. Also see [FVxx].

THEOREM 0.1G.1. Let T be a consistent set of sentences in MSL, in which Q is interpretable. The sets of all sentences in MSL that are i) provable in T, ii) refutable in T, iii) provable or refutable in T, are not recursive.

Proof: Let π be an interpretation of Q in T. Use π to convert the claims to a claim concerning extensions of Q. See Theorem 0.1A.2. This is the approach taken in [TMR53]. QED

We can obtain the following strong form of Gödel's First Incompleteness Theorem as an immediate corollary.

THEOREM 0.1G.2. Let T be a recursively enumerable consistent set of sentences in MSL, in which Q is interpretable. There is a sentence in L(T) that is neither provable nor refutable in T.

Gödel's Second Incompleteness Theorem is used in an essential way to prove the following fundamental fact about interpretations, from [Fe60]. See [Fr07], lecture 1, Theorem 2.4, p. 7.

THEOREM 0.1G.3. For every consistent sentence φ in MSL, there is a consistent sentence ψ in MSL, such that φ is interpretable in ψ, and ψ is not interpretable in φ.

Gödel's Second Incompleteness Theorem also is used in an essential way to prove the following well known fact about PA.

THEOREM 0.1G.4. No consistent extension T of PA in L(PA) is interpretable in any consequence of T.

We can view Theorem 0.1G.4 as a form of Gödel's Second Incompleteness Theorem for extensions of PA, since it immediately implies the following strong form of Gödel's Second Incompleteness Theorem for extensions of PA.

THEOREM 0.1G.5. Let T be a consistent extension of PA in L(PA), and S be a finite fragment of T. No S sufficient formalization of Con(T) is provable in T.

0.2. Some Basic Completeness.

Note that General Incompleteness depends on being able to interpret a certain amount of arithmetic.

However, there are some significant portions of mathematics, which do not involve any significant amount of arithmetic.

This opens the door to there being recursive axiomatizations for such significant portions of mathematics. This is in sharp contrast to Gödel's First Incompleteness Theorem.

A powerful way to present such completeness theorems is to identify a relational structure M and give what is called an axiomatization of M. For judiciously chosen M, the assertions that hold in M generally form a significant portion of mathematics.

Specifically, an axiomatization of M is a set T of sentences in L(M) (the language of M) such that

For any sentence φ of L(M),
φ is true in M if and only if
φ is provable in T.

We say that T is a finite (or recursive) axiomatization of M if and only if T is an axiomatization of M, where T is finite (or recursive).

We frequently encounter M which are recursively axiomatizable but not finitely axiomatizable. The important intermediate notion is that of being axiomatizable by finitely many relational schemes.

Axiom schemes arise in many fundamental axiomatizations. Three particularly well known examples are not axiomatizations of structures. These are PA (Peano Arithmetic), Z (Zermelo Set Theory), and ZFC (Zermelo Set Theory with the Axiom of Choice).

We will not give a careful formal treatment of relational schemes here, but be content with the following semiformal description.

To simplify the discussion, it is convenient to work entirely within the first order predicate calculus with equality, rather than the more general MSL.

Fix a language L' in first order predicate calculus with equality. A scheme is a formula in L' possibly augmented with extra relation symbols called schematic relation symbols. The instances of a relational scheme consists of the result of making any legitimate substitutions of the schematic relation symbols appearing by formulas of L'. One must treat different occurrences of the same schematic symbol in the same way, and put the appropriate restriction on the free variables of the formulas used for substitutions.

Schemes can be generalized to include schematic function symbols. However, we will be using only schematic relation symbols here.

Note that Induction in PA, Comprehension in Z, and both Comprehension and Replacement in ZFC, are schemes. Induction and Comprehension use a single unary schematic relation symbol, whereas Replacement uses a single binary schematic relation symbol. Replacement can also be formalized with a single unary schematic function symbol.

Here we provide axiomatizations by finitely many schemes for each of the 21 basic structures given below.

We use the method of quantifier elimination throughout. The quantifier elimination arguments that we use are well known, and we will not give details.

It is typical in the use of quantifier elimination, that the structures at hand do not admit quantifier elimination themselves, but need to be expanded in order to admit quantifier elimination. Then the quantifier elimination for the expansion is used to derive conclusions about the original structure.

An expansion of a structure is obtained by merely adding new relations, functions, or constants to the structure. A definitional expansion of a structure is an expansion whose new symbols have explicit definitions in the language of the original structure.

We say that M' is the definitional expansion of M via $\pi = \varphi_1,\ldots,\varphi_n$ if M' is the expansion of M whose components are given by the definitions in π made in the language of M.

A typical example is the definitional expansion (N,<,+) of (N,+) via the definition

$$x < y \leftrightarrow x \neq y \wedge (\exists z)(x+z = y).$$

Sometimes we make a definitional expansion, followed by the introduction of new constants. Specifically, we definitionally expand (Z,+) to (Z,0,+,-,2|,3|,...), and then introduce the constant 1 to form (Z,0,1,+,-,2|,3|,...). Note that the constant 1 is not definable in (Z,+).

The following easy results are quite useful when working with axiomatizations. They were used, essentially, by Tarski.

THEOREM 0.2.1. Let M' be the definitional expansion of M via π, and M'' expand M' with constants new to M'. Let S be a set of sentences that hold in M. Let T be an axiomatization of M''. Assume that S proves the well definedness of π for the constant and function symbols new in M'. Assume S proves the result of existentially quantifying out the new constants in the conjunction of any given finite subset of T after π is used to replace the new symbols of T in the conjunction. Then S is an axiomatization of M.

Proof: Let M,M',S,T be as given. Let φ hold in M. Then φ holds in M'', and so φ is provable in T. In any given proof of φ in T, let T' result from conjuncting the axioms of T used, replacing the new symbols of M' by their definitions given by π, and then existentially quantify out the new constants in M''. Then T' logically implies φ, and also S proves T'. Hence S proves φ. Also by hypothesis, S holds in M. QED

THEOREM 0.2.2. Let M,M',M'' be as given in Theorem 0.2.1, where the language of M'' is finite. M is finitely axiomatizable if and only if all (some) axiomatizations of M are logically equivalent to a finite subset. M is finitely axiomatizable if and only if M' is finitely axiomatizable. If M'' is finitely axiomatizable then M is finitely axiomatizable.

Proof: The first claim (well known), involving only M, is left to the reader.

For the third claim, the process of converting an axiomatization of M'' to an axiomatization of M given by Theorem 0.2.1, results in a finite axiomatization of M if the given axiomatization of M'' is finite.

For the second claim, it suffices to show that if M is finitely axiomatizable then M' is finitely axiomatizable. The axiomatization of M' consists of the axiomatization of M together with the definitions given by the interpretation of M in M'. QED

There has been considerable work locating basic mathematical structures with recursive - and usually simple and informative - axiomatizations. We believe that there are many striking cases of this that are yet to be discovered across mathematics.

Here is the list of 21 fundamental mathematical structures with recursive axiomatizations.

LINEAR ORDERINGS

$(N,<)$, $(Z,<)$, $(Q,<)$, $(\Re,<)$.

SEMIGROUPS, GROUPS

$(N,+)$, $(Z,+)$, $(Q,+)$, $(\Re,+)$, $(C,+)$.

LINEARLY ORDERED SEMIGROUPS/GROUPS

$(N,<,+)$, $(Z,<,+)$, $(Q,<,+)$, $(\Re,<,+)$.

BASE TWO EXPONENTIATION

$(N,+,2^x)$.

FIELDS

$(\Re,+,\bullet)$, $(C,+,\bullet)$, $(RALG,+,\bullet)$, $(CALG,+,\bullet)$.

Here RALG is the subfield of real algebraic numbers. CALG is the subfield of complex algebraic numbers.

ORDERED FIELDS

$(\Re,<,+,\bullet)$, $(RALG,<,+,\bullet)$.

EUCLIDEAN GEOMETRY

$(\mathfrak{R}^2,B,E)$.

Here B is the three place relation of betweenness. I.e., $B(x,y,z) \leftrightarrow x,y,z$ lie on a line and y is strictly between x and z. Also E is the four place relation of equidistance. I.e., $E(x,y,z,w) \leftrightarrow d(x,y) = d(z,w)$.

Among these 21, (N,<), (Z,<), (Q,<), $(\mathfrak{R},<)$ are finitely axiomatizable. The axioms for the remaining 17 are not usually presented as finitely many axiom schemes, and some thought is required in order to put them in this form. Of the 17, all but $(N,+,2^x)$ are not finitely axiomatizable. We conjecture that $(N,+,2^x)$ is not finitely axiomatizable.

Below, we freely invoke Theorems 0.2.1 and 0.2.2.

THEOREM 0.2.3. (N,<) is finitely axiomatized by
i. < is a strict linear ordering.
ii. There is a < least element.
iii. Every element has an immediate successor.
iv. Every element with a predecessor has an immediate predecessor.

Proof: i-iv clearly hold in (N,<). We use Theorem 0.2.1 with the definitional expansion (N,<,0,S) via π, where π defines 0 as "the least element", and π defines S as "the immediate successor". (N,<,0,S) has the following well known axiomatization, using elimination of quantifiers. See, e.g., [En72], p. 184.

a. < is a strict linear ordering.
b. 0 is < least.
c. $x \neq 0 \rightarrow (\exists y)(x = S(y))$.
d. $x < S(y) \leftrightarrow x < y \vee x = y$.

Since π is provably well defined in i-iv, and the results of applying π to a-d are provable in i-iv, we see that i-iv is an axiomatization of (N,<). QED

THEOREM 0.2.4. (Z,<) is finitely axiomatized by
i. < is a strict linear ordering.
ii. Every element has an immediate predecessor and an immediate successor.

Proof: i-ii clearly hold in (Z,<). We use Theorem 0.2.1 with the definitional expansion (Z,<,S) via π, where π defines S as "the immediate successor". (Z,<,S) has the following well known axiomatization, using elimination of quantifiers.

a. $<$ is a strict linear ordering.
b. $(\exists y)(x = S(y))$.
c. $x < S(y) \leftrightarrow x < y \vee x = y$.

Since π is provably well defined in i,ii, and the results of applying π to a-c are provable in i,ii, we see that i,ii is an axiomatization of $(N,<)$. QED

THEOREM 0.2.5. $(Q,<)$, $(\Re,<)$ are finitely axiomatized by
i. $<$ is a strict linear ordering.
ii. There is no least and no greatest element.
iii. Between any two elements there is a third.

Proof: This is a particularly well known application of elimination of quantifiers, resulting in this axiomatization. No expansion is needed. QED

THEOREM 0.2.6. $(N,+)$ is axiomatized with a single scheme by
i. $(x+y)+z = x+(y+z)$, $x+y = x+z \rightarrow y = z$.
ii. There are unique $0 \neq 1$ such that $(x+y = 0 \leftrightarrow x,y = 0) \wedge (x+y = 1 \leftrightarrow \{x,y\} = \{0,1\})$.
iii. Every definable set containing 0 and closed under +1 is everything.
$(N,+)$ is not finitely axiomatizable.

Proof: i-iii clearly hold in $(N,+)$. We use Theorem 0.2.1 with the definitional expansion $(N,<,0,S,+,\equiv_2,\equiv_3,\ldots)$ via π, where π defines

$<$ as $x \neq y \wedge (\exists z)(x+z = y)$.
0 as the 0 from ii.
$S(x) = x+1$, where 1 is from ii.
$\equiv_d$, $d \geq 2$, as $x \equiv_d y \leftrightarrow (\exists z)(x = y+dz \vee y = x+dz)$.

Obviously, i-iii proves π is well defined.

We now use the well known elimination of quantifiers for $(N,<,0,S,+,\equiv_2,\equiv_3,\ldots)$ from [Pr29], [En72], p. 188. Here $\equiv_d$, $d \geq 2$, is congruence modulo d. This results in the following axiomatization of $(N,<,0,S,+,\equiv_2,\equiv_3,\ldots)$.

a. $<$ is a strict linear ordering.
b. 0 is the least element.
c. $x \neq 0 \rightarrow (\exists y)(x = S(y))$.
d. $x < S(y) \leftrightarrow x < y \vee x = y$.

e. + is commutative, associative.
f. $x+0 = x$.
g. $x+S(y) = S(x+y)$.
h. $x+z < y+z \leftrightarrow x < y$.
i. $x < y \leftrightarrow (\exists z)(S(x+z) = y)$.
j. $dx < dy \leftrightarrow x < y$.
k. $x \equiv_d y \leftrightarrow (\exists z)(x = y + dz \vee y = x + dz)$.
l. $(\exists y)(x \equiv_d y \wedge y < S^d(0))$.

where $d \geq 2$.

We prove that the results of applying π to a-l are provable in i-iii.

This is the same as treating $<,0,S,\equiv_d$ as abbreviations in 1-iii, and verifying a-l in i-iii. It is convenient to also use the abbreviation $x \leq y \leftrightarrow x < y \vee x = y$, in i-iii.

By ii), $1+1 \neq 0 \wedge 1+1 \neq 1$.

We claim $x+1 \neq 0$. Suppose $x+1 = 0$. Then $x+(1+1) = (x+1)+1 = 0+1 = 1$. By ii), $1+1 \in \{0,1\}$, which is impossible.

We claim $x+0 = x$. Let $E = \{x: x+0 = x\}$. By ii), $0 \in E$. Let $x \in E$. Then $x+0 = x$, and by i),ii), $(x+1)+0 = x+(1+0) = x+1$. Hence E contains 0 and is closed under +1. By iii), E is everything.

We claim $x \neq 0 \rightarrow (\exists y)(x = y+1)$. Let $E = \{x: (\exists y)(x = y+1)\} \cup \{0\}$. Then E contains 0 and is closed under +1. Hence by iii), E is everything.

We claim $0+x = x$. Let $E = \{x: 0+x = x\}$. Then $0 \in E$. Let $x \in E$. Then $0+(x+1) = (0+x)+1 = x+1$. Apply iii).

We claim $x+y = y+x$. Let $E = \{y: x+y = y+x\}$. By the previous paragraph, $0 \in E$. Let $x \in E$. Then $x+y = y+x$, $x+(y+1) = (x+y)+1 = (y+x)+1 = y+(x+1)$. Apply iii).

We claim $x \leq y \leftrightarrow (\exists z)(x+z = y)$. Suppose $x \leq y$. If $x < y$ then we are done. If $x = y$ then use $z = 0$. Now suppose $x+z = y$. If $z = 0$ then we are done. If $z \neq 0$, write $z = w+1$. Hence $z = S(w)$, and we are done.

Obviously $\leq$ is reflexive. We claim $\leq$ is transitive. Let $x+u = y \wedge y+v = z$. Then $x+u+v = z$, and so $x \leq z$.

We claim $y \leq x \rightarrow y+1 \leq x \vee y = x$. Let $y \leq x$. Write $y+z = x$. If $z = 0$ then $y = x$, and we are done. Assume $z \neq 0$, and write $z = w+1$. Then $y+w+1 = x = y+1+w$, and so $y+1 \leq x$.

We claim $x \leq y \vee y \leq x$. Let $E = \{y: x \leq y \vee y \leq x\}$. Obviously $0 \in E$. We now show that E is closed under +1. Suppose $y \in E$. Then $x \leq y \vee y \leq x$. We want $x \leq y+1 \vee y+1 \leq x$.

We are done if $x \leq y$. So assume $y \leq x$. By the previous claim, $y+1 \leq x \vee y = x$. In either case, we are done.

We claim $x \leq y \wedge y \leq x \rightarrow x = y$. Let $x+z = y \wedge y+z = x$. Then $x+z+z = x = x+0$, $z+z = 0$, $z = 0$, $x = y$.

We have established that $\leq$ is a reflexive linear ordering. Hence $<$ is a strict linear ordering.

I.e., we have proved the result of applying π to a) in i-iii.

For b), suppose $x < 0$. Let $x+y = 0$. Then $x,y = 0$, which is impossible.

For c), this has already been proved.

For d), let $x < y+1$. Write $y+1 = x+z+1$. Then $y = x+z$, and so $x \leq y$. Suppose $x < y$. Then $x < y+1$. Suppose $x = y$. Then $x < y+1$.

For e), associativity is from i), and commutativity has been proved.

For f), we have proved $x+0 = x$.

For g), use associativity.

For h), let $x+z < y+z$. Let $x+z+w = y+z$, $w \neq 0$. By cancellation and commutativity, $x+w = y$, and so $x \leq y$. If $x = y$ then $x+z = y+z$, which is impossible. Hence $x < y$. Now let $x < y$. Write $x+w+1 = y$. Then $x+z+w+1 = y+z$, and so $x+z < y+z$.

For i), let $x < y$. Write $y = x+z+1$. Then $S(x+z) = y$. Now let $S(x+z) = y$. Then $y = x+z+1$, and so $x < y$.

For j), let dx < dy. We want x < y, and so assume y ≤ x and write y+z = x. Then d(y+z) < dy. Hence dy+dz < dy+0. By h), dz < 0, which is impossible.

For k), this is by definition.

For l), let E = {x: (∃y,z)(x = dy+z ∧ z < $S^d(0)$)}. Obviously, 0 ∈ E. Suppose x ∈ E. Let x = dy+z ∧ z < $S^d(0)$. Then x+1 = dy+z+1 ∧ z+1 ≤ $S^d(0)$. If z+1 < $S^d(0)$ then x+1 ∈ E. Otherwise, x+1 = dy+$S^d(0)$ = d(y+1)+0 ∧ 0 < $S^d(0)$. In either case, x+1 ∈ E. Hence E contains 0 and is closed under +1. By iii), E is everything. Hence (∀x)(∃y)(x $\equiv_d$ y ∧ y < $S^d(0)$).

To show that (N,+) is not finitely axiomatizable, by Theorem 0.2.2 it suffices to show that any finite fragment of a-l has a model not satisfying all of a-l. This is because a-l is a definitional extension of i-iii.

Let p be any prime. Let D consist of all expressions nx/m + t, where (n,m) = 1, n,t ∈ N, m ∈ N\{0}, and p does not divide m. Define the structure (D,<,0,S,+) in the obvious way, and extend it to (D,<,0,S,+,$\equiv_2$,$\equiv_3$,...) via π.

Evidently, a-i hold in (D,<,0,S,+,$\equiv_2$,$\equiv_3$,...). Also, l) holds provided d ≥ 2 is not divisible by p.

But l) fails for d = p. This is because we cannot write any of x,x-1,...,x-p+1 as a multiple of p in this structure. QED

THEOREM 0.2.7. (Z,+) is axiomatized with two schemes by
i. (Z,+) is an Abelian group.
ii. Every definable subgroup of + with a definable linear ordering is {0}.
iii. R,S be definable binary relations. Suppose for all x, {y: R(x,y)} is a subgroup of + containing x, and {y: S(x,y)} is a proper subgroup of +. Then (∃x)((∀y)(R(x,y) ∧ ¬S(y,x)).
(Z,+) is not finitely axiomatizable.

Proof: Clearly i) holds in (Z,+).

For iii), the proper subgroups of + are the multiples of some fixed d = 0,2,3,... . Hence 1 lies outside of all of them. Set x = 1.

For ii), we use the definitional expansion (Z,0,+,-,2|,3|,...) of (Z,+) via π, where 0 is defined as the additive identity, +,- as addition and the additive inverse, and d|x as $(\exists y)(dy = x)$, $d \geq 2$.

We use the well known elimination of quantifiers for linear arithmetic adapted to the structure (Z,0,1,+,-,2|,3|,...).

The quantifier elimination boils down to considering statements of the form

$$(\exists x)(d_1|s_1 \wedge \ldots \wedge d_n|s_n \wedge \neg e_1|t_1 \wedge \ldots \wedge \neg e_n|t_n \wedge r_1 = 0 \wedge \ldots \wedge r_n = 0 \wedge v_1 \neq 0 \wedge \ldots \wedge v_n \neq 0)$$

where the d_i,e_i are integers ≥ 2, and the s_i,t_i,r_i,v_i are terms. We can replace negated divisibilities by disjunctions of divisibilities, and then rewrite the divisibilities as congruences, obtaining the form

$$(\exists x)(a_1x \equiv_{d\_1} s_1 \wedge \ldots \wedge a_nx \equiv_{d\_n} s_n \wedge r_1 = 0 \wedge \ldots \wedge r_n = 0 \wedge v_1 \neq 0 \wedge \ldots \wedge v_n \neq 0)$$

where the a_i,d_i are integers, $a_i \geq 1$, $d_i \geq 2$, and the s_i,t_i,r_i,v_i are terms, and x does not appear in the s_i. We then consolidate all coefficients on x, obtaining the forms

$$(\exists x)(cx \equiv_{d\_1} s_1 \wedge \ldots \wedge cx \equiv_{d\_n} s_n \wedge cx = r_1 \wedge \ldots \wedge cx = r_n \wedge cx \neq v_1 \wedge \ldots \wedge cx \neq v_n)$$

$$(\exists x)(x \equiv_{d\_1} s_1 \wedge \ldots \wedge x \equiv_{d\_n} s_n \wedge x = r_1 \wedge \ldots \wedge x = r_n \wedge x \neq v_1 \wedge \ldots \wedge x \neq v_n)$$

where the d_i are integers ≥ 2, and the s_i,t_i,r_i,v_i are terms in which x does not appear. We can assume that there are no equations, obtaining the form

$$(\exists x)(x \equiv_{d\_1} s_1 \wedge \ldots \wedge x \equiv_{d\_n} s_n \wedge x \neq v_1 \wedge \ldots \wedge x \neq v_n).$$

This is clearly equivalent to

$$(\exists x)(x \equiv_{d\_1} s_1 \wedge \ldots \wedge x \equiv_{d\_n} s_n)$$

and hence has a solution if and only if it has a solution among the nonnegative integers below the product of the d's. This results in a quantifier free formula.

For ii), first note that every subgroup of + is the set of multiples of some $d \geq 0$. If the multiples of $d > 0$ has a definable linear ordering in (Z,+), then Z has a definable linear ordering in (Z,+), in which case N is definable in (Z,+). Then N is definable in (Z,0,1,+,-,|2,|3,...), and so N is quantifier free definable in (Z,0,1,+,-,|2,|3,...). This is impossible (left to the reader).

We now use this quantifier elimination to complete the proof. In order to support the manipulations for this quantifier elimination, it suffices to have

a. (Z,0,+,-) is an Abelian group, with inverse - and identity 0.
b. $d|x \leftrightarrow (\exists y)(x = dy)$.
c. $dx = dy \rightarrow x = y$.
d. $dx \neq 1$.
e. $d|x \vee d|x+1 \vee d|x+1+1 \vee \ldots \vee d|x+1+\ldots+1$ with d disjuncts.

where $d \geq 2$.

We claim that every quantifier free sentence in 0,1,+,-,2|,3|,... is provable or refutable in a-e. This is left to the reader.

It now follows that a-e is an axiomatization of (Z,0,1,+,-,2|,3|,...).

We now verify the condition in Theorem 0.2.1. Accordingly, fix a positive integer t, let K consist of a) and those instances of b-e based on $2 \leq d \leq t$. Let K' be the result of applying π, and then existentially quantifying out the constant 1.

We can pull out the conjuncts emanating from a)-c) since they do not mention 1. We claim that the result of applying π to a-c, is provable in i-iii. This is obvious for a),b).

For c), suppose $dx = dy \wedge x \neq y$. Then $dz = 0$, $z \neq 0$, where $z = x-y$. Let G be the group $\{0,z,2z,\ldots,(d-1)z\}$ under +. Obviously G is definable since it has at most d elements. It also has a definable linear ordering since it has at most d elements. By ii), it is $\{0\}$, which is a contradiction. Hence c) has been proved in i-iii.

It remains to prove

$$\#)\ (\exists x)(\neg 2|x \wedge \ldots \wedge \neg t!|x \wedge (\forall y)(t!|y \vee t!|y+x \vee \ldots \vee t!|y+(t!-1)x))$$

in i-iii, after applying π. Here $t \geq 2$.

Let $R(x,y)$ be

$$t!|y \vee t!|y+x \vee \ldots \vee t!|y+(t!-1)x.$$

and let $S(y,x)$ be

$$(y = 2 \wedge 2|x) \vee \ldots \vee (y = t! \wedge t!|x) \vee (y \neq 2 \wedge \ldots \wedge y \neq t! \wedge x = 0).$$

Note that i-iii proves $(\forall x)(\{y: R(x,y)\}$ is a group under + containing x), and $(\forall y)(\{x: S(x,y)\})$ is a proper subgroup of +. Hence # immediately follows using iii). Therefore i-iii is an axiomatization of (Z,+).

To show that (Z,+) is not finitely axiomatizable, we give another axiomatization of (Z,+), and show that it is not logically equivalent to any finite subset, and invoke Theorem 0.2.2.

i'. (Z,+) is an Abelian group.
ii'. $dx = dy \rightarrow x = y$.
iii'. $(\exists x)((\neg 2|x \wedge \ldots \wedge \neg d|x) \wedge (\forall y)(d|y \vee d|y+x \vee \ldots \vee d|y+(d-1)x))$.

where $d \geq 2$ and $d|x$ is the usual abbreviation. It is clear from the above that the existential closure of every finite subset of a-e is provable in i'-iii'. Therefore i'-iii' is a complete axiomatization of (Z,+).

Let p be any prime. Let D consist of all expressions $nx/m + t$, where $(n,m) = 1$, $n,t \in Z$, $m \in N\backslash\{0\}$, and p does not divide m. Define the structure (D,+) in the obvious way.

Evidently, i',ii' hold in (D,+) for $2 \leq d < p$. Also iii') holds in (D,+) for $2 \leq d < p$ with $x = 1$.

We claim that iii') fails in (D,+) for $d = p$. To see this, let

$$(\forall y)(p|y \vee p|y+z \vee \ldots \vee p|y+(p-1)z).$$

Now suppose $z = nx/m + t$. By setting $y = 1$, we have

$$p|1 \vee p|1+z \vee \ldots \vee p|1+(p-1)z).$$

It follows that $p|n \wedge p|t$. Now set $y = x$. Then we obtain

$$p|x \vee p|(n+m)x/m \vee p|(2n+m)x/m \vee \ldots \vee p|((p-1)n+m)x/m.$$

Now $(p,m) = 1$, and so the numerators and denominators of the displayed fractions are not divisible by p. Thus we have a contradiction. QED

THEOREM 0.2.8. $(Q,+)$, $(\mathfrak{R},+)$, $(C,+)$ are axiomatized with a single scheme by
i. $(X,+)$ is an Abelian group with at least two elements.
ii. Every definable subgroup of $(X,+)$ with at least two elements is $(X,+)$.
$(Q,+)$, $(\mathfrak{R},+)$, $(C,+)$ are not finitely axiomatizable.

Proof: There is a well known quantifier elimination without expansion. This gives the axiomatization

a. $(X,+)$ is an Abelian group with at least two elements.
b. $dx = dy \rightarrow x = y$.
c. $(\exists y)(dy = x)$.

where $d \geq 2$. From this we obtain that the definable subsets in $(X,+)$ are finite or cofinite. Every subgroup of $(X,+)$ is either infinite or $\{0\}$. Hence every subgroup of $(X,+)$ definable in $(X,+)$ is either cofinite or $\{0\}$. But if it is cofinite then it is obviously $(X,+)$. This establishes that i,ii hold in $(X,+)$.

a) is provable in i,ii. For b), suppose $dx = 0$, $x \neq 0$, $d \geq 2$, and form the finite subgroup $\{0,x,\ldots,(d-1)x\}$. This contradicts ii).

For c), let $d \geq 2$ and form the subgroup of multiples of d. By a,b, this subgroup has at least two elements. By ii), this subgroup is $(X,+)$. Hence c) holds.

Let p be a prime. Let D be the rationals which, in reduced form, has denominator not divisible by p. Form $(D,+)$. Then a,b hold, and c) holds for $2 \leq d < p$. $d \geq 2$, However, c) fails for $d = p$. Hence $(X,+)$ is not finitely axiomatizable. QED

THEOREM 0.2.9. $(N,<,+)$ is axiomatized with a single scheme by
i. $(x+y)+z = x+(y+z)$, $x+y = x+z \rightarrow y = z$.

ii. There are unique $0 \neq 1$ such that $x+y = 0 \leftrightarrow x,y = 0$, and $x+y = 1 \leftrightarrow \{x,y\} = \{0,1\}$.
iii. $x < y \leftrightarrow x \neq y \wedge (\exists z)(x+z = y)$.
iv. Every definable set containing 0 and closed under +1 is everything.
(N,<,+) is not finitely axiomatizable.

Proof: Obviously i-iv hold in (N,<,+). Let φ hold in (N,<,+). Replace all occurrences of $s < t$ in φ by the definition according to iii). Then the resulting formula φ' holds in (N,+), and so by Theorem 0.2.6, is provable in the i-iii of Theorem 0.2.6. Hence φ' is provable in the above i-iv. Also $\varphi \leftrightarrow \varphi'$ is provable in the above i-iv. Hence φ is provable in the above 1-iv. Hence φ is provable in the above i-iv.

(N,<,+) is not finitely axiomatizable since (N,<,+) is a definitional extension of (N,<), and (N,<) is not finitely axiomatizable by Theorem 0.2.6. QED

THEROEM 0.2.10. (Z,<,+) is axiomatized with a single scheme by
i. (Z,+) is an Abelian group.
ii. < is a strict linear ordering.
iii. $x+y < x+z \rightarrow y < z$.
iv. Every definable set with an element > 0 has a least element > 0.
(Z,<,+) is not finitely axiomatizable.

Proof: i-iv clearly hold in (Z,<,+). We use Theorem 0.2.1 with the definitional expansion (Z,<,0,1,+,-,2|,3|,...) via π, where π defines

0 as the additive identity.
1 as the immediate successor of 0.
x-y as the additive inverse.
$d|x \leftrightarrow (\exists y)(x = dy)$.

where $d \geq 2$. The well known quantifier elimination for (Z,<,0,1,+,-,2|,3|,...) leads to the complete axiomatization

a. (Z,0,+,-) is an Abelian group, with inverse - and identity 0.
b. < is a strict linear ordering.
c. $x+y < x+z \rightarrow y < z$.
d. $d|x \leftrightarrow (\exists y)(x = dy)$.
e. x+1 is the immediate successor of x.

f. $x > 0 \rightarrow (\exists y)(0 \leq y < d(1) \wedge d|x-y)$.

where $d \geq 2$. It is easy to see that the result of applying π to a-f is provable in i-iv. Hence i-iv is an axiomatiation of $(Z,<,+)$.

To see that $(Z,<,+)$ is not finitely axiomatizable, we argue that a-f is not logically equivalent to any finite subset of a-f.

Let p be any prime. Let D consist of all expressions $nx/m + t$, where $(n,m) = 1$, $n,t \in Z$, $m \in N\backslash\{0\}$, and p does not divide m. Define the structure $(D,<,0,1,+,-,2|,3|,...)$ in the obvious way. Then a-e hold. Also f) holds for $2 \leq d < p$. But f) fails for $d = p$. QED

THOEREM 0.2.11. $(Q,<,+)$, $(\Re,<,+)$ are axiomatized with a single scheme by
i. + is an Abelian group.
ii. < is a dense linear ordering without endpoints.
iii. $x+y < x+z \rightarrow y < z$.
iv. Every definable subgroup of $(X,+)$ with at least two elements is $(X,+)$.
$(Q,<,+)$, $(\Re,<,+)$ are not finitely axiomatizable.

Proof: $(X,<,+)$ has a well known quantifier elimination, which yields the following axiomatization.

a. + is an Abelian group.
b. < is a dense linear ordering without endpoints.
c. $x+y < x+z \rightarrow y < z$.
d. $(\exists y)(dy = x)$.

where $d \geq 2$. It is clear from the quantifier elimination that every set definable in $(X,<,+)$ is a finite union of intervals with endpoints in $X \cup \pm\infty$. Hence i-iv hold in $(X,<,+)$. Also d) is derived from i-iv by forming the subgroup of all multiples of $d \geq 2$, and applying iv). This establishes that i-iv is an axiomatization of $(X,<,+)$.

To see that $(X,<,+)$ is not finitely axiomatizable, argue as in the last paragraph of the proof of Theorem 0.2.8. QED

THEOREM 0.2.12. $(N,+,2^x)$ is axiomatized with a single scheme by
i. $(x+y)+z = x+(y+z)$, $x+y = x+z \rightarrow y = z$.
ii. There are unique $0 \neq 1$ such that $x+y = 0 \leftrightarrow x,y = 0$, and $x+y = 1 \leftrightarrow \{x,y\} = \{0,1\}$.

iii. $2^0 = 1$, $2^{x+1} = 2^x + 2^x$.
iv. Every definable set containing 0 and closed under +1 is everything.

Proof: Obviously i-iv hold in $(N,+,2^x)$. We use the definitional expansion of $(N,+,2^x)$ and its axiomatization given in Appendix B, p. 3. The definitional expansion is M = $(N,+,-',\leq,0,1,\div n,2^x,l_2,\lambda_2)$, $n \geq 0$, where π is as follows.

$x -' y = 0$ if $y > x$; $x - y$ otherwise.
$x \leq y \leftrightarrow (\exists z)(x+z = y)$.
0 is the 0 of ii).
1 is the 1 of ii).
For $n > 0$, $x\div n$ is the unique y such that $ny \leq x < n(y+1)$.
For $n = 0$, $x\div n = 0$.
$l_2(x)$ is the unique y such that $2^y \leq x < 2^{y+1}$ if $x > 0$: 0 otherwise.
$\lambda_2(x) = 2^{l\_2(x)}$ if $x > 0$; 0 otherwise.

By Theorem 0.2.6, i-iv proves every sentence true in M that has only +. I.e., i-iv contains Presburger Arithmetic. Hence π is provably well defined in i-iv, except possibly for $l_2(x)$ and $\lambda_2(x)$.

Let $E = \{x: (\forall y < x)(2^{y+1} \leq 2^x)\}$. Then $0 \in E$. Let $x \in E$. Since $(\forall y \leq x)(2^{y+1} \leq 2^{x+1})$, we have $x+1 \in E$. We conclude that E is everything. From this, we see that there is at most one y such that $2^y \leq x < 2^{y+1}$.

Let $E = \{x: (\exists y)(2^y \leq x < 2^{y+1})\} \cup \{0\}$. Obviously $0 \in E$. Let $x \in E$, $2^y \leq x < 2^{y+1}$. To see that $x+1 \in E$, note that $2^y \leq x+1 < 2^{y+1}$, holds or $x+1 = 2^{y+1}$. Hence E is everything.

We have established that $l_2(x)$ is well defined.

Appendix B does quantifier elimination for M, with an axiomatization of M on page 3. We briefly sketch why the result of applying π to these axioms is provable in i-iv.

The axiomatization uses the Euler function, $\phi(m)$ = the number of positive integers $\leq m$ that are relatively prime with m. Of course, this function is only used externally.

Appendix B uses the following well known fundamental fact about the Euler totient function. If m is an odd positive integer then $2^{\phi(m)}-1$ is a multiple of m.

(1) T_{Pres}. Presburger Arithmetic. We have already remarked that by Theorem 0.2.6, the result of applying π to T_{Pres} is provable in 1-iv.

(2) $(\forall x)(\lambda_2(x) \leq x < 2\lambda_2(x))$. Obvious from π at λ_2, l_2.

(3) $(\forall x,y)(x \geq y \rightarrow l2(x) \geq l2(y))$. Obvious from π at l_2.

(4) $l_2(1) = 0$. Obvious from π at l_2.

(5) $(\forall x)(x \geq 1 \rightarrow l_2(2x) = l_2(x)+1)$. Obvious from π at l_2 and iii).

(6) $(\forall x)(x \geq 1 \rightarrow 2^{l\_2(x)} = \lambda_2(x))$. Obvious from π at l_2, λ_2.

(7) $(\forall x)(l_2(2^x) = x)$. Obvious from π at l_2.

(8) $(\forall x)(2^{x+1} = 2^x + 2^x)$. By iii).

(9) $(\forall x)(x \geq 1 \rightarrow 2^{x-1} \geq x)$. Let $E = \{x: 2^{x+1} \geq x\} \cup \{0\}$. Obviously $0 \in E$. Suppose $x \in E$. Then $x+1 \in E$. Hence by iv), E is everything.

(10) $(\forall x)$(if x is a multiple of $\phi(m)$ then 2^x-1 is a multiple of m), where m is an odd positive integer. It suffices to prove that for all y, $2^{\phi(m)y}-1$ is a multiple of m. We apply iv). Let $E = \{y: 2^{\phi(m)y}-1$ is a multiple of $m\}$. Obviously, $0 \in E$. Let $y \in E$. Then $2^{\phi(m)y}-1$ is a multiple of m. Now if we keep multiplying $2^{\phi(m)y}$ by 2, $\phi(m)$ times, then the exponent raises by m, and so we arrive at $2^{\phi(m)(y+1)}$. Hence $2^{\phi(m)}(2^{\phi(m)y}-1) = 2^{\phi(m)(y+1)}-2^{\phi(m)}$ is a multiple of m. Since $2^{\phi(m)}-1$ is a multiple of m, we see that $2^{\phi(m)(y+1)}-1$ is a multiple of m. Hence $y+1 \in E$. Since we have established that E contains 0 and is closed under +1, we apply iv) to obtain that for all y, $2^{\phi(m)y}-1$ is a multiple of m. QED

We conjecture that $(N,+,2^x)$ is not finitely axiomatizable.

THEOREM 0.2.13. $(\Re,+,\bullet)$, $(RALG,+,\bullet)$ are axiomatized with a single scheme by
i. $(X,+,\bullet)$ is a field.
ii. The relation y-x is a nonzero square, is a strict linear ordering of x,y.
iii. Every definable nonempty bounded set has a least upper bound.
$(\Re,+,\bullet)$, $(RALG,+,\bullet)$ are not finitely axiomatizable.

Proof: It is well known that i-iii hold in $(X,+,\bullet)$. We now use Theorem 0.2.1 and the definitional expansion $(X,<,0,1,+,\bullet)$ via π, where < is defined by $x < y \leftrightarrow y-x$ is a nonzero square, 0 is defined as the unique x with $x+x = x$, 1 is defined as the unique x with $(\forall y)(xy = y)$.

The well known elimination of quantifiers leads to the axiomatization

a. $(X,0,1,+,\bullet)$ is a field.
b. < is a strict linear ordering.
c. $x < y \rightarrow x+z < y+z$.
d. $0 < x \wedge 0 < y \rightarrow 0 < x\bullet y$.
e. $0 < x \rightarrow (\exists y)(x = y^2)$.
f. Every polynomial of odd degree ≥ 1 with leading coefficient 1 has a zero.

We claim that the result of applying π to a-f is provable in i-iii. Clearly this holds of a,b.

For c), suppose y-x is a nonzero square. Then $(y+z)-(x+z)$ is a nonzero square.

For d), suppose x,y are nonzero squares. Then $x\bullet y$ is a nonzero square.

For e), suppose x is a nonzero square. Then x is a square.

This also verifies the usual ordered field axioms, formulated with <, within i-iii. Hence we can show in i-iii that every monic polynomial of odd degree ≥ 1 is positive for all sufficiently positive x, and negative for all sufficiently negative x.

Let E be the set of all x such that $P(x) < 0$. Then E is obviously nonempty and bounded. Let w be the < least upper bound of E, according to iii. Using the ordered field axioms, we see that $P(w) = 0$.

We have thus proved that i-iii is an axiomatization of $(X,+,\bullet)$.

It is well known that a-f, the theory of ordered real closed fields, is not finitely axiomatizable. Fix an odd prime p. We can build the partial real closure K[p] of the field of rationals, adding square roots of positive elements and roots of odd degree monic polynomials of degree < p only. The p-th root of 2 is missing, but axioms a-e hold, and axiom f) holds for odd degree < p. Hence by Theorem 0.2.2, (X,+,•) is not finitely axiomatizable. QED

We will be using the following combinatorial lemma.

LEMMA 0.2.14. If (A,<) is an uncountable linear ordering, then there exists $a \in A$ such that $(-\infty,a)$ and (a,∞) are infinite.

Proof: Suppose not. Then for all $a \in A$, $(-\infty,a)$ or (a,∞) is uncountable.

Define the equivalence relation a ~ b if and only if there are finitely many points between a and b.

Since every equivalence class is countable, there are uncountably many equivalence classes. Let $1 \leq \alpha \leq \omega$ be such that there are uncountably many equivalence classes of cardinality α.

case 1. $\alpha < \omega$. Let [a,b], [c,d] be equivalence classes of cardinality α, a < b < c < d. Then b is a limit point from the right, and c is a limit point from the left. Hence $(-\infty,b)$, (b,∞) are infinite.

case 2. $\alpha = \omega$. Let I < J < K be three equivalence classes of cardinality ω. For all $a \in J$, $(-\infty,a)$, (a,∞) are infinite. QED

THEOREM 0.2.15. (C,+,•), (CALG,+,•) are axiomatized with two schemes by
i. (X,+,•) is a field.
ii. Every definable subgroup of (X,+) with at least two elements is (X,+).
iii. Let $f:X^2 \to X$ be definable. Let (A,<) be a definable strict linear ordering, $A \subseteq X$. Assume that for all $z \in A$, $f_z:X \to X$ is either constant, or the identity, or the sum or product of two $f_w:X \to X$ with w < z. Then for all $z \in A$, $f_z:X \to X$ is constant or onto.
(C,+,•) and (CALG,+,•) are not finitely axiomatizable.

Proof: We use Theorem 0.2.1 and the definitional expansion (X,+,•,0,1) by π, where 0 is the unique z with $(\forall w)(z+w = w)$ and 1 is the unique $z \neq 0$ with $(\forall w)(z \bullet w = w)$.

(X,+,•,0,1) has a very well known quantifier elimination leading to the very well known axiomatization

a. $(X,+,\bullet,0,1)$ is a field.
b. $dz = dw \rightarrow z = w$.
c. Every polynomial of degree ≥ 1 has a zero.

where $d \geq 2$. Using the quantifier elimination, we easily obtain the well known crucial property that every set definable in $(X,+,\bullet)$ is finite or cofinite. We also see that X has no strict linear ordering.

Obviously i) holds in $(X,+,\bullet)$. For ii), let G be a definable subgroup with at least two elements. Obviously G is infinite. But G is finite or cofinite. Hence G is cofinite. Therefore G = X.

For iii), we first show that in $(C,+,\bullet)$, every definable linear ordering on a definable subset of C is finite. To see this, we have A is finite or cofinite. Suppose A is cofinite. By Lemma 0.2.14, there exists $a \in A$, such that $\{x: x < a\}$ and $\{x: x > a\}$ are infinite. This is impossible.

It then follows by the well known elementary equivalence of $(C,+,\bullet)$ and $(CALG,+,\bullet)$, that in $(CALG,+,\bullet)$, every definable linear ordering on a definable subset of CALG is finite.

To complete the verification of iii), let f,A,< be as given. By the above, A is finite. It is clear by finite induction that every f_z is a polynomial. Polynomials in $(X,+,\bullet)$ are constant or onto because $(X,+,\bullet)$ is algebraically closed.

The result of applying π to a) is obviously provable in i-iii. For b), assume $dz = 0$, $z \neq 0$, and form the group $\{0,z,\ldots,(d-1)z\}$. This group is definable in $(X,+,\bullet)$, and so by ii), it is $(X,+)$. This is a contradiction.

For c), let P be a polynomial of degree ≥ 1 with leading coefficient 1. Let $Q_1,\ldots,Q_n$ be polynomials, where each Q_i is either constant, the identity, or the sum or product of two Q_j, $j < i$, and where $Q_n = P$. Use $A = \{1,\ldots,n\} \subseteq X$ with the usual < to apply iii). Use $f:X^2 \rightarrow X$, where

$$f(z,w) = Q_z(w) \text{ if } z \in \{1,\ldots,n\};\ 0 \text{ otherwise.}$$

By iii), $Q_n = P$ is constant or onto. It remains to prove in i-iii that P is not constant.

Every model of i-iii is a field of characteristic zero. Form algebra, in every field of characteristic zero, every polynomial of degree ≥ 1 is not constant. By the Gödel completeness theorem, i-iii proves that P is not constant.

We have established that i-iii is an axiomatization of (X,+,•).

To see that (X,<,•) is not finitely axiomatizable, let p be a prime, and let F be the algebraically closed field of characteristic p. Then a-c hold in F. Also b) holds for 2 ≤ d < p. But b) fails for d = p. QED

THEOREM 0.2.16. ($\mathfrak{R}$,<,+,•), (RALG,<,+,•) are axiomatized with a single scheme by
i. (X,+,•) is a field.
ii. < is a strict linear ordering.
iii. x < y ↔ y-x is a nonzero square.
iv. Every definable nonempty set with an upper bound has a least upper bound.
($\mathfrak{R}$,+,•), (RALG,+,•) are not finitely axiomatizable.

Proof: Clearly i-iv hold in ($\mathfrak{R}$,<+,•), (RALG,<,+,). Also ($\mathfrak{R}$,<,+,•), (RALG,<,+,) are respective definitional extensions of ($\mathfrak{R}$,+,•,), (RALG,+,•) by the interpretation π that defines

x < y if and only if y-x is a nonzero square.

So an axiomatization consists of the above definition of <, together with the axioms i-iii from Theorem 0.2.13. This axiomatization is equivalent to the present i-iv.

By Theorems 0.2.2, 0.2.13, ($\mathfrak{R}$,+,•), (RALG,+,•) are not finitely axiomatizable. QED

THEOREM 0.2.17. ($\mathfrak{R}^2$,B,E) is axiomatized with a single scheme. ($\mathfrak{R}^2$,B,E) is not finitely axiomatizable.

Proof: Tarski's axiomatization of Euclidean geometry uses B = betweenness, and E = equidistance, equality, and points, as the primitives. It has finitely many axioms together with an axiom scheme of continuity. See [Ta51], [TG99].

($\mathfrak{R}^2$,B,E) is well known to be not finitely axiomatizable, using the ($K[p]^2$,B,E), where K[p] is as defined in the last paragraph of the proof of Theorem 0.2.13. By the axiomatization of real closed fields a-f there, we see that any finite set of sentences true in ($\mathfrak{R}^2$,B,E) is true in some ($K[p]^2$,B,E). Furthermore, the existence of a p-th root of 2 in $\Re$ corresponds to a true statement in ($\Re$2,B,E) that fails in (K[p],B,E). Hence there cannot be a finite axiomatization of ($\Re^2$,B,E). QED

We shall briefly mention three additional fundamental structures that have been investigated intensively.

The first is ($\Re$,+,•,e^x). It has been proved that every subset of $\Re$ definable in ($\Re$,+,•,e^x) is a finite union of intervals with endpoints in $\Re \cup \{\pm\infty\}$. It is not known if ($\Re$,+,•,e^x) is recursively axiomatizable. However, it has been shown that if a famous conjecture in transcendental number theory, called the Schanuel Conjecture, is true, then ($\Re$,+,•,e^x) is recursively axiomatizable. See [MW96], [Wi96], [Wi99].

The second is the field ($\mathbf{Q}_p$,+,•) of all p-adic numbers and its finite algebraic extensions, where p is any given prime. See [AK65], [AK65a], [AK66], [Co69], [Eg98].

The third is the structure S2S. This is a two sorted structure ($\{0,1\}^*$,$\wp(\{0,1\}^*)$,$\in$,S_0,S_1), where S_0 and S_1 are the two successor functions on the set $\{0,1\}^*$ of finite bit strings defined by $S_0(x) = x_0$, $S_1(x) = x_1$. It is more common to present S2S, equivalently, either ($\{0,1\}^*$,S_0,S_1), or (T,<), where second order logic is used instead of the customary first order logic. Here T is the full binary tree viewed abstractly, with its usual partial order <.

A recursive axiomatization of S2S was first given using automata, in [Rab68]. For a modern treatment using game theory, see [BGG01], section 7.1.

Is is often said that in "tame" contexts such as the ordered group of integers, or the ordered field of reals, we avoid the Gödel Incompleteness Phenomena.

However, the Gödel Incompleteness Phenomena simply shifts to the computational complexity context, where the results are based on diagonal constructions pioneered by Kurt Gödel. Even in these "tame" structures, one has the same kind of no algorithm results. One also has Gödelian type results involving lengths of proofs. We conjecture that there is a rich theory of Concrete Mathematical Incompleteness, involving lengths of proofs, in such "tame" contexts. See, e.g., [FR74], [Rab77], and [FeR79].

0.3. Abstract and Concrete Mathematical Incompleteness.

The focus of this book is on Concrete Mathematical Incompleteness. We use the following working definition of the Mathematically Concrete:

Mathematical statements concerning Borel measurable sets and functions of finite rank in and between complete separable metric spaces.

We take the Mathematically Abstract to begin with the transfinite levels of the Borel hierarchy, and continue in earnest with the low levels of the projective hierarchy of subsets of functions between complete metric spaces, starting with the analytic sets, followed by the higher levels of the projective hierarchy. Here there are still only continuumly many such subsets and functions.

Yet higher abstract levels include arbitrary subsets of and functions between complete separable metric spaces. Here there are more than continuumly many such subsets and functions. At still higher levels, the objects are no longer subsets or functions between complete separable metric spaces.

The overwhelming majority of mathematicians work within the Mathematically Concrete as defined above. In fact, the overwhelming majority work considerably below this level.

An indication of the special status of the functions and sets highlighted here is afforded by the following result, which is proved by standard techniques, and is part of the folklore of descriptive set theory.

THEOREM 0.3.1. Let X be a complete separable metric space. The following classes of functions from X into X are the same.
i. The Borel measurable functions of finite rank from X to X.
ii. The closure under composition of the pointwise limits of sequences of continuous functions from X to X.
iii. The bold faced arithmetic functions from X into X in the sense of recursion theory.
This equivalence also holds for functions of several variables, using generalized composition in ii).

Clause ii) shows that we get to finite rank Borel by means of composition, and a family of reasonable discontinuous functions. Pointwise limits of continuous functions occur in classical mathematics, particularly in connection with power series and Fourier series. Often these are not everywhere convergent, and we can use a default value where the limit does not exist. This is a variant of ii), for which Theorem 0.3.1 obviously still holds. One also sees functions defined as the sup of an infinite sequence of continuous functions, where we have uniform boundedness, or a point at infinity, so that the sups exist everywhere. This clearly falls under ii).

It would be very interesting to understand the closure under composition of special classes of functions, or the closure under composition of continuous functions with various specific simply presented discontinuous functions.

The highlight of this section is a discussion of various aspects of Concreteness in core mathematics, including levels of Concreteness. Many interesting issues arise, including a rather systematic program.

This systematic program, which we call Mathematical Statement Theory, is spelled out more carefully and applied to the Hilbert Problem List of 1900 in section 0.17.

A somewhat different, but well established program, which we founded in the late 1960's to mid 1970's, is Reverse Mathematics, and is discussed in detail in section 0.4.

We close this section with a brief history of Incompleteness, in which Abstract Mathematics plays a central role.

In order to proceed informatively and robustly, we will make free use of the standard analysis from logic of the quantifier complexity of formal sentences. The relevant standard robust categories of sentences from logic based on quantifier complexity are

$$\Pi^0_0,\ \Pi^0_1,\ \ldots\ .$$
$$\Sigma^0_0,\ \Sigma^0_1,\ \ldots\ .$$
$$\Pi^1_0,\ \Pi^1_1,\ \ldots\ .$$
$$\Sigma^1_0,\ \Sigma^1_1,\ \ldots\ .$$

Here Π^0_n (Σ^0_n) refers to sentences starting with n quantifiers ranging over N, the first of which is universal (existential), followed by formulas using only bounded numerical quantifiers, connectives, and equations and inequalities involving multivariate primitive recursive functions from N into N.

Also Π^1_n (Σ^1_n) refers to sentences starting with n quantifiers ranging over subsets of N, the first of which is universal (existential), followed by a formula using only numerical quantifiers, connectives, equations and inequalities involving multivariate primitive recursive functions from N into N, and membership in subsets of N.

In practice, one normally encounters blocks of like quantifiers. It is a standard fact from mathematical logic that blocks of like quantifiers, in our context, behave like a single quantifier.

Since the languages on which these quantifier complexity classes are based are streamlined for logical simplicity, we make free use of the so called coding techniques from logic in order to actually gauge the strength of real mathematical statements. The appropriate robustness of the method of coding for such purposes is well established.

Another approach is to base the quantifier complexity classes on rich languages. This is less standard, and we will not take that approach here. The results obtained using this alternate approach would be essentially the same.

We do not use superscripts higher than 1 because any Mathematically Concrete assertion can be viewed as a Π^1_n sentence, for some $n \geq 1$.

In fact, actual Mathematically Concrete assertions are often Π^0_3 or simpler. The quantifier complexity classes Π^0_1, Π^0_2, and Π^0_3 play very special roles at the concrete end of the spectrum.

The $\Pi^0_0 = \Sigma^0_0$ sentences have the special property that we can prove or refute them by running a computer - at least in principle. The computer resources needed may or may not be practical. A particularly interesting example of this is the proof of the Four Color Conjecture. The statement

existence of an unavoidable
finite set of reducible configurations

is a Σ^0_1 sentence because unavoidability and reducibility are local properties (unavoidability only involves graphs of size related to the set). This Σ^0_1 sentence immediately implies the Four Color Conjecture. Appel and Haken gave an explicit instantiation of the outermost existential quantifier, and then proceeded to prove the resulting Π^0_0 sentence with the help of a computer.

The Π^0_1 sentences have the special property that if they are false, then we can find a counterexample and verify that it is a counterexample by computer - at least this can be done in principal. Obviously, any counterexample may be so huge that verifying it directly is impractical. Of course, the use of theory may make it practical even if the actual counterexample is so huge - by greatly reducing the actual computer resources.

A particularly well known example of a Π^0_1 sentence refuted by counterexample is Euler's Quartic Conjecture, which states that no fourth power of a positive integer is the sum of three fourth powers of positive integers. It was refuted in [El88] with

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Of course, here verifying that this is a counterexample barely requires a computer. Roger Frye subsequently found the counterexample

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

by a computer search using techniques suggested by Elkies, and demonstrated that this is the counterexample in fourth powers with smallest right hand side. Apparently, some theory is needed to obtain minimality. See [Gu94], p. 140. Note that Frye's minimality result is a $\Pi^0_0 = \Sigma^0_0$ sentence.

The category $\Pi^0_\infty = \cup_n \Pi^0_n$ also has special significance. This is the category of "arithmetic sentences". Many scholars feel that the integers and associated finite objects have a kind of objective existence that is not shared by arbitrary infinite objects such as an infinite sequence of integers. They often believe that statements involving only such finite objects - no matter how much quantification over all such finite objects are present - have a matter of factness that protects them from foundational issues in a way that statements involving infinite objects do not.

Some scholars have this kind of attitude towards only, say, Π^0_1 sentences. Others have varying degrees of cautiousness about the matter of factness of even $\Pi^0_0 = \Sigma^0_0$ sentences, which can involve integers far too large for computer processing. For example, the number $A_{7198}(158,386)$, which arises in Theorem 0.7.11, or even an exponential stack of 100 2's.

We have the following noteworthy representatives.

Π^0_1. Fermat's Last Theorem (Wiles' Theorem), Goldbach's Conjecture, the Riemann Hypothesis.

Π^0_2. Collatz Conjecture.

Π^0_3. Falting's Theorem (Mordell's Conjecture), Thue-Siegel-Roth Theorem.

Note that some of these statements are conjectures and some of these statements are theorems. There are a number of interesting issues related to these classifications above.

Consider the known FLT. It could be argued that FLT is in fact Π^0_0, since it is known to be equivalent to 0 = 0. However, that equivalence depends on some substantial portion of the new ideas in its proof. In fact, that equivalence relies on all of the new ideas in its proof!

So in this classification scheme applied to theorems, we must only use equivalence proofs that are orthogonal to the proof of the theorem. Perhaps surprisingly, in practice this requirement is sufficiently robust to support our classification scheme.

In section 0.17, we formulate Mathematical Statement Theory, where we are sensitive to such issues, so that this classification theory meaningfully applies to actual theorems.

FLT and Goldbach's Conjecture are obviously, on the face of it, Π^0_1. One need go no further than consider their utterly standard formulations.

However, RH is quite a different matter. Looking at the standard formulation, we only obtain Π^1_1, because of the quantification over all real numbers. This is hugely higher than any Π^0_n.

But there are well known concrete equivalences of RH. We present one of many well known Π^0_1 equivalences in section

0.17, when we discuss H8 = Hilbert's Eighth Problem. There is also a Π^0_1 equivalence of RH in [Mat93], Chapter 7. Hence RH is what we call essentially Π^0_1.

The Collatz Conjecture is stated as follows. Define $f:Z^+ \rightarrow Z^+$ by f(n) = n/2 if n is even; 3n+1 if n is odd. For all n $\in Z^+$, if we keep iterating f starting at n, then we eventually arrive at 1.

Note that the Collatz Conjecture takes the form

$(\forall n \in Z^+)(\exists$ a finite sequence ending in 1, which starts with n and continues by applying f).

This can be put in Π^0_2 form using standard coding techniques from logic that rely on the fact that a finite sequence form Z^+ is a finite object of a basic kind.

Π^0_2 sentences practically beg to become Π^0_1 sentences through the use of an upper bound. Thus, if we could show, e.g., that

#) $(\forall n \in Z^+)(\exists$ a finite sequence ending in 1, which starts with n and continues by applying f, where all terms are at most (8n)!!)

without using ideas in the proof of Collatz Conjecture (at the moment we are not even close to being able to do this), then we would say that the Collatz Conjecture is essentially Π^0_1.

Another possibility is that after we prove the Collatz Conjecture, we actually prove a stronger theorem that is Π^0_1 - such as #). In this case, we won't say that the Collatz Conjecture is, or is essentially, Π^0_1, since we are relying on the proof of the Collatz Conjecture. But we would certainly want to note that

The Collatz Conjecture is implied by a Π^0_1 theorem.

Of course, another possibility is that we are able to prove the equivalence of the Collatz Conjecture with, say, #), without using ideas in the proof of the Collatz Conjecture - but in fact, historically, we only saw this after we proved the Collatz Conjecture. In this case, we would say that the Collatz Conjecture is essentially Π^0_1.

Of course, independently of the discussion above, if we were to prove the equivalence of the Collatz Conjecture with #), we would have made a major contribution that would be readily recognized.

We now come to Falting's Theorem. This asserts that there are finitely many solutions to an effectively recognizable class of Diophantine problems over Q. This takes the form

(∀n)(there are finitely many m such that P(n,m))

where P is an appropriate (primitive recursive) binary relation. Because of standard coding techniques, we can collapse several integers to a single integer for our purposes.

This in turn takes the form

$$(\forall n)(\exists r)(\forall m)(P(n,m) \rightarrow m < r)$$

which is obviously Π^0_3. Note how this is significantly higher - i.e., less concrete - than Π^0_2 (Collatz Conjecture).

Π^0_3 sentences also practically beg to become Π^0_1 sentences through the use of an upper bound - just like Π^0_2 sentences.

Suppose we could show, e.g., that Mordell's Conjecture is equivalent to

##) $(\forall n)(\forall m)(P(n,m) \rightarrow m < (8n)!!)$

without using ideas in the proof of Mordell's Conjecture (Falting's Theorem), then we would say that Mordell's Conjecture is essentially Π^0_1.

Of course, independently of the discussion above, if we prove ##) then we would have made a major contribution that would be readily recognized.

A situation quite analogous to Falting's Theorem, in this sense, is the Thue-Siegel-Roth Theorem. It states that if α is an irrational algebraic number, and $\varepsilon > 0$, the inequality

$$|\alpha - p/q| < 1/q^{2+\varepsilon}$$

has finitely many solutions in integers p and q. This is also in Π^0_3 for the same reason - and also begs to graduate to Π^0_1.

We now jump to the upper reaches of the quantifier complexity classes that we are using. These most commonly appear as Π^1_1, Π^1_2, Σ^1_1, Σ^1_2.

This level of quantifier complexity has special significance for our purposes.

THEOREM 0.3.2. Let φ be a Π^1_2 or Σ^1_2 sentence. The main methods of set theory - inner models and forcing - cannot establish that φ is unprovable in ZFC. In particular, any two transitive models of ZFC with the same ordinals agree on the truth value of φ.

Theorem 0.3.2 essentially tells us that if a sentence is Π^1_2 or Σ^1_2, then establishing its unprovability in ZFC requires something quite different than standard techniques from set theory. The only techniques available for establishing the unprovability in ZFC of mathematical sentences in these complexity classes are essentially those used for sections 0.13, 0.14, and laid out in detail in Chapters 4,5 of this book.

Furthermore, we claim that mathematics has, for many decades, been focused on problems that are well within the Π^1_2 and Σ^1_2 classes. This seems to be increasingly the case in recent years, particularly with the steady increase in the power of computation. The question "can you compute this" and "how efficiently can you compute this" have become more attractive now that many answers to the second question are actually implemented. This has inevitably affected the interest in the Concrete, even if one is still far removed from implementability.

It is still the case that you will see abstract mathematical statements from time to time considered by core mathematicians. The usual situation in which this arises is where the great generality is not causing its own inherent difficulties.

But if difficulties arise, traced to the generality and abstraction - not to the intended mathematical purposes - then interest wanes in the abstract formulation, and attention shifts to more concrete formulations where these "foreign" difficulties are absent.

This basically amounts to a kind of separation of the "set theoretic difficulties" from the "fundamental mathematical difficulties".

For instance, we still teach that every field has a unique (in the appropriate sense) algebraic closure. This is a highly abstract assertion, because the field is completely arbitrary. However, the set theoretic difficulties, which are not negligible, are highly manageable through Zorn's Lemma.

On the other hand, the highly abstract continuum hypothesis (discussed below under H1) is now well known to cause major difficulties disconnected from the normal issues in analysis.

Borel measurable sets and functions in separable metric spaces, lie at the outer cusp of what mathematicians generally accept as appropriate for the formulation of problems of genuine mathematical interest.

Thus the "Borel Continuuum Hypothesis" arises, and is a rather basic and striking classical result in descriptive set theory. See [Ke95] and the discussion below in H1 of section 0.17.

Sometimes a highly abstract statement not only causes no logical difficulties, but it even is obviously equivalent to a much more concrete statement. See the discussion below in H14 of section 0.17.

These points are elaborated in some detail, as we discuss the levels of Concreteness associated with Hilbert's famous list of 23 problems, 1900, in section 0.17.

It appears that exactly one of the Hilbert problems lies outside Concrete Mathematics, according to our working definition above. This is H1, the first one in the list.

We conjecture that all of the other problems on this list, and all closely related problems, are

i. Essentially Π^1_2 or essentially Σ^1_2; or
ii. Will get proved or refuted in ZFC, and stronger statements will emerge from those proofs that are essentially Π^1_2 or essentially Σ^1_2 (and in most cases, much lower).

Two other problem lists, created one hundred years later, are the 18 Smale problems, 1998, and the 7 Clay Millennium Prize Problems, 2000. See [Sm00] and [http://www.claymath.org/millennium/].

We also conjecture that all of the problems on these other two lists, and all closely related problems, have properties i,ii above.

So what are we to make of this adequacy of the usual foundations of mathematics through ZFC with regard to these problem lists?

This matter is addressed in some detail in the Preface. Specifically, the development of mathematics is still extremely primitive on evolutionary - let alone cosmological - time scales. Although the scope of deep mathematical activity represented by these three lists of problems and the efforts leading up to them may look incredibly impressive to us, they are certain to look mundane in a few centuries (or even earlier), let alone in thousands (or millions!) of years.

We maintain that Boolean Relation Theory is just one of many subjects of gigantic scope (see section 1.2) that are yet to be discovered or developed, but which are entirely inevitable given their internal coherence, motivating themes, and simplicity of concept.

We believe that Concrete Mathematical Incompleteness - where large cardinals are shown to be sufficient, and weaker large cardinals are shown to be insufficient - will ultimately become commonplace.

What is much less clear is whether mathematicians will ultimately decide to accept large cardinal hypotheses, even under such utility. A major drawback of the large cardinal hypotheses in this regard is that they postulate objects that are radically foreign to mathematical practice.

It would seem more palatable to have forms of the large cardinal hypotheses involving objects that are least familiar to mathematicians, if not used generally in mathematical practice.

This is not possible in terms of literal equivalence. However, for applications of large cardinals such as the ones in this book (the Exotic case), as well as any Π^0_2 consequence, an alternative is to use only the 1-consistency of the large cardinal hypotheses, and not the actual existence of the large cardinal. This opens the door to reformulations of large cardinal hypotheses in terms of familiar, or at least more familiar, objects.

One radical possibility along these lines is through the axiomatization of concepts that are entirely foreign to mathematics, but are, instead, a part of common everyday thinking. Plausible, or perhaps compelling, principles might be identified involving such concepts. Formal systems based on such principles may emerge, and imply the 1-consistency of the relevant large cardinal hypotheses. See [Fr06] and [Fr11] for work along these lines.

Another possibility is to directly analyze the mental pictures that are used to process large cardinals. Mental pictures are normally a crucial component in sophisticated mathematical reasoning, whether or not large cardinals are involved. They are a crucial component in the widespread acceptance of the usual ZFC axioms.

Moreover, mental movies are a particularly powerful component in mathematical reasoning, in the sense of short coherent sequences of mental pictures.

Mental pictures, and the more powerful mental movies, are combinatorial objects of very limited finite size.

The idea is to develop a combinatorial analysis of such finite movies, and discover some fundamental principles about them that imply the consistency or the 1-consistency of a range of large cardinal hypotheses.

We now close with a brief history of Incompleteness in which Abstract Mathematics plays a central role.

Let us review the initial stages of work on Incompleteness.

We can view Gödel's First Incompleteness Theorem as an existence theorem only, or we can view it as proving the independence of an arithmetization of the Liar's paradox. In either case, one cannot view it as providing an intelligible instance of mathematical incompleteness.

Gödel's Second Incompleteness Theorem does provide an important and intelligible example - e.g., Con(ZFC).

However, the intelligibility of Con(ZFC) depends on an understanding of "formalizations of abstract set theory".

One can object to this comment on the grounds that Con(ZFC) can be stated purely in terms of the ring of integers, or the hereditarily finite sets - using the standard coding devices. This "removes" the reference to abstract set theory and to formalizations.

However, when one removes the references to formalizations of abstract set theory, the presentation of Con(ZFC) becomes unintelligible - in particular, unintelligibly complex. This is a crucially important point, even though we do not have (yet) any kind of surrounding rigorous theory that formally supports important distinctions of this kind.

We are beginning to get a sense of definite criteria for judging the intelligibility or naturalness of mathematical statements. We believe that there are ways of judging intelligibility or mathematical naturalness that are independent of particular mathematical research interests or the sociology of mathematics. This topic lies well beyond the scope of this book.

The next big development in Incompleteness involved two obviously important problems in abstract set theory - the first implicitly used by Cantor, and the second emphasized by Cantor. These were the axiom of choice, and the continuum hypothesis. The consistency of ZFC + CH relative to ZF was established in [Go38]. The consistency of ZF + ¬AxC, and ZFC + ¬CH, relative to ZF, was later established in [Co63,64].

Note that here there is no reference to formalizations of abstract set theory. AxC and CH are problems directly in abstract set theory.

However, AxC and CH are not concrete - in anything like the way that Con(ZFC) is.

Con(ZFC) is formulated in terms of finite objects only. It asserts the nonexistence of a finite configuration. Its intelligibility depends on some understanding of abstract set theory. But nevertheless, with the help of coding, it asserts the nonexistence of a finite configuration.

In contrast, AxC and CH cannot be formulated in this way, regardless of coding devices. These statements live inherently in the abstract set theoretic universe.

Subsequent developments in Incompleteness initially centered around analyzing a large backlog of problems from abstract set theory, mostly with the help of Cohen's method of forcing introduced in [Co63,64]. Some of the problems in this backlog were well known from the set theoretic parts of analysis, group theory, and other subjects. Early pioneers in this extensive development include Donald Martin, Saharon Shelah, Robert Solovay, and others. See [Je78,06] for a comprehensive treatment.

A notably different method of attack on Abstract Incompleteness arose from Ronald Jensen's work on Gödel's constructible universe, which provides tools for establishing that various statements hold in L (Gödel's constructible universe). This establishes relative consistency with ZFC, where the independence is normally establishes by forcing. E.g., see [Jen72], [De84].

These applications of forcing and constructible sets established that ZFC neither proved nor refuted many problems in Abstract Mathematics, but generally did not determine or even shed light on their truth or falsity, from the abstract set theoretic point of view.

Work on the projective hierarchy of sets of reals took hold, forming an entry point for large cardinals in Incompleteness.

The projective hierarchy begins with Borel and analytic sets (analytic sets are projections of Borel sets), and forms a hierarchy indexed by the natural numbers.

Classical analysts from the first half of the twentieth century sought to extend their impressive understanding of the structure of Borel and analytic sets to the more general projective sets.

During the 1960s and 1970s, it was discovered that projective determinacy implies all of these sought after generalizations to projective.

Large cardinal hypotheses were shown to imply projective determinacy in [MSt89]. Specifically, Martin and Steel proved in ZFC that if there are infinitely many Woodin cardinals then projective determinacy holds. In addition, projective determinacy establishes all of the generalizations

Woodin has proved in ZFC that if there are infinitely many Woodin cardinals below a measurable cardinal, then $L(\mathfrak{R})$ determinacy holds, extending the work of Martin and Steel. See [St09], [Lar04]. These results are shown to be roughly optimal. For a detailed account, see [KW10]. (Here $L(\mathfrak{R})$ is the constructible closure of $\mathfrak{R}$, and $L(\mathfrak{R})$ determinacy asserts that in all infinite length games with integer moves and winning set in the constructible closure of $\mathfrak{R}$, one player has a winning strategy).

For a much more detailed picture of set theoretic incompleteness, see [Je78,06].

We close with a brief account of an important development initiated by Richard Laver, taken from [DJ97].

In [La92], properties of the free left-distributive algebra on one generator are proved using an extremely large cardinal - a nontrivial elementary embedding from some $V(\lambda)$ into $V(\lambda)$. These consequences included the recursive solvability of the word problem for this algebra.

These algebraic results were later proved in [Deh94], [Deh00] using completely different methods based on braid groups and generalizations thereof. The new proofs use only very weak fragments of ZFC, and in fact weak fragments of PA.

But some further algebraic results were obtained using the large cardinal. [La95] produces a sequence of finite left-distributive algebras A_n, which can be constructed in simple combinatorial terms without the large cardinal. [La95] proves that A_∞ is also free.

"A_∞ is free" can be rephrased in purely algebraic form, as a Π^0_2 sentence asserting that certain equations do not imply certain other equations under the left distributive law.

In [DJ97a], it is shown that "A_∞ is free" is not provable in PRA (primitive recursive arithmetic). At present, the only proof of "A_∞ is free" uses the extremely large cardinal.

Even if (as many expect) the large cardinal is subsequently removed, this does show how large cardinals can provide insights into Concrete Mathematics.

But here we give an application of large cardinals to combinatorics that is proved in Chapter 4 from large cardinals, and shown to be necessary (unremoveable) in Chapter 5.

In fact, we believe that in the future, large cardinals will be systematically used for a wide variety of Concrete Mathematics in an essential, unremoveable, way.

0.4. Reverse Mathematics.

The ZFC axioms (Zermelo Frankel with the axiom of choice) have served for nearly a century as the de facto standard by which we judge whether a mathematical theorem has been proved.

Early on, it was clear that ZFC serves as convenient overkill for this purpose. Mathematical results generally require use of only a "small part" of the power of the ZFC axioms.

Interest naturally developed in determining which fragments of ZFC are sufficient to prove which specific theorems.

In order to systematize this work in an informative way, a collection of standard fragments of ZFC are needed. This turns out to be rather awkward given the way the axioms of ZFC are laid out.

The advantages of working with the pair of primitives, natural numbers and sets of natural numbers (or natural numbers, and the closely related alternative choice of functions from natural numbers into natural numbers), became apparent, both for proof theory and for the logical analysis of mathematical theorems. See [Kre68], [Fe64], [Fe70].

Thus Feferman, Kreisel, and others, began to use the system Z_2 and its fragments for the purpose of identifying logical principles sufficient to prove various mathematical theorems.

Reverse Mathematics (RM) is an open ended project in which a wide range of mathematical theorems are systematically classified in terms of the "minimum" logical principles sufficient to prove them.

After RM was founded through [Fr74], [Fr75-76], and [Fr76], S. Simpson focused on the area, made important advances in RM, supervised many Ph.D. students in RM, and wrote the authoritative book [Si99,09] covering RM.

But how can we identify the "minimum" logical principles sufficient to prove a given mathematical theorem?

Our key insight goes back to at least 1969 (cited in [Fr75-76]), and culminated in the polished formulations of [Fr74], [Fr76].

We first identify a weak "base theory" T of core fundamental principles, in the form of a subsystem of Z_2.

We then realize through experimentation with examples, that the base theory is strong enough so that the equivalence relation

base theory T proves A is equivalent to B

on basic mathematical theorems, has relatively few equivalence classes.

These insights already supported a robust theory of "logical strength" of mathematical theorems, although the phrase "logical strength" now has a more focused meaning. See the DEEP UNEXPLAINED OBSERVED FACT below.

We went further and identified natural preferred logical systems associated with the various equivalence classes of mathematical theorems that arise.

We identified a group of natural fragments of Z_2 such that many mathematical theorems correspond exactly to one of these fragments in the sense that

base theory T proves that theorem A is
equivalent to the formal system S

so that theorem A is calibrated by the system S.

Note that under this conception, we have both the usual

proving of mathematical theorems from formal systems

and the unusual

proving of formal systems from mathematical theorems (over the base theory).

Hence we introduced the name "reverse mathematics" for this classification project.

Our choice of base theory for RM underwent some evolution, culminating with RCA in [Fr74] and the improved, weaker, finitely axiomatized RCA_0 in [Fr76]. The choice of RCA_0 has remained the working standard for RM since that time.

In [Fr75-76], one of our earliest results is cited in these terms:

"1. In 1969 I discovered that a certain subsystem of second order arithmetic based on a mathematical statement (that every perfect [sic] tree that does not have at most countably many paths, has a perfect subtree) was provably equivalent to a logical principle (the weak Π^1_1 axiom of choice) modulo a weak base theory (comprehension for arithmetic formulae)."

The use of the first "perfect" here was an apparent typographical error, and should be struck out here [sic].

Already in [Fr74], [Fr76], we used the system ATR_0 for that level instead of the weak Π^1_1 axiom of choice.

But note that our use of arithmetic comprehension as the base theory, at least for this early reversal from 1969. This is what appears as ACA in [Fr74] - but not as the base theory.

Our choice of base theory in [Fr74] is the much weaker RCA = recursive comprehension axiom scheme, which has full induction in its language (the language of Z_2). We subsequently sharply weakened the induction axiom to what is really essential, resulting in the base theory RCA_0 of [Fr76].

The most commonly occurring systems of RM were first introduced as a group (with some additional systems) in [Fr74]. These are

RCA, WKL, ACA, ATR, Π^1_1-CA

and were later weakened, in [Fr76], to the finitely axiomatized systems

RCA_0, WKL_0, ACA_0, ATR_0, $\Pi^1{}_1$-CA_0

by limiting the induction axioms to what is essential. Many reversals of some basic mathematical theorems are also presented in [Fr74] and [Fr76].

Two additional levels are also introduced in [Fr74] and [Fr76]. These levels had figured prominently in earlier investigations of fragments of Z_2. These are the closely related

HCA, HAC, HDC, and HCA_0, HAC_0, HDC_0

of hyperarithmetic comprehension, choice, dependent choice, better known as

$\Delta^1{}_1$-CA, $\Sigma^1{}_1$-AC, $\Sigma^1{}_1$-DC, $\Delta^1{}_1$-CA_0, $\Sigma^1{}_1$-AC_0, $\Sigma^1{}_1$-DC_0

and the system TI of transfinite induction, better known as BI (bar induction of lowest type).

All of these systems above, starting with RCA, that are based on full induction (i.e., without the naught), figured prominently in earlier work on fragments of Z_2 by S. Feferman and G. Kreisel and others. Their main motivation was proof theoretic. The development of the naught systems with restricted induction serves the particular needs of Reverse Mathematics.

The hyperarithmetic systems above have not played an important role in RM until recently. But now see [Mo06], [Mo∞], [Ne09], [Ne∞1], [Ne∞2].

TI, or at least significant fragments of TI, have figured importantly in the metamathematics of Kruskal's theorem. For example,

RCA_0 + Kruskal's theorem for wqo labels
with bounded valence;

and

the theory $\Pi^1{}_2$-TI_0

prove the same $\Pi^1{}_1$ sentences. See [RW93] and [Fr84].

In the development of RM, many systems have arisen beyond the most frequently occurring ones discussed above. In the main Chapters of this book alone, which is not focused on RM, the systems ACA' and ACA^+ arise (Definitions 1.4.1, 6.2.1). In [Si99,09], we find, additionally, Σ^1_1-IND, Π^1_1-TR_0, Σ^1_1-TI_0, and $WWKL_0$.

Incomparability under provability does naturally arise in Reverse Mathematics. A particularly clear example, that involves only modest amounts of coding, is as follows. Consider

i. Every ideal in the polynomial ring in n variables over any finite field is finitely generated.

ii. Every infinite tree of finite sequences of 0's and 1's has an infinite path.

In [Si88], it is shown that i) above is provably equivalent to "ω^ω is well ordered" over RCA_0. WKL_0 is RCA_0 + ii).

Now RCA_0 + "ω^ω is well ordered" does not imply WKL_0 since the former has the ω model consisting of the recursive subsets of ω, whereas this does not form a model of WKL_0.

Also, WKL_0 does not imply RCA_0 + "ω^ω is well ordered" since the ordinal, in the sense of proof theory, of WKL_0 is ω^ω, whereas the ordinal of the former is considerably higher. See [Si99,09], p. 391.

The systems that arise above form a hierarchy - but not in the sense of being linearly ordered under provability. Instead, we have linearity under interpretability. Moreover, we expect that as the range of systems used in RM expands from the analysis more and more mathematical theorems, we will maintain this linearity under interpretability.

We summarize this observed phenomena as follows.

DEEP UNEXPLAINED OBSERVED FACT. For any two naturally occurring mathematical theorems A,B, naturally formulated in the language of RM, either RCA_0 + A is interpretable in RCA_0 + B, or RCA_0 + B is interpretable in RCA_0 + A.

This phenomenon also holds in wide ranging contexts, including in set theories, provided a suitable base theory is chosen.

This phenomenon begs for an explanation. At present, there isn't any. Theoretically, lots of incomparability arise under interpretability. See [Fr07], Lecture 1.

In light of this observed comparability, the phrase "logical strength" for formal systems has come to mean "interpretation power". Sometimes it also means "consistency strength". We have shown that interpretation power and consistency strength are equivalent, in a certain precise sense. See [Fr80a], [Smo84], [Vi90], [Vi92], [Vi09], [FVxx].

The principal theme of [Fr75-76] is actually a criticism of the use of fragments of Z_2 for RM. Our idea was that the language of Z_2 is far too impoverished to adequately represent mathematical statements. We categorically rejected the use of coding, which is generally required for formalization within Z_2.

Nevertheless, we quickly came to realize that there were just too many unresolved issues involved in setting up a coding free RM. We chose not to publish the approach of [Fr75-76] (although we circulated those manuscripts widely), but rather focus initially on the more straightforward approach of [Fr74], [Fr76], initiating the Reverse Mathematics program.

The setup in [Fr76] is a compromise. It uses variables over N and variables over unary, binary, and ternary functions from ω into ω, with the numerical constant 0 and a unary function constant for successor.

The system ETF - elementary theory of functions - is then formulated in this language, which is equivalent to the now standard RCA_0 (adapted in the obvious way to the language of ETF). Note that ETF avoids any use of axiom schemes, or reliance in any way on formulas with bounded quantifiers.

As we expected, these subtle issues were put aside by the community, and the much more manageable version of RM using RCA_0 was pursued using the standard coding apparatus used for many years in recursion theory.

In particular, the normal presentation of RCA_0 is simply the axioms for RCA that we gave in [Fr74], with the Induction Axiom Scheme replaced by the weaker Σ^0_1 Induction Axiom Scheme. E.g., see [Si99,09], Definition II.1.5. We preferred the equivalent formulation of ETF.

Our deep interest in coding free RM was, in retrospect, premature. Any reasonably stated equivalent form of RCA_0 was adequate to drive the subsequent development of RM.

Recently, we have come back to the development of coding free RM under the banner of SRM = Strict Reverse Mathematics. Our initial publication on SRM has appeared in [Fr09]. Also see the abstract [Fr09a].

This initial development of SRM is focused on arithmetic (integers and finite sets and finite sequences of integers), and provides strictly mathematical assertions that generate the bounded induction scheme. Integer exponentiation is also investigated in this context, both as an additional principle, and as a derived construction (geometric progressions).

Thus SRM can suitably operate with robustness at a level considerably lower than RCA_0. This promises to refine the reverse mathematics idea to analyze the considerable range of interesting mathematics that is already provable in RCA_0 when suitably formalized.

An intermediate approach is to weaken the base theory RCA_0 to RCA_0*. Here we drop Σ^0_1 induction in favor of the weaker Σ^0_0 induction. See [Si99,09], p. 410-411.

We believe that SRM (strict reverse mathematics), which aims to remove coding entirely, is the appropriate vehicle for greatly expanding the scope of RM.

For the convenience of the reader, we now present the axioms of our now standard RM systems RCA_0, WKL_0, ACA_0, ATR_0, and Π^1_1-CA_0. Of course, these are entirely unsuitable for our new SRM.

The language is two sorted, with variables over natural numbers and variables over subsets of N. We use 0,S,+,•,<,= on sort N, and ∈ between natural numbers and sets of natural numbers.

A formula is Σ^0_1 (Π^0_1) if it begins with an existential (universal) numerical quantifier, and is followed by a formula with only bounded quantifiers (using <).

A formula is Π^1_1 if it begins with a universal set quantifier, followed by a formula with no set quantifiers.

The axioms of RCA_0 are

i. Basics. $\neg S(n) = 0$, $S(n) = S(m) \rightarrow n = m$, $n + 0 = n$, $n + S(m) = S(n + m)$, $n \bullet 0 = 0$, $n \bullet S(m) = (n \bullet m) + n$. $n < m \leftrightarrow (\exists r)(n + S(r) = m)$.
ii. Σ^0_1 induction. $\varphi[n/0] \wedge (\forall n)(\varphi \rightarrow \varphi[n/S(n)]) \rightarrow \varphi$, where φ is Σ^0_1.
iii. Δ^0_1 comprehension. $(\forall n)(\varphi \leftrightarrow \psi) \rightarrow (\exists A)(\forall n)(n \in A \leftrightarrow \varphi)$, where φ is Σ^0_1, ψ is Π^0_1, and A is not free in φ.

The axioms of WKL_0 are RCA_0 together with "every infinite tree of finite sequences of 0's and 1's has an infinite path" suitably coded in RCA_0.

The axioms of ACA_0 are

i. Basics. See RCA_0.
ii. Set induction. $0 \in A \wedge (\forall n)(n \in A \rightarrow S(n) \in A) \rightarrow n \in A$.
iii. Arithmetic comprehension. $(\exists A)(\forall n)(n \in A \leftrightarrow \varphi)$, where φ has no set quantifiers, and A is not in φ.

The axioms of ATR_0 are ACA_0 together with "transfinite recursion can be performed along any well ordering using any arithmetic formula" suitably coded in ACA_0.

The axioms of $\Pi^1_1\text{-}CA_0$ are

i. Basics. See RCA_0.
ii. Set induction. See ACA_0.
iii. Π^1_1 comprehension. $(\exists A)(\forall n)(n \in A \leftrightarrow \varphi)$, where φ is Π^1_1, and A is not free in φ.

0.5. Incompleteness in Exponential Function Arithmetic.

Exponential Function Arithmetic, or EFA, is a fragment of Peano Arithmetic (PA) that we explicitly named, identified, and used, in [Fr78], p. 2, and continue to use in [Fr78], p. 23, [Fr79], p. 6, [Fr80a], p. 2, to this day.

The language of PA consists of $0,S,+,\bullet,=$. The axioms of PA are

1. $\neg Sx = 0$, $Sx = Sy \rightarrow x = y$.
2. $x + 0 = x$, $x + Sy = S(x + y)$.
3. $x \bullet 0 = 0$, $x \bullet Sy = (x \bullet y) + x$.
4. Induction for all formulas in the language of PA.

The language of EFA consists of 0,S,+,•,2^,≤,=. The axioms of EFA are

1. The axioms of Q. (See section 0.1A).
2. 2^0 = 1, 2^Sy = 2^y + 2^y.
3. Induction for all bounded formulas in the language of EFA.

In bounded formulas, all quantifiers must be bounded (≤) to terms not mentioning the variable being bounded.

Technically speaking, EFA is not a fragment of PA since its language is not even a fragment of the language of PA. However, PA is a definitional extension of EFA whose symbols of PA are unmodified.

We focused on EFA long ago because it is the most obvious natural weak fragment of PA for which finite sequence coding provably behaves as expected.

EFA is called EA, or elementary arithmetic, in [Av03], where a major conjecture of mine is discussed in great detail. He writes

"From the point of view of finitary number theory and combinatorics, EA turns out to be surprisingly robust. So much so that Harvey Friedman has made the following Grand conjecture: Every theorem published in the Annals of Mathematics whose statement involves only finitary mathematical objects (i.e., what logicians call an arithmetical statement) can be proved in elementary arithmetic."

A special case of this conjecture is that Fermat's Last Theorem is provable in EFA. However, we are a long way from establishing this, although there is an attack on showing that FLT is provable in PA (see [Mac11]). However, [Mac11] explicitly denies confidence that FLT is provable in EFA. Also see [Mc10].

EFA is essentially identical to what is now called $I\Sigma_0$(exp) (see [HP93]). It is synonymous with $I\Sigma_0$ + exp. EFA is more convenient than $I\Sigma_0$ + exp, in the sense that in order to formulate the latter, we need a suitable formalization of exp in $I\Sigma_0$ - which is cumbersome.

EFA is known to be finitely axiomatizable. This is credited to J. Paris (see [HP93], p. 366).

We are unaware of any presentation of EFA earlier than our [Fr78]. The system $I\Sigma_0 = I\Delta_0$ = bounded arithmetic (which we like to call PFA for polynomial function arithmetic), was introduced much earlier in [Pa71]. Here PFA is Q is extended with the Δ_0 induction scheme. It is open whether PFA is finitely axiomatizable. This question has been seen to be related to issues in computational complexity theory (see [HP93]).

Here is the key property of EFA that is behind the incompleteness from EFA that we discuss.

We write $2^{[y]}(x)$ for 2^...^2^x, where there are y 2's. We take $2^{[0]}(x) = x$.

THEOREM 0.5.1. Suppose EFA proves a sentence of the form $(\forall x_1,\ldots,x_n)(\exists y_1,\ldots,y_m)(\varphi)$, where φ is bounded. There exists r such that $(\forall x_1,\ldots,x_n)(\exists y_1,\ldots,y_m < 2^{[r]}(\max(x_1,\ldots,x_n)))(\varphi)$. Furthermore, there exists r such that EFA proves $(\forall x_1,\ldots,x_n)(\exists y_1,\ldots,y_m < 2^{[r]}(\max(x_1,\ldots,x_n)))(\varphi)$.

This is an instance of what is known as Parikh's theorem. See [HP93], Theorem 1.4, p. 272.

The best known example of a finite theorem that is not provable in EFA but is provable just beyond EFA, is the ordinary finite Ramsey theorem. We give two standard forms of this theorem.

FINITE RAMSEY THEOREM 1. For all $k,p,r \geq 1$ there exists n so large that the following holds. In any coloring of the unordered k tuples from $\{1,\ldots,n\}$ using p colors, there is an r element subset of $\{1,\ldots,n\}$ whose unordered k tuples have the same color.

FINITE RAMSEY THEOREM 2. For all $k,p,r \geq 1$ there exists n so large that the following holds. For all $f:\{1,\ldots,n\}^k \to \{1,\ldots,p\}$, there exists $S \subseteq \{1,\ldots,n\}$ of cardinality r, such that for any $x,y \in S^k$ of the same order type, $f(x) = f(y)$.

These two formulations are easily proved to be equivalent in EFA.

There has been considerable work on upper and lower bounds for these statements. For our purposes, we need only the following.

Let $R_k(l)$ be the least n such that the following holds. In any coloring of the unordered k tuples from {1,...,n} using 2 colors, there is an l element subset of {1,...,n} whose unordered k tuples have the same color.

THEOREM 0.5.2. For all k ≥ 4, there is a constant c_k, such that the following holds. For all l ≥ 1, $R_k(l) \geq 2^{[k-2]}(c_k l^2))$.

For a proof of Theorem 0.5.2, see [GRS80], p. 91-93.

There is ongoing work on sharper estimates of such higher Ramsey numbers of various kinds. For example, see [CFS10].

By Theorems 0.5.1 and 0.5.2, we obtain

COROLLARY 0.5.3. The Finite Ramsey Theorem, even for 2 colors, is not provable in EFA.

The status of the Finite Ramsey Theorem over EFA is completely known. It is given by a so called reversal (as in reverse mathematics).

Consider the statement

$$(\forall n)(2^{[n]} \text{ exists}).$$

This can be formalized in EFA as follows. For all n, there is a (coded) finite sequence with n terms, starting with 1, where each term is the base 2 exponential of the previous term. It is immediate from Theorem 0.5.1 that this sentence is not provable in EFA.

We also consider the following obvious generalization.

$$(\forall n,m)(n^{[m]} \text{ exists}).$$

THEOREM 0.5.4. EFA proves the equivalence of the following.
i. Finite Ramsey Theorem.
ii. Finite Ramsey Theorem for p = 2.
iii. $(\forall n)(2^{[n]}$ exists).
iv. $(\forall n,m)(n^{[m]}$ exists).

$n^{[m]}$ is often referred to as the superexponential. Accordingly, we can define the system SEFA =

superexponential function arithmetic, as follows.

The language of SEFA consists of 0,S,+,•,2^,2^^,≤. The axioms of SEFA are

1. The axioms of EFA.
2. 2^^0 = 1, 2^^Sy = 2^(2^^y).
3. Induction for all bounded formulas in the language of SEFA.

SEFA has the finite sequence coding of EFA. This can be used to treat the obvious generalization, n^^m.

THEOREM 0.5.5. SEFA proves the Finite Ramsey Theorem. SEFA and EFA + (∀n)($2^{[n]}$ exists) prove the same sentences from L(EFA).

There is a very attractive weakening of the Finite Ramsey Theorem, which we call the Adjacent Ramsey Theorem.

THEOREM 0.5.6. Adjacent Ramsey Theorem. For all k,p ≥ 1 there exists t so large that the following holds. For all $f:\{1,...,t\}^k \to \{1,...,p\}$, there exist $1 \le x_1 < ... < x_{k+1} \le t$ such that $f(x_1,...,x_k) = f(x_2,...,x_{k+1})$.

We have shown that this behaves like the Finite Ramsey Theorem. We have also shown that for p = 2, we can set t = 2k+1. [Fr08], [Fr10a].

THEOREM 0.5.7. EFA proves the equivalence of the following.
i. Adjacent Ramsey Theorem.
ii. (∀n)($2^{[n]}$ exists).
iii. (∀n,m)($n^{[m]}$ exists).

We became aware of work that is pretty close to the Adjacent Ramsey Theorem, again with iterated exponential lower bounds - that predates our work. See [DLR95].

A sketch of our work appears in [Fr99b], [Fr10a]. A full self contained manuscript will appear elsewhere.

0.6. Incompleteness in Primitive Recursive Arithmetic, Single Quantifier Arithmetic, RCA_0, and WKL_0.

This level of incompleteness is unusually rich, and we organize the discussion as follows.

0.6A. Preliminaries.

0.6A. Preliminaries.

PRA (primitive recursive arithmetic), $I\Sigma_1$ (single quantifier arithmetic), RCA_0 (our base theory for Reverse Mathematics), and WKL_0 (another of our theories for Reverse Mathematics), are well known systems that represent the same "level", in a sense made explicit below.

PA = Peano arithmetic, is most commonly formulated in the language 0,S,+,•,=, with the following axioms.

1. ¬Sx = 0.
2. Sx = Sy → x = y.
3. x+0 = x, x+Sy = S(x+y).
4. x•0 = 0, x•Sy = x•y + x.
5. Induction for all formulas in L(PA).

The Σ_n (Π_n) formulas are the formulas which begin with an existential (universal) quantifier, followed by at most n-1 quantifiers, followed by a bounded formula.

$I\Sigma_n$ ($I\Pi_n$) denotes the fragment of PA based on induction for Σ_n ($I\Pi_n$) formulas.

There is a fair amount of robustness here. For instance, we can allow blocks of like quantifiers in the definition of Σ_n,(Π_n) and we get the same fragments of PA.

It is well known that for n ≥ 1, $I\Sigma_n$ and $I\Pi_n$ are equivalent. See [HP93], p. 63.

By single quantifier arithmetic, we will mean $I\Sigma_1 \cup I\Pi_1$, which is equivalent to $I\Sigma_1$.

Another important system is PRA = primitive recursive arithmetic. The language of PRA includes 0,S, and symbols for every primitive recursive function (the primitive recursive function symbols). The axioms of PRA are as follows.

1. ¬Sx = 0.
2. Sx = Sy → x = y.

3. The primitive recursive defining equations.
4. Induction for all quantifier free formulas of PRA.

Some authors work with a quantifier free version of PRA. See, e.g., [Min73].

The systems RCA_0 and WKL_0 are from Reverse Mathematics. See [Fr74], [Fr76], [Si99,09], and the end of section 0.4.

We will use the following proof theoretic information about the systems PRA, $I\Sigma_1$, RCA_0, and WKL_0.

THEOREM 0.6A.1. PRA proves induction for all bounded formulas of PRA. WKL_0 proves RCA_0 proves $I\Sigma_1$ proves PRA. The implications are strict. $I\Sigma_1$, RCA_0, WKL_0 prove the same arithmetic sentences. $I\Sigma_1$, PRA prove the same Π^0_2 sentences. $I\Sigma_1$ and RCA_0 prove the same arithmetic sentences. RCA_0 and WKL_0 prove the same Π^1_1 sentences. These results are provable in SEFA. If we remove the second "PRA", then these results are provable in EFA.

For proofs, see [Si99,09], Corollary IX.1.11, Corollary IX.2.7, and Theorem IX.3.16. The proof of the fifth claim, involving $I\Sigma_1$ and PRA, is model theoretic, not formalizable in weak fragments of arithmetic. However, it has been proved in SEFA. See the last paragraph before section 0.1.

Recall that bounded quantifiers are allowed after the unbounded existential quantifier in Π^0_2 formulas. In Π^1_1 sentences, we start with one universal set quantifier, followed by an arithmetic formula.

We also need the following relationship between RCA_0, WKL_0, and the ordinal ω^ω.

THEOREM 0.6A.2. Let T be a primitive recursively given finite sequence tree. If RCA_0 proves that T is well founded, then there exists $n \in N$ and a primitive recursive function h such that RCA_0 proves that h is a map from vertices of T into notations $< \omega^n$, such that if v' extends v in T, then h(v') < h(v). The same holds for WKL_0. These results are provable in SEFA.

Proof: This can be established through the use of $I\Sigma_1(F)$, which is $I\Sigma_1$ extended by a single unary function symbol F. The induction allows use of F. This system has a natural proof theoretic analysis. The last claim follows from the fact that WKL_0 and RCA_0 prove the same Π^1_1 sentences, due to L. Harrington. See [Si99,09], p. 372. QED

We note that the h in Theorem 0.6A.2 can be chosen to be elementary recursive by an observation in [Ara98].

We define the strict Π^1_1 sentences to be sentences asserting the well foundedness of a particular primitive recursively given finite sequence tree.

We obtain the following from Theorem 0.6A.2.

THEOREM 0.6A.3. The following are provably equivalent in RCA_0.
i. Every strict Π^1_1 sentence provable in RCA_0 is true.
ii. Every strict Π^1_1 sentence provable in WKL_0 is true.
iii. ω^ω is well ordered.

THEOREM 0.6A.4. Suppose PRA proves a sentence $(\forall x_1,\ldots,x_n)(\exists y_1,\ldots,y_m)(\varphi)$, where φ is bounded. There is a primitive recursive function f such that $(\forall x_1,\ldots,x_n)(\exists y_1,\ldots,y_m < f(x_1,\ldots,x_n))(\varphi)$. Furthermore, there are primitive recursive function symbols $F_1,\ldots,F_m$ such that PRA proves $\varphi(x_1,\ldots,x_n,F_1(x_1,\ldots,x_n),\ldots,F_m(x_1,\ldots,x_n))$. The same is true of $I\Sigma_1$, RCA_0, and WKL_0. These results are provable in SEFA.

Proof: Since PRA has a universal axiomatization, we can obtain this using Herbrand's theorem (in a sharper form, with < replaced by =). Or we can apply Parikh's theorem to each finite fragment of PRA. See [HP93], Theorem 1.4, p. 272, and [Sie91]. QED

Note that Theorems 0.6A.1 and 0.6A.4 are closely related. They are used in the same way. Thus, if a Π^0_2 sentence has an associated growth rate higher than all primitive recursive functions, then we know that it is not provable in PRA, or even WKL_0, by Theorem 0.6A.4.

0.6B. Sequences of Vectors.

We now consider termination of lexicographic descent in the natural numbers.

For $k \geq 1$, $x,y \in N^k$, write $x <_{lex} y$ if and only if at the first coordinate at which x,y differ, x is less than y.

THEOREM 0.6B.1. Every sequence from N^k that is decreasing in the lex ordering terminates.

Note that Theorem 0.6B.1 is a strict Π^1_1 sentence. Its status is well known over the base theory, RCA_0, of reverse mathematics.

THEOREM 0.6B.2. For each fixed k, Theorem 0.6B.1 is provable in RCA_0. The following are provably equivalent in RCA_0.
i. Theorem 0.6B.1.
ii. ω^ω is well ordered.

Theorem 0.6B.2 follows from the identification of each ω^k with the lexicographic ordering on N^k. Use the straightforward provability in RCA_0 of $(\forall k)(\omega^k$ is well ordered $\rightarrow \omega^{k+1}$ is well ordered).

There is an important sharper form of Theorem 0.6B.1. For $x,y \in N^k$, write $x \leq_c y$ if and only if for all i, $x_i \leq y_i$. Here "c" means "coordinatewise".

THEOREM 0.6B.3. Every infinite sequence from N^k has a finite initial segment such that every term is $\geq_c$ some term in that finite initial segment.

The equivalence of Theorem 0.6B.3 with ω^ω is well ordered is more delicate.

THEOREM 0.6B.4. For each fixed k, Theorems 0.6B.1 and 0.6B.3 are provable in RCA_0. The following are provably equivalent in RCA_0.
i. Theorem 0.6B.1.
ii. Theorem 0.6B.3.
iii. ω^ω is well ordered.
The first claim is provable in SEFA.

Proof: We have already seen that for each fixed k, Theorem 0.6B.1 is provable in RCA_0. It is obvious that Theorem 0.6B.3 implies Theorem 0.6B.1 in RCA_0.

We first show that for each k, RCA_0 proves that every infinite sequence from N^k has an infinite increasing ($\leq_c$) subsequence. This is proved by induction on k. The case k = 1 asserts that every infinite sequence from N has an infinite increasing ($\leq$) subsequence. If the sequence is bounded, then it has a constant infinite subsequence. Otherwise, use primitive recursion.

Suppose RCA_0 proves this for k. Now let $x_1,x_2,... \in N^{k+1}$. Consider the infinite sequence of first terms, take an infinite increasing ($\leq$) subsequence, and then chop the first terms off, forming $y_1,y_2,... \in N^k$. By the induction hypothesis, we can prove that the y's have an infinite increasing ($\leq_c$) subsequence, which immediately gives rise to an infinite increasing ($\leq_c$) subsequence of the x's.

We claim that $RCA_0 + \omega^\omega$ is well ordered proves

for all k, for every $x_1,x_2,...$ from N^k,
there exists $i < j$ such that $x_i \leq_c x_j$

because for each fixed k, the above is strict Π^1_1, and we can apply Theorem 0.6A.3. (The RCA_0 proofs for each k are a primitive recursive function of k).

Now the above proves Theorem 0.6B.3 by the following argument.
Let $x_1,x_2,... \in N^k$ be such that for all n there exists x_m that is not $\geq_c$ any of $x_1,...,x_n$. By primitive recursion, build an infinite subsequence $y_1,y_2,...$ of the x's such that no y_i is $\geq_c$ any of $y_1,...,y_{i-1}$. Choose $i < j$ such that $y_i \leq_c y_j$. This is a contradiction.

Hence iii → ii → i. We have already seen that i → iii. QED

Theorem 0.6B.4 was first proved in [Si88] using combinatorial methods. Note that here we have avoiding the combinatorial argument in favor of proof theory.

We now discuss finite forms of Theorems 0.6B.1 and (a weak form of) 0.6B.3. These are Π^0_2 sentences, thus falling within the scope of PRA and $I\Sigma_1$.

THEOREM 0.6B.5. For all $k \geq 1$ there is a longest sequence $x_1 >_{lex} x_2 >_{lex} ... >_{lex} x_n$ from N^k such that each $\max(x_i) \leq i$.

THEOREM 0.6B.6. For all k there exists n such that the following holds. For all $x_1,...,x_n$ from N^k such that each $\max(x_b) \leq b$, there exists $1 \leq i < j \leq n$ such that $x_i \leq_c x_j$.

It is also natural to add a parameter as follows.

THEOREM 0.6B.7. For all $k \geq 1$ and $p \geq 0$, there is a longest sequence $x_1 >_{lex} x_2 >_{lex} ... >_{lex} x_n$ from N^k such that each $\max(x_i) \leq i+p$.

THEOREM 0.6B.8. For all $k \geq 1$ and $p \geq 0$, there exists n such that the following holds. For all $x_1,\ldots,x_n$ from N^k such that each $\max(x_b) \leq b+p$, there exists $1 \leq i < j \leq n$ such that $x_i \leq_c x_j$.

THEOREM 0.6B.10. EFA proves 0.6B.8 ↔ 0.6B.6 → 0.6B.7 ↔ 0.6B.5.

Proof: This is easily seen by raising the dimension. E.g., to derive Theorem 0.6B.8, apply Theorem 0.6B.6 in N^{k+p} to $(0,\ldots,0;1,\ldots,0),(0,\ldots,0;0,1,\ldots,0),\ldots,(0,\ldots,0;0,\ldots,1)$,
$(x_1;0,\ldots,0),(x_2;0,\ldots,0),\ldots,(x_n;0,\ldots,0)$. QED

We show below that → can be replaced by ↔.

THEOREM 0.6B.11. For each fixed $k \geq 1$, Theorem 0.6B.8 is provable in WKL_0, and hence in PRA. For fixed $k \geq 1$, Theorem 0.6B.8 has a primitive recursive witness function (of p). This applies to Theorems 0.6B.5 - 0.6B.7. The first claim is provable in SEFA.

Proof: We argue in WKL_0. Fix k,p, and form the appropriate finitely branching tree. By Theorem 0.6B.3, there is no infinite path through this tree. Hence this tree is finite. QED

To pin down the status of Theorems 0.6B.5 - 0.6B.8, we need the analog of Theorem 0.6A.3 for Π^0_2 sentences. This is given through a formalization of the primitive recursive functions in EFA.

Now EFA cannot treat an arbitrary primitive recursive function, because they grow too fast - see Theorem 0.5.1. So the primitive recursive functions are instead treated in EFA as partial recursive functions given by specific algorithms.

We work in EFA. We assume that each primitive recursive function symbol comes with an associated primitive recursive derivation, using terms rather than projection functions and composition introduction.

We let PRCT be the class of closed terms in this language. We define the all important reduction function RF:PRCT → PRCT as follows. Let t ∈ PRCT. Let s be the leftmost subterm of t which has exactly one occurrence of a primitive recursive function symbol F other than S. Replace s by its expansion given by the derivation associated with F. If there is no such subterm of t, set RF(t) = t.

Let F be a primitive recursive function symbol. We associate the following algorithm ALG(F). Given $p_1,\ldots,p_k \geq 0$, apply RF successively starting at $F(p_1^*,\ldots,p_k^*)$. Stop when we arrive at a fixed point of RF, say q*. Output q.

From the point of view of EFA, ALG(F) defines a k-ary partial recursive function, where the arity of F is k.

We can now state the analog of Theorem 0.6A.3.

THEOREM 0.6B.12. The following are provably equivalent in SEFA.
i. 1-Con(PRA).
ii. 1-Con(WKL_0).
iii. Every primitive recursive definition defines a total function (i.e., each ALG(F) computes a total function).

Proof: Here i ↔ ii is by Theorem 0.6A.1. It is straightforward in EFA to construct, for each primitive recursive function symbol F, a proof in WKL_0 that ALG(F) is total. It is easiest to make use of Σ^0_1 induction in WKL_0. Hence ii → iii. Using iii, first obtain super exponentiation, and hence cut elimination. Then use the primitive recursive semantics of cut free proofs in PRA to obtain i. QED

THEOREM 0.6B.13. SEFA proves that for each fixed k, Theorems 0.6B.5 - 0.6B.8 are provable in PRA. The following are provably equivalent in SEFA.
i. Any of Theorems 0.6B.5 - 0.6B.8.
ii. Every primitive recursive definition defines a total function.
iii. 1-Con(PRA).

Proof: For the first claim, fix k. Prove Theorem 0.6B.8 by assuming that it is false, constructing an associated finitely branching tree, taking an infinite path, and applying Theorem 0.6A.7 to get a contradiction. This proves the first claim with PRA replaced by WKL_0. Now apply Theorem 0.6A.1. From the first claim, we obtain iii → i. For ii → iii, see Theorem 0.6B.12.

For i → ii, we argue in EFA. We have to be careful to avoid use of Σ^0_1 induction. Assume first that Theorem 0.6B.7 holds.

We need to handle the reduction process RFCT:PRCT → PRCT in EFA.

For any t ∈ PRCT, we can use a numerical measure #(t) computed as follows. Let r be the largest depth of the primitive recursive function symbols appearing in t, other than S. Form the length r sequence, where the i-th term, 1 ≤ i ≤ r, is the number of occurrences in t of primitive recursive function symbols whose derivation has depth r-i+1.

It is clear that if t is not a fixed point of RFCT, then #(t) $>_{lex}$ #(RF(t)). We can almost use Theorem 0.6B.7 to show that iteration of RFCT comes to a fixed point. However, the growth in the max's of the #'s is greater than 1. Nevertheless, the growth is at most a constant, for each ALG(F), that depends only on the derivation of F. Hence we can Theorem 0.6B.7, by raising the dimension, and using dummy variables.

Also by raising the dimension, it is easily seen that Theorem 0.6B.6 implies Theorem 0.6B.7. Thus we obtain ii → i. QED

0.6C. Walks in N^k.

A walk in N^k is a finite or infinite sequence in N^k such that each successive vector is "close" to the preceding vector.

There are several interesting notions of "close" that we can use. We restrict attention to only these four:

1. The Euclidean distance $|x-y|_2$ is at most 1.
2. The Euclidean distance $|x-y|_2$ is at most 1.5.
3. The Euclidean distance $|x-y|_2$ is at most 2.
4. The sup norm distance $|x-y|_\infty$ is at most 1.

These all have combinatorial equivalents that are easier to think about for our purposes.

1. At most one coordinate is changed, and it is changed by 1.
2. At most two coordinates are changed, and they are changed by 1.
3. Either no change, or one coordinate is changed by 1 or 2, or two coordinates are each changed by 1.
4. All coordinates are changed by at most 1.

Recall the definition of $\leq_c$ in N^k. We can think of $x \leq_c y$ as "x points outward to y".

Let $W_1, W_2, \ldots$ be a walk in N^k. We look for $i < j$ such that $W_i \leq_c W_j$.

THEOREM 0.6C.1. For all $x \in N^k$, in every sufficiently long walk W in N^k starting with x, there exists $i < j$ such that $W_i \leq_c W_j$. Here we can use any of 1-4. If we use 1), then a walk of length $|x|_1 + k + 1$ is sufficient.

Proof: This is proved the same way that Theorem 0.6B.8 was proved using Theorem 0.6B.3. For the final claim, note that we cannot keep going down for that long. Hence there exists $i < j$ such that the i-th and (i+1)-st terms are the same, or the former goes up to the latter, according to 1. QED

Note that the weakest of 1-4, except for the trivial 1), is 2). Hence we now focus on 2).

We now develop lower bounds for the functions $f_1, f_2, \ldots : Z^+ \rightarrow Z^+$ given by

$f_k(n)$ = the of terms in the longest walk $(n,0,\ldots,0) = x_1, x_2, \ldots, x_r \in N^k$, such that for no $i < j$ is $x \leq_c x_j$. (Here we take the length of a walk as the number of terms, r).

This particular definition of $f_k(n)$ is used for convenience. Note that any longest such walk must have $x_r = (0,\ldots,0)$.

First consider the case k = 2. Clearly for all $n \geq 1$, $f_2(n) \geq 2n$, by looking at the walk

(n,0)
...
(0,n)
(0,n-1)
...
(0,0)

We now develop a lower bound on $f_{k+2}(n)$ in terms of f_k. $f_{k+2}(1) \geq 2$.

Now consider the following walk in N^{k+2}, which is divided into n blocks. In the i-th block, $f_k f_k \ldots f_k(1)$ appears, where there are i f_k's.

$(n,0,...,0)$
$(n-1,1,1,...,0)$
...
$(n-1,f_k(1),0,...,0)$
$(n-2,f_k(1),0...,1)$
...
$(n-2,0,...,0,f_kf_k(1))$
(n-3,1,...,0,fkfk(1))
...
$(n-3,f_kf_kf_k(1),0,...,0)$
...
$(0,...,0,f_kf_k...f_k(1))$, or $(0,f_kf_k...f_k(1),0,...,0)$
...
$(0,...,0)$

where there are n f_k's in the second to last displayed tuple.

The first block starts with $(n-1,1,1,...,0)$. It walks from $(1,0,...,0)$ to $(0,...,0)$ in dimension k, for $f_k(1)$ steps, using coordinates 3 through k+2. Meanwhile, the first term stays unchanged at n-1, and the second term counts from 1 to $f_k(1)$.

We continue in this way, creating n blocks.

In this walk, no x_i is $\leq_c$ any later x_j. Hence $f_{k+2}(n) \geq f_kf_k...f_k(1)$, where $k,n \geq 1$, and there are n f_k's.

Note that

$f_2(n) \geq 2n$, $f_{k+2}(1) \geq 2$, $f_{k+2}(n) \geq f_kf_k...f_k(1)$.

It now follows immediately that $f_{2k}(n) \geq A_k(n)$, $k,n \geq 1$. See the definition of the A_k, $k \geq 1$, just before Theorem 0.7.10.

From these considerations, and from Theorem 06B.13, we obtain the following.

THEOREM 0.6C.2. For each fixed k, Theorem 0.6C.1 is provable in PRA. EFA + 1-Con(PRA) proves Theorem 0.6C.1.

THEOREM 0.6C.5. SEFA proves that for each fixed k, Theorem 0.6C.2 is provable in PRA. The following are provably equivalent in SEFA.
i. Theorem 0.6C.1.
ii. Theorem 0.6C.2.

iii. Every primitive recursive definition defines a total function.
iv. 1-Con(PRA).

Here 1-Con(T) means T is 1-consistent; i.e., every Σ^0_1 sentence provable in T is true.

0.6D. Hilbert's Basis Theorem.

We now come to a discussion of concrete formulations of the Hilbert basis theorem for polynomial rings in several variables over fields.

THEOREM 0.6D.1. HBT (Hilbert's Basis Theorem). Let $P_1,P_2,...$ be an infinite sequence of polynomials from the polynomial ring in k variables over a countable field. There exists n such that each P_i is in the ideal generated by $P_1,P_2,...,P_n$.

Here a countable field in RCA_0 consists of operations $0,1,+,-,\bullet,^{-1}$ obeying the field axioms, on a domain which is a subset of ω.

Let us review a proof of the above concrete strict Π^1_1 form of HBT.

Order the monomials in k variables lexicographically. First let Q_1,Q_2, ... enumerate all polynomials in the ideal generated by the P's. For each i, look at the leading monomial M_i of Q_i.

Apply Theorem 0.6B.3 to the sequence $M_1,M_2,...$, obtaining n such that all M's are multiples of at least one of $M_1,...$, M_n. This gives us n such that the leading coefficient of every Q_i is a multiple of the leading coefficient of at least one of $Q_1,...,Q_n$. Then every Q_i is ideal generated by $Q_1,...,Q_n$, using iterated division with remainder.

From this sketch, and by looking at monomial ideals, we see the following.

LEMMA 0.6D.2. RCA_0 proves 0.6B.3 $\rightarrow$ HBT $\rightarrow$ 0.6B.1. In fact, this implication works for HBT over the two element field. We write this special case as HBT(2).

THEOREM 0.6D.3. HBT is provable in RCA_0 for each fixed k. RCA_0 proves the equivalence of
i. HBT.
ii. HBT(2).

ii. ω^ω is well ordered.

This is obtained immediately from Theorem 0.6B.2 and Lemma 0.6D.2.

Theorem 0.6D.3 was proved in [Si88].

We also have the following finite form of HBT.

THEOREM 0.6D.4. FHBT (Finite Hilbert's Basis Theorem). For each $k \geq 1$ there exists n so large that the following holds. Let F be a countable field. Let $P_1,P_2,...P_n$ be polynomials in k variables with coefficients from F. Assume that the degree of each P_i is at most i. There exists $1 \leq i \leq n$ such that P_i is in the ideal generated by $P_1,...,P_{i-1}$.

The above result is stronger than expected, in that it has a strong uniformity - the integer n depends only on k, and not on the field. It is true for all fields F, but we want to stay within countable objects.

We also have the form with an additional numerical parameter.

THEOREM 0.6D.5. FHBT' (Finite Hilbert's Basis Theorem'). For each $k \geq 1$ and $p \geq 0$, there exists n so large that the following holds. Let F be a countable field. Let $P_1,P_2,...P_n$ be polynomials in k variables with coefficients from F. Assume that the degree of each P_i is at most i+p. There exists $1 \leq i \leq n$ such that P_i is in the ideal generated by $P_1,...,P_{i-1}$.

We sketch a proof of FHBT' in WKL_0 + HBT. Fix k,r,p, and assume FHBT' is false. Write down the countable field axioms, and the infinitely many axioms with infinitely many constants asserting that we have polynomials $P_1,P_2,P_3,...$. The number of constants used for each P_i is dictated by the bound $\deg(P_i) \leq i+p$. For each i, assert that P_i is not in the ideal generated by $P_1,...,P_{i-1}$ using infinitely many universal axioms. Call this theory T, and let $T_0 \subseteq T$ be finite. Using the counterexample $F,P_1,P_2,...$, we see that T_0 is consistent (with the help of cut elimination in WKL_0). Hence T is consistent, and has a model. A model of T violates HBT.

The statement of FHBT' is not in explicitly Π^0_2 form. If F is a finite field or the field of rationals, then FHBT and FHBT' are in Π^0_2 form.

THEOREM 0.6D.6. SEFA proves that for each $k \geq 1$, FHBT and FHBT' for finite fields and the field of rationals is provable in PRA. The following are provably equivalent in SEFA.
i. FHBT on any finite field or the rationals.
ii. FHBT' on any finite field or the rationals.
iii. Every primitive recursive definition defines a total function.

We can put FHBT' in Π^0_2 form using the uniform algorithm and bounds for ideal membership in polynomial rings over fields, from [He26]. For a modern treatment of ideal membership, see [As04].

Alternatively, note that for fixed k,p, the conclusion quantifying over countable fields F is equivalent, over WKL_0, to a Σ^0_1 sentence, using the formalized completeness theorem. This gives us a Π^0_2 sentence which appropriately strengthens FHBT from the point of view of WKL_0.

Using either argument, and applying Theorem 0.6B.11, and using monomials, we obtain the following.

THEOREM 0.6D.7. In FHBT', for each $k \geq 1$, there is a primitive recursive upper bound on n as a function of p. There is no universal primitive recursive bound for FHBT or FHBT'. The following are provably equivalent in RCA_0.
i. FHBT.
ii. FHBT'.
iii. Every primitive recursive definition defines a total function.

A proof of the first two claims of Theorem 0.6D.7 has appeared in [Soc92].

0.6E. Sequences of Algebraic Sets.

We now consider the following well known consequence of HBT: every decreasing chain of algebraic sets is eventually constant. We will formulate this directly in terms of polynomials.

THEOREM 0.6E.1. Let $P_1,P_2,\ldots$ be an infinite sequence of polynomials from the polynomial ring in k variables over a countable field. There exists n such that every simultaneous zero of $P_1,\ldots,P_n$ is a zero of all P's.

It is somewhat tricky to show that Theorem 0.6E.1 implies ω^ω is well ordered. We cannot just use monomials. Also, this cannot be done if the P's represent irreducible algebraic sets, by Krull's theorem for chains of prime ideals. So we must consider reducible algebraic sets.

Fix the dimension k and an infinite field F. Let T be a finite tree with at least one vertex, where every path has at most k vertices (excluding the root), and where the vertices other than the root are labeled with different elements of the field F. We call these k-good trees.

The algebraic meaning of a vertex at the i-th level above the root with label c is the equation $x_i = c$ (the root is at the 0-th level). The algebraic meaning of a path is the conjunction of the algebraic meaning of the vertices along that path other than the root. The algebraic meaning of the tree T is the disjunction of the algebraic meanings of the paths of T. Take [T] to be this union of intersections. Rewrite this as an intersection of unions. Each union is the zero set of a polynomial obtained by multiplying the relevant x_i-c. [T] becomes an algebraic subset of F^k, given by polynomials of degree ≤ #T = the number of terminal vertices of T.

We need to have a sufficient criterion for [T] to properly contain [T'].

LEMMA 0.6E.2. Let T,T' be k-good trees. Suppose T' is obtained from T by adding one or more children to a terminal vertex. Or suppose T' is obtained from T by deleting one of the children of a vertex that has at least two children (and of course all vertices above the one deleted). Then [T] properly contains [T'].

Now all we have to do is to deal with the combinatorics of these two tree operations.

There is a nice way of assigning ordinals < ω^k to k-good trees. For each terminal node x of height 1 ≤ i ≤ k, assign the ordinal ω^{i-1}. Now take the sum of the ordinals assigned to the terminal nodes, in decreasing (≥) order. This is ord(T).

The two tree operations lower ordinals. Also, ord(T) is onto the ordinals < ω^k. Even more is true and useful. Given α < ord(T), there exists T' obtained from T by successive applications of the two tree operations in some combination, such that ord(T′) = α.

We have just provided a way of assigning an algebraic set to ordinals < ω^k so that if the algebraic set decreases then the ordinal lowers. We do require that that the field be infinite.

THEOREM 0.6E.3. The following are provably equivalent in RCA_0.
i. HBT.
ii. HBT(2).
iii. Theorem 0.6E.1.
iv. Theorem 0.6E.1 for the field of rationals.
v. ω^ω is well ordered.

We can also develop a finite form for Theorem 0.6E.1 that is analogous to the finite forms discussed above for HBT.

THEOREM 0.6E.4. Let k ≥ 1 and F be a field. There is a bound on the length of chains of algebraic sets $A_1 \supseteq \ldots \supseteq A_n$ in F^k, where each A_i is of presentation degree ≤ i. Furthermore, the bound can be taken to depend on k only, and not on F.

We can show that the witness function for Theorem 0.6E.4 is (roughly) at least the witness function for our finite form of lex descent using the above way of assigning algebraic sets to ordinals (see Theorems 0.6B.5, 0.6B.7). In fact, the analog of Theorem 0.6D.7 holds here.

0.6F. Relatively Large Ramsey Theorem for Pairs.

We discuss the Relatively Large Ramsey Theorem in section 0.8C. [EM81] considers this theorem for pairs.

THEOREM 0.6F.1. Relative Large Ramsey Theorem for Pairs. For all p,r there exists n so large that the following holds. In any coloring of the unordered pairs from {1,...,n} using p colors, there is a relatively large subset of {1,...,n} with at least r elements whose unordered pairs have the same color.

The following is proved in [EM81].

THEOREM 0.6F.2. For each p, consider the function f_p of r that outputs the least n that makes Theorem 0.6F.1 true. Then each f_p is primitive recursive, and each primitive recursive function is dominated by some f_p.

0.7. Incompleteness in Nested Multiply Recursive Arithmetic, and Two Quantifier Arithmetic.

The material in this section is taken from [Fr01c], until the last four paragraphs.

The well known proof theoretic analysis of $I\Sigma_n$, $n \geq 1$, is based on the ordinal $\omega[n+1] = \omega\hat{}...\hat{}\omega$, a tower of n+1 ω's. In particular, the proof theory of $I\Sigma_2$ is based on the ordinal $\omega^{\omega\hat{}\omega}$.

Nested multiple recursion on the nonnegative integers is given by the scheme

$$f(x_1,...,x_k,y_1,...,y_m) = t(f_{<x\_1,...,x\_k}(y_1,...,y_m))$$

where

i) $f_{<x\_1,...,x\_k}$ is the function given by

$f_{<x\_1,...,x\_k}(z_1,...,z_k,y_1,...,y_m) = f(z_1,...,z_k,y_1,...,y_m)$ if $(z_1,...,z_k) <_{lex} (x_1,...,x_k)$; 0 otherwise;

ii) t is any term involving $f_{<x\_1,...,x\_k}$, variables $x_1,...,x_k,y_1,...,y_m$, the successor function, constants for integers, previously defined functions, and IF THEN ELSE based on <,=.

The functions generated in this way are called the nested multiply recursive functions (on the integers). This is a rather robust collection of functions on the integers, whose
definition does not involve ordinal notations. It coincides with the $<\omega^{\omega\hat{}\omega}$ recursive functions, and the $<\omega^{\omega}$ nested recursive functions; see [Ros84], pages 93,94, going back to
[Tai61]. For a general treatment of $<\lambda$ recursive functions via descent recursion, see [FSh95]).

Combining this with the proof theory of $I\Sigma_2$ based on $\omega^{\omega\hat{}\omega}$, gives the following.

THEOREM 0.7.1. The provably recursive functions of $I\Sigma_2$ are the $<\omega^{\omega\hat{}\omega}$ recursive functions (via descent recursion, [FSh95])), and the nested multiply recursive functions. Every $\Pi^0{}_2$ sentence provable in $I\Sigma_2$ has a nested multiply recursive witness function. The first result is provable in SEFA.

NMRA (nested multiply recursive arithmetic) is the analog of PRA (primitive recursive arithmetic). It extends the usual axioms for successor by the defining equations for the nested multiply recursive functions, and the induction scheme for quantifier free formulas in its language.

THEOREM 0.7.2. $I\Sigma_2$ and NMRA prove the same Π^0_2 sentences. The following are provably equivalent over SEFA.
i. 1-Con($I\Sigma_2$).
ii. 1-Con(NMRA).
iii. Every primitive recursive (elementary recursive, polynomial time computable) sequence from $\omega^{\omega^\wedge\omega}$ stops descending.
These are provable in $I\Sigma_3$ but not in $I\Sigma_2$.

Let us start with the following simple problem.

THEOREM 0.7.3. There is a longest finite sequence $x_1,x_2,\ldots,x_n$ from {1,2} in which no consecutive block $x_i,\ldots,x_{2i}$ is a subsequence of any later consecutive block $x_j,\ldots,x_{2j}$.

Let us call this property of finite sequences property *.

One can easily show that the maximal length of a sequence from {1,2} with property * is 11, and that the only examples are 12221111111 and 21112222222.

THEOREM 0.7.4. There is a longest finite sequence from {1,2,3} with property *.

Since the above is a Σ01 statement, it is provable in extremely weak fragments of arithmetic. However, such a proof is not of reasonable size.

The simplest known proof of reasonable size is truly exotic compared with the statement; this proof is conducted in Π^1_1-CA_0 (see section 0.4). With some considerable trouble, it can be replaced with a considerably less exotic proof, of reasonable size, that is formalizable in $I\Sigma_2$. Of course, this is still rather exotic compared to the statement.

We sketch the simplest known proof, which uses the Nash Williams minimal bad sequence argument, from [NW65], in this context. First we shift context to infinite sequences of finite sequences.

THEOREM 0.7.5. Let $k \geq 1$ and $x_1,x_2,\ldots$ be an infinite sequence of finite sequences from $\{1,\ldots,k\}$. There exists $i < j$ such that x_i is a subsequence of x_j.

Proof: Suppose this is false. Call an infinite sequence bad if it is a counterexample. Let x_1 be of least length so that it starts an infinite bad sequence. Let x_2 be of least length
so that x_1,x_2 starts a bad sequence. Continue in this way, getting a "minimal" bad sequence $x_1,x_2,\ldots$. There is an infinite subsequence $x_{i\_1},x_{i\_2},\ldots$, all of which start with the
same number. Note that $x_{i\_1}',x_{i\_2}',\ldots$ is bad, where the primes mean "chop off the first term" (no x can be empty). Hence $x_1,\ldots,x_{i1\ -1},x_{i\_1}',x_{i\_2}',\ldots$ is also bad. But x_{i_1}' is shorter than x_{i_1}, contradicting the choice of x_{i_1}. QED

Proof of Theorem 0.7.4: Suppose there are arbitrarily long such. Build the finitely branching tree of such. Let $x_1,x_2,\ldots$ be an infinite branch, which therefore has property *. Consider the infinite sequence

x_1,x_2
x_2,x_3,x_4
x_3,x_4,x_5,x_6
...

By Theorem 0.7.5, one is a subsequence of a later one. This contradicts property *. QED

Obviously we did not use that there are only three letters.

THEOREM 0.7.6. The Block Subsequence Theorem. For all $k \geq 1$, there is a longest finite sequence $x_1,\ldots.,x_n$ in k letters in which no consecutive block $x_i,\ldots,x_{2i}$ is a subsequence of a later consecutive block $x_j,\ldots,x_{2j}$.

THEOREM 0.7.7. For each fixed k, the Block Subsequence Theorem is provable in $I\Sigma_2$ and NMRA. This is provable in EFA.

Proof: In order to tame the proof of The Block Subsequence Theorem, we need to tame Theorem 0.7.5. I.e., we need to replace the minimal bad sequence argument with something more concrete.

The sharpest way to do this is to effectively assign (names for) ordinals < ω^{ω^k} to finite bad sequences in the partial order of finite sequences from {1,...,k+1} under subsequence, where if one is extended to another, then the corresponding ordinal decreases. This is for each fixed k ≥ 1. This construction appears in [Si88]. Also see [Has94].

For fixed k, we now build the tree T of bad finite sequences in the sense of the Block Subsequence Theorem for {1,...,k+1}. Each bad finite sequence here gives rise to a bad sequence in the partial order of finite sequences from {1,...,k+1}. Therefore we can assign ordinals < ω^{ω^k} to vertices in T according to the preceding paragraph.

For each level n of the tree T, we have finitely many vertices of that level, whose assigned ordinals are $\alpha_1,\ldots,\alpha_p < \omega^{\omega^k}$, where p ≥ 0. We define β_n to be the ordinal $\omega^{\alpha_1'} + \ldots + \omega^{\alpha_p'}$, where $\alpha_1',\ldots,\alpha_p'$ is $\alpha_1,\ldots,\alpha_p$ put in decreasing order.

It is obvious that if $\beta_n > 0$ then $\beta_{n+1} < \beta_n$. Hence for some n, $\beta_n = 0$. Therefore T is finite, and the Block Sequence Theorem is proved.

Note that this proof is carried out in just EFA, together with the fact that there is no double exponential time computable infinite descending sequence through ω^{ω^k}. However, the latter is well known to be provable in $I\Sigma_2$ and in NMRA. Or we can prove the latter in $I\Sigma_2$ and appeal to Theorem 0.7.2. If we follow that route, we need SEFA and not just EFA. QED

THEOREM 0.7.8. The Block Subsequence Theorem is provable in $I\Sigma_3$.

Proof: We argue in $I\Sigma_3$. By Theorem 0.7.7, we see that for each k, The Block Subsequence Theorem for k is provable in $I\Sigma_2$. Note that for each k, the Block Subsequence Theorem is a Σ^0_1 sentence. It is well known that $I\Sigma_3$ proves 1-Con($I\Sigma_2$). E.g., see [HP93], Corollary 4.34, p. 108. Hence we have The Block Subsequence Theorem. QED

In [Fr01c], it is shown how to reverse this process in order to show how descent recursion through ω^{ω^ω} can be suitably handled in EFA + the block subsequence theorem. Hence from Theorems 0.7.1, 0.7.2, we obtain the following.

THEOREM 0.7.9. The Block Subsequence Theorem is provable in

$I\Sigma_3$ but not in NMRA and $I\Sigma_2$. The witness function for The Block Subsequence Theorem dominates all multiply recursive functions. The following are provably equivalent in SEFA.
i. The Block Subsequence Theorem.
ii. 1-Con($I\Sigma_2$).
iii. 1-Con(NMRA).

To prove this, use Theorems 0.7.1, 0.7.8.

We now return to the block subsequence theorem with 3 letters. The exotic lower bounds are obtained in [Fr01c].

The construction is rather intricate, and uses a seed that we constructed by hand. This seed is a particular sequence of length 216 with property *. This sequence α is displayed on p. 126 of [Fr01c]. (Actually, its blocks $\alpha[i],\ldots,\alpha[2i]$, $1 \leq i \leq 108$, are displayed). It is important that α has the following two additional properties from [Fr01c], p. 122.

i. α is of the form $u13^{108}$.
ii. For all $i \leq 108$, $\alpha[i],\ldots,\alpha[2i]$ has at least one 1.

In [Fr01c], we use a convenient version of the Ackermann hierarchy of functions. We define functions $A_1,A_2,\ldots$ from Z^+ into Z^+ as follows. A_1 is doubling. $A_{k+1}(n) = A_k\ldots A_k(1)$, where there are n A_k's.

It is worth noting that $A_k(1) = 2$, $A_k(2) = 4$, and $A_k(3)$ goes to ∞ as k goes to ∞.

We take the Ackermann function to be given by $A(k) = A_k(k)$.

It is easy to see that all primitive recursive functions are eventually dominated by some A_k. In fact, all primitive recursive functions are dominated by some A_k at all arguments ≥ 3.

In [Fr01c], this seed is extended to a sequence of length > $A_7(184)$, thus obtaining the following.

THEOREM 0.7.10. The longest length of a sequence from {1,2,3} with * is > $A_7(184)$.

Randall Dougherty wrote some software that looks for sequences from {1,2,3} with * obeying i,ii above, 108 replaced by much higher even integers. He was able to find such a seed with length 187,196; i.e., 108 replaced by 93,598. Using this seed, we obtain the following in

[Fr01c].

THEOREM 0.7.11. The longest length of a sequence from {1,2,3} with * is > $A_{7198}(158,386)$.

As for an upper bound, we haven't worked this out, but are confident that A(A(5)) is a crude upper bound.

If we consider 4 letters, then the numbers grow considerably more exotic. The maximal length is greater than AA...A(1), where there are A(5) A's.

Let J(k) be the maximal length of a sequence in k letters with property *. By Theorem 0.7.9, J grows faster than all multiply recursive functions. By comparison, the Ackermann function $A_k(k)$ is a puny little doubly recursive function.

The ordinal $\omega^{\omega^\wedge\omega}$ is also used in [Si88] in connection with the Robson basis theorem, involving polynomial rings based on noncommuting indeterminates (see [Robs78a], [Robs78b]). It is shown there that RBT is provably equivalent to "$\omega^{\omega^\wedge\omega}$ is well ordered" over RCA_0.

We close with a brief discussion of braids. The following is obtained from [CDW10].

Artin's braid groups are algebraic structures of substantial importance in core mathematics. There has emerged a standard ordering on braids, called the Dehornoy order.

It is known that the restriction of this standard ordering to B^+_n, which consists of the Garside positive braids, is a well ordering of type ω^ω^{n-2}. This allows for the development of combinatorial theorems based on this restricted ordering, that are provable in $I\Sigma_3$ but not in $I\Sigma_2$, and whose associated functions are just beyond being multiply recursive. This has been accomplished in [CDW10].

0.8. Incompleteness in Peano Arithmetic and ACA_0.

This level of incompleteness is unusually rich. We will not try to be exhaustive.

We will organize the discussion as follows.

0.8A. Preliminaries.
0.8B. Goodstein Sequences.

0.8A. Preliminaries.

The earliest mathematical example of incompleteness in Peano Arithmetic (PA) appeared in [Goo44], although it wasn't known until [KP82] that the result was not provable in PA. The result is the termination of Goodstein sequences.

This was followed by an entirely different example in [PH77], that is closely related to well known existing mathematical developments - i.e., Ramsey theory. This was the Paris-Harrington Ramsey theorem.

0.8E is a direct spin-off of 0.8B. 0.8D is a direct spin-off of 0.8C. 0.8F, 0.8G, and 0.8H break new ground, and represent the current state of the art with regard to incompleteness at the level of Peano Arithmetic.

0.8H is particularly flexible, and is a specialization to the binary case of incompleteness results from far stronger systems than PA. These are discussed in sections 0.9 and 0.10.

The relevant proof theoretic information about PA, ACA_0, ACA' is as follows. For the definition of ACA', see Definition 1.4.1.

THEOREM 0.8A.1. ACA_0 is a conservative extension of PA. The provably recursive functions of ACA_0 and PA are the $<\epsilon_0$ recursive functions. ACA_0 proves WKL_0. The following are provably equivalent in RCA_0.
i. Π^1_1 reflection on ACA_0.
ii. ϵ_0 is well ordered.
These are provable in ACA' but not in ACA_0.
The first claim is provable in SEFA.

For a general treatment of $<\lambda$ recursive functions via descent recursion, see [FSh95]).

THEOREM 0.8A.2. The following are provably equivalent in SEFA.

i. 1-Con(ACA_0).
ii. 1-Con(PA).
iii. Every primitive recursive (elementary recursive, polynomial time) sequence from ϵ_0 stops descending.

0.8B. Goodstein Sequences.

Let b ≥ 2. We can write any n ≥ 0 uniquely in base b, where we think of the exponents as nonnegative integers. Then we can write these exponents in base b, again creating perhaps more exponents. Of course, numbers < b do not get rewritten. This process must end, and we obtain a fully base b representation of n. It has the structure of a finite tree, and the only integers appearing are b's and numbers from [1,b).

Let n ≥ 0. We define the Goodstein sequence starting at n as follows.

Firstly, write n completely in base 2.
Next raise the base to 3, evaluate the number, and subtract 1.
Secondly, write this completely in base 3.
Next raise the base to 4, evaluate the number, and subtract 1.
Thirdly, write this completely in base 4.
...

This process is terminated once 0 is reached. E.g., the Goodstein sequence starting at 0 is of length 1.

THEOREM 0.8B.1. Goodstein's Theorem. The Goodstein sequence starting at any n ≥ 0 eventually terminates.

This was proved in [Goo44]. The idea is that if we change the base to the infinite ordinal ω in all of the complete representations that occur starting at n, then the ordinals so represented form a strictly decreasing sequence. Hence we must have termination.

Let G(n) be the length of the Goodstein sequence starting at n.

THEOREM 0.8B.2. Goodstein's Theorem can be proved in ACA' but not in PA. It is provably equivalent to 1-Con(PA) over EFA. The function G is ϵ_0 recursive but eventually dominates every $<\epsilon_0$ recursive function.

This was proved in [KP82]. Also see [Ci83] and [BW87].

0.8C. Relatively Large Ramsey Theorem.

Here is the original infinite Ramsey theorem.

THEOREM 0.8C.1. Infinite Ramsey Theorem. In any coloring of the unordered k tuples from the positive integers using p colors, there is an infinite set of positive integers whose unordered k tuples have the same color.

This is proved in [Ra30], and applied there to a fundamental decision problem in predicate calculus.

A set of positive integers is said to be relatively large if and only if its cardinality is at least its minimum element.

THEOREM 0.8C.2. Infinite Relatively Large Ramsey Theorem. In any coloring of the unordered k tuples from any infinite set of positive integers using p colors, there is a relatively large finite set of positive integers with at least r elements whose unordered k tuples have the same color.

Proof: This is an immediate consequence of the Infinite Ramsey Theorem, as observed in [PH77]. QED

THEOREM 0.8C.3. Relatively Large Ramsey Theorem. For all k,p,r there exists n so large that the following holds. In any coloring of the unordered k tuples from {1,...,n} using p colors, there is a relatively large subset of {1,...,n} with at least r elements whose unordered k tuples have the same color.

Proof: This is proved in [PH77] from Theorem 0.8C.2, using a finitely branching infinite tree argument. QED

This should be compared with the Finite Ramsey Theorem 1 of section 0.5.

Let PH(k,p,r) be the least n in Theorem 0.8C.3.

THEOREM 0.8C.4. The Relatively Large Ramsey Theorem can be proved in ACA' but not in PA. It is provably equivalent to 1-Con(PA) over EFA. The function PH is ϵ_0 recursive, but the unary function PH(k,k,k) eventually dominates every $<\epsilon_0$ recursive function.

Proof: See [PH77]. QED

Theorem 0.8C.4 has been proved even if we fix p = 2 (i.e., for 2 colors). See [LN92], p. 824.

0.8D. Regressive Ramsey Theorem.

The Regressive Ramsey Theorem and its independence from PA can be gleaned from [PH77], as it was used as a kind of unadvertised intermediate step. The statement is also essentially present in [Sc74], but without any discussion or results, except to note that it follows from the usual infinite Ramsey theorem. However, The Regressive Ramsey Theorem was first focused on and perfected in [KM87].

Let N be the set of all nonnegative integers. We write $[A]^k$ for the set of all unordered k element subsets of A ⊆ N. Also, write $[n]^k$ for the set of all unordered k element subsets of {0,...,n-1}.

We say that $f:[N]^k \to N$ is regressive if and only if for all $x \in [N]^k$, if min(x) > 0 then f(x) < min(x).

We say that f is min homogenous on A ⊆ N if and only if for all $x,y \in [A]^k$, min(x) = min(y) → f(x) = f(y).

THEOREM 0.8D.1. Infinite Regressive Ramsey Theorem. Any regressive $f:[N]^k \to N$ is min homogenous on some infinite A ⊆ N.

It is well known that RCA_0 proves the equivalence of the Infinite Ramsey Theorem and the Infinite Regressive Ramsey Theorem. They are both equivalent, over RCA_0, to ACA'. See Definition 1.4.1.

THEOREM 0.8D.2. Finite Regressive Ramsey Theorem. For all k,r there exists n so large that the following holds. Every regressive $f:[n]^k \to [n]$ is min homogenous on some r element A ⊆ [n].

This is obtained from the Infinite version by a finitely branching infinite tree argument, in [KM87]. Also, in [KM87], the equivalence of Theorems 0.8C.3 and 0.8D.2 is established. Thus we have the following result from [KM87].

Let KM(k,r) be the least n in Theorem 0.8D.2.

THEOREM 0.8D.3. The Finite Regressive Ramsey Theorem can be proved in ACA' but not in PA. It is provably equivalent to 1-Con(PA) over EFA. The function KM is ϵ_0 recursive, but KM(k,k) eventually dominates every $<\epsilon_0$ recursive function.

0.8E. Hercules Hydra Game and Worms.

In [KP82], Goodstein's Theorem (Theorem 0.8B.1) is analyzed, and also the closely related Hercules Hydra games are introduced and analyzed.

Let T be a hydra, which is simply a finite rooted tree. We draw trees with the root at the bottom, and v < v' means that v is a parent of v' (equivalently, v' is a child of v).

Hercules goes to battle with $T_1 = T$. Hercules first removes a leaf, and the hydra reacts by growing new vertices in the manner below, creating T_2. Then Hercules removes a leaf from T_2, and the hydra grows new vertices as below, thus creating T_3. This continues as long as the tree has at least two vertices.

Suppose Hercules removes the leaf, x, from T_n, creating the temporary tree T_n'. Since we are assuming that T_n has at least two vertices, let y be the parent of x. If y is the root of T_n', then set $T_{n+1} = T_n'$. Otherwise, let z be the parent of y. Let $T_n'|\geq y$ be the subtree of T' with root y. The hydra grafts n copies of $T_n'|\geq y$ on top of z, so that the roots of these copies become children of z. This results in the tree T_{n+1}.

By assigning ordinals to trees, [KP82] proves the following.

THEOREM 0.8E.1. Every strategy for Hercules in the Hercules hydra game is a winning strategy. I.e., the hydra is eventually cut down to a single vertex.

[KP82] also proves the following.

THEOREM 0.8E.2. Theorem 0.8E.1 can be proved in ACA' but not in PA. It is provably equivalent to 1-Con(PA) over EFA.

In [Bek06], a Worm Principle is introduced and investigated. It is a flattened and deterministic version of the Hercules Hydra game, and metamathematcal properties corresponding to those of the Hercules Hydra game are established.

0.8F. Regressive Counting Theorems.

Our Counting Theorems appear in section 1 of [Fr98].

THEOREM 0.8F.1. Let k,r,p > 0 and $F:N^k \to N^r$ obey the inequality $\max(F(x)) \le \min(x)$. There exists $E \subseteq N$, $|E| = p$, such that $|F[E^k]| \le (k^k)p$.

We now turn this around so that it asserts a combinatorial property of any function $F:N^k \to N^r$.

Let $A,B \subseteq N^k$, and $F: A \to N^r$. We say that y is a regressive value of F on B if and only if there exists $x \in B$ such that $F(x) = y$ and $\max(y) < \min(x)$.

THEOREM 0.8F.2. Let k,r,p > 0 and $F:N^k \to N^r$. F has $\le (k^k)p$ regressive values on some $E^k \subseteq N^k$, $|E| = p$.

We now state the obvious finite forms of Theorems 0.8F.1 and 0.8F.2.

THEOREM 0.8F.3. For all k,r,p > 0 there exists n so large that the following holds. Let $F:\{0,...,n-1\}^k \to \{0,...,n-1\}^r$ obey the inequality $\max(F(x)) \le \min(x)$. There exists $E \subseteq \{0,...,n-1\}$, $|E| = p$, such that $|F[E^k]| \le (k^k)p$.

THEOREM 0.8F.4. For all k,r,p > 0 there exists n so large that the following holds. Let $F:\{0,...,n-1\}^k \to \{0,...,n-1\}^r$. F has $\le (k^k)p$ regressive values on some $E^k \subseteq \{0,...,n-1\}^k$, $|E| = p$.

In [Fr98], equivalences are established between these Theorems and the Regressive Ramsey Theorems. We obtain the following.

THEOREM 0.8F.5. Theorems 0.8F.1 and 0.8F.2 are provable in ACA' but not in ACA_0. They are provably equivalent to "ϵ_0 is well ordered" over RCA_0. These results hold even if we fix r = 2 and merely state the existence of constants c_k depending only on k.

THEOREM 0.8F.6. Theorems 0.7.3 and 0.7.4 are provable in ACA' but not in PA. They are provably equivalent to 1-Con(PA) over PRA. These results hold even if we fix r = 2 and merely state the existence of constants c_k depending only on k.

0.8G. The Shift Inequality.

Recall that Adjacent Ramsey Theory studies the shift equation

$$F(x_1,\ldots,x_k) = F(x_2,\ldots,x_{k+1})$$

over N. See the Adjacent Ramsey Theorem (Theorem 0.5.6). We saw that Adjacent Ramsey Theory corresponds to EFA in the same way that Finite Ramsey Theory does.

We have intensively studied the inequality

$$F(x_1,\ldots,x_k) \leq F(x_2,\ldots,x_{k+1})$$

over the nonnegative integers, N. This is far more exotic than the Adjacent Ramsey Theory, in that it corresponds, not to EFA, but to PA.

These results are from [Fr08], [Fr10a].

For $x,y \in N^k$, we write $x \leq_c y$ if and only if for all $1 \leq i \leq k$, $x_i \leq y_i$.

THEOREM 0.8G.1. For all $k \geq 1$ and $f:N^k \to N^2$, there exist distinct $x_1,\ldots,x_{k+1}$ such that $f(x_1,\ldots,x_k) \leq_c f(x_2,\ldots,x_{k+1})$.

THEOREM 0.8G.2. For all $k \geq 1$ and $f:N^k \to N$, there exist distinct $x_1,\ldots,x_{k+3}$ such that $f(x_1,\ldots,x_k) \leq f(x_2,\ldots,x_{k+1}) \leq f(x_3,\ldots,x_{k+2})$.

THEOREM 0.8G.3. For all $k \geq 1$ and $f:N^k \to N$, there exist distinct $x_1,\ldots,x_{k+1}$ such that $f(x_2,\ldots,x_{k+1})-f(x_1,\ldots,x_k) \in 2N$.

THEOREM 0.8G.4. For all $k,r \geq 1$ and $f:N^k \to N^r$, there exist distinct $x_1,\ldots,x_{k+1}$ such that $f(x_1,\ldots,x_k) \leq_c f(x_2,\ldots,x_{k+1})$.

THEOREM 0.8G.5. For all $k,r,t \geq 1$ and $f:N^k \to N^r$, there exist distinct $x_1,\ldots,x_{k+t-1}$ such that $f(x_1,\ldots,x_k) \leq_c \ldots \leq_c f(x_t,\ldots,x_{t+k-1})$.

THEOREM 0.8G.6. For all $k,r,t \geq 1$ and $f:N^k \to N^r$, there exist distinct $x_1,\ldots,x_{k+1}$ such that $f(x_2,\ldots,x_{k+1})-f(x_1,\ldots,x_k) \in tN^r$.

THEOREM 0.8G.7. Theorems 0.8G.1 - 0.8G.6 are provable in ACA' but not in ACA_0. They are provably equivalent to "$\in_0$ is well ordered" over RCA_0.

We can weaken these Theorems by restricting to complexity classes. These restrictions are obviously arithmetic sentences.

THEOREM 0.8G.8. Theorems 0.8G.1 - 0.8G.6 hold for recursive f. These are explicitly Π^0_3 sentences.

THEOREM 0.8G.9. Theorems 0.8G.1 - 0.8G.6 hold for primitive recursive (elementary recursive, polynomial time in base 2 representations) f. These are explicitly Π^0_2 sentences.

For $p \geq 0$, we define p-Con(T) to be the sentence "every Σ^0_p sentence provable in T is true".

THEOREM 0.8G.10. Theorem 0.8G.8 (all forms) is provably equivalent to 2-Con(PA) over EFA. Theorem 0.8G.9 (all forms) is provably equivalent to 1-Con(PA) over EFA.

We say that $f:N^k \rightarrow N^r$ is limited if and only if for all $x \in N^k$, $\max(f(x)) \leq \max(x)$.

THEOREM 0.8G.11. Theorems 0.8G.1 - 0.8G.6 hold for limited functions.

THEOREM 0.8G.12. Theorem 0.8G.9 (all forms) is provably equivalent to 1-Con(PA) over RCA_0.

THEOREM 0.8G.13. Theorems 0.8G.1 - 0.8G.6 hold for limited functions defined on some $[0,n]^k$, n depending on the given numerical parameters.

Note that Theorem 0.8G.13 (all forms) is explicitly Π^0_2.

THEOREM 0.8G.14. Theorem 0.8G.13 (all forms) is provably equivalent to 1-Con(PA) over EFA. The associated witness function (all forms) is $\in_0$ recursive but eventually dominates all $<\in_0$ recursive functions.

We have applied the shift inequality to polynomials with integer coefficients, and to the tangent function.

Let $n_1,...,n_k \in Z$. The translates of $(n_1,...,n_k)$ in coordinate $1 \le i \le k$ are the vectors obtained by adding an integer to the i-th coordinate.

THEOREM 0.8G.15. The Polynomial Shift Translation Theorem. For all polynomials $P:Z^k \to Z^k$, there exist distinct positive integers $n_1,...,n_{k+1}$ such that, in each coordinate, the number of translates of $(n_1,...,n_k)$ which are values of P is at most the number of translates of $(n_2,...,n_{k+1})$ which are values of P.

THEOREM 0.8G.16. Theorem 0.8G.15 is provable in ACA' but not in Peano Arithmetic. It implies 2-Con(PA) over EFA.

A *block* is a subsequence that does not skip over terms. A k-block is a block of length k.

Tangent here means the trigonometric tan function. We exploit the periodic and surjective properties of tan. There have been earlier results of ours and others concerning sine. See [Bo07].

THEOREM 0.8G.17. Let $k \ge 1$. Every infinite sequence of integers contains an infinite subsequence, where the tangents of the products of its k-blocks lie within 1 of each other, or go to $+-\infty$.

We make Theorem 0.8G.17 successively more concrete as follows.

THEOREM 0.8G.18. Let $k,n \ge 1$. Every infinite sequence of integers contains a subsequence of length n, where the tangents of the products of its k-blocks lie within 1 of each other, or are strictly increasing and positive, or are strictly decreasing and negative.

THEOREM 0.8G.19. Let $k \ge 1$. Every infinite sequence of integers contains a subsequence of length k+2, where the tangents of the products of its k-blocks lie within 1 of each other, or are strictly increasing and positive, or are strictly decreasing and negative.

THEOREM 0.8G.20. For $k \ge 1$ there exists n such that the following holds. Every finite sequence of integers of length n obeying $|x[i]| \le i$, $i \ge 1$, contains a subsequence of length k+2, where the tangents of the products of its k-blocks lie within 1 of each other, or are strictly increasing and positive, or are strictly decreasing and negative.

THEOREM 0.8G.21. Theorems 0.8G.17 - 0.8G.20 are provable in ACA' but not in ACA_0. Theorems 0.8G.17 - 0.8G.19 are provably equivalent to "ϵ_0 is well ordered" over RCA_0. Theorem 0.8G.20 is provably equivalent to 1-Con(PA) over EFA. The witness function associated with Theorem 0.8G.20 is ϵ_0 recursive but grows faster than all $<\epsilon_0$ recursive functions.

0.8H. Tree Embedding Theorems.

We will postpone a full discussion of Kruskal's Tree Theorem until section 0.9B. We refer the reader to section 0.9B for definitions not given here.

We will consider three immediate consequences of Kruskal's Theorem here. We know that these are equivalent. Various natural variants can also be seen to be equivalent.

EBTE. Exactly Binary Tree Embedding Theorem.
TE. Tree Embedding Theorem.
STE. Structured Tree Embedding Theorem.

These are presented below. STE $\rightarrow$ TE $\rightarrow$ EBTE is immediate.

Kruskal's Theorem involves inf preserving embeddings. Here we will use only embeddings. Here is the reason behind this.

THEOREM 0.8H.1. The following is provable in EFA. If there is an embedding from a finite binary tree S into a finite binary tree T, then there is an inf preserving embedding from S into T. If there is a structure preserving embedding from a finite structured binary tree S into a finite structured binary tree T, then there is a structure and inf preserving embedding from S into T.

Proof: This is well known. Use induction on the sum of the number of vertices in S and T. QED

An exactly binary tree is a tree all of whose vertices have valence 0 or 2.

In reading the next theorem (and later), note that according to the definitions in section 0.9, embeddings between finite structured trees are required to preserve structure. However, inf preservation must be explicitly stated.

THEOREM 0.8H.2. i. Exactly Binary Tree Embedding Theorem (EBTE). In any infinite sequence of exactly binary trees, some tree is embeddable into a later tree.
ii. Tree Embedding Theorem (TE). In any infinite sequence of finite trees, some tree is embeddable into a later tree.
iii. Structured Tree Embedding Theorem (STE). In any infinite sequence of finite structured trees, some tree is embeddable into a later tree.

Proof: These are very special cases of Kruskal's Theorem [Kr60]. EBTE is also a very special case of Higman's Wqo Theorem from [Hig52]. QED

THEOREM 0.8H.3. The following are provably equivalent in RCA_0.
i. EBTE.
ii. TE.
iii. STE.
iv. ϵ_0 is well ordered.
i-iv are provable in ACA' but not in ACA_0.

Proof: i → iv is due to [VV05] and A. Weiermann (advisor), and will appear in [FWa], together with a different proof of ours. These proofs yield very effective ordinal assignments f to binary trees onto ϵ_0, where if S is embeddable into T then $f(S) \leq f(T)$.

That iv) implies structured EBTE is in [Fr84]. Specifically, In [Fr84], calculations are made of the ordinals of the trees of bad sequences for various restricted forms of Kruskal's Theorem, including structured EBTE. In general, these calculations used a theory of ordinals - i.e., ATR_0. However, in this case, the proof shows that for each starting exactly binary structured tree, ACA_0 proves that there are no infinite bad sequences extending it. Hence structured EBTE can be proved using Π^1_1 reflection on ACA_0. Now apply Theorem 0.8A.1.

We have recently proved that structured EBTE implies STE as follows. We inductively define a very effective map h from finite structured trees into finite exactly binary structured trees, so that if h(S) is structure preserving embeddable into h(T) then S is structure preserving embeddable into T. This will appear in [FWa]. This establishes that structured EBTE implies STE.

By combining the last two paragraphs, we have iv → iii. Note that iii → ii → i is trivial. QED

The following two Theorems are immediate consequences of EBTE, TE, STE, respectively.

THEOREM 0.8H.4. Subrecursive EBTE, TE, STE. In any infinite primitive recursive (elementary recursive, polynomial time computable) sequence of finite exactly binary trees (trees, structured trees), one tree is embeddable in a later tree.

THEOREM 0.8H.5. Recursive EBTE, TE, STE. In any infinite recursive sequence of finite exactly binary trees (trees, structured trees), one tree is embeddable in a later tree.

THEOREM 0.8H.6. Finite EBTE, TE, STE. For all $c \geq 0$ there exists n such that the following holds. Let $T_1,...,T_n$ be exactly binary trees (trees, structured trees), where each T_i has at most $i+c$ vertices. There exist $i < j$ such that T_i is embeddable in T_j.

Proof: The argument is in [Fr81a]. Also see [Si85]. Let $c \geq 0$ be given and assume this is false. Build a finitely branching tree of counterexamples. By STE, the tree has no infinite paths, and therefore is finite. QED

The following Theorem provides the required link between these effective and finite forms of EBTE, TE, STE, and proof theory.

THEOREM 0.8H.7. The following are provably equivalent in EFA.
i. Every primitive recursive sequence from ϵ_0 stops descending.
ii. Every elementary recursive sequence from ϵ_0 stops descending.
iii. Every polynomial time computable sequence from ϵ_0 stops descending.
iv. 1-Con(PA).

Proof: This is well known from standard proof theory - except for iii. Here we follow the usual practice in computational complexity theory, where the base 2 representation is used for nonnegative integers - not only for representing the indexation of the infinite sequences, but also for the coefficients in notations below ϵ_0. It is straightforward to check that the required manipulations can be done in polynomial time. QED

An interesting question is how small a subclass of poly time can be used for iii above. At very low computational levels, we expect that some interesting detailed issues should naturally arise.

THEOREM 0.8H.8. The following are provably equivalent in EFA.
i. Every recursive sequence from ϵ_0 stops descending.
ii. 2-Con(PA).

Proof: Assume ii. Fix k ≥ 1. Let M be a TM set up to compute a partial recursive function from N into $\omega^{[k]}$. Obviously PA proves

if M computes a total recursive function from N into $\omega^{[k]}$, then that function is not everywhere descending.

The above sentence is obviously $\Sigma^0{}_2$. Hence we have

for all k ≥ 1, if M is a TM set up to compute a partial recursive function from N into $\omega^{[k]}$, and if M computes a total recursive function from N into $\omega^{[k]}$, then that function is not everywhere descending.

for all k ≥ 1, every recursive function from N into $\omega^{[k]}$ stops descending.

every recursive function from N into ϵ_0 stops descending.

This establishes ii → i.

For i → ii, we argue in EFA. Assume i. In particular, every polynomial time computable computable sequence from ϵ_0 stops descending. Hence by Theorem 0.8H.7, we have 1-Con(PA). Therefore we have access to all of the < ϵ_0 recursive functions.

We now use the standard Schütte infinitary proof theory for PA. See [Sch77] and [Bu91].

We start with a proof in PA of a $\Sigma^0{}_2$ sentence. We use primitive recursive function symbols, and so the $\Sigma^0{}_2$ sentence φ takes the form $(\exists n)(\forall m)(F(n,m) = 0)$.

By effective infinitary cut elimination, we obtain an infinitary cut free proof, tagged with ordinals < ϵ_0, that is < ϵ_0 recursive. We now examine this infinitary proof.

We go up the proof tree (backwards in the proof), starting at the root, through vertices of valence 1 only. By 1-Con(PA), we see that this process must stop. It is clear that it must stop at a vertex of valence > 1. This must be a vertex which is the result of ∀ introduction. But then we must have introduced F(t(n),0) = 0, F(t(n),1) = 0, and so on. Here t(n) is a term which may or may not mention the variable n. By 1-Con(PA), these equations can only be introduced here if they are true. Hence we obtain (∀m)(F(t(n),m) = 0). Therefore (∃n)(∀m)(F(n,m) = 0). QED

THEOREM 0.8H.9. The following are provably equivalent in EFA.
i. Subrecursive EBTE.
ii. Subrecursive TE.
iii. Subrecursive STE.
iv. 1-Con(PA).

Proof: Assume i. Using the very effective surjective assignment of ordinals < ϵ_0 to exactly binary trees referred to in the proof of Theorem 0.8H.3, we obtain i in Theorem 0.8H.7. Hence 1-Con(PA).

Assume 1-Con(PA). Fix a primitive recursive sequence f of finite exactly binary structured trees. Let T be the first tree in the sequence. The proof from [Fr84] discussed in the proof of Theorem 0.8H.3, shows how to prove in PA that for some i < j, f(i) ≤ f(j). Hence i holds, for exactly binary structured trees.

We then have iii by applying the very effective map from finite structured trees to finite exactly binary structured trees, referred to in the proof of Theorem 0.8H.3.

Thus we have shown i → iv → iii. Obviously iii → ii → i. QED

THEOREM 0.8H.10. The following are provably equivalent in EFA.
i. Recursive EBTE.
ii. Recursive TE.
iii. Recursive STE.
iv. 2-Con(PA).

Proof: Assume i. Using the very effective surjective assignment of ordinals < ϵ_0 to exactly binary trees referred to in the proof of Theorem 0.8H.3, we obtain i) in Theorem 0.8H.8. Hence 2-Con(PA).

Assume 2-Con(PA). We argue similarly to the proof of ii → i in Theorem 0.8H.8. Fix a finite exactly binary structured tree T. Let TM be set up to compute a partial recursive function from N into finite exact binary trees. From [Fr84], as discussed in the proof of Theorem 0.8H.3, PA proves

if TM computes a total recursive function f from N into finite exactly binary trees, starting with T, then there exist i < j such that f(i) ≤ f(j).

The above sentence is obviously Σ^0_2. Hence we have

for all finite exactly binary structured T, if a TM is set up to compute a partial recursive function from N into finite exactly binary structured trees, starting with T, and if that TM computes a total recursive function from N into finite exactly binary structured trees, then there exist i < j such that f(i) ≤ f(j).

for all finite exactly binary structured trees T, for every recursive function f from N into finite exactly binary structured trees, starting with T, there exist i < j such that f(i) ≤ f(j).

for all recursive functions f from N into finite exactly binary structured trees, there exist i < j such that f(i) ≤ f(j).

This establishes iv → i for exactly binary structured trees.

We then have iii by applying the very effective map from finite structured trees to finite exactly binary structured trees, referred to in the proof of Theorem 0.8H.3.

Thus we have shown i → iv → iii. Obviously iii → ii → i. QED

THEOREM 0.8H.11. The following are provably equivalent in EFA.
i. Finite EBTE.
ii. Finite TE.

iii. Finite STE.
iv. 1-Con(PA).

Proof: Assume i. Using the very effective surjective assignment of ordinals < ϵ_0 referred to in the proof of Theorem 0.8H.3, we obtain the "slow well foundedness of ϵ_0" or CWF = "combinatorial well foundedness of ϵ_0", in the sense of [Fr81a] and [Fr01c], p. 71. This is bootstrapped up (as in [Fr81a] and [Fr01c]) to obtain the elementary recursive or even primitive recursive well foundedness of ϵ_0. By the proof theory of PA, 1-Con(PA) follows.

Assume 1-Con(PA). Fix c ≥ 0. We can obtain a proof in PA of i for finite exactly binary structured trees, for this fixed c, very effectively in c, as follows. Assume that i for this fixed c is false, using structured binary trees. Now form the tree T of appropriately bad sequences, and hypothesize in PA that T is infinite. Then there is an arithmetically defined infinite bad sequence. Now there are only finitely many first terms that this infinite bad sequence can have. For each of these terms, we argue from [Fr84] as in the proof of Theorem 0.8H.3, to obtain a contradiction. Therefore T is finite.

Since the statement of i with structure, for fixed c is Σ^0_1, we see that the statement must be true for any c, by 1-Con(PA). This establishes iv → i for exactly binary structured trees. We can obviously use, say, a double exponential growth rate in the formulation of i for exactly binary structured trees, and the same argument will apply. I.e., we will obtain that also from 1-Con(PA). But this modification of i for exactly binary structured trees obviously implies iii using the very effective map from finite structured trees into finite exactly binary structured trees, referred to in the proof of Theorem 0.8H.3. This establishes iv → iii. Note that iii → ii → i is immediate. QED

In section 0.10, my Extended Kruskal Theorem is discussed, in which we impose a gap condition on the inf preserving embeddings. It is provable in Π^1_1-CA but not in Π^1_1-CA$_0$ (see Theorems 0.10A.4 and 0.10A.5).

In [SS85], the Extended Kruskal Theorem is specialized to valence 1, which is just for finite sequences. The resulting statement is much weaker, and is shown to correspond to ϵ_0.

In [Gor89], the Extended Kruskal Theorem for valence 1 is generalized allowing ordinal labels (with a suitable natural weakening of the gap condition), still at valence 1. The logical strength for α corresponds roughly to the Turing jump hierarchy on α.

0.9. Incompleteness in Predicative Analysis and ATR_0.

0.9A. Predicative analysis, Γ_0, and ATR_0.

The philosophy of mathematics known as predicativity focuses on the legitimacy of forming a subset of N via the construction {n: φ(n)}.

H. Poincaré, in [Po06], argued that this is not legitimate if the condition φ refers to all subsets of N. He argued that φ must only refer to subsets of N that have already been constructed, thus implicitly introducing a notion of abstract time. Note that this criterion is easily met if φ is arithmetical, even if it has parameters for subsets of N. Poincare referred to this as the Vicious Circle Principle.

His ideas were taken up by Weyl, in [Wey18,87], and others. Russell articulated the basic idea earlier than Poincaré, but in the context of the paradoxes. Russell in effect abandoned the Vicious Circle Principle through his adoption of his highly impredicative Theory of Types, [Ru08,67].

S. Feferman and K. Schütte, independently sought to analyze predicative analysis formally. The initial analyses appeared in [Fe64] and [Sch65]. Subsequently, Feferman refined his analysis in many papers, culminating with [Fe05].

What is constant throughout all of these formal analyses is that

i. The provably recursive functions of predicative analysis consists of the < Γ_0 recursive functions.

ii. The finite sequence trees, presented arithmetically, that are provably well founded within predicative analysis, have ordinals up to, but not including, Γ_0.

iii. The subsets of N present in the first Γ_0 levels of the hyperarithmetical hierarchy form (the subset of N part of) a model of predicative analysis.

For a general treatment of $<\lambda$ recursive functions via descent recursion, see [FSh95]).

These analyses have been generally accepted as reasonably representing predicative analysis according to its historical informal descriptions. The degree of acceptance is not nearly as great as it is for Turing's analysis of algorithms. It is an open question whether it is possible to attain such a high level of acceptance. Nevertheless, there is no competing analysis of predicative analysis with anything like the same level of acceptance.

This usual analysis of predicativity takes the form of what amounts to the formal system $ATR(<\Gamma_0)$ of arithmetic, based on ACA_0 and arithmetic transfinite recursion up to any ordinal (notation) $< \Gamma_0$. Its minimum ω model consists of the hyperarithmetic sets of level $< \Gamma_0$.

Competing analyses of predicativity generally differ only in the choice of ordinal, but do take the form of a system $ATR(<\lambda)$, for some effectively given ordinal λ.

Recall our system ATR_0, which plays a prominent role in Reverse Mathematics. We proved a striking matchup between ATR_0 and the standard formalization of predicative analysis.

THEOREM 0.9A.1. ATR_0 is a conservative extension of $ATR(<\Gamma_0)$ for Π^1_1 sentences. The provably recursive functions of ATR_0 and $ATR(<\Gamma_0)$ are the $<\Gamma_0$ recursive functions. The following are provably equivalent in RCA_0.
i. Π^1_1 reflection on ATR_0.
ii. Γ_0 is well ordered.
These are provable in ATR but not in ATR_0. For ATR, use Γ_{ϵ_0}. throughout instead of Γ_0. The first claim is provable in SEFA.

Proof: For these results of ours about ATR_0, see our announcement [Fr76], our proof in [FMS82], section 4, and [Si02]. For ATR, see [Ja80]. QED

Let (N,R) be a primitive recursively given well ordering of N. The system ATI(<R) is in L(PA), and extends PA by the

scheme of arithmetic transfinite induction on any proper initial segment of R determined by any given point.

Below, ATI($<\Gamma_0$) refers to ATI(<R), where R is a standard notation system for Γ_0. All such standard R lead to equivalent systems ATI(<R).

THEROEM 0.9A.2. ATR_0 is a conservative extension of ATI($<\Gamma_0$). The following are provably equivalent in SEFA.
i. 1-Con(ATR_0).
ii. 1-Con(ATR($<\Gamma_0$).
iii. 1-Con(ATI($<\Gamma_0$)).
iv. Every primitive recursive (elementary recursive, polynomial time computable) sequence from Γ_0 stops descending.
These are provable in ATR but not in ATR_0. For ATR, use $\Gamma_{\in\_0}$. throughout instead of Γ_0.

Proof: For these results of ours about ATR_0, see [FMS82], section 4, and [Si02]. For ATR, see [Ja80]. QED

However, ATR_0 cannot be considered part of predicative analysis because of the following.

THEOREM 0.9A.3. Every ω-model of ATR_0 properly includes all hyperarithmetic subsets of N.

Proof: See [Si99,09], p. 346, notes for section VIII.4. QED

Theorem 0.9A.3 is especially powerful for establishing that a Π^1_2 sentence cannot be proved predicatively. By showing that the Π^1_2 sentence implies ATR_0 over RCA_0 (or even ACA_0), it is clear that the Π^1_2 sentence cannot hold in any subset of the hyperarithmetic sets, and therefore cannot be proved in any system ATR($<\lambda$), where λ is effectively given.

Let TI be the subsystem of second order arithmetic consisting of ACA_0 plus the scheme of transfinite induction on all countable well orderings. Often this is referred to as BI = bar induction, but we prefer to call this TI = transfinite induction.

For n ≥ 1, we define Π^1_n-TI_0 and Σ^1_n-TI_0 as ACA_0 together with transfinite induction on all countable well orderings, with respect to Π^1_n and Σ^1_n formulas, respectively. Here Π^1_n (Σ^1_n) formulas start with a universal (existential) set quantifier, followed by at most n-1 set quantifiers, followed by an arithmetical formula. If we use ACA instead

of ACA_0 (which is ACA_0 with full induction), then we write Π^1_n-TI and Σ^1_n-TI.
Also, ATR is ATR_0 with full induction.

THEOREM 0.9A.4. ATR and Σ^1_1-TI are equivalent. ATR_0 and Σ^1_1-TI have the same ω-models. ATR_0 + Σ^1_1 induction and Σ^1_1-TI_0 are equivalent.

Proof: See [Si82]. QED

The next two theorems are proved in [RW93]. Here $<\theta\Omega^\omega$ refers to a standard notation system for the proof theoretic ordinal $\theta\Omega^\omega$, as defined in [RW93].

THEOREM 0.9A.5. Π^1_2-TI_0 is a conservative extension of ATR($<\theta\Omega^\omega$) for Π^1_1 sentences. The provably recursive functions of Π^1_2-TI_0 and ATR($<\theta\Omega^\omega$) are the $<\theta\Omega^\omega$ recursive functions. The following are provably equivalent in RCA_0.
i. Π^1_1 reflection on Π^1_2-TI_0.
ii. $\theta\Omega^\omega$ is well ordered.
These are provable in Π^1_2-TI but not in Π^1_2-TI_0.

THEROEM 0.9A.6. Π^1_2-TI_0 is a conservative extension of ATI($<\theta\Omega^\omega$). The following are provably equivalent in SEFA.
i. 1-Con(Π^1_2-TI_0).
ii. 1-Con(ATR($<\theta\Omega^\omega$)).
iii. 1-Con(ATI($<\theta\Omega^\omega$)).
iv. Every primitive recursive (elementary recursive, polynomial time computable) sequence from $\theta\Omega^\omega$ stops descending.
These are provable in Π^1_2-TI but not in Π^1_2-TI_0.

0.9B. Kruskal's Theorem.

A poset is a pair $(D,\leq)$ where D is a nonempty set and $\leq$ is a reflexive transitive relation obeying

$$(x \leq y \wedge y \leq x) \rightarrow x = y.$$

A tree is a poset $T = (V,\leq)$ where there is a minimum element called the root, and where for each $x \in V$, $\{y: y \leq x\}$ is linearly ordered by $\leq$.

The elements of $V = V(T)$ are called the vertices of T. A tree is said to be finite if it has finitely many vertices.

If $x < y$ then we call x a predecessor of y and y a successor of x.

If $x < y$ and there is no z such that $x < z < y$ then we call y an immediate successor of x and y the immediate predecessor of y.

We say that x,y are comparable if and only if $x = y \vee x < y \vee y < x$. Otherwise, we say that x,y are incomparable.

For finite trees, we have the crucial inf operation on V, where x inf y is the greatest z such that $z \leq x \wedge z \leq y$.

The valence of a vertex is the number of its immediate successors. The valence of a tree is the maximum of the valences of its vertices (for finite trees).

The vertices of valence 0 are called the terminal vertices. The remaining vertices are called the internal vertices.

For definiteness, we will require that the domain of any finite tree is $\{1,...,n\}$, where n is the number of its vertices. Thus the set of all finite trees exists. Note that many pairs of distinct finite trees are isomorphic.

We will also consider what we call structured trees. These are finite trees with a left/right structure. I.e., where for any vertex i, there is a strict linear ordering (left/right) of the immediate successors of i. This induces the following relation on vertices: x is to the left of y if and only if x,y are incomparable and the immediate successor of x inf y comparable with x is to the left of the immediate successor of x inf y comparable with y. This relation is irreflexive and transitive.

A quasi order is a pair $(D,\leq)$ where D is a nonempty set and $\leq$ is a reflexive and transitive relation on D.

A well quasi order (wqo) is a quasi order $(D,\leq)$, where for any $x_1,x_2,...$ from D, there exists $i < j$ such that $x_i \leq x_j$.

Let $(D,\leq)$ be a quasi order. A $(D,\leq)$ labeled (structured) tree is a (structured) tree with a labeling function from its vertices into D. We write $l(x)$ for the label of x. Although we consider only finite $(D,\leq)$ labeled (structured) trees, the D itself may be infinite.

We introduce the following notation for certain important tree classes. Here Q is a quasi order.

TR(n). The finite trees of valence ≤ n.
TR(<∞). The finite trees.
TR(n;Q). The finite Q labeled trees of valence ≤ n.
TR(<∞;Q). The finite Q labeled trees.
STR(n). The finite structured trees of valence ≤ n.
STR(<∞). The finite structured trees.
STR(n;Q). The finite Q labeled structured trees of valence ≤ n.
STR(<∞;Q). The finite Q labeled trees.

If we write an integer r ≥ 2 instead of Q, then we mean the quasi order Q = {1,...,r} under =. If we write ω instead of Q, then we mean the quasi order of ω under ≤ (which is the usual linear ordering).

All of these tree classes come with their own notion of embedding.

TR(n), TR(<∞). We say that h is an embedding from S into T if and only if h:V(S) → V(T), where for all x,y ∈ V(S), $x \leq_S y \leftrightarrow hx \leq_T hy$.

STR(n), STR(<∞). We say that h is an embedding from S into T if and only if h:V(S) → V(T), where for all x,y ∈ V(S)
i. $x \leq_S y \leftrightarrow hx \leq_T hy$.
ii. x is to the left of y in S if and only if hx is to the left of hy in T.

TR(n;Q), TR(<∞;Q). We say that h is an embedding from S into T if and only if h:V(S) → V(T), where for all x,y ∈ V(S),
i. $x \leq_S y \leftrightarrow hx \leq_T hy$.
iii. $l(x) \leq_Q l(hx)$.

STR(n;Q), STR(<∞;Q). We say that h is an embedding from S into T if and only if h:V(S) → V(T), where for all x,y ∈ V(S),
i. $x \leq_S y \leftrightarrow hx \leq_T hy$.
ii. x is to the left of y in S if and only if hx is to the left of hy in T.
iii. $l(x) \leq_Q l(hx)$.

Additional conditions are often placed on embeddings.

Inf Preservation. h:V(S) → V(T) is said to be inf preserving if and only if for all x,y ∈ V(S), h(x inf y) = hx inf hy.

Valence Preservation. $h:V(S) \to V(T)$ is said to be valence preserving if and only if for all x in V(S), the valence of x is the same as the valence of hx.

In this section, we will always use inf preservation.

THEOREM 0.9B.1. Kruskal's Tree Theorem. If Q is a wqo then STR(<∞;Q) is a wqo under inf preserving embeddability.

Proof: This was proved in [Kr60]. The simplest proof is in [NW65]. The proof is not any easier for TR(<∞,Q). QED

THEOREM 0.9B.2. Higman's Wqo Theorem. If Q is a wqo then STR(n;Q) is a wqo under inf and valence preserving embeddability.

Proof: See [Hig52]. This is weaker than Kruskal's Theorem (except for the valence preserving), but predates it. It is easy to encode the valence in the labels, so that this is easily obtained from Kruskal's Tree Theorem. The original language in [Hig52] is couched in algebraic terms, and our present reformulation is in terms of trees. QED

THEOREM 0.9B.3. Theorems 0.9B.1 and 0.9B.2 are provable in Π^1_2-TI. For each fixed $n \geq 1$, Theorem 0.9B.2 is provable in Π^1_2-TI_0.

Proof: This is proved in [Fr84]. Provability in TI is in [Fr81a]. QED

THEOREM 0.9B.4. The following are provably equivalent in RCA_0.
i. TR(<∞) is a wqo under inf preserving embeddability.
ii. For all n, TR(n) is a wqo under inf preserving embeddability.
iii. For all n,r, TR(n;r) is a wqo under inf and valence preserving embeddability.
iv. For all n, TR(n;ω) is a wqo under inf and valence preserving embeddability.
v. STR(<∞) is a wqo under inf preserving embeddability.
vi. For all n, STR(n) is a wqo under inf preserving embeddability.
vii. For all n,r, STR(n;r) is a wqo under inf and valence preserving embeddability.
viii. For all n, STR(n;ω) is a wqo under inf and valence preserving embeddability.
ix. $\theta\Omega^\omega$ is well ordered.

In particular, i-ix are provable in Π^1_2-TI, but not in Π^1_2-TI_0.

THEOREM 0.9B.4. The following are provably equivalent in RCA_0.
i. STR(<∞) is a wqo under inf preserving embeddability.
ii. For all n, TR(n) is a wqo under inf preserving embeddability.
iii. For all n, STR(n;ω) is a wqo under inf and valence preserving embeddability.
iv. $\theta\Omega^\omega$ is well ordered.
In particular, i-iii are provable in Π^1_2-TI, but not in Π^1_2-TI_0.

Proof: The equivalence of i,iii,iv is in [Fr84], using Theorem 0.9A.6. The implication iii → iv is by assigning ordinals to trees. The implication iv → iii uses the provability in Π^1_2-TI_0 of iii for each fixed n.

For unstructured trees, ii → Γ_0 is well ordered was shown in [Fr81a], and appeared in [Si85]. ii → iv appears in [RW93], p. 53, extending the construction (it was attributed to us in [Si85]). Hence i-iii are equivalent to iv. QED

THEOREM 0.9B.5. The following are provable in Π^1_2-TI.
i. If Q is a countable wqo then STR(<∞;Q) is a wqo under inf preserving embeddability.
ii. If Q is a countable wqo and n < ω, then STR(n;Q) is a wqo under inf and valence preserving embeddability.
For each fixed n, ii) is provable in Π^1_2-TI_0.

Proof: This is proved in [Fr84]. QED

We now come to effective and finite forms of Kruskal's Theorem.

THEOREM 0.9B.6. Subrecursive Kruskal Theorem. In any infinite primitive recursive (elementary recursive, polynomial time computable) sequence of finite trees, one tree is embeddable in a later tree.

THEOREM 0.9B.7. Recursive Kruskal Theorem. In any infinite recursive sequence of finite trees, one tree is inf preserving embeddable in a later tree.

THEOREM 0.9B.8. Finite Kruskal Theorem. For all c ≥ 0 there exists n such that the following holds. Let $T_1,...,T_n$ be finite trees, where each T_i has at most i+c vertices. There exist i < j such that T_i is inf preserving embeddable in T_j.

The finite Kruskal theorem has been refined in an interesting way in [LM87].

For $f:N \to N$, let FKT_f assert the following.

For all $c \geq 0$ there exists n such that the following holds. Let $T_1,...,T_n$ be finite trees, where each T_i has at most f(i)+c vertices. There exist i < j such that T_i is inf preserving embeddable in T_j.

The following is proved in [LM87].

Let $f_r(i)$ be $r(\log_2(i))$. If $r \leq 0.5$ then PA does prove FKT_{f_r}.
If $r \geq 4$ then PA does not prove FKT_{f_r}.

Note the gap between .5 and 4. In [We03] there is an exact calculation of the transition point from PA provability to PA unprovability, using analytic combinatorics.

This result led to further systematic investigations on critical phenomena related to independence results. For example, the phase transition corresponding to the relatively large Ramsey theorem is classified in [We04]. Also see [We09].

There is also a phase transition analysis of the regressive Ramsey theorems (see section 0.8D and [KM87]). See [CLW11].

We now proceed from Theorem 0.9B.4 exactly as we proceeded from Theorem 0.8H.3 in section 0.8H.

THEOREM 0.9B.9. The following are provably equivalent in SEFA.
i. Subrecursive Kruskal Theorem.
ii. Finite Kruskal Theorem.
iii. Every primitive recursive sequence from $\theta\Omega^\omega$ stops descending.
iii. 1-Con(ATI(<$\theta\Omega^\omega$)).
iv. 1-Con(Π^1_2-TI_0).

THEOREM 0.9B.10. The following are provably equivalent in SEFA.
i. Recursive Kruskal Theorem.
ii. Every recursive sequence from $\theta\Omega^\omega$ stops descending.

iii. 2-Con(ATI($<\theta\Omega^\omega$)).
iv. 2-Con(Π^1_2-TI_0).

We now focus on Γ_0 and ATR_0.

THEOREM 0.9B.11. The following are provably equivalent in RCA_0.
i. TR(2;2) is a wqo under inf preserving embeddability.
ii. STR(2;2) is a wqo under inf preserving embeddability.
iii. Γ_0 is well ordered.
In particular, i-iii are provable in ATR but not in ATR_0.

Proof: ii ↔ iii is in [Fr84]. i → ii is a result of A. Weiermann that will appear in [FWa]. QED

Again, proceeding as before, we obtain the following.

THEOREM 0.9B.12. The following are provably equivalent in SEFA.
i. Subrecursive Kruskal Theorem for TR(2;2).
ii. Finite Kruskal Theorem for STR(2;2).
iii. Every primitive recursive sequence from Γ_0 stops descending.
iv. 1-Con(ATI($<\Gamma_0$)).
v. 1-Con(ATR_0).

An old unpublished result of ours from the 1980's also concerns binary trees. See [FMW∞] for planned publication. Here is the result in its most primitive form.

THEOREM 0.9B.13. RCA_0 + "If Q is a countable wqo, then TR(2;Q) is a wqo under inf preserving embeddability", proves ATR_0.

Here is a more refined form. Let TR*(2;Q) be the set of finite trees of valence ≤ 2, where vertices of valence 2 are unlabeled, and vertices of valence 0 or 1 are labeled from Q. Embeddings are required to be label increasing (≥) on the labeled vertices. Both forms will appear in [FWb].

THEOREM 0.9B.14. The following are provably equivalent in RCA_0.
i. If Q is a countable wqo, then TR*(2;Q) is wqo under inf preserving embeddability.
ii. If X is a well ordering then $\theta X0$ is a well ordering.
iii. ATR_0.

In [Fr02] the innovation was to use internal tree embeddings in favor of sequences of trees.

We use the following important subclass of TR(k;n). We define FUTR(n;m) as the set of all T ∈ TR(k;n) such that

i. All vertices of valence 0 have the same height.
ii. All vertices are of valence 0 or k.

Here FU means "full".

The height of a vertex in a finite tree is the number of its predecessors. Thus the height of the root is 0. The height of a finite tree is the maximum of the heights of its vertices.

Let T ∈ FUTR(k;n). The truncations of T are obtained by restricting T to all vertices whose height is at most a given nonnegative integer. Thus the number of truncations of T is exactly one more than the height of T.

THEOREM 0.9B.15. Internal Finite Tree Embedding Theorem. Let k,n ≥ 1 and T ∈ FUTR(k;n) be sufficiently tall. There is an inf and valence preserving embedding from some truncation of T into some truncation of T of greater height.

Proof: This appears as Theorem 1.3 in [Fr02]. Fix k,n ≥ 1, and suppose this is false. Then we obtain a finitely branching tree of counterexamples, growing in height as we go up the tree. Therefore there is an infinite path, which forms an infinite full n-labeled tree S of valence k. Now look at its sequence of finite truncations, $S_0,S_1,\ldots$. As a consequence of iii in Theorem 0.9B.4, there exists i < j such that S_i is inf and valence preserving embeddable into S_j. This contradicts the construction of the tree of counterexamples. QED

THEOREM 0.9B.16. The following are provably equivalent in SEFA.
i. Internal Finite Tree Embedding Theorem.
ii. Version of i) for structured trees.
iii. Every primitive recursive descending sequence through $\theta\Omega^\omega$ stops descending.
iv. 1-Con(ATI($<\theta\Omega^\omega$)).
v. 1-Con(Π^1_2-TI_0).
For valence 2, SEFA proves that i) implies 1-Con(ATI($<\Gamma_0$)), and, equivalently, 1-Con(ATR_0).

Proof: See [Fr02]. For valence 2, Γ_0 here can be raised to ordinals considerably higher than, say, Γ_{ϵ_0}, thereby going past ATR. QED

0.9C. Comparability.

A number of Comparability Theorems are known to be equivalent to ATR_0 over RCA_0. They are naturally in Π^1_2 form. By Theorem 0.9A.3 and the comments after its proof, they are not predicatively provable in a strong sense.

The original Comparability Theorem equivalent to ATR_0, was the comparability of well orderings. See i) in the next theorem.

THEOREM 0.9C.1 The following are provably equivalent in RCA_0.
i. For any two countable well orderings, there is an order preserving map from one onto an initial segment of the other.
ii. For any two countable well orderings, there is an order preserving map from one into the other.
iii. ATR_0.

Proof: i ↔ iii is a result of ours that appears in [Si99,09], section V.6. (The derivation of ATR_0 (ATR) from i) in [St76], that was cited in [Si99,09] as an "early" version, uses a technical strengthening of Δ^1_1-CA for the base theory.) For ii ↔ iii, see [FH90]. QED

THEOREM 0.9C.2. The following are provably equivalent in RCA_0.
i. For any two countable metric spaces, there is a pointwise continuous one-one map from one into the other.
ii. For any two sets of rationals, there is a pointwise continuous one-one map from one into the other.
iii. For any two compact well ordered sets of rationals, there is a pointwise continuous one-one map from one into the other.
iv. For any two closed sets of reals, there is a pointwise continuous one-one map from one into the other.
v. ATR_0.

Proof: See [Fr05a]], Theorem 4.5. We were the first to prove i,ii even in ZFC. Comparability for closed sets of reals was known much earlier - although we don't know of a reference.

We now verify v → iv. If A is uncountable, then A has a perfect subset (uses ATR_0). Hence B will continuously embed in A, unless B has interior (this requires at most ACA_0). But if B has interior, then A continuously embeds in B (this is obviously in RCA_0). This establishes comparability if at least one of the two sets is uncountable. If both are countable, then we are in a special case of i). QED

There is a natural descriptive set theoretic consequence one can draw immediately from the fact that a Π^1_2 sentence implies ATR_0 over RCA_0. Actually we can use ACA.

THEOREM 0.9C.3. Let φ be a Π^1_2 sentence, and suppose that ACA proves $\varphi \rightarrow ATR_0$. Then φ has no Borel choice function.

Proof: Suppose φ is $(\forall x)(\exists y)(A(x,y))$, where A is arithmetical, and ACA proves $\varphi \rightarrow ATR_0$. Suppose $(\forall x)(A(x,fx))$, where f is Borel. Choose a countable set $K \subseteq \wp(\omega)$ such that K is f closed and arithmetically closed. Then K forms an ω model of ACA + φ, where K is contained in the hyperarithmetic sets. Hence K forms an ω model of ATR_0, contradicting Theorem 0.9A.3. QED

0.10. Incompleteness in Iterated Inductive Definitions and Π^1_1-CA_0.

0.10A. Preliminaries.
0.10B. Extended Kruskal and Graph Minors.
0.10C. Extended Hercules Hydra Game.
0.10D. Equivalences with Π^1_1-CA_0.

0.10A. Preliminaries.

We discuss three kinds of Concrete Mathematical Incompleteness in this section.

The first is our extension of the work on finite trees discussed in section 0.9B. The second is an extension of the work on the Hercules Hydra Game discussed in section 0.8E. The third is equivalences with Π^1_1-CA_0.

Here is the basic proof theoretic information on Π^1_1-CA_0. The theories of iterated inductive definitions, ID_n, do not have any quantifiers over sets, but instead introduce predicate symbols for inductively defined sets. The predicates introduced in ID_1 correspond to Π^1_1 sets, whereas, the predicates introduced in ID_n, $n \geq 2$, correspond to sets Π^1_1 in the (n-1)-st hyperjump of 0. $ID_{<\omega}$ is the union of the ID_n, n ≥ 1. See [BFPS81].

The following reduction of Π^1_1-CA_0 to $ID_{<\omega}$ prepared the way for a proof theoretic analysis of Π^1_1-CA_0 via a proof theoretic analysis of the ID_n.

THEOREM 0.10A.1. Π^1_1-CA_0 proves Con(TI). In fact, Π^1_1-CA_0 proves the existence of a β-model of TI. Π^1_1-CA_0 is a conservative extension of $ID_{<\omega}$ for arithmetical sentences. In fact, it is a conservative extension of $ID_{<\omega}$ for sentences of the form "n lies in Kleene's O".

Proof: For the first two claims, see [Fr69]. For the last two claims, see [Fr70]. These papers appeared before my focus on systems with only set induction, such as RCA_0, ACA_0, WKL_0, ATR_0, and Π^1_1-CA_0, in connection with our introduction of the Reverse Mathematics program. These systems were introduced in [Fr76] (the systems RCA. WKL, ATR in [Fr75], with ACA, Π^1_1-CA having been previously formulated by others, including S. Feferman and G. Kreisel). The proof in [Fr69] is carried out in Π^1_1-CA_0. In [Fr70], the considerably more involved result that Π^1_1-CA (even Σ^1_2-AC) is a conservative extension $ID^{<\epsilon\_0}$ is established. After we introduced the naught systems, it was evident that a specialization and simplification of the proof establishes the last two claims (even for Σ^1_2-AC_0). QED

Here is the basic proof theory for Π^1_1-CA_0. See [BFPS81], [Tak75], and [Sch77] for proofs.

THEOREM 0.10A.2. Π^1_1-CA_0 is a conservative extension of $ATR(<\theta\Omega_\omega)$ for Π^1_1 sentences. The provably recursive functions of Π^1_1-CA_0 and $ATR(<\theta\Omega_\omega)$ are the $<\theta\Omega_\omega$ recursive functions. The following are provably equivalent in RCA_0.
i. Π^1_1 reflection on Π^1_1-CA_0.
ii. $\theta\Omega_\omega$ is well ordered.
These are provable in Π^1_1-CA but not in Π^1_1-CA_0.

For a general treatment of $<\lambda$ recursive functions via descent recursion, see [FSh95]).

THEROEM 0.10A.3. Π^1_1-CA_0 is a conservative extension of $ATI(<\theta\Omega_\omega)$. The following are provably equivalent in SEFA.
i. 1-Con(Π^1_1-CA_0).
ii. 1-Con($ATR(<\theta\Omega_\omega)$).
iii. 1-Con($ATI(<\theta\Omega_\omega)$).

iv. Every primitive recursive (elementary recursive, polynomial time computable) sequence from $\theta\Omega_\omega$ stops descending.
These are provable in Π^1_1-CA but not in Π^1_1-CA_0.

0.10B. Extended Kruskal and Graph Minors.

In [Fr82], we sought to strengthen Kruskal's theorem in a way that would make it independent of yet stronger systems such as Π^1_1-CA_0. We succeeded with this through our introduction of the gap embedding condition. This turned out to have profound connections with ongoing work at the time by Robertson and Seymour on their Graph Minor Theorem. In fact, it completely encapsulates the only logically high level part of their proof, at least in the case of bounded tree width.

The gap condition concerns the tree classes TR(k;n) and STR(k;n) from section 0.9B. Let S,T ∈ TR(k;n) (or STR(k;n)). We say that h is a gap embedding from S into T if and only if h is an embedding from S into T such that for all x,y ∈ V(S), if y is an immediate successor of x, then for all z in the gap (hx,hy), l(z) ≥ l(hy).

THEROEM 0.10B.1. The Extended Kruskal Theorem. For k,n ≥ 1, TR(k;n) (STR(k;n)) is wqo under inf preserving gap embeddability.

Proof: See [Fr82], [Si85]. QED

THEOREM 0.10B.2. The following are provably equivalent in RCA_0.
i. Extended Kruskal Theorem (structured and unstructured).
ii. Extended Kruskal Theorem for full binary trees (structured and unstructured).
iii. $\theta\Omega_\omega$ is well ordered.
These are provable in Π^1_1-CA but not in Π^1_1-CA_0.

Proof: See [Fr82] for i → iii (unstructured), and a proof of i) (structured) for each k,n, in Π^1_1-CA_0. Applying 0.10A.2, we have i ↔ iii. For ii → i (unstructured), see [FRS87]. Also see [Si85] and [Fr02]. QED

Let G,H be finite graphs. We say that G is minor included in H if and only if G can be obtained from H (up to isomorphism) by successive applications of the following operations.

i. Deleting a vertex (and all edges involving that vertex).
ii. Deleting an edge.
iii. Contracting an edge. I.e., if v,w is an edge, v ≠ w, remove w and replace all edges involving w that are not loops by replacing w with v.

The Graph Minor Theorem asserts that in any infinite sequence of finite graphs, one graph is minor included in a later one. The Graph Minor Theorem is proved in a series of papers culminating with [RS04].

The entire proof consists of very detailed structure theory, with a brief logically strong part, involving minimal bad sequence constructions. We communicated our earlier Extended Kruskal Theorem to Robertson and Seymour. Robertson and Seymour adapted and extended these ideas to their later proof of the Graph Minor Theorem.

The Bounded Graph Minor Theorem is the Graph Minor Theorem specialized to trees of bounded tree width (see [FRS87]).

Our work on the Extended Kruksal Theorem was applied in a striking way to the Graph Minor Theorem in [FRS87].

THEOREM 0.10B.3. The following are provably equivalent in RCA_0.
i. Extended Kruskal Theorem (structured and unstructured).
ii. Bounded Graph Minor Theorem.
iii. $\theta\Omega_\omega$ is well ordered.
These are provable in Π^1_1-CA but not in Π^1_1-CA_0.

Proof: See [FRS87]. QED

As before, we obtain subrecursive, recursive, and finite forms.

THEOREM 0.10B.4. The following are provably equivalent in SEFA.
i. Extended Kruskal Theorem for primitive recursive (elementary recursive, polynomial time computable) sequences of finite trees (all four forms above).
ii. Bounded Graph Minor Theorem for primitive recursive (elementary recursive, polynomial time computable) sequences of finite graphs.
iii. 1-Con(Π^1_1-CA_0).
iv. 1-Con(ATI($<\theta\Omega_\omega$)).
These are provable in Π^1_1-CA but not in Π^1_1-CA_0.

Proof: The ordinal assignments involved are very effective, and i,ii are Π^0_2 statements. Use that for a fixed number of labels, or fixed tree width, the statements are provable in Π^1_1-CA_0. QED

THEOREM 0.10B.5. The following are provably equivalent in SEFA.
i. Extended Kruskal Theorem for recursive sequences of finite trees (all four forms above).
ii. Bounded Graph Minor Theorem for recursive sequences of finite graphs.
iii. Every recursive sequence from $\theta\Omega_\omega$ stops descending.
iii. 2-Con(Π^1_1-CA_0).
iv. 2-Con(ATI($<\theta\Omega_\omega$)).
These are provable in Π^1_1-CA but not in Π^1_1-CA_0.

Proof: See the proof of Theorem 0.8H.10. QED

We can proceed with the finite forms. For the Extended Kruskal Theorems, there are no surprises. We can use my usual finite sequences where the i-th term has at most i+c vertices, where the parameter c is universally quantified.

THEOREM 0.10B.6. The following are provably equivalent in SEFA.
i. The Finite Extended Kruskal Theorem (all four forms above).
ii. 1-Con(Π^1_1-CA_0).
iii. 1-Con(ATI($<\theta\Omega_\omega$)).
These are provable in Π^1_1-CA but not in Π^1_1-CA_0.

In [Fr02], the following Internal Embedding Theorem is treated.

THEOREM 0.10B.7. The Internal Finite Tree Gap Embedding Theorem. Let $k,n \geq 1$ and $T \in$ FUTR(k;n) be sufficiently tall. There is an inf and valence preserving gap embedding from some truncation of T into some truncation of T of greater height.

Proof: This appears as Theorem 7.7 in [Fr02]. QED

THEOREM 0.10B.8. The following are provably equivalent in SEFA.
i. Internal Finite Tree Gap Embedding Theorem.
ii. Variants of i) with structure and/or with valence 2.
iii. Every primitive recursive sequence from $\theta\Omega_\omega$ stops descending.

iii. 1-Con(ATI($<\theta\Omega_\omega$)).
iv. 1-Con(Π^1_2-TI_0).
For valence 2, EFA proves that i) implies 1-Con(ATI($<\Gamma_0$)), and, equivalently, 1-Con(ATR_0).

Proof: See [Fr02]. QED

The following Finite Bounded Graph Minor Theorem is treated in [FRS87].

THEOREM 0.10B.9. Finite Bounded Graph Minor Theorem. For all p,c ≥ 1 there exists n such that the following holds. Let $G_1,\ldots,G_n$ be finite graphs of tree-width ≤ p, where each $|G_i| \geq i+c$. There exist i < j such that $G_i \leq_m G_j$.

Here |G| denotes the sum of the number of vertices and edges in G, and $\leq_m$ denotes graph minor inclusion.

THEOREM 0.10B.10. The following are provably equivalent in SEFA.
i. The Finite Bounded Graph Minor Theorem.
ii. Every primitive recursive sequence from $\theta\Omega_\omega$ stops descending.
iii. 1-Con(ATI($<\theta\Omega_\omega$)).
iv. 1-Con(Π^1_1-CA_0).

Proof: See [FRS87]. QED

It remains unclear just what is required to prove the full Graph Minor Theorem. Its proof has not been subject to a logical analysis sufficient to determine a reasonable upper bound.

0.10C. Extended Hercules Hydra Game.

The following treatment is taken directly from [Bu87].

A (Buchholz) hydra is a finite rooted planar labeled tree H which has the following properties:

i. The root has label +.
ii. Any other node of A is labeled by some ordinal $\alpha \leq \omega$,
iii. All nodes immediately above the root of H have label 0.

If Hercules chops off a head (i.e. a top node) s of a given hydra, the hydra will choose an arbitrary number n and transform itself into a new hydra H(s,n) as follows. Let t be the node of H which is immediately below s, and let H^- denote the part of H which remains after s has been chopped off. The definition of H(s,n) depends on the label of s.

case 1. label(s) = 0. If t is the root of H, we set H(s,n) = H^-. Otherwise H(s,n) results from H^- by sprouting n replicas of $H_{t^\wedge-}$, from the node immediately below t. Here $H_{t^\wedge-}$ denotes the subtree of H^- determined by t.

case 2. label(s) = u+1. Let e be the first node below s with a label v ≤ u. Let T be that tree which results from the subtree H_e by changing the label of e to u and the label of s to 0. H(s,n) is obtained from H by replacing s by T. In this case H(s,n) does not depend on n.

Case 3: label(s) = ω. H(s,n) is obtained from H simply by changing the label of s (which is ω) to n+1.

Let H(n) be H(s,n) where s is the rightmost head. Let (+) be the hydra which consists of one node, namely its root. Let H^n be the hydra consisting of a chain of n+2 nodes where the root has label +, the successor of the root has label 0 and where all other nodes have label ω.

THEOREM. Let H be a fixed hydra. Π^1_1-CA + BI proves that for all number theoretic functions F there exists k such that H(F(1))(F(2))...(F(k)) = (+).

THEOREM. Π^1_1-CA + BI does not prove that for all n there exists a k such that H^n(1)(2)...(k) = (+).

0.10D. Equivalences with Π^1_1-CA_0.

There are a number of interesting equivalences with Π^1_1-CA_0.

THEOREM 0.10D.1. The following are provably equivalent in RCA_0.
i. Every tree of finite sequences of natural numbers with an infinite path, has a leftmost infinite path.
ii. Every tree of finite sequences of natural numbers (bits) has a perfect subtree which contains all perfect subtrees.
iii. If a quasi order on N is not a wqo then it has a minimal bad sequence.
iv. Every countable Abelian group G has a divisible subgroup which contains all divisible subgroups of G.
v. Π^1_1-CA_0.

Proof: Clearly v) → i). Assume i). Let $T_1,T_2,...$ be any infinite sequence of finite sequence trees from N. We will derive the existence of {i: Ti has an infinite path}. This is a well known equivalent of Π^1_1-CA_0 over RCA_0 (see [Si99,09], Lemma VI.1.1).

Let S be the tree of sequences x[1],...,x[n], n ≥ 0, from N, with the following properties.

a. If p ≤ n is not a power of a prime, then x[p] = 1.
b. Let p ≤ n be a prime, and r ≥ 1 be largest such that p^r ≤ n. Then

b.1. $x[p],x[p^2],...,x[p^r] = 1$; or

b.2. x[p] = 0, and $x[p^2],...,x[p^r]$ forms a path of length r-1 through T_i, starting at an immediate successor of the root (a length 1 sequence), where p is the i-th prime, and we view each term as coding a finite sequence from N.

S will have the infinite path 1,1,... . Let x[1],x[2],... be a (the) leftmost infinite path P through S. Let p be the i-th prime. If x[p] = 0 then there is a path through T_i. Suppose x[p] = 1 and there is a path Q through T_i. Then we can retain the first p-1 terms, lower the p-th term to 0, and use Q so that we have another infinite path through S which is to the left of P. This is a contradiction. Hence x[p] = 0 if and only if there is an infinite path through T_i. Therefore {i: T_i has an infinite path} exists.

For ii ↔ v, see [Si99,09], Theorem VI.1.3.

For iii ↔ v, see [Mar96], Theorem 6.5.

In Π^1_1-CA_0, we can construct the union of all divisible subgroups, and so obviously v → iv. Now suppose iv.

In [FSS87] it is shown that "every countable Abelian group is a direct sum of a divisible group and a reduced group" is equivalent to Π^1_1-CA_0 over RCA_0 (see [Si99,09], Theorem VI.4.1).

With a little bit of care, the derivation of Π^1_1-CA_0 there can be accomplished with just iv). QED

Here is a somewhat different kind of example.

THEOREM 0.10D.2. The following are provably equivalent in RCA_0.

i. Every countable algebra with an infinitely generated subalgebra has a maximal infinitely generated subalgebra.
ii. Proposition i) for a single binary function.
iii. Proposition i) for two unary functions.
iv. Π^1_1-CA_0.

Proof: See [Fr05b]. QED

The Borel Ramsey theorem, also known as the Galvin/Prikry theorem, asserts the following. Let $S \subseteq \wp(N)$ be Borel. There exists an infinite $A \subseteq N$ such that all infinite subsets of A lie in S, or all infinite subsets of A lie outside S.

With its use of Borel measurable sets of arbitrary high countable rank, the Borel Ramsey theorem is an example just beyond Concrete Mathematics.

We rely on the standard treatment of Borel sets in $\wp(N)$ in order to formulate the Borel Ramsey theorem in the language of RCA_0. This is achieved through the use of Borel codes, and is discussed in some detail in section 0.11.

Π^1_1-TR_0 consists of ACA_0 together with Π^1_1 transfinite recursion. This is the same as arithmetic transfinite recursion - as in ATR_0 - except that the formula to which transfinite recursion is being applied is allowed to be Π^1_1. This is equivalent to the existence of the hyperjump hierarchy on every countable well ordering, starting with any subset of ω.

Borel sets in and functions between complete separable metric spaces lie just beyond what we regard as Concrete Mathematics. We take finitely Borel to be at the outer limits of Concrete Mathematics.

Everything in sections 0.11, 0.12, and much of section 0.13, will be focused at this borderline between Concrete and Abstract Mathematics.

Some care is needed to properly formalize Borel sets and functions in RCA_0. A standard way of doing this has emerged. This will be discussed in section 0.11.

The Borel Ramsey Theorem sits in the context of $\wp(N)$ as a complete separable metric space, under $d(A,B) = 2^{-n}$, where n $= \min(A \Delta B)$ if $A \neq B$; 0 otherwise. It asserts that for any

Borel S ⊆ $\wp$(N), there exists infinite A ⊆ N such that $\wp$(A) ⊆ S or $\wp$(A) ∩ S = ∅.

THEOREM 0.10D.3. The following are provably equivalent in RCA_0.
i. The Borel Ramsey Theorem (or Galvin/Prikry Theorem).
ii. Π^1_1-TR_0.

Proof: See [Tan89]. QED

THEOREM 0.10D.4. The following are provably equivalent in RCA_0.
i. The Borel Ramsey Theorem (or Galvin/Prikry Theorem) for finitely Borel subsets of $\wp$(N).
ii. (∀x ⊆ N)(∀n)(the n-th hyperjump of x exists).
In particular, i implies Π^1_1-CA_0, and follows from Π^1_1-CA (Π^1_1-CA_0 with full induction).

L. Gordeev and I. Kriz have proved some transfinite extensions of my Extended Kruskal Theorem (Theorem 0.10B.1) using much stronger principles than Π^1_1-CA_0. See [Gor89], [Gor90], [Gor93], [Kri89a], [Kri89b], [Kri95]. The proof of the main theorem of [Kri89b] given there (which was a conjecture of mine) requires Π^{-}_2-CA_0. However, this was later sharply reduced to Π^1_1-TR_0 by [Gor90], [Gor93], with a reversal to a level corresponding to Π^1_1-TR_0.

There are a number of interesting mathematical statements which have been proved using systems significantly stronger than Π^1_1-CA_0 - but it remains unknown whether that is necessary. We have already mentioned the Graph Minor Theorem.

Nash-Williams proved that infinite trees are wqo under inf preserving embeddability. See [NW65], [NW68], where his notions of better quasi orders and minimal bad arrays were introduced. He uses much stronger principles than Π^1_1-CA_0. It is not known whether this is required. [Si85a] simplifies the notion of better quasi order. Also see [EMS87].

R. Laver proved in [La71] that the linear orderings on N form a wqo under embeddability. This is known as Fraïssé's conjecture. In [Sho93] this theorem is shown to imply ATR_0 over RCA_0. However, it is not known if ATR_0 is sufficient, or even whether Π^1_1-CA_0 and much stronger systems are sufficient. Π^1_2-CA_0 certainly suffices. [Si85a] simplifies the proof of Fraïssé's conjecture.

0.11. Incompleteness in Second Order Arithmetic and ZFC\P.

0.11A. Preliminaries.

The system Z_2 of "(full) second order arithmetic", and the closely related ZFC\P, ZF\P, have been discussed in section 0.4.

It will be useful to have a system stronger than Z_2, which suffices to prove the various statements presented in this section, that are not provable in Z_2.

For this purpose, it is convenient to use a weak fragment of Z_3 = "(full) third order arithmetic". Here Z_3 has three sorts: N, PN, PPN. We use $0,S,+,\bullet,\in$, where $0,S,+,\bullet$ live in N, and $\in$ connects N to PN, and PN to PPN. We will have equality only for sort N.

Recall the axioms of Z_2:

1. $Sx \neq 0$, $Sx = Sy \to x = y$, $x+0 = x$, $x+Sy = S(x+y)$, $x\bullet 0 = 0$, $x\bullet Sy = (x\bullet y)+x$.
2. $0 \in A \wedge (\forall x)(x \in A \to Sx \in A) \to x \in A$.
3. $(\exists A)(\forall x)(x \in A \leftrightarrow \varphi)$, where φ is any formula in $L(Z_2)$ in which A is not free.

The axioms of Z_3 are very similar. The terms of sort N are the same as for Z2. The atomic formulas are the equations between terms of sort N, and $t \in x$, $x \in A$, where x is a variable of sort PN and A is a variable of sort PPN. Formulas are built up as usual using the connectives and sorted quantifiers.

1. $Sx \neq 0$, $Sx = Sy \to x = y$, $x+0 = x$, $x+Sy = S(x+y)$, $x\bullet 0 = 0$, $x\bullet Sy = (x\bullet y)+x$.
2. $0 \in A \wedge (\forall x)(x \in A \to Sx \in A) \to x \in A$.
3. $(\exists A)(\forall x)(x \in A \leftrightarrow \varphi)$, where φ is any formula in $L(Z_3)$ in which A is not free.
4. $(\exists \alpha)(\forall A)(A \in \alpha \leftrightarrow \varphi)$, where φ is any formula in $L(Z_3)$ in which α is not free.

The axioms of WZ_3 are very convenient (W for "weak"). The only change is that in axiom 4, we require that there be no quantifiers over PPN. WZ_3 is enough to extend the projective hierarchy along ω_1. Z_3 proves the existence of a beta model of WZ_3, and much more.

In this section 0.11, we will focus entirely on the outer limits of Concrete Mathematical Incompleteness, in that we will be using

Borel measurable sets in and functions between
complete separable metric spaces

throughout. We take finitely Borel to lie within Concrete mathematics, and arbitrary Borel to lie just outside.

In each case in this section, the incompleteness from Z_2 will emerge already using only Borel objects of finite rank in the Borel hierarchy (i.e., finitely Borel). In section 0.12, when we use Zermelo set theory, the incompleteness will emerge at Borel rank ω.

Our position that the finite levels of the Borel hierarchy for complete separable metric spaces lies at the outer limit of the Mathematically Concrete was discussed in section 0.3, with Theorem 0.3.1 used as some justification - particularly item ii there.

Let X be a complete separable metric space. We define the classes Σ_α and Π_α of subsets of X, $\alpha < \omega_1$, as follows.

Σ_0 consists of the sets of the form $\{y: d(x,y) < q\}$, for $x \in X$ and positive rationals q. Π_0 consists of the sets of the form $\{y: d(x,y) \geq q\}$, for $x \in X$ and positive rationals q.

For $0 < \alpha < \omega_1$, Σ_α consists of unions of sequences of sets from the Π_β, $\beta < \alpha$, and Π_α consists of intersections of sequences of sets from the Σ_β, $\beta < \alpha$.

The Borel subsets of X are the sets that are in Σ_α, for some $\alpha < \omega_1$. It is easily seen that the Borel sets form the least σ algebra of subsets of X containing all elements of Σ_0.

It is also clear that each Π_α is the set of complements of the elements of Σ_α. Also, for $0 \leq \alpha \leq \beta < \omega_1$, $\Sigma_\alpha \subseteq \Sigma_\beta$ and $\Pi_\alpha \subseteq \Pi_\beta$.

If X is uncountable, then for all $\beta < \omega_1$, $\Sigma_\beta \neq \Sigma_{\beta+1}$, and $\Pi_\beta \neq \Pi_{\beta+1}$.

This is equivalent to the definition of the Borel hierarchy given in [Ke95], 11.B, p. 68, where these claims are proved.

We focus on the functions $f:X \to Y$, where X,Y are complete separable metric spaces. We say that f is Borel (Borel measurable) if and only if the inverse image of every open subset of Y is a Borel subset of X.

We also define the following important hierarchy of functions.

Baire class 0 consists of the $f:X \to Y$ which are pointwise limits of continuous $f:X \to Y$.

For $0 < \alpha < \omega_1$, Baire class α consists of the $f:X \to Y$ that are the pointwise limit of a sequence of $g:X \to Y$ that pointwise converges, where for each g there exists $\beta < \alpha$ such that g is in Baire class β.

We say that $f:X \to Y$ is Baire if and only if f is in Baire class α, for some $\alpha < \omega_1$.

It is a standard theorem of descriptive set theory that the Baire functions are exactly the Borel functions (in the context of $f:X \to Y$, where X,Y are complete separable metric spaces). See [Ke95], Theorem 24.3, p. 190,

Some authors define the Baire classes a little differently, where they start at Baire class 1, and define $f:X \to Y$ to be of Baire class 1 if and only if the inverse image of every open subset of Y is a Σ_2 subset of X.

According to [Ke95], Theorem 24.10, this definition agrees with our definition above (pointwise limits of continuous functions) in the case $Y = \Re$.

We must formalize these notions appropriately in $L(RCA_0)$. Some care is required. We adopt the approach of [Si99,09].

Firstly, complete separable metric spaces are defined in $L(RCA_0)$ by means of codes. We henceforth refer to these spaces as Polish spaces.

As in [Si99,09], Definition II.5.1, a code for a Polish space T is a nonempty set A ⊆ N together with a function $d:A^2 \rightarrow \Re$ obeying the usual metric conditions. Points in T are then defined as infinite sequences from A that form a Cauchy sequence (using the estimates 2^{-i}). We don't factor out by the obvious equivalence relation. Similarly, when developing $\Re$ as Cauchy sequences, we also don't factor out.

The metric d extends naturally to T, A becomes dense in T, and Cauchy completeness holds for the elements of T.

Open subsets of X are coded by sequences of pairs (a,q), where a ∈ A and q > 0 is rational. Membership of x ∈ T in the open set means that d(a,x) < q. Closed subsets of X are viewed as complements of open sets.

Continuous functions from X into Y are coded in $L(RCA_0)$ by means of systems of neighborhood conditions. In [Si99,09], Definition II.6.1, they are sets of quintuples from N x A x Q^+ x B X Q^+, where A,B ⊆ N are attached to the Polish spaces X,Y.

For Borel subsets of X, the usual vehicle for formalization in the language of RCA_0 is through Borel codes. These are well founded trees of finite sequences from N where at the terminal vertices, there is a label (a,q), where a ∈ A and q > 0 is rational. The idea is that x ∈ X is accepted at a terminal vertex with label (a,q) if and only if d(a,x) < q, and accepted at an internal vertex v if and only if

case 1. v is of odd length (as a finite sequence from N). x is accepted at some immediate successor of v.

case 2. v is of even length. x is not accepted at any immediate successor of v.

Finally, x is considered to be in the Borel set with the given Borel code, if and only if x is accepted at the root of the tree.

A similar Borel coding scheme can be introduced for Borel functions f:X → Y that corresponds to the Baire classes.

This whole coding apparatus is very delicate for weak systems, particularly for RCA_0, since in order to get accepted, a certain transfinite recursion must be realized. In weak systems, we can only provably realize very special transfinite recursions. To a much lesser extent, issues arise in weak systems with regard to the codings of open and closed sets, and continuous functions.

We have no need to confront these issues in this section 0.11. The statements being reversed here derive ATR_0 over RCA_0, using very little of this coding. We are then free to use ATR_0 as a base theory when dealing with Borel sets in and functions between Polish spaces.

0.11B. Borel Determinacy in Z_2.

Determinacy concerns (two person zero sum) infinite games, where players I,II alternately play nonnegative integers, starting with player I. The outcome of the game is the element of N^∞ that results from the play of the game.

Specifically, for any $A \subseteq N^N$, we consider the game G[A], where player I is considered the winner if the outcome of the game is an element of A. Otherwise, player II is considered to be the winner.

We say that G[A] is determined if and only if one of the two players has a winning strategy. It is well known that there exists $A \subseteq N^N$ for which G[A] has no winning strategy. See [GS53], [Ka94], chapter 6.

However, the proof of the existence of non determined G[A] does not produce an A that is definable in set theory. There has been much work concerning the determinacy of G[A], where A is explicitly definable in various senses. These investigations are tied up with large cardinal hypotheses. We refer the reader to [Mart69], [MSt89], [Ke95], [Lar04], [St09], [Ne∞], [KW∞].

Let K be a class of subsets of N^N. K determinacy asserts that for all $A \in K$, the game G[A] is determined. Henceforth, we will be focused on K contained in the class of all Borel subsets of N^N.

The original "proof" of Borel determinacy was not conducted in ZFC.

THEOREM 0.11B.1. Assume that a measurable cardinal exists. Then Borel determinacy holds. I.e., all Borel subsets of N^N are determined. In fact, the weaker large cardinal hypothesis $(\forall\alpha < \omega_1)(\exists\kappa)(\kappa \to \alpha)$ suffices.

Proof: See [Mart69], [Ke95], section 20. QED

Later, we showed that any proof of Borel determinacy in ZFC is not going to be "normal".

THEOREM 0.11B.2. There is no proof of Borel determinacy in Zermelo set theory with the axiom of choice (ZC). In fact, no countable transfinite iteration of the power set operation suffices.

Proof: See [Fr71]. We will discuss what exactly we mean by the second claim, in section 0.12. QED

A few years later, the gap between Theorems 0.11B.1 and 0.11B.2 was filled.

THEOREM 0.11B.3. Borel determinacy can be proved in ZFC. In fact, it suffices to use all countably transfinite iterations of the power set operation.

Proof: See [Mart75], [Ke95]. QED

Note that Theorems 0.11B.2 and 0.11B.3 properly lie in the domain of section 0.12.

There has been considerable work on determining just where in the Borel hierarchy determinacy is provable in full second order arithmetic, Z_2. This investigation has culminated in [MS∞], providing a complete answer.

Note that determinacy for the classes Borel, $\Sigma^0{}_n$, $\Pi^0{}_n$, and $\Delta^0{}_n$, are $\Pi^1{}_3$ statements. So we can use ZFC\P or ZF\P, as all three of these systems prove the same $\Pi^1{}_3$ sentences. In fact, they prove the same $\Sigma^1{}_4$ sentences, as is shown in [MS∞], Proposition 1.4 (although this is certainly not due to them, but it is not clear who first proved this). Here \P indicates "without the power set axiom".

Here is the historical record of Borel determinacy in Z_2.

Borel determinacy. Not provable in Zermelo set theory with the axiom of choice. Not provable using only countably many transfinite iterations of the power set operation, [Fr71]. See section 0.12 for precise formulations.

$\Sigma^0{}_5$ determinacy. Not provable in Z_2. [Fr71].

Borel determinacy. Proved in ZFC\P + "the cumulatively hierarchy on any well ordering of ω exists". [Mart75].

Σ^0_4 determinacy. Not provable in Z_2. [Mart74].

Σ^0_1 determinacy. Equivalent to ATR over RCA. [St76]. Refined in [Si99,09] to equivalence with ATR_0 over RCA_0.

$\Sigma^0_1 \wedge \Pi^0_1$ determinacy. Equivalent to Π^1_1-CA_0 over RCA_0. [Tan90].

Δ^0_2 determinacy. Equivalent to Π^1_1-TR_0 over RCA_0. [Tan90].

Σ^0_2 determinacy. Provable in Π^1_2-CA_0, but not in Π^1_1-TR_0. [Tan91].

Δ^0_3 determinacy. Provable in Δ^1_3-CA, but not in Δ^1_3-CA_0. [MT08].

Σ^0_3 determinacy. Provable in Π^1_3-CA_0. [Wel09].

Boolean combinations of Σ^0_3 determinacy. Not provable in Z_2. For n-fold combinations, fixed $n < \omega$, provable in Z_2, [MS∞].

0.11C. Borel diagonalization on $\mathfrak{R}$.

We discovered Borel diagonalization on $\mathfrak{R}$ by reflecting on Cantor's proof that $\mathfrak{R}$ is uncountable. Put in very basic terms, Cantor proved by diagonalization that

*) in any infinite sequence of real numbers, some real number is missing.

It occurred to me to consider witness functions for *). Let us say that $F:\mathfrak{R}^\infty \to \mathfrak{R}$ is a diagonalizer if and only if $(\forall x \in \mathfrak{R}^\infty)(\forall n \in Z^+)(F(x) \neq x_n)$.

For any topological space X, X^∞ is the infinite product space defined in the usual way. It is well known that if X is (can be made into) a complete separable metric space, then X^∞ is (can be made into) a complete separable metric space.

Cantor's diagonalization argument easily establishes the existence of a diagonalizer $F:\mathfrak{R}^\infty \to \mathfrak{R}$.

LEMMA 0.11C.1. There is no continuous diagonalizer $F:\mathfrak{R}^\infty \to \mathfrak{R}$. There is no continuous diagonalizer $F:I^\infty \to I$.

Proof: Let $F:\Re^\infty \to \Re$ be a continuous diagonalizer. Let $\alpha \in \Re^\infty$ be an enumeration of the rationals. Consider $F(x,\alpha)$ as a function of $x \in \Re$.

case 1. F is constant. Let c be the constant. Then $F(c,\alpha) = c$, which is impossible.

case 2. F is not constant. Let $F(x,\alpha) \neq F(y,\alpha)$, $x < y$. By the intermediate value theorem there exists $x < z < y$ such that $F(z,\alpha) \in Q$. This is also impossible.

We can easily repeat the argument with $\Re$ replaced by I. QED

We now construct a diagonalizer $F:I^\infty \to I$ in Baire class 1.

Let $x \in I^\infty$. First write the coordinates of x in base 2, always using infinitely many 0's. Then diagonalize in the usual way to construct $u \in \{0,1\}^\infty$ which differs from these base 2 expansions. I.e., $u_i = 1 - x_i'$, where xi' is this expansion of xi in base 2. Take F(x) to be the evaluation of u in I.

For $w \in \{0,1\}^k$, $k \geq 1$, write $w^* \in I$ for the evaluation of w in base 2.

LEMMA 0.11C.2. Let $w \in \{0,1\}^k$, $k \geq 1$. $A = \{x \in I^\infty: F(x) \in [w^*,w^*+2^{-k})\}$ is Δ^0_2 in I^∞.

Proof: Let w be given. Let $x \in I^\infty$. Note that $x \in A$ if and only if

F(x) has base 2 expansion starting with w.

$(\exists v_1,\ldots,v_k \in \{0,1\}^k)(\forall i \in \{1,\ldots,k\})$($v_i$ is the first k terms of the base 2 expansion of x_i, and the standard diagonal construction produces w from $v_1,\ldots,v_k$).

$(\exists v_1,\ldots,v_k \in \{0,1\}^k)(\forall i \in \{1,\ldots,k\})(x_i \in [v_i,v_i+2^{-k})$ and the standard diagonal construction produces w from $v_1,\ldots,v_k$).

QED

LEMMA 0.11C.3. Let $V \subseteq I$ be open. Then $F^{-1}(V)$ is Σ^0_2 in I^∞.

Proof: Since every open subset of I is the countable union of intervals of the form $[w^*,w^*+2^{-k})$, $w \in \{0,1\}^k$, $k \geq 1$, this is immediate from Lemma 0.11C.2. QED

LEMMA 0.11C.4. Let $F:I^\infty \to I$, and suppose that the inverse image of any open set in I under F is $\mathbf{\Sigma}^0{}_2$ in I^∞. Then F is in Baire class 1.

Proof: By Theorem 24.3 in [Ke95], p. 190, credited to Lebesgue, Hausdorff, and Banach. QED

THEOREM 0.11C.5. There is a diagonalizer $F:I^\infty \to I$ in Baire class 1, but none that is continuous. There is a diagonalizer $G:\mathfrak{R}^\infty \to \mathfrak{R}$ in Baire class 1, but none that is continuous. There is a continuous diagonalizer $H:X^\infty \to X$, where X is {0,1} or X = N.

Proof: The first claim is immediate from Lemmas 0.11C.1, 0.11C.3, and 0.11C.4. For the second claim, take G(x) = f(x'), where each $x'_i = 0$ if $x_i \leq 0$; 1 if $x_i \geq 1$; x otherwise. Note that $G:\mathfrak{R}^\infty \to \mathfrak{R}$ is a diagonalizer, and x' defines a continuous function of x. Hence G is in Baire class 1. The last claim is essentially due to Cantor, with his diagonal argument. QED

We realized that in the constructions of diagonalizers $F:\mathfrak{R}^\infty \to \mathfrak{R}$, the values $F(x_1,x_2,...)$ seem to depend critically on the order in which the x's appear.

So we were led to the question: is there a diagonalizer $F:\mathfrak{R}^\infty \to \mathfrak{R}$ which is suitably invariant? I.e., where for all $x,y \in \mathfrak{R}^\infty$, if x is "similar" to y, then F(x) = F(y)?

The weakest notion of "similar" that we consider in this section is "having the same coordinates" or "having the same image". I.e., rng(x) = rng(y), for $x,y \in \mathfrak{R}^\infty$. Here rng(x) is the set of all coordinates of x.

Thus we say that $f:\mathfrak{R}^\infty \to \mathfrak{R}$ is image invariant if and only if for all $x,y \in \mathfrak{R}^\infty$, $rng(x) = rng(y) \to F(x) = F(y)$.

Of course, this definition applies to $f:X^\infty \to X$, where X is any set whatsoever.

THEOREM 0.11C.6. There is an image invariant diagonalizer $f:\mathfrak{R}^\infty \to \mathfrak{R}$. In fact, there is an image invariant diagonalizer $f:X^\infty \to X$ if and only if X is uncountable.

Proof: By the axiom of choice. QED

Note that the proof of Theorem 0.11C.6 does not produce a definable example - even for the first claim. A related observation is that it proves the claim in ZFC, but not even the first claim is proved in ZF.

We will take this matter up in section 0.13, where we show that there is no definition that ZFC proves is an example for the first claim, and that ZF does not suffice to prove the existence of an example for the first claim.

We now come to a Concrete Mathematical Incompleteness result.

THEOREM 0.11C.7. Borel Diagonalization Theorem. There is no image invariant Borel diagonalizer $f:\mathfrak{R}^\infty \to \mathfrak{R}$. This is provable in WZ_3 but not in Z_2.

Proof: See [Fr81]. The unprovability from Z_2 was proved there by first considering pZ_2, which is Z_2 formulated without parameters. We established the equiconsistency of pZ_2 and Z_2, and other relationships, and then showed how the Borel Diagonalization Theorem gives rise to an ω model of pZ_2, and hence of Z_2. We relied on our earlier experience with ZF formulated without parameters, from our Ph.D. thesis. See [Fr67] and [Fr71a]. QED

0.11D. Borel Inclusion for $\mathfrak{R}^\infty \to \mathfrak{R}$, $\mathfrak{R}^\infty \to \mathfrak{R}^\infty$, GRP $\to$ GRP.

We now consider these three notions of similarity.

1. y is a permutation of x.
2. y is a permutation of x that moves only finitely many positions. Such permutations are called finitary permutations.
3. x,y have the same image.

The associated conditions on $F:\mathfrak{R}^\infty \to \mathfrak{R}$ are respectively called permutation invariant, finitary permutation invariant, and image invariant.

We also consider shift invariance. We say that $F:\mathfrak{R}^\infty \to \mathfrak{R}$ is shift invariant if and only if for all $x \in \mathfrak{R}^\infty$, $F(sx) = F(x)$. Here sx = shift of x, is the result of removing the first term of x.

We also find it convenient to switch to positive phraseology. We define an inclusion point of $F:\mathfrak{R}^\infty \to \mathfrak{R}$ as an $x \in \mathfrak{R}^\infty$ such that F(x) is a coordinate of x.

THEOREM 0.11D.1. Borel Inclusion Point Theorem for $\Re^\infty,\Re$. Every permutation (finitary permutation, image, shift) invariant Borel $F:\Re^\infty \to \Re$ has an inclusion point. All four forms are provable in WZ_3, but none are provable in Z_2.

Proof: These results are proved by straightforward adaptations of the methods in [Fr81]. QED

We now consider $F:\Re^\infty \to \Re^\infty$. Here we say that x is an inclusion point for F if and only if F(x) is a subsequence of x.

There are many natural notions of invariance here.

a. Permutation commuting. This means that for all $x \in \Re^\infty$ and permutations π, $f(\pi x) = \pi f(x)$.

b. Finitary permutation commuting. This means that for all $x \in \Re^\infty$ and finite permutations π, $f(\pi x) = \pi f(x)$.

c. Permutation invariant. This means that for all $x,y \in \Re^\infty$, if y is a permutation of x then F(x) = F(y).

d. Finitary permutation invariant. This means that for all $x,y \in \Re^\infty$, if y is a finite permutation of x then F(x) = F(y).

e. Permutation preserving. This means that for all $x,y \in \Re^\infty$, if y is a permutation of x then F(y) is a permutation of F(x).

f. Finitary permutation preserving. This means that for all $x,y \in \Re^\infty$, if y is a finitary permutation of x then F(y) is a finitary permutation of F(x).

g. Image invariant. This means that for all $x,y \in \Re^\infty$, $rng(x) = rng(y) \to F(x) = F(y)$.

h. Image preserving. This means that for all $x,y \in \Re^\infty$, $rng(x) = rng(y) \to rng(F(x)) = rng(F(y))$.

i. Shift invariant. This means that for all $x \in \Re^\infty$, $F(sx) = F(x)$.

j. Shift commuting. This means that for all $x \in \Re^\infty$, $F(sx) = s(F(x))$.

k. Tail invariant. This means that for all $x,y \in \Re^\infty$, if x,y have a common tail, then F(x) = F(y).

l. Tail preserving. This means that for all $x,y \in \Re^\infty$, if x,y have a common tail, then F(x),F(y) have a common tail.

THEOREM 0.11D.2. Borel Inclusion Theorem for $\Re^\infty,\Re^\infty$. Every Borel $F:\Re^\infty \to \Re^\infty$ with any of a-l has an inclusion point. All twelve forms are provable in WZ_3, but none are provable in Z_2.

Proof: These results are proved by straightforward adaptations of the methods in [Fr81]. QED

Let GRP be the space of groups whose domain is N or a finite subset of N. Then GRP is a low level Borel subspace of a natural Baire space.

Let F:GRP → GRP. An inclusion point for F is some G ∈ GRP such that F(G) is embeddable into G.

We say that F:GRP → GRP is isomorphic preserving if and only if for all G,H ∈ GRP, $G \approx H \to F(G) \approx F(H)$.

We write FGG for the subspace of finitely generated elements of GRP.

LEMMA 0.11D.3. Any two elements of FGG that agree on their intersection have a common extension in FGG.

Proof: This is by the free product construction. QED

Let FGG be the subspace consisting of the finitely generated G ∈ GRP.

THEOREM 0.11D.4. Every isomorphic preserving Borel function F:GRP → GRP has an inclusion point. This is provable in WZ_3 but not in Z_2. In fact, Z_2 does not even prove this for F:GRP → FGG. The same results hold for finitely Borel functions.

Proof: Let F be as given with Borel code u. Let M be a countable transitive model of a weak fragment of ZFC + V = L containing u. Then F will remain isomorphic preserving in M. Build a generic tower of finitely generated groups of length ω, using finite length towers of finitely generated groups as the forcing conditions (this will collapse ω_1 to ω). Let G be the union of the tower. Then F(G) is embeddable into G using Lemma 0.11D.3, and that the FGG of the generic extension is the same as the FGG of the ground model. The proof can be adapted to be formalized in WZ_3. For the final claim, let G ∈ GRP. Look at the union V of all Turing degrees associated with the finitely generated subgroups of G, and get a Turing degree that's missing, assuming that V is not a model of parameterless Z_2. Then output the H ∈ FGG associated with this Turing degree, as in [Fr07a]. The reduction of Z_2 to parameterless Z_2 is presented and used in [Fr81]. QED

THEOREM 0.11D.5. Let X be a Borel set of relational structures in a finite relational type with domain N or a finite subset of N. Suppose any two finitely generated substructures of any two respective elements of X that agree on their intersection have a common extension in X. Then every isomorphic preserving Borel function F:X → X has an inclusion point.

Proof: We have just isolated the essential feature needed to carry out the proof of Theorem 0.11D.4, which is Lemma 0.11D.3. QED

THEOREM 0.11D.6. Theorem 0.11D.5 is provable in WZ_3 but not in Z_2. The same holds for finitely Borel sets and functions.

Proof: By Theorem 0.11D.4 and the proof of Theorem 0.11D.5. QED

0.11E. Borel Squaring Theorem and Function Agreement.

We seek a one dimensional form of the results on $\mathfrak{R}^\infty$. Let K be the Cantor space $\{0,1\}^\infty$, indexed from 1. For x ∈ K, the "square" of x, written $x^{(2)}$, is given by

$$x^{(2)} = (x_1,x_4,x_9,x_{16},\ldots).$$

THEOREM 0.11E.1. Borel Squaring Theorem. Every shift invariant Borel F:K → K maps some argument into its "square". I.e., there exists x ∈ K such that $F(x) = x^{(2)}$. This is provable in WZ_3 but not in Z_2. The same results hold for finitely Borel F.

Proof: See [Fr83]. QED

In [Fr83], we went on to try to prove such a one dimensional theorem for the circle group S, where 2x on S replaces s(x) on K. Thus we say that F:S → S is doubling invariant if and only if for all x ∈ S, F(2x) = F(x).

But we were not able to find a nice function on S like "squaring" on K. However, we were able to find a continuous function on S that works.

THEOREM 0.11E.2. There is a continuous F:S → S which agrees somewhere with every doubling invariant Borel G:S → S. This is provable in WZ_3 but not in Z_2. The same results holds for finite Borel G.

Proof: See [Fr83]. QED

This opens up two closely related research topics:

Find a simple function that agrees somewhere with every function satisfying a given condition.

Find a function obeying a first given condition that agrees somewhere with every function satisfying a second given condition.

The results of section 0.11D can be put into the same form illustrated by Theorems 0.11E.1 and 0.11E.2, as follows.

THEOREM 0.11E.3. The first coordinate function from $\mathfrak{R}^\infty$ into $\mathfrak{R}$ agrees somewhere with every invariant Borel F:$\mathfrak{R}^\infty$ → $\mathfrak{R}$, in the various senses discussed in section 0.11D.

Proof: By [Fr81], [Fr83], and sometimes straightforward adaptation of the methods there. QED.

0.12. Incompleteness in Russell Type Theory and Zermelo Set Theory.

0.12A. Preliminaries.

By Russell's Type Theory, we will mean his impredicative theory (obtained from his predicative theory using his axiom of reducibility), with the ground type corresponding to N. This modern form, which we call RTT, uses infinitely many sorts N,PN,PPN,..., with 0,S,+,• operating at type N, and ∈ connecting each sort with the next. We use equality only at sort N. The axioms are as follows.

1. $Sx \neq 0$, $Sx = Sy \rightarrow x = y$, $x+0 = 0$, $x+Sy = S(x+y)$, $x \bullet 0 = 0$, $x \bullet Sy = x \bullet y + x$, where x,y have type N.
2. $0 \in A \wedge (\forall x)(x \in A \rightarrow Sx \in A) \rightarrow x \in A$, where x has type N and A has type PN.
3. $(\exists A)(\forall B)(B \in A \leftrightarrow \varphi)$, where φ is a formula of L(RTT), and A has type one higher than B.

The fragment involving only variables of the first n types, including N, is called Z_n, or n-th order arithmetic.

It proved quite awkward to formalize mathematics in RTT, even in its modern form. So it was supplanted by the single sorted system Z (Zermelo set theory), and later with Fraenkel's addition of Replacement, forming ZF. Still later, the axiom of choice became fully accepted, forming ZFC.

Z is a one sorted system with one binary relation symbol ∈, in first order predicate calculus with equality. The axioms of Z are as follows.

EXTENSIONALITY. $(\forall x)(x \in y \leftrightarrow x \in z) \rightarrow y = z$.
PAIRING. $(\exists x)(y \in x \wedge z \in x)$.
UNION. $(\exists x)(\forall y)(\forall z)(y \in z \wedge z \in w \rightarrow y \in x)$.
SEPARATION. $(\exists x)(\forall y)(y \in x \leftrightarrow y \in z \wedge \varphi)$, where x is not free in φ.
POWER SET. $(\exists x)(\forall y)((\forall z)(z \in y \rightarrow z \in w) \rightarrow y \in x)$.
INFINITY. $(\exists x)(\emptyset \in x \wedge (\forall y,z)(y \in x \wedge z \in x \rightarrow y \cup \{z\} \in x))$.

This modern version of Z differs from what Zermelo wrote in [Ze08]. There he included the Axiom of Choice, and also used this form of Infinity:

$$(\exists x)(\emptyset \in x \wedge (\forall y)(y \in x \rightarrow \{y\} \in x)).$$

In the case of ZF, this, and other reasonable formulations of Infinity such as the most common

$$(\exists x)(\emptyset \in x \wedge (\forall y)(y \in x \rightarrow y \cup \{y\} \in x))$$

are provably equivalent from the remaining axioms. This is not the case for Z - see [Math01], Concluding Remarks. However, it is known that the variants of Z determined by reasonable formulations of Infinity are mutually interpretable.

Note that this version of Z can prove $(\forall n < \omega)(V(\omega+n)$ exists), but cannot prove the existence of $V(\omega+\omega)$. The former is enough to prove the consistency of RTT (see below).

We write ZC for Z together with the axiom of choice:

CHOICE. If x is a set of pairwise disjoint nonempty sets, there is a set which has exactly one element in common with each of the elements of x.

It is natural to weaken Separation in Z, where only Δ_0 formulas are allowed. We refer to this as WZ, where W indicates "weak". This is also sometimes called MacLane set theory. We also consider WZC = WZ + AxC.

We also use $WZ(\Omega)$, which is WZ + "every well ordering of ω is isomorphic to an ordinal" + "for all countable ordinals α, $V(\alpha)$ exists".

The notions of ω model and β model are used for theories whose language extends that of Z_2, or the language of set theory. An ω model is a model where the internal natural numbers are standard. A β model is an ω model where if an internal binary relation on the internal natural numbers is, internally, a well ordering, then it is a well ordering.

THEOREM 0.12A.1. Z proves the existence of a countable β model of RTT and WZC. WZ is a conservative extension of RTT, in the sense that any theorem of WZ that is suitably typed, is also a theorem of RTT.

Proof: For the first claim, Z can develop truth for bounded formulas, construct the proper class of constructible elements of the proper class $V(\omega+\omega)$, and pass to the internally definable elements. This forms the required β model. The conservative extension result is most easily proved model theoretically, expanding any model of RTT to a model of WZ. QED

In this section, we prove a number of equivalences over ATR_0. Four main principles arise in this connection.

We make the following definition in ATR_0. Let (A,R) be a well ordering, A ⊆ N. A countable R model is a triple (B,S,rk), where

i. B ⊆ N, S ⊆ B^2, and rk:B → A is surjective.
ii. rk(x) ≤ u ↔ (∀y)(S(y,x) → rk(y) < u).
iii. If E ⊆ B is definable in (B,S) and u ∈ A, then there is a unique x ∈ B whose S predecessors are exactly the elements of E of rank < u.

Assume (A,R) has length > ω, and let (B,S,rk) be a countable R model. There is an obvious mapping from every n ∈ ω to a point n* in (B,S,rk) with rk(n*) = n. We say that (B,S,rk) encodes x ⊆ ω if and only if there exists u ∈ B such that x = {n: S(n*,u)}.

FRA (finite rank axiom). For each n < ω and x ⊆ ω, there is a countable ω+n model that encodes x.

BFRA (beta finite rank axiom). For each n < ω and x ⊆ ω, there is a countable ω+n model that encodes x, which is a β model.

CRA (countable rank axiom). For each well ordering (A,R), A ⊆ N, with a limit point, and x ⊆ ω, there is a countable R model that encodes x.

BCRA (beta countable rank axiom). For each well ordering (A,R), A ⊆ N, with a limit point, and x ⊆ ω, there is a countable R model that encodes x, which is a β model.

THEOREM 0.12A.2. BFRA is provable in Z. FRA is not provable in WZC. BCRA is provable in WZ(Ω). CRA is not provable in ZC. The following is provable in ATR_0. FRA is equivalent to (∀n)(∀x ⊆ ω)(Z_n has an ω model encoding x). BFRA is equivalent to (∀n)(∀x ⊆ ω)(Z_n has a β model encoding x). If CRA then ZC has a countable ω model encoding any given x ⊆ ω. If BCRA then ZC has a countable β model encoding any given x ⊆ ω.

Proof: For the first claim, fix n < ω and x ⊆ ω. Use a countable elementary substructure of the V(ω+n) of the constructible universe relative to x.

For the second claim, suppose that FRA is provable in WZC. By a model theoretic argument, FRA is provable in the fragment of WZC obtained by replacing the power set axiom with the existence of V(ω+n), for some fixed n. However, the consistency of that fragment is provable in FRA, violating Gödel's second incompleteness theorem.

For the third claim, let (A,R) and x be given, and use a countable elementary substructure of the V(α) of the constructible universe relative to x, where (A,R) has type α.

For the fourth claim, suppose CRA is provable in ZC. Apply CRA to a specific well ordering of type ω+ω. Then CRA proves the consistency of ZC, which contradicts second incompleteness.

For the fifth claim, countable ω models of Zn encoding x correspond to countable ω+n models encoding x.

For the sixth claim, countable β models of Zn encoding x correspond to countable ω+n models encoding x that are β models.

For the seventh and eighth claims, use (A,R) of type ω+ω. QED

Let φ be a sentence in the language of set theory. We want to define what we mean by "φ cannot be proved using a definite countable iteration of the power set operation". This issue was addressed in [Fr81], [Fr05], [Fr07a].

We define the system DCIPS (definite countable iterations of the power set) as follows. The language has only ∈ in logic with equality. The axioms of DCIPS are given as follows.

i. Every axiom of ZFC\P is an axiom of DCIPS.
ii. Suppose φ(x) is a Σ_1 formula of set theory with only the free variable shown, where ZFC\P proves (∃x)(φ(x) ∧ x is an ordinal). Then (∃x)(φ(x) ∧ V(x) exists) is an axiom of DCIPS.

We say that a sentence can be proved using a definite countable iteration of the power set operation if and only if it can be proved in DCIPS.

THEOREM 0.12A.3. ATR_0 + CRA proves the existence of an ω model of DCIPS. CRA is not provable in DCIPS.

Proof: It is clear that the second claim follows from the first. We work in ATR_0 + CRA.

By applying CRA to, say, $\omega+\omega$, we obtain a countable β model M of ZFC + V = L. Let S be the set of all sentences $(\exists x)(\varphi(x) \wedge x$ is an ordinal), with only the free variable x, where φ is Σ_1, that are provable in ZFC\P. Clearly all sentences in S hold in M.

Let λ be the height of M. Apply CRA to a well ordering of type $\lambda+\omega$, obtaining a suitable (B,R), B of type $\lambda+\omega$. Within (B,R), cut back to the inner model of constructible sets in the sense of (B,R). Thus M will correspond to the first λ levels of (B,R). Then for each sentence $(\exists x)(\varphi(x) \wedge x$ is an ordinal) in S, the corresponding sentence $(\exists x)(\varphi(x) \wedge V(x)$ exists) holds in (B,R), since the x can be taken to be an ordinal $< \lambda$.

(B,R) is not quite an ω model of DCIPS. We have only to extend (B,R) using the constructible hierarchy internally defined in (B,R). QED

So in particular, if a sentence in $L(Z_2)$ implies CRA over ATR_0, then that sentence "cannot be proved using a definite countable iteration of the power set operation".

0.12B. Borel Determinacy and Symmetric Borel Sets.

In [Fr71], we proved that Borel Determinacy is not provable in Z (or ZC). As was well known at the time, this can be strengthened to any "definite" countably transfinite iteration of the power set axiom. In [Fr71], we focused on the critical case of Z.

We also formulated the conjecture that Borel Determinacy could be proved in (a weak variant of) WZ + $(\forall\alpha < \omega_1)(V(\alpha)$ exists). Also, we recognized a problem with coming up with an appropriate proof theoretic formulation of "cannot be proved using any definite countable transfinite iteration". See the definition of DCIPS and Theorem 0.12A.3.

With the benefit of hindsight, we can place Borel Determinacy nicely in the realm of Reverse Mathematics.

THEOREM 0.12B.1. The following are provably equivalent in RCA_0.
i. Finitely Borel Determinacy.
ii. BFRA.
In particular, i) is provable in Z but not in WZC.

Proof: Assume i). First use Borel Determinacy for open sets to obtain ACA_0 and then ATR_0, as in [Si99,09]. Then argue as in [Fr71] for any given level $n < \omega$ of the Borel hierarchy. Build the ramified hierarchy of level n+5 as far as it goes, starting with x, using well orderings on ω, and use Σ^0_n determinacy with parameter x to show that the hierarchy must stop.

Assume ii). From the formulation using Tarski's satisfaction relation, ACA_0 is immediate. Now $\Pi^1_1\text{-}CA_0$ is immediate. By [Mart75], for each n, we have a proof that Σ^0_n sets are determined from Z_{n+c}, for some universal constant c. Let A be in Σ^0_n with code $u \subseteq \omega$, and let M be a β model of Z_{n+c} containing u. Then M satisfies that the Σ^0_n set with code u is determined. Since M is a β model, A is determined. QED

THEOREM 0.12B.2. The following are provably equivalent in RCA_0.
i. Borel Determinacy.
ii. BCRA.
In particular, i) is provable in $WZ(\Omega)$ but not provable in DCIPS.

Proof: A straightforward adaptation of the proof of Theorem 0.12B.1. Also uses Theorem 0.12A.3. QED

We now come to our method of converting Borel determinacy to a statement in classical analysis. In [Fr71], we presented the following asymmetric form:

For every Borel $Y \subseteq K \times K$,
either Y contains the graph of a
continuous function on K,
or the converse of Y is disjoint from
the graph of a continuous function on K.

In [Fr71], we claimed that the independence proofs work equally well for the above. The proof from Borel Determinacy is utterly straightforward, the winning strategy giving us the continuous function F.

Later we discovered that we can work with only symmetric Borel $Y \subseteq K\times K$, and still have the same independence results. Here a set of ordered pairs E is said to be symmetric if and only if for all $(x,y) \in E$, we have $(y,x) \in E$.

THEOREM 0.12B.3. The following are provably equivalent in ATR_0 (all forms).
i. Every symmetric finitely Borel set in $K\times K$ ($N^N\times N^N$) contains or is disjoint from the graph of a continuous (finitely Borel, Borel) function on K (N^N).
ii. Every symmetric finitely Borel set in $\Re\times\Re$ (I×I) contains or is disjoint from the graph of a left continuous (right continuous, finitely Borel, Borel) selection on $\Re$ (I).
iii. Finitely Borel Determinacy.
iv. BFRA.
In particular, i-iv are provable in Z but not in WZC.

THEOREM 0.12B.4. The following are provably equivalent in ATR_0 (all forms).
i. Every symmetric Borel set in $K\times K$ ($N^N\times N^N$) contains or is disjoint from the graph of a continuous (Borel) function on K (N^N).
ii. Every symmetric Borel set in $\Re\times\Re$ (I×I) contains or is disjoint from the graph of a left continuous (right continuous, finitely Borel, Borel) selection on $\Re$ (I).
iii. Borel Determinacy.
iv. BCRA.
In particular, i-iv are provable in WZ(Ω) but not in ZC.

We need to explain the choices allowed in Theorems 0.12B.3 and 0.12B.4. Note that in each of the two Theorems, we have the following items for making a choice:

$K\times K$ ($N^N\times N^N$)
continuous (finitely Borel, Borel)
K (N^N)

$\Re\times\Re$ (I×I)
left continuous (right continuous, finitely Borel, Borel)
$\Re$ (I)

Here is the list of choices that can be made:

$K\times K$; any of continuous, finitely Borel, Borel; K
$N^N x N^N$; any of continuous, finitely Borel, Borel; N^N

$\Re x \Re$; any of left continuous, right continuous, finitely Borel, Borel; either of $\Re$, I

Proof: The above two theorems are essentially proved in [Fr81]. QED

0.12C. Borel Selection.

The work in this section appears in [Fr05], and was inspired by [DS96], [DS99], [DS01], [DS04], and [DS07].

Let S be a set of ordered pairs and A be a set. Then f is a selection for S on A if and only if dom(f) = A and for all $x \in A$, $(x,f(x)) \in S$.

The following statement is well known to be refutable from ZFC + V = L, and relatively consistent with ZFC by a forcing argument.

DOM. $(\forall f \in N^N)(\exists g \in N^N)(\forall h \in N^N \cap L[f])$(g eventually strictly dominates h).

All of the statements considered here are local/global in the sense that if we have a continuous or Borel selection on every compact subset of E, then we have a continuous or Borel section on all of E.

We consider the following two Templates.

TEMPLATE A. Let $S \subseteq N^N \times N^N$ be Borel (finitely Borel). If there is a constant (continuous, finitely Borel, Borel) selection for S on every compact subset of N^∞, then there is a constant (continuous, finitely Borel, Borel) selection for S on N^N.

TEMPLATE B. Let $S \subseteq N^N \times N^N$ and $E \subseteq N^N$ be Borel (finitely Borel). If there is a constant (continuous, finitely Borel, Borel) selection for S on every compact subset of E, then there is a constant (continuous, finitely Borel, Borel) selection for S on E.

Note that Template A is just Template B for $E = N^N$.

The choices in these Templates are independent of each other. In other words, each Template has 32 instances - with two first options, four second options, and four third options.

THEOREM 0.12C.1. The following fourteen instances of Templates A,B are refutable in RCA_0:

i. Borel or finitely Borel, constant, constant.
ii. Borel or finitely Borel, continuous, constant.
iii. Borel or finitely Borel, finitely Borel, constant.
iv. Borel or finitely Borel, finitely Borel, continuous.
v. Borel or finitely Borel, Borel, constant.
vi. Borel or finitely Borel, Borel, continuous.
vii. Borel or finitely Borel, Borel, finitely Borel.

Proof: To refute i-iii,v, set $S(x,y) \leftrightarrow$ y everywhere dominates x. To refute iv,vi, let S be the graph of some $f:N^N \to N^N$ that is finitely Borel but not continuous. To refute vii), let S be the graph of some $f:N^N \to N^N$ that is Borel but not finitely Borel. QED

THEOREM 0.12C.2. The following eight instances below of Templates A,B are provable in Z but not in WZC.

finitely Borel, constant, continuous.
finitely Borel, constant, finitely Borel.
finitely Borel, constant, Borel.
finitely Borel, continuous, continuous.
finitely Borel, continuous, finitely Borel.
finitely Borel, continuous, Borel.
finitely Borel, finitely Borel, finitely Borel.
finitely Borel, finitely Borel, Borel.

Proof: In each case, the provability is implicit in [DS04], and reproved in [Fr05]. The unprovability is from [Fr05]. QED

THEOREM 0.12C.3. The following eight instances below of Templates A,B are provable in WZ(Ω), but are unprovable in DCIPS.

Borel, constant, continuous.
Borel, constant, finitely Borel.
Borel, constant, Borel.
Borel, continuous, continuous.
Borel, continuous, finitely Borel.
Borel, continuous, Borel.
Borel, finitely Borel, finitely Borel.
Borel, finitely Borel, Borel.

Proof: In each case, the provability is implicit in [DS04], and reproved in [Fr05]. The unprovability is from [Fr05]. QED

THEOREM 0.12C.4. The following two instances below of Templates A,B are provably equivalent, over ZFC, to DOM.

finitely Borel, Borel, Borel.
Borel, Borel, Borel.

Proof: The provability in ZFC + DOM for Templates A,B, is due to [DS07]. We prove DOM from these instances, for Templates A,B, over ZFC, in [Fr05]. We also give a proof of these instances from ZFC + DOM for Template A only, in [Fr05]. QED

We can use $\mathfrak{R}$ instead of the Baire space N^N as follows.

TEMPLATE A'. Let $S \subseteq \mathfrak{R} \times \mathfrak{R}$ be Borel (finitely Borel). If there is a constant (continuous, finitely Borel, Borel) selection for S on every compact set of irrationals, then there is a constant (continuous, finitely Borel, Borel) selection for S on the irrationals.

TEMPLATE B'. Let $S \subseteq \mathfrak{R} \times \mathfrak{R}$ and E be a Borel (finitely Borel) set of irrationals. If there is a constant (continuous, finitely Borel, Borel) selection for S on every compact subset of E, then there is a constant (continuous, finitely Borel, Borel) selection for S on the irrationals in E.

As in Templates A,B, the choices in these Templates are independent of each other. Thus each Template has 32 instances - with two first options, four second options, and four third options.

THEOREM 0.12C.1. The 32 instances of Template A and the corresponding instances of Template A' are respectively provably equivalent in ATR_0. The 32 instances of Template B and the corresponding instances of Template B' are respectively provably equivalent in ATR_0.

Proof: See [Fr05]. QED

The reason that we have run into independence from ZFC here is that in the

(finitely) Borel, Borel, Borel

instance of the Templates, the second Borel uses arbitrarily high levels of the Borel hierarchy. We regard this as just beyond the scope of Concrete Mathematical Incompleteness.

We also point out that these instances that are independent of ZFC, are Π^1_4, and since they are provably equivalent to DOM, they are refutable in ZFC + V = L. (V = L is Gödel's axiom of constructibility [Go38], [Je76,06]).

In sections 13 and 14, we will encounter Concrete Mathematical Incompleteness from ZFC. In section 13, the use of finitely Borel leads to independence from ZFC.

For all of our examples of Concrete Mathematical Incompleteness from ZFC, we have independence from ZFC + V = L. For all of our examples of Concrete Mathematical Incompleteness from fragments T of ZFC, we have independence from T + V = L, where V = L is the standard analog of the axiom of constructability adapted to T.

0.12D. Borel Inclusion with Equivalence Relations.

Let $E \subseteq \Re^2$ be a Borel equivalence relation with field $\Re$. There has been considerable work in descriptive set theory concerning the classification of Borel equivalence relations under the Borel reducibility notion that was introduced in [FSt89]. See, e.g., [Ke95], [BK96], [HK96], [HK97], [HKL98], [HK01].

We say that x,y are E equivalent if and only if E(x,y). We write E* for the equivalence relation on $\Re^\infty$ given by

E*(x,y) ↔ every coordinate of x is E equivalent to a coordinate of y, and vice versa.

We give two forms of Borel Inclusion for E.

i. Let $F:\Re^\infty \to \Re$ be Borel, where E* equivalent arguments are sent to E equivalent values. There exists $x \in \Re^\infty$ such that F(x) is E equivalent to a coordinate of x.
ii. Let $F:\Re^\infty \to \Re^\infty$ be Borel, where E* equivalent arguments are sent to E* equivalent values. There exists $x \in \Re^\infty$ such that every coordinate of F(x) is E equivalent to a coordinate of x.

THEOREM 0.12D.1. Both forms of Borel Inclusion for Borel equivalence relations hold.

Proof: The first claim is proved in [Fr81], p. 235. For the second claim, let $F:\mathfrak{R}^\infty \to \mathfrak{R}^\infty$ be Borel, where E* equivalent arguments are sent to E* equivalent values. Let $G:(\mathfrak{R}^\infty)^\infty \to \mathfrak{R}^\infty$ be defined for all $x \in (\mathfrak{R}^\infty)^\infty$ by

$$G(x) = F(x_{11},x_{12},x_{21},x_{13},x_{22},x_{31},\ldots).$$

We use E** for the Borel equivalence relation on $(\mathfrak{R}^\infty)^\infty$. given by

E**(x,y) ↔ every coordinate of x is E* equivalent to a coordinate of y, and vice versa.

We claim that G maps E** equivalent arguments to E* equivalent values. To see this, let $x,y \in (\mathfrak{R}^\infty)^\infty$ be E** equivalent. Then

$$(x_{11},x_{12},x_{21},x_{13},x_{22},x_{31},\ldots)$$
$$(y_{11},y_{12},y_{21},y_{13},y_{22},y_{31},\ldots)$$

are E* equivalent, and so their values under F are E* equivalent.

By the first claim, let G(x) be E* equivalent to x_i.

$F(x_{11},x_{12},x_{21},x_{13},x_{22},x_{31},\ldots)$ is E* equivalent to $(x_{i1},x_{i2},x_{i3},\ldots)$.

QED

THEOREM 0.12D.2. The following are provably equivalent in ATR_0.
i. Both forms of (finitely) Borel Inclusion for finitely Borel Equivalence Relations.
ii. FRA.
In particular, i) is provable in Z but not in WZC.

Proof: See [Fr81]. QED

THEOREM 0.12D.3. The following are provably equivalent in ATR_0.
i. Both forms of Borel Inclusion for Borel Equivalence Relations.
ii. CRA.
In particular, i) is provable in WZ(**Ω**) but not in DCIPS.

Proof: See [Fr81]. QED

In [Fr81], we go on to deal with Borel Inclusion for N^N under conjugation. I.e., $f \approx g \leftrightarrow (\exists h)(g = hgh^{-1})$. This is a complete analytic equivalence relation. We again obtain Theorems 0.12D.2, 0.12D.3 for this equivalence relation. Subsequently, we improved this to analytic equivalence relations.

THEOREM 0.12D.4. The following are provably equivalent in ATR_0.
i. Both forms of Borel Inclusion for Analytic Equivalence Relations, N^N under conjugation, graphs on N under isomorphism (a total of 6 forms).
ii. CRA.
In particular, each of the 6 forms of i) can be proved in $WZ(\Omega)$ but not in DCIPS.

Proof: For our proof of Borel Inclusion for Analytic Equivalence Relations, see [Sta85], p. 23. The second form is obtained from the first form as in the proof of Theorem 0.12D.1. QED

0.12E. Borel Functions on Linear orderings and Graphs.

The formulations in this section avoid infinite sequences, and attain the same level of strength as the statements in section 0.12D.

It is particularly convenient to think of countable linear orderings, up to isomorphism, as subsets of Q up to order isomorphism. Thus we have the nice Cantor space $\wp Q$ of subsets of Q. We say that $A,B \in \wp Q$ are isomorphic if and only if they are isomorphic as linearly ordered sets, in the induced order.

We say that $F:\wp Q \rightarrow \wp Q$ is isomorphic preserving if and only if isomorphic arguments are assigned isomorphic values.

Let $A_1,A_2,... \in \wp Q$. A dense mix is obtained by starting with Q, and replacing each point with some A_i, in such a way that for all i,j, strictly between any two copies of A_i, there is a copy of A_j. (We regard the A's as distinct for this purpose). Note that all dense mixes of $A_1,A_2,...$ are isomorphic.

THEOREM 0.12E.1. Every isomorphic preserving Borel F:℘Q → ℘Q sends some A to an isomorphic copy of an interval in A with endpoints in A.

Proof: See [Sta85], where the result is derived from Borel Inclusion for Analytic Equivalence Relations. The idea is as follows. Given F, define $G:(\wp Q)^\infty \to \wp Q$ by $G(A_1,A_2,...) = F(B)$, where $B \in \wp Q$ is a canonically constructed dense mix of $A_1',A_2',...$, where each A_i' is the result of adding a left and right endpoint to A_i.

Now apply Borel inclusion for Analytic Equivalence Relations to G, and take the dense mix of the coordinates of the infinite sequence from ℘Q, after adding endpoints to these coordinates. QED

Let GPH be the space of all graphs whose vertex set is N or a finite subset of N. Here graphs are viewed as irreflexive symmetric relations on their vertex set.

We say that F:GPH → GPH is isomorphic preserving if and only if isomorphic arguments have isomorphic values (via ordinary graph isomorphism).

Let CGPH be the subspace of all connected graphs.

THEOREM 0.12E.2. Every isomorphic preserving Borel F:GPH → CGPH maps some G to an isomorphic copy of a connected component of G.

Proof: Let F be as given, and define $H:CGPH^\infty \to CGPH$ by $H(G_1,G_2,...) = F(G^*)$, where G* is the disjoint union of the G's. Apply Borel inclusion for Analytic Equivalence Relations to H, and take the disjoint union of the infinite sequence from GPH. Thus we have G' such that F(G') is isomorphic to one of the terms in the disjoint union representation of G'. I.e., F(G') is isomorphic to a connected component of G'. QED

THEOREM 0.12E.3. The following are provably equivalent in ATR_0.
i. Every isomorphic preserving Borel F:℘Q → ℘Q maps some A to an isomorphic copy of an interval in A (with endpoints in A).
ii. Every isomorphic preserving Borel F:GPH → CGPH maps some G to an isomorphic copy of a connected component of G.
iii. CRA.

In particular, i),ii) can be proved in WZ(Ω) but not in DCIPS.

Proof: For iii → i,ii, use Theorem 0.12D.3, and the proofs of Theorems 0.12E.1, and 0.12E.2. For i → ii, see [Sta85], p. 31. For ii → iii, use a similar coding mechanism that associates hereditarily countable sets of a given countable rank or less, to connected graphs. QED

0.12F. Borel Functions on Borel Quasi Orders.

We say that $(\mathfrak{R},\leq)$ is a quasi order if and only if ≤ is transitive and reflexive. We write a ≅ b if and only if (a ≤ b ∧ b ≤ a), a < b if and only if a ≤ b ∧ ¬b ≤ a.

We say that $(\mathfrak{R},\leq)$ is ω-closed if every strictly increasing sequence from X has a (unique up to ≅) least upper bound, and ω-complete if and only if every countable set has a least upper bound.

We say that $F:\mathfrak{R} \to \mathfrak{R}$ is invariant if and only if a ≅ b → F(a) ≅ F(b). A fixed point for F is an x such that F(x) ≅ x.

The following three Theorems are proved in [Fr81] using Borel determinacy.

THEOREM 0.12F.1. Let $(\mathfrak{R},\leq)$ be an ω-closed (ω-complete) Borel quasi order. Let $F:\mathfrak{R} \to \mathfrak{R}$ be an invariant Borel function such that for all x, F(x) ≥ x. Then F has a fixed point.

THEOREM 0.12F.2. Let $(\mathfrak{R},\leq)$ be an ω-closed (ω-complete) Borel quasi order. Then there is no invariant Borel function such that for all x, F(x) > x.

THEOREM 0.12F.3. Let $(\mathfrak{R},\leq)$ be an ω-complete Borel quasi order. Let $F:\mathfrak{R} \to \mathfrak{R}$ be an invariant Borel function. Then for some x, F(x) ≤ x.

THEOREM 0.12F.4. The following is provable in ATR_0. BCRA → Theorems 0.12F.1 - 0.12F.3 → CRA. In particular, Theorems 0.12F.1 - 0.12F.3 are provable in WZ(Ω) but not in DCIPS.

Proof: This is proved in [Fr81]. QED

Note that the definitions of ω-closed and ω-complete are Π^1_3. In [Fr81], we strengthen these two notions to explicitly ω-closed and explicitly ω-complete, by requiring that there be a Borel witness function giving a least upper bound.

THEOREM 0.12F.5. The following are provably equivalent in ATR_0.
i. Theorems 0.12F.1 - 0.12F.3 with explicitly ω-closed and ω-complete.
ii. CRA.
In particular, i) is provable in WZ(**Ω**) but not in DCIPS.

Proof: This is proved in [Fr81]. QED

0.12G. Countable Borel Equivalence Relations and Quasi Orders.

In this section, we consider Borel equivalence relations E on $\mathfrak{R}^n$. We say that $A \subseteq \mathfrak{R}^n$ is E invariant if and only if $E(x,y) \rightarrow (x \in A \leftrightarrow y \in A)$. We say that $f:\mathfrak{R}^n \rightarrow \mathfrak{R}$ is E invariant if and only if $E(x,y) \rightarrow f(x) = f(y)$.

Let $x_1,x_2,\ldots$ be a sequence of real numbers that converges absolutely. We write $SUM(x_1,x_2,\ldots)$ for the set of all sums of one or more of the x's, without repetition of subscripts. We make this definition only if the x's converge absolutely.

We say that a Borel equivalence relation E on $\mathfrak{R}$ has the (finitely) Borel translation property if and only if every E invariant (finitely) Borel set contains or is disjoint from some translate of $SUM(4^{-1},4^{-2},\ldots)$.

We now present a stronger property.

We say that a Borel equivalence relation E on $\mathfrak{R}$ has the strong (finitely) Borel translation property if and only if every E invariant (finitely) Borel $F:\mathfrak{R} \rightarrow \mathfrak{R}$ is constant on some translate of $SUM(4^{-1},4^{-2},\ldots)$.

THEOREM 0.12G.1. $\{(x,y): x,y \in \mathfrak{R} \wedge x = y\}$ does not satisfy the finitely Borel translation property.

Proof: In [Fr07a], Lemma 2.2, we showed how to construct elements of each $SUM(4^{-1},4^{-2},\ldots)+x$ from which we can reconstruct x. Let A be the set of all reals so constructed. Then obviously A meets every translate of $SUM(4^{-1},4^{-2},\ldots)$. Also every $y \in A$ lies in exactly one $SUM(4^{-1},4^{-2},\ldots)+x$.

Suppose A contains SUM($4^{-1},4^{-2}$,...)+x. Then Let s,t be distinct elements of SUM($4^{-1},4^{-2}$,...). Then s+x,t+x ∈ A. Hence s+(x+t-s) ∈ A. Therefore s+x lies in SUM($4^{-1},4^{-2}$,...)+x and SUM($4^{-1},4^{-2}$,...)+x+t-s. Thus some element of A lies in more than one translate of SUM($4^{-1},4^{-2}$,...). This is a contradiction.

Clearly A neither contains nor is disjoint from some translate of SUM($4^{-1},4^{-2}$,...). It is easily seen that A is finitely Borel by its construction. QED

THEOREM 0.12G.2. There is a countable finitely Borel equivalence relation on $\Re$ with the strong Borel translation property. Turing equivalence has the strong Borel summation property.

Proof: This is proved in [Fr07a], Theorem 2.6. QED

THEOREM 0.12G.3. The following are equivalent over ATR_0.
i. There is a countable (finitely) Borel equivalence relation on $\Re$ with the finitely Borel translation property.
ii. There is a countable (finitely) Borel equivalence relation on $\Re$ with the strong finitely Borel translation property.
iii. BFRA.
In particular, i,ii are provable in Z but not in WZC.

Proof: This is proved in [Fr07a], Theorems 2.9, 2.11. QED

THEOREM 0.12G.4. The following are equivalent over ATR_0.
i. There is a countable (finitely) Borel equivalence relation on $\Re$ with the Borel translation property.
ii. There is a countable (finitely) Borel equivalence relation on $\Re$ with the strong Borel translation property.
iii. BCRA.
In particular, i) is provable in WZ(Ω) but not in DCIPS.

Proof: This is proved in [Fr07a], Theorems 2.9, 2.11. QED

It is clear that if a countable Borel equivalence relation on $\Re$ has the Borel translation property, then any more inclusive countable Borel equivalence relation on $\Re$ also has the Borel translation property. In fact, in [Fr07a], we assert that all sufficiently inclusive countable Borel equivalence relations on $\Re$ have the (strong) Borel translation property.

So there remains the unanswered question of how to describe the threshold, whereby the (strong) Borel translation property kicks in.

What about Lebesgue or Baire measurable functions? Then the (finitely) Borel translation property is impossible.

THEOREM 0.12G.5. There is no countable Borel equivalence relation on $\Re$, where every E invariant set of measure 0 (or meager) contains or is disjoint from some translate of SUM(4^{-1},4^{-2},4^{-3},...).

Proof: This is proved in [Fr07a}, Theorem 2.12. QED

In higher dimensions, these results take on a more geometric meaning. A curve is a homeomorphic image of [0,1] in $\Re^n$.

We say that a Borel equivalence relation E on $\Re^2$ has the (finitely) Borel line, curve, vertical line, horizontal line, circle about the origin, property if and only if every invariant (finitely) Borel set contains or is disjoint from a line, curve, vertical line, horizontal line, circle about the origin.

We now present a stronger property.

We say that a Borel equivalence relation E on $\Re^2$ has the (finitely) Borel line, curve, vertical line, horizontal line, circle about the origin, property if and only if every invariant (finitely) Borel $F:\Re^2 \to \Re$ is constant on a line, curve, vertical line, horizontal line, circle about the origin.

THEOREM 0.12G.6. There is a countable finitely Borel equivalence relation on $\Re^2$, with the strong Borel vertical line, horizontal line, circle about the origin, property.

Proof: This is proved in [Fr07a], Theorem 3.1, using Borel Turing degree determinacy. QED

Once again, there is the unanswered question of the threshold, since evidently all sufficiently inclusive countable (finitely) Borel equivalence relations on $\Re^2$ have these properties.

THEOREM 0.12G.7. The following are provably equivalent in ATR_0.
i. There is a countable (finitely) Borel equivalence relation on $\Re^2$ with the finitely Borel line, curve, vertical line, horizontal line, circle about the origin, property.
ii. There is a countable (finitely) Borel equivalence relation on $\Re^2$ with the strong finitely Borel line, curve, vertical line, horizontal line, circle about the origin, property.
iii. BFRA.
In particular, i),ii) can be proved in Z but not in WZC.

Proof: This is implicit in [Fr07a]. QED

THEOREM 0.12G.8. The following are provably equivalent in ATR_0.
i. There is a countable (finitely) Borel equivalence relation on $\Re^2$ with the Borel line, curve, vertical line, horizontal line, circle about the origin, property.
ii. There is a countable (finitely) Borel equivalence relation on $\Re^2$ with the strong Borel line, curve, vertical line, horizontal line, circle about the origin, property.
iii. BCRA.
In particular, i-iii can be proved in $Z(\Omega)$ but not in DCIPS.

Proof: This is proved in [Fr07a]. QED

We say that $(\Re,\leq)$ is a quasi order if and only if $\leq$ is reflexive and transitive on X. We define $x \equiv y \leftrightarrow x \leq y \wedge y \leq x$. We say that $(\Re,\leq)$ is an ω_1 like quasi order if and only if $(X,\leq)$ is a quasi order where each $\{y: y \leq x\}$ is countable.

We say that $B \subseteq \Re$ is invariant if and only if $x \equiv y \rightarrow (x \in B \leftrightarrow y \in B)$. We say that $F:\Re \rightarrow \Re$ is invariant if and only if $x \equiv y \rightarrow f(x) = f(y)$.

A cone in $(\Re,\leq)$ is a set of the form $\{y: x \leq y\}$, $x \in \Re$.

We say that a Borel quasi order $\leq$ on $\Re$ has the (finitely) Borel cone property if and only if every invariant (finitely) Borel set A contains or is disjoint from a cone.

We say that a Borel quasi order $\leq$ on $\Re$ has the strong (finitely) Borel cone property if and only if every invariant (finitely) Borel $F:\Re \rightarrow \Re$ is constant on a cone.

THEOREM 12G.9. There is a countable finitely Borel quasi order $\leq$ on $\mathfrak{R}$ with the strong Borel cone property.

Proof: This is proved in [Fr07a]. Turing reducibility, $\leq_T$, has the strong Borel cone property. QED

THEOREM 0.12G.10. The following are provably equivalent in ATR_0.
i. There is a countable (finitely) Borel quasi order on $\mathfrak{R}$ with the finitely Borel cone property.
ii. There is a countable (finitely) Borel quasi order on $\mathfrak{R}$ with the strong finitely Borel cone property.
iii. BFRA.
In particular, i),ii) are provable in Z but not in WZC.

Proof: This is implicit in [Fr07a]. QED

THEOREM 0.12G.11. The following are provably equivalent in ATR_0.
i. There is a countable (finitely) Borel quasi order on $\mathfrak{R}$ with the Borel cone property.
ii. There is a countable (finitely) Borel quasi order on $\mathfrak{R}$ with the strong Borel cone property.
iii. BCRA.
In particular, i),ii) are provable in $Z(\Omega)$ but not in DCIPS.

Proof: This is proved in [Fr07a]. QED

Let $\leq$ be a quasi order on $\mathfrak{R}$. We say $F:\mathfrak{R}^\infty \to \mathfrak{R}$ is left/right invariant if and only if for all $x,y \in \mathfrak{R}^\infty$, if x,y are coordinatewise $\approx$, then $F(x) \approx F(y)$.

THEOREM 0.12G.12. There is a countable finitely Borel quasi order $\leq$ on $\mathfrak{R}$ such that the following holds. For all left/right invariant Borel $F:\mathfrak{R}^\infty \to \mathfrak{R}$, there exists $x \in \mathfrak{R}^\infty$ and $n < \omega$ such that $F(x) \leq x_n$.

Proof: We established in [Sta85], using Turing degrees. The proof lies in ZF\P + $V(\omega+\omega)$ exists. QED

THEOREM 0.12G.13. Theorem 0.12G.12 is provable in ZF\P + $V(\omega+\omega)$. Theorem 0.12G.12 is not provable in ZC, even for Borel $\leq$ and finitely Borel F.

Which countable Borel quasi orders have the (strong) Borel cone property? $\{(x,y): x,y \in \Re \wedge y-x \in N\}$ does not have the finitely Borel cone property, using the invariant set $\{x \in \Re$: the integer part of x is even$\}$. What can we say about the threshold?

We have recently discovered a kind of universality condition on a countable Borel quasi order $\leq$ on 2^N that is sufficient for the strong Borel cone property.

Let $\leq$ be a Borel quasi order on 2^N. We say that $\leq$ is continuously full if and only if for all continuous $F:2^N \to 2^N$, there is a cone C in $\leq$ such that $(\forall x \in C)(F(x) \leq x)$.

We say that $\leq$ is strongly continuously full if and only if for all continuous $F_i:2^N \to 2^N$, $i \geq 1$, there is a cone C in $\leq$ such that $(\forall x \in C)(\forall i \geq 1)(F_i(x) \leq x)$.

We now formulate the Borel cone property, and the strong Borel cone property for $\leq$, using 2^N everywhere instead of $\Re$.

THEOREM 0.12G.14. There is a finitely Borel quasi order on 2^N which is strongly continuously full. In fact, $\leq_T$ on 2^N is strongly continuously full.

Proof: Let $F_i:2^N \to 2^N$ be continuous, $i \geq 1$. Let $u_i \in 2^N$ appropriately code F_i, respectively. Let u be the join of the u_i, $i \geq 1$. Let C be the cone in $\leq_T$ with base u. We have only to verify that $v \geq_T u \to F_i(v) \leq_T v$. This is clear. QED

THEOREM 0.12G.15. Every continuously full Borel quasi order on 2^N has the Borel cone property.

Proof: Let $\leq$ be a continuously full Borel quasi order on 2^N. Let $A \subseteq 2^N$ be Borel and $\leq$ invariant.

I,II play a game, with outcomes $x,y \in 2^N$. II wins if and only if $x \notin A \vee (\neg y < x \wedge y \notin A)$.

A winning strategy H is a continuous function from 2^N into 2^N, with the identity function as a modulus of continuity. By continuous fullness, let u be the base of a cone C where $x \in C \to H(x) \leq x$.

case 1. I wins. If II plays $y \in C\backslash A$ then I plays $H(y) \leq y$, and we have $H(y) \in A$, $\neg(\neg y < H(y) \wedge y \notin A)$, which is a contradiction. Hence A contains the cone C.

case 2. II wins. If I plays $x \in C \cap A$ then II plays $H(x) \leq x$, and we have $\neg H(x) < x$, $H(x) \notin A$, $H(x) \equiv x$, $H(x) \in A$, which is a contradiction. Hence A is disjoint from the cone C.

QED

LEMMA 0.12G.16. In every strongly continuously full Borel quasi order on 2^N, every infinite sequence has an upper bound ($\geq$).

Proof: Let $x_1,x_2,\ldots$. Use the sequence of continuous functions which are constantly $x_1,x_2,\ldots$. QED

THEOREM 0.12G.17. Every strongly continuously full Borel quasi order on 2^N has the strong Borel cone property.

Proof: Apply Lemma 0.12G.16 to the bases of the cones given by Theorem 0.12G.15. QED

THEOREM 0.12G.18. The following are provably equivalent in ATR_0.
i. Every continuously full finitely Borel quasi order on 2^N has the finitely Borel cone property.
ii. Every strongly continuously full finitely Borel quasi order on 2^N has the strong finitely Borel cone property.
iii. BFRA.
In particular, i,ii are provable in Z but not in WZC.

Proof: From the above, and the metamathematics of Borel determinacy and Borel Turing degree determinacy. QED

THEOREM 0.12G.19. The following are provably equivalent in ATR_0.
i. Every continuously full (finitely) Borel quasi order on 2^N has the Borel cone property.
ii. Every strongly continuously full (finitely) Borel quasi order on 2^N has the strong Borel cone property.
iii. BCRA.
In particular, i,ii are provable in $Z(\Omega)$ but not in DCIPS.

Proof: From the above, and the metamathematics of Borel determinacy and Borel Turing degree determinacy. QED

0.12H. Borel Sets and Functions in Groups.

As in section 0.11D, we define GRP as the space of groups whose domain is N or a finite subset of N. We let FGG be the subspace of GRP consisting of the finitely generated elements of GRP.

We say that F:GRP → $\mathfrak{R}$ is isomorphically invariant if and only if for all G,H ∈ GRP, if G,H are isomorphic then F(G) = F(H).

We say that A ⊆ GRP is unbounded if and only if every G ∈ GRP is embeddable in an element of A.

THEOREM 0.12H.1. Every isomorphically invariant finitely Borel function F:FGG → $\mathfrak{R}$ is constant on an unbounded Borel subset of FGG of finite rank. In fact, Borel rank ≤ 4 suffices.

Proof: This is proved in [Fr07a], Theorem 5.4. The exact rank needed depends on the exact setup of FGG as a Borel space. Here 4 is a crude upper bound that works for even naïve setups. QED

THEOREM 0.12H.2. Every isomorphically invariant Borel subset of FGG contains or is disjoint from an unbounded Borel set of finite Borel rank. In fact, Borel rank ≤ 4 suffices.

Proof: Immediate from Theorem 0.12H.1. QED

THEOREM 0.12H.3. Theorem 0.12H.1 is provable in Z but not in WZC. Theorem 12H.2 is provable in Z(Ω) but not using any countable iteration of the power set operation.

Proof: See [Fr07a]. QED

We now consider Borel F:FGG$^\infty$ → FGG. We say that F is isomorphic preserving if and only if for all α,β ∈ FGG$^\infty$, if α,β are coordinatewise isomorphic, then F(α),F(β) are isomorphic.

THEOREM 0.12H.4. For all isomorphic preserving Borel F:FGG$^\infty$ → FGG, there exists α ∈ FGG$^\infty$ such that F(α) is embeddable in a coordinate of α.

Proof: See [Sta85], p. 35. QED

We consider Borel F:FGG$^\infty$ → GRP. We say that F is isomorphic preserving if and only if for all α,β ∈ FGG$^\infty$, if α,β are coordinatewise isomorphic, then F(α),F(β) are isomorphic.

THEROEM 0.12H.5. For all isomorphic preserving Borel $F:FGG^\infty \to GRP$, there exists $\alpha \in FGG^\infty$ such that $F(\alpha)$ is embeddable in some direct limit of $\alpha_1,\alpha_2,\ldots$.

Proof: Implicit in [Sta85]. QED

THEOREM 0.12H.6. Theorems 0.12H.4 and 0.12H.5 are provable in ZFC\P + "$V(\omega+\omega)$ exists" but not in ZC. Theorems 0.12H.4 and 0.12H.5 for finitely Borel F are not provable in ZC.

Proof: Implicit in [Sta85]. QED

0.13. Incompleteness in ZFC using Borel Functions.

0.13A. Preliminaries.
0.13B. Borel Ramsey Theory.
0.13C. Borel Functions on Groups.
0.13D. Borel Functions on Borel Quasi Orders.
0.13E. Borel Functions on Countable Sets.

0.13A. Preliminaries.

ZF is the following well known axiom system with one binary relation symbol $\in$, in one sorted first order predicate calculus with equality.

EXTENSIONALITY. $(\forall x)(x \in y \leftrightarrow x \in z) \to y = z$.
PAIRING. $(\exists x)(y \in x \wedge z \in x)$.
UNION. $(\exists x)(\forall y)(\forall z)(y \in z \wedge z \in w \to y \in x)$.
SEPARATION. $(\exists x)(\forall y)(y \in x \leftrightarrow y \in z \wedge \varphi)$, where x is not free in φ.
POWER SET. $(\exists x)(\forall y)((\forall z)(z \in y \to z \in w) \to z \in x)$.
INFINITY. $(\exists x)(\emptyset \in x \wedge (\forall y)(y \in x \to y \cup \{y\} \in x))$.
FOUNDATION. $y \in x \to (\exists y)(y \in x \wedge (\forall z)(\neg(z \in x \wedge z \in y)))$.
REPLACEMENT. $(\forall x)(x \in u \to (\exists! y)(\varphi)) \to (\exists z)(\forall x)(x \in u \to (\exists y \in z)(\varphi))$, where $\varphi \in L(\in)$, and z is not free in φ.

ZFC is ZF together with

CHOICE. If x is a set of pairwise disjoint nonempty sets, there is a set which has exactly one element in common with each of the elements of x.

As discussed in section 0.3, we sharply distinguish typical statements in set theory from statements involving at most finitely Borel sets and functions on complete separable metric spaces. In this section we will consider only Concrete Mathematical Incompleteness involving finitely

Borel sets and functions on complete separable metric spaces.

Recall that we have already presented the following Mathematical Incompleteness from ZFC in section 0.12C, using Borel sets.

FROM TEMPLATE A. Let $S \subseteq N^N \times N^N$ be (finitely) Borel. If there is a Borel selection for S on every compact subset of E, then there is a Borel selection for S on E.

FROM TEMPLATE B. Let $S \subseteq N^N \times N^N$ and $E \subseteq N^N$ be (finitely) Borel. If there is a Borel selection for S on every compact subset of E, then there is a Borel selection for S on E.

We don't classify these as Concrete Mathematical Incompleteness, as it is not confined to finitely Borel sets. See the last four paragraphs of section 0.12C.

In section 0.12C, we also discussed the versions with N^N replaced by $\Re$, above.

The Concrete Mathematical Incompleteness in this section overshoots ZFC considerably.

In section 0.13B, we use strongly Mahlo cardinals of finite order. These also represent the level associated with the Exotic Case which preoccupies Chapters 4-6 of this book. The Mahlo cardinals of finite order are defined in section 0.14A.

In sections 0.13C and 0.13D, we use the much stronger large cardinal hypotheses asserting the existence of Ramsey cardinals and measurable cardinals. Yet stronger large cardinal hypotheses are used in section 0.13E.

A Ramsey cardinal is a cardinal κ with the partition property $\kappa \rightarrow \kappa^{<\omega}{}_2$, which asserts the following. If we partition the nonempty finite sequences from κ into 2 pieces, then there exists $A \subseteq \kappa$ of cardinality κ such that for all $1 \leq n < \omega$, all of the n-tuples from κ lie in the same piece.

A measurable cardinal is an uncountable cardinal κ such that there is a {0,1} valued measure μ on $\wp(\kappa)$ which is $<\kappa$ additive, $\mu(\kappa) = 1$, and each $\mu(\{\alpha\}) = 0$.

It is well known that the first measurable cardinal (if it exists) is much larger than the first Ramsey cardinal. See, e.g., [Ka94], p. 83, and [Je78], p. 328.

In section 0.13E, we will use the yet much stronger Woodin cardinals. The notion of Woodin cardinal is a specialized notion that matches up exactly with determinacy (corresponding to infinitely many Woodin cardinals); see [MS89], [KW∞].

A Woodin cardinal is a cardinal κ such that for any $f:\kappa \to \kappa$, there exists an elementary embedding $j:V \to M$, M transitive, with critical point $\alpha < \kappa$ such that $f[\alpha] \subseteq \alpha$ and $V_{j(f)(\alpha)} \subseteq M$.

A Woodin cardinal is a weakening of the more natural notion of superstrong cardinal: there exists an elementary embedding $j:V \to M$, M transitive, with critical point κ such that $V_{j(\kappa)} \subseteq M$. See [Ka94], p. 361. Every superstrong cardinal is a Woodin cardinal, but not vice versa (assuming there is a Woodin cardinal).

A Woodin cardinal is also a strengthening of the specialized notion of strong cardinal, in terms of consistency strength. We refer the reader to [Ka94], p. 358, for its definition.

Our first Concrete Mathematical Incompleteness from ZFC was Borel Ramsey Theory, involving (finitely) Borel functions on $\mathfrak{R}^\infty$. We have already encountered such functions in section 0.11C.

Later, we discovered statements involving Borel functions from infinite sequences of Turing degrees into Turing degrees, which can be proved using a measurable cardinal but not a Ramsey cardinal. An account of this work appears in [Sta85].

Still later, we converted the Turing degrees into finitely generated groups (FGG), and more recently, points in countable Borel quasi orders. See sections 0.13C and 0.13D. The extensions involving (finitely) Borel functions on countable sets discussed in section 0.13E are the strongest of all - reaching the level of multiple Woodin cardinals.

0.13B. Borel Ramsey Theory.

Recall the Borel Ramsey Theorem (otherwise known as the Galvin/Prikry theorem) discussed in section 0.10D. This combines Borel measurability with Ramsey theory.

We discovered yet more powerful combinations of Borel measurability with Ramsey theory, that go beyond ZFC.

For this development, we use the infinite product space $\mathfrak{R}^\infty$, which is a complete separable metric space in the natural way. We write $x \sim y \leftrightarrow x,y \in \mathfrak{R}^\infty \wedge y$ is a permutation of x.

PROPOSITION 0.13B.1. Let $F:\mathfrak{R}^\infty \times (\mathfrak{R}^\infty)^n \to \mathfrak{R}$ be a (finitely) Borel function such that if $x \in \mathfrak{R}^\infty$, $y,z \in (\mathfrak{R}^\infty)^n$, and $y \sim z$, then $F(x,y) = F(x,z)$. Then there is a sequence $\{x_k\}$ from $\mathfrak{R}^\infty$ of length $m \leq \omega$ such that for all indices $s < t_1 < \ldots < t_n \leq m$, $F(x_s,x_{t\_1},\ldots,x_{t\_n})$ is the first coordinate of x_{s+1}.

THEOREM 0.13B.2. Proposition 0.13B.1 for Borel functions is provable in ZFC + $(\forall n)\exists\kappa)(\kappa$ is strongly n-Mahlo). However, for all n, ZFC + $(\exists\kappa)(\kappa$ is strongly n-Mahlo) + V = L does not prove Proposition 0.13B.1 for finitely Borel functions, using $m < \omega$ (instead of $m \leq \omega$). ZFC + V = L does not prove Proposition 0.13B.1 for n = 4 and finitely Borel functions, using $m < \omega$ (instead of $m \leq \omega$).

Proof: This is proved in [Fr01], section 5. QED

In [Fr01], Proposition 0.13B.1 is couched in terms of the Hilbert cube I^∞, which is, of course, equivalent to $\mathfrak{R}^\infty$ for present purposes.

In [Ka89], a more refined analysis of Proposition 0.13B.1 is presented. In [Ka91], a strengthening of Proposition 0.13B.1 that corresponds to the subtle cardinal hierarchy is presented. The subtle cardinal hierarchy is presented in section 0.14A.

0.13C. Borel Functions on Borel Quasi Orders.

Let $\leq$ be a quasi order on $\mathfrak{R}$. We say that $F:\mathfrak{R}^\infty \to \mathfrak{R}$ is $\approx$ preserving if and only if for all $x,y \in \mathfrak{R}^\infty$, if x,y are coordinatewise $\approx$, then $F(x) \approx F(y)$.

Recall that a quasi order is said to be countable if and only if the set of predecessors of any point is countable.

A finite deletion subsequence is a subsequence obtained by deleting finitely many terms.

PROPOSITION 0.13C.1. There is a countable (finitely) Borel quasi order $\leq$ on $\mathfrak{R}$ such that the following holds. For all $\approx$ preserving (finitely) Borel $F:\mathfrak{R}^\infty \to \mathfrak{R}$, there exists $x \in \mathfrak{R}^\infty$ such that for all infinite subsequences y of x, there exists n such that $F(y) \leq x_n$.

PROPOSITION 0.13C.2. There is a countable (finitely) Borel quasi order $\leq$ on $\mathfrak{R}$ such that the following holds. For all $\approx$ preserving (finitely) Borel $F:\mathfrak{R}^\infty \to \mathfrak{R}$, there exists $x \in \mathfrak{R}^\infty$ and $n < \omega$ such that for all infinite (finite deletion) subsequences y of x, $F(y) \leq y_n$.

THEOREM 0.13C.3. All forms of Proposition 0.13C.1 and 0.13C.2 are provable in ZFC + "there exists a measurable cardinal" but not in ZFC + "there exists a Ramsey cardinal". The same holds for their relativizations to the constructible universe, L, or even to the sets recursive in the first ω hyperjumps of $\emptyset$.

Proof: We originally proved this with "there exists a Ramsey cardinal" replaced by "$(\forall x \subseteq \omega)(x\#$ exists)", at least breaking the constructibility barrier in large cardinals (see [Sta85]). However our arguments can be combined with the inner model theory of large cardinals below a measurable cardinal - as was first observed by R. Solovay (private communication and lectures). QED

PROPOSITION 0.13C.4. There is a countable (finitely) Borel quasi order $\leq$ on $\mathfrak{R}$ such that the following holds. For all $\approx$ preserving (finitely) Borel $F:\mathfrak{R}^{\omega+\omega} \to \mathfrak{R}$, there exists $x \in \mathfrak{R}^{\omega+\omega}$ and $\alpha < \omega+\omega$ such that for all finite deletion subsequences y of x, $F(y) \leq y_\alpha$.

THEOREM 0.13C.5. All forms of Proposition 0.13C.4 are provable in ZFC + "there exists a strong cardinal", but not in ZFC + "there exists arbitrarily large measurable cardinals". The same holds for their relativizations to the constructible universe, L, or even to the sets recursive in the first ω hyperjumps of $\emptyset$.

Proof: This also combines work of ours reported in [Sta85] with the inner model theory of "strongly" measurable cardinals. QED

0.13D. Borel Functions on Groups.

This section is basically a reworking of section 0.13C using the space FGG of finitely generated groups. However, there are some additional statements involving the space GRP of all countable groups. Recall that we have already introduced these spaces in section 0.12H.

We say that x in GRP^∞ is towered if and only if for all n, x_n is a subgroup of x_{n+1}.

We say that $F:FGG^\infty \to GRP$ is isomorphic preserving if and only if for all $x,y \in \mathfrak{R}^\infty$, if x,y are coordinatewise isomorphic, then F(x),F(y) are isomorphic.

PROPOSITION 0.13D.1. For all isomorphic preserving (finitely) Borel $F:FGG^\infty \to GRP$, ($F:FGG^\infty \to FGG$), there exists towered $x \in FGG^\infty$ such that for all infinite subsequences y of x, F(y) is embeddable in $\cup_n x_n$.

PROPOSITION 0.13D.2. For all isomorphic preserving (finitely) Borel $F:FGG^\infty \to FGG$, there exists $x \in FGG^\infty$ and $n < \omega$ such that for all infinite (finite deletion) subsequences y of x, F(y) is embeddable in y_n.

THEOREM 0.13D.3. All forms of Proposition 0.13D.1 and 0.13D.2 are provable in ZFC + "there exists a measurable cardinal" but not in ZFC + "there exists a Ramsey cardinal". The same holds for their relativizations to the constructible universe, L, or even to the sets recursive in the first ω hyperjumps of $\emptyset$.

Proof: We originally proved this with "there exists a Ramsey cardinal" replaced by "$(\forall x \subseteq \omega)$(x# exists)", at least breaking the constructibility barrier in large cardinals (see [Sta85]). However our arguments can be combined with the inner model theory of large cardinals below a measurable cardinal - as was first observed by R. Solovay (private communication and lectures). QED

PROPOSITION 0.13D.4. For all isomorphic preserving (finitely) Borel $F:FGG^{\omega+\omega} \to FGG$, there exists $x \in \mathfrak{R}^{\omega+\omega}$ and $\alpha < \omega+\omega$ such that for all finite deletion subsequences y of x, F(y) is embeddable in y_α.

THEOREM 0.13D.5. All forms of Proposition 0.13D.4 are provable in ZFC + "there exists two measurable cardinals", but not in ZFC + "there exists a measurable cardinal". The same holds for their relativizations to the constructible universe, L, or even to the sets recursive in the first ω hyperjumps of ∅.

Proof: This also combines work of ours reported in [Sta85] with the inner model theory of a measurable cardinal. QED

0.13E. Borel Functions on Countable Sets.

We write CS($\mathfrak{R}$) for the space of countable subsets of $\mathfrak{R}$. This is to be viewed as the space $\mathfrak{R}^\infty$, under the equivalence relation "having the same range".

The notions of a Borel function F:CS($\mathfrak{R}$) → $\mathfrak{R}$, or F:CS($\mathfrak{R}$) → CS($\mathfrak{R}$) are very natural. For the former, we mean that there is a Borel function G:$\mathfrak{R}^\infty$ → $\mathfrak{R}$ such that F(rng(x)) = G(x). Note that G must be invariant in the sense used in section 0.11C.

For the latter, we mean that there exists a Borel function H:$\mathfrak{R}^\infty$ → $\mathfrak{R}^\infty$ such that F(rng(x)) = rng(H(x)). Note that H must be image preserving in the sense used in section 0.11D.

THEOREM 0.13E.1. For all Borel F:CS($\mathfrak{R}$) → $\mathfrak{R}$, there exists x ∈ CS($\mathfrak{R}$) such that F(x) ∈ x. For all Borel F:CS($\mathfrak{R}$) → CS($\mathfrak{R}$), there exists x ∈ CS($\mathfrak{R}$) such that F(x) ⊆ x.

Proof: The first claim is equivalent to Theorem 0.11D.1 using image invariance. The second claim is equivalent to Theorem 0.11D.2 using image preserving. Thus these two statements correspond to roughly Z_2. QED

Now let ≤ be a quasi order on $\mathfrak{R}$, and A,B ⊆ $\mathfrak{R}$. We say that x is a break point for A in B,≤ if and only if x ∈ A ⊆ B, and

i. (∀y ∈ B)(y ≥ x → (∃z ∈ A)(z ≡ y)); or
ii. (∀y ∈ B)(y ≥ x → (∃z ∉ B)(z ≡ y)).

PROPOSITION 0.13E.2. There is a countable (finitely) Borel quasi order ≤ such that for all (finitely) Borel F:$\mathfrak{R}^2$×CS($\mathfrak{R}$) → CS($\mathfrak{R}$), there exists nonempty A such that each F(x,y,A), x,y ∈ A, has a break point in A,≤.

Let λ be a countable limit ordinal. A λ-model of Z_2 is an ω model M ⊆ ℘ω, of Z_2, where every subset of ω lying in the first λ levels of the constructible hierarchy starting with M and its elements, lies in M.

LEMMA 0.13E.3. Proposition 0.13E.2 (all four forms) is provable in ZFC + $L(\mathfrak{R})$ determinacy. In fact, ZFC + $L_{\omega\_1}(\mathfrak{R})$ determinacy suffices. For finitely Borel, ZFC + projective determinacy suffices.

Proof: We argue in ZFC +$L_{\omega\_1}(\mathfrak{R})$ determinacy. We set $\leq\ =\ \leq_T$. Let $\lambda < \omega_1$, $u \subseteq \omega$, code $F:\mathfrak{R}^2\times CS(\mathfrak{R}) \rightarrow CS(\mathfrak{R})$. Let M be the transitive collapse of a countable elementary substructure of $V(\omega_1+\lambda)$ that contains the elements $\lambda+1$,u, and the subset λ. Let A = M $\cap$ $\wp\omega$. Then A is a countable λ-model of Z_2 containing u, and $L_\lambda(\mathfrak{R})$ determinacy holds in M.

By using an M generic enumeration of A (with finite conditions), we see that for all x,y $\in$ A, F(x,y,A) is a subset of A lying in the internal $L_\lambda(\mathfrak{R})$ of M. Therefore we can apply $L_\lambda(\mathfrak{R})$ determinacy within M, which implies $L_\lambda(\mathfrak{R})$ Turing degree determinacy. Thus we obtain the required break points in A. QED

By a degree, we mean a pair $\lambda < \omega_1$ and $x \subseteq \omega$ coding λ, where we use $y \leq_{\lambda,x} z \leftrightarrow y \in L_\lambda(x,z)$. By projective degree determinacy, we mean "there exists a degree such that every projective set of degrees contains or is disjoint from a cone".

LEMMA 0.13E.4. Proposition 0.13E.2 with "finitely" implies the existence of an ω model of $\boldsymbol{\Sigma}^1_n$-CA + "$\boldsymbol{\Sigma}^1_n$ degree determinacy holds for some degree", for each $n < \omega$, over ATR_0. Proposition 0.13E.2 implies the existence of an ω model of $L_{\omega+\omega}(\mathfrak{R})$-CA + "$L_{\omega+\omega}(\mathfrak{R})$ determinacy holds for some degree".

Proof: This uses the techniques from [Fr81] for constructing ω models from Borel statements of this general form. Let $\leq$ be given by Proposition 0.13E.2. Let u be a Borel code for $\leq$. Let $F:\mathfrak{R}^2\times CS(\mathfrak{R}) \rightarrow CS(\mathfrak{R})$ be a finitely Borel function such that

i. If $x < y$ then F(x,y,A) is singleton of the $\lfloor x\rfloor$-th Σ^1_n subset of ω with parameters x,y, provided u $\in$ A; u otherwise.

ii. If $x \geq y$ then F(x,y,A) is the $\lfloor x\rfloor$-th Σ^1_n subset of A with parameters x,y, provided u $\in$ A; u otherwise.

Let A be nonempty, where each F(x,y,A), x,y $\in$ A, has a break point in A,$\leq$. In particular, each F(x,y,A), x,y $\in$ A, is a subset of A. It is now clear that u $\in$ A, and that A is an ω model of $\mathbf{\Sigma^1_n}$-CA. We also see by the break points that A satisfies $\mathbf{\Sigma^1_n}$ determinacy for $\leq$.

The second claim is proved analogously. QED

LEMMA 0.13E.5. ZFC + "there exists infinitely many Woodin cardinals" proves projective determinacy. ZFC + "there exists a measurable cardinal above infinitely many Woodin cardinals" proves $L(\mathfrak{R})$ determinacy.

Proof: The first claim is from [MSt89]. The second claim is from [Wo88] and [Lar04]. QED

THEOREM 1.13E.6. Proposition 0.13E.2 (all four forms) are provable in ZFC + "there exists a measurable cardinal above infinitely many Woodin cardinals", but not in ZFC + "there exists infinitely Woodin cardinals". Proposition 0.13E.2 for finitely Borel is provable in ZFC + "there exists infinitely many Woodin cardinal", but not in ZFC + "there exists at least n Woodin cardinals", for any $n < \omega$.

Proof: The provability claims are from Lemma 0.13E.3. The unprovability claims follow from Lemma 0.13E.4 together with the reversal of the $\mathbf{\Sigma^1_n}$ determinacy, $n < \omega$, for any degree, and of the reversal of $L_{\omega+\omega}(\mathfrak{R})$ determinacy for any degree. The reversals can be carried out without choice and over Z_2, and weak extensions thereof (communication from W. Woodin). See [KW10]. QED

0.14. Incompleteness in ZFC using Discrete Structures.

0.14A. Preliminaries.
0.14B. Function Assignments.
0.14C. Boolean Relation Theory.
0.14D - 0.14J. NEW MATERIAL AS AGREED.

0.14A. Preliminaries.

The first arguably natural examples of incompleteness in ZFC using discrete structures appeared in [Fr98], and are discussed in section 0.14B.

The second examples of incompleteness in ZFC using discrete structures are from Boolean Relation Theory, which is the subject of this book. BRT represents a more natural and far more systematic approach than Function Assignments, with much greater points of contact with existing mathematical contexts. In section 0.14C, we give a brief account of BRT, reserving the extended account for section 0.15.

The third examples of incompleteness in ZFC using discrete structures are the culmination of recent developments since 2009, culminating with announcements made in May, 2011. These take a different direction from BRT, but rely on many technical insights from BRT. They result in statements equivalent to the consistency of certain large cardinal hypotheses, and thus are equivalent to Π^0_1 sentences. In contrast, function assignments and BRT result in statements equivalent to the 1-consistency of large cardinals, and thus equivalent to Π^0_2 sentences.

These new developments are discussed in sections 0.14D - 0.14I. This is work in progress, and proofs will appear elsewhere.

There are two hierarchies of large cardinal hypotheses relevant to this section (except for 0.14G). The weaker of the two is the hierarchy of strongly n-Mahlo cardinals. These are defined inductively as follows.

The strongly 0-Mahlo cardinals are the strongly inaccessible cardinals (uncountable regular strong limit cardinals).
The strongly n+1-Mahlo cardinals are the infinite cardinals all of whose closed unbounded subsets contain a strongly n-Mahlo cardinal.

We define $SMAH^+ = ZFC + (\forall n < \omega)(\exists \kappa)(\kappa$ is a strongly n-Mahlo cardinal). $SMAH = ZFC + \{(\exists\kappa)(\kappa$ is a strongly n-Mahlo cardinal$)\}_n$.

Mahlo cardinals were introduced surprisingly early, in [Mah11], [Mah12], [Mah13]. For more information about the strongly Mahlo hierarchy, and the related Mahlo hierarchy, see section 4.1.

The second, stronger hierarchy of large cardinal hypotheses relevant to this section is the stationary Ramsey cardinal hierarchy. This hierarchy originated with [Ba75]. Also see [Fr01].

We say that λ has the k-SRP if and only if λ is a limit ordinal, $k \geq 1$, and every partition of the unordered k-tuples from λ into two pieces has a homogeneous stationary subset of λ.

We define $SRP^+ = ZFC + (\forall k < \omega)(\exists\kappa)(\kappa$ has the k-SRP). SRP = ZFC + $\{(\exists\kappa)(\kappa$ has the k-SRP$)\}_k$.

The SRP hierarchy is intertwined with the more technical subtle cardinal hierarchy. See [Fr01] for a detailed treatment of this level of the large cardinal hierarchy.

0.14B. Function Assignments.

The first published examples of arguably mathematically natural arithmetic sentences independent of ZFC appeared in [Fr98]. These examples are Π^0_2, although it was left open in [Fr98] whether they are provably equivalent to 1-Con(SRP), as we expect.

A function assignment for a set X is a mapping U which assigns to each finite subset A of X, a unique function

$$U(A): A \to A.$$

The following is easily obtained from Theorem 0.8F.4 (Theorem 0.4 in [Fr98]). See section 0.8F for the definition of regressive values.

THEOREM 0.14B.1. Let k,p > 0 and U be a function assignment for N^k. Then some U(A) has $\leq (k^k)p$ regressive values on some $E^k \subseteq A$, $|E| = p$.

In the set theoretic world, we have the following analog (Theorem 0.5 in [Fr98]).

THEOREM 0.14B.2. Let k,r,p > 0 and $F:\lambda^k \to \lambda^r$, where λ is a suitably large cardinal. Then F has $\leq k^k$ regressive values on some $E^k \subseteq \lambda^k$, $|E| = p$. It suffices that λ has the k-SRP.

We placed a natural condition on function assignments for N^k so that we get the improved estimate k^k in Theorem 0.14B.2 rather than the $(k^k)p$ in Theorem 0.14B.1.

Let U be a function assignment for N^k. We say that U is #-decreasing if and only if for all finite $A \subseteq N^k$ and $x \in N^k$,

$$\text{either } U(A) \subseteq U(A \cup \{x\}) \text{ or there exists } |y| > |x| \text{ such that } |U(A)(y)| > |U(A \cup \{x\})(y)|.$$

Here we have used | | for max.

An alternative definition of #-decreasing is as follows. For all finite $A \subseteq N^k$ and $x \in N^k$, either $U(A) \subseteq U(A \cup \{x\})$, or there exists $|y| > |x|$ such that

i. $|U(A)(y)| > |U(A \cup \{x\})(y)|$.
ii. for all $z \in A$, if $|z| < |y|$, then $U(A)(z) = U(A \cup \{x\})(z)$.
iii. for all $z \in A$, if $|z| = |y|$, then $U(A)(z) = U(A \cup \{x\})(z)$ or $|U(A)(z)| > |U(A \cup \{x\})(z)|$.

The following infinitary proposition is Proposition A in [Fr98].

PROPOSITION 0.14B.3. Let $k,p > 0$ and U be a #-decreasing function assignment for N^k. Then some U(A) has $\leq k^k$ regressive values on some $E^k \subseteq A$, $|E| = p$.

The finite form is Proposition B in [Fr98].

PROPOSITION 0.14B.4. Let $n >> k,p > 0$ and U be a #-decreasing function assignment for $[n]^k$. Then some U(A) has $\leq k^k$ regressive values on some $E^k \subseteq A$, $|E| = p$.

Proposition 0.14B.4 takes the form

for all k,p there exists n such that every gadget bounded by n has an internal property

and is therefore explicitly Π^0_2.

As remarked in [Fr98], p. 808, Proposition 0.14B.3 immediately implies Proposition 0.14B.4, using a standard compactness (finitely branching tree) argument. The implication from Proposition 0.14B.4 to Proposition 0.14B.3 is immediate. So clearly Proposition 0.14B.3 is provably equivalent to a Π^0_2 sentence, over RCA_0.

The following is proved in [Fr98]. See Theorems 4.18, 5.91.

THEOREM 0.14B.5. SRP^+ proves Propositions 0.14B.3, 0.14B.4, but not from any consequence of SRP that is consistent with ZFC. Propositions 0.14B.3, 0.14B.4 imply Con(SRP) over ZFC.

We conjecture that Propositions 0.14B.3, 0.14B.4 are provably equivalent to 1-Con(SRP) over ZFC.

In fact, we conjecture that Proposition 0.14B.3 is provably equivalent to 1-Con(SRP) over ACA', and Proposition 0.14B.4 is provably equivalent to 1-Con(SRP) over EFA.

0.14C. Boolean Relation Theory.

We give a brief account of some highlights of Boolean Relation Theory (BRT), the subject of this book. A much more detailed account will be given in section 0.15.

BRT begins with two theorems proved well within ZFC that provides an excellent point of departure.

Let N be the set of all nonnegative integers.

COMPLEMENTATION THEOREM. Let $f:N^k \to N$ obey the inequality $f(x) > \max(x)$. There exists a (unique) $A \subseteq N$ with $f[A^k] = N\backslash A$.

THIN SET THEOREM. Let $f:N^k \to N$. There exists an infinite $A \subseteq N$ such that $f[A^k] \neq N$.

These theorems are discussed in detail in sections 1.3 and 1.4.

Note that the Complementation Theorem (without uniqueness) has the following structure:

> for every function of a certain kind there is a set of a certain kind such that a given Boolean equation holds involving the set and its image under the function.

The Thin Set Theorem has the following structure:

> for every function of a certain kind there is a set of a certain kind such that a given Boolean inequation holds involving the set and its image under the function.

In fact, the inequation in the Thin Set Theorem involves only the image of the set under the function.

Here, and throughout BRT, we use a particular notion of the image of a set A under a multivariate function f - namely $f[A^k]$. For notational brevity, we suppress the arity of f, and simply write fA for $f[A^k]$. In all contexts under consideration, the arity, k, of f will be apparent.

In addition, here N serves as the universal set for the Boolean algebra.

More specifically, we use MF for the set of all f such that for some $k \geq 1$, $f:N^k \to N$. SD for the set of all $f \in MF$ such that for all $x \in dom(f)$, $f(x) > max(x)$. INF for the set of all infinite $A \subseteq N$.

We can restate these two theorems in the form

COMPLEMENTATION THEOREM. For all $f \in SD$ there exists $A \in INF$ such that $fA = N \setminus A$.

THIN SET THEOREM. For all $f \in MF$ there exists $A \in INF$ such that $fA \neq N$.

The Complementation Theorem is an instance of what we call

EBRT in A,fA on (SD,INF).

The Thin Set Theorem is an instance of what we call

IBRT in A,fA on (MF,INF).

Here EBRT means "equational BRT", and IBRT means "inequational BRT".

For our independence results, we use a somewhat different class of functions. We let ELG be the set of all $f \in MF$ of expansive linear growth; i.e., where there exist rational constants $c,d > 1$ such that for all but finitely many $x \in dom(f)$,

$$c|x| \leq f(x) \leq d|x|$$

where $|x|$ is the maximum coordinate of the tuple x.

The core finding of this book is the discovery and analysis of a particular instance of

EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF)

that is independent of ZFC. More specifically, we show that this "special instance" has the following three metamathematical properties:

i. It is provable in $SMAH^+$.

ii. It is not provable from any set of consequences of SMAH that is consistent with ACA'.
iii. It is provably equivalent to the 1-consistency of SMAH over ACA'.

In fact, the special instance is an instance of

EBRT in A,B,C,fA,fB,gB,gC on (ELG,INF).

Although this special instance is far simpler than a randomly chosen instance, it does not convey any clear compelling information.

We were very anxious to establish the necessary use of large cardinals in order to analyze EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF).

CONJECTURE. Every instance of EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF) is provable or refutable in $SMAH^+$.

This conjecture would establish a necessary and sufficient use of large cardinals in BRT in light of the "special instance".

There are 2^{512} instances of EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF), there being nine terms involved. This proved far too difficult to analyze, even using theoretical considerations.

There are 2^{64} instances of EBRT in A,C,fA,fB,gB,gC on (ELG,INF), and the special instance referred to above comes under this smaller set.

CONJECTURE. Every instance of EBRT in A,C,fA,fB,gB,gC on (ELG,INF) is provable or refutable in $SMAH^+$.

Unfortunately, this conjecture also appears out of reach.

What was needed is a natural fragment of EBRT in A,B,C,fA,fB,fC,gA,gB,gC that is small enough to be completely analyzable, yet large enough to include our instance.

We discovered the following class of $3^8 = 6561$ instances of EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF).

TEMPLATE. For all $f,g \in ELG$ there exist $A,B,C \in INF$ such that

$$X \cup. fY \subseteq V \cup. gW$$
$$P \cup. fR \subseteq S \cup. gT.$$

Here X,Y,V,W,P,R,S,T are among the three letters A,B,C.

Here we have used ∪. for disjoint union. I.e.,

$$D \cup. E \text{ is } D \cup E \text{ if } D \cap E = \emptyset;$$
$$\text{undefined otherwise.}$$

The special instance is called the Principal Exotic Case throughout the book. It appears as Proposition A in section 4.2.

PRINCIPAL EXOTIC CASE. For all $f,g \in ELG$ there exist $A,B,C \in INF$ such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

There are obviously 12 symmetric forms of the Principal Exotic Case obtained by permuting A,B,C, and switching the two clauses. These 12 are called the Exotic Cases. The remaining 6561 - 12 = 6549 instances of the Template are shown to be provable or refutable in Chapter 3.

In section 4.2, we prove the Principal Exotic Case from $SMAH^+$. In section 4.4, we sharpen this by proving the Exotic Case from ACA' + 1-Con(SMAH).

In Chapter 5, we derive 1-Con(SMAH) from ACA' + the Exotic Case. In section 5.9, we establish that the Principal Exotic Case (Proposition A) is not provable from any set of consequences of SMAH that is consistent with ACA'.

In section 3.15, we also consider the modified, weaker Template

TEMPLATE'. For all $f,g \in ELG$ there exist arbitrarily large finite $A,B,C \subseteq N$ such that

$$X \cup. fY \subseteq V \cup. gW$$
$$P \cup. fR \subseteq S \cup. gT.$$

In section 3.15, we show that every instance of Template' is provable or refutable in RCA_0, and that Template and Template' are equivalent for all but the 12 Exotic Cases.

We also show that the 12 Exotic Cases become provable in RCA_0 under Template'.

We then draw the conclusion that the assertion

Template and Template' are equivalent

which we refer to as the BRT Transfer Principle, has the same metamathematical properties i-iii enumerated two pages earlier. In this sense, the above assertion represents a necessary use of large cardinals for obtaining arguably clear and compelling information in the realm of discrete mathematics.

0.14D - 0.14J. NEW MATERIAL GOES HERE AS AGREED.

0.15. Detailed Overview of Book Contents.

We give an informal discussion of the contents of the book, section by section. This discussion is far more detailed than the overview given in section 0.14C above.

Chapter 1 Introduction to BRT
1.1. General Formulation

Here we begin with two Theorems that lie at the heart of Boolean Relation Theory (abbreviated BRT). These are the Thin Set Theorem and the Complementation Theorem. We repeat these here.

THIN SET THEOREM. Let $k \geq 1$ and $f:N^k \to N$. There exists an infinite set $A \subseteq N$ such that $f[A^k] \neq N$.

COMPLEMENTATION THEOREM. Let $k \geq 1$ and $f:N^k \to N$. Suppose that for all $x \in N^k$, $f(x) > \max(x)$. There exists an infinite set $A \subseteq N$ such that $f[A^k] = N\backslash A$.

Note that the Thin Set Theorem asserts that for every function in a certain class there is a set in a certain class such that a Boolean inequation holds between the set and its forward image under the function. In fact, the Boolean inequation does not even use the set.

Similarly, the Complementation Theorem asserts that for every function in a certain class there is a set in a certain class such that a Boolean equation holds between the set and its forward image under the function.

The notion of forward image used throughout BRT is the set of values of the multivariate function at arguments drawn from the set. Throughout BRT, we abbreviate this construction, $f[A^k]$, by fA.

Thus we can rewrite the Thin Set Theorem and the Complementation Theorem in the following form.

THIN SET THEOREM. For all f ∈ MF there exists A ∈ INF such that fA ≠ N.

COMPLEMENTATION THEOREM. For all f ∈ SD there exists A ∈ INF such that fA = N\A.

We say that the Thin Set Theorem is an instance of IBRT (inequatonal BRT) on the BRT setting (MF,INF), and the Complementation Theorem is an instance of EBRT (equational BRT) on the BRT setting (SD,INF).

More specifically, we say that

i. The Thin Set Theorem is an instance of: IBRT in fA on (MF,INF).
ii. The Complementation Theorem is an instance of: EBRT in A,fA on (SD,INF).

We then present the general formulation. We define the following concepts, starting with Definition 1.1.4.

As an aid to the reader, we give examples of most of these concepts based on the Thin Set Theorem (TST), and the Complementation Theorem (CT).

1. BRT set variable, BRT function variable. For CT, TST we use A and f.

2. BRT term. For CT, we use fA,U\A. For TST, we use fA,U.

3. BRT equation, BRT inequation, BRT inclusion. For CT, we use the BRT equation fA = U\A. For TST, we use the BRT inequation fA ≠ U.

4. BRT formula. These are quantifier free. For CT, we use fA = U\A. For TST, we use fA ≠ U.

5. Formal treatment of multivariate function, arity, and the forward imaging fE.

6. BRT setting. For CT we use (SD,INF). For TST we use (MF,INF).

7. BRT assertion. BRT,⊆ assertion. For CT, we use $(\forall f \in V)(\exists A \in K)(fA = U\backslash A)$. For TST, we use $(\forall f \in V)(\exists A \in K)(fA \neq U)$.

8. BRT valid formula, BRT,⊆ valid formula.

9. BRT equivalent formulas, BRT,⊆ equivalent formulas.

10. BRT environments. For CT, we use EBRT. For TST, we use IBRT.

11. BRT signatures. For CT, we use A,fA. For TST, we use fA.

12. BRT fragment. For CT, we use EBRT in A,fA on (SD,INF). For TST, we use IBRT in fA on (MF,INF).

13. The standard BRT signatures. For CT and TST, we use A,fA.

14. Standard BRT fragments. For CT we use EBRT in A,fA on (SD,INF). For TST we use IBRT in A,fA on (MF,INF).

The highlight of the book is the proof of the Principal Exotic Case (see Appendix A) from large cardinals, and its unprovability from weaker large cardinals. The proof is in Chapter 4, and the unprovability is from Chapter 5.

The Principal Exotic Case arises in Chapter 3, and lies in the standard BRT fragment

EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF).

Here ELG is the class of $f \in MF$ which are of expansive linear growth (see section 0.14C)).

In fact, the Principal Exotic Case lives in the considerably reduced flat BRT fragment

EBRT in A,C,fA,fB,gB,gC,⊆ on (ELG,INF)

since Proposition A is not affected by inserting $A \subseteq B \subseteq C$ in its conclusion (see Appendix A).

Even the above BRT fragment is too rich for us to completely analyze at this time, let alone the standard fragment above.

In Chapter 2, we do give a complete analysis of several much more restricted BRT fragments, as indicated by their section headings.

The main BRT settings considered in this book are (MF,INF), (SD,INF), and (ELG,INF). See Definitions 1.1.2 and 2.1.

The state of the art with regard to complete analyses of BRT fragments on these BRT settings can be summarized as follows.

In both EBRT and IBRT, we completely understand one function and two sets with ⊆, in the sense that RCA_0 suffices to prove or refute every instance. See sections 2.4 - 2.7.

However, it remains to analyze one function and two sets without the substantial simplifier ⊆. This is a very substantial challenge, although we are convinced that this is a manageable project.

Only very special parts of the standard fragment EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF) are presently amenable to complete analysis. One very symmetric part consisting of 3^8 = 6561 cases is completely analyzed in Chapter 3. All instances are provable or refutable in RCA_0 - expect for the Principal Exotic Case and its eleven symmetric forms, forming the twelve Exotic Cases.

Section 1.1 presents a very useful canonical form for any Boolean equation (arising in the BRT fragments analyzed in the book) as a finite conjunction of Boolean inclusions of certain forms. This greatly facilitates work with the general Boolean equations that arise.

For instance, see the 16 A,B,fA,fB pre elementary inclusions listed right after Lemma 2.4.5 according to Definition 1.1.35. Also see the 9 A,B,fA,fB,⊆ elementary inclusions listed right after Lemma 2.4.5 according to Definition 1.1.37.

1.2. Some BRT settings

In this section, we give an indication of the tremendous variety of BRT settings that arise from standard mathematical considerations.

We conjecture that the behavior of BRT fragments in BRT settings depends very delicately on the choice of BRT setting. Generally speaking, we believe that even small changes in the BRT setting lead to different classifications, even with BRT fragments in modest signatures.

This leads us to the conviction that BRT is a mathematically fruitful problem generator of unprecedented magnitude and scope.

Indications of this sensitivity are already present in the classifications of Chapter 2 as well as the results of section 1.4.

Even in the realm of natural subsets of the set MF of all functions from some N^k into N, the variety of subclasses is staggering. These are discussed in part I of section 1.2. In addition, a large variety of subclasses of INF are also very natural.

It is very compelling to use $\mathbf{Z}$, $\mathbf{Q}$, $\mathfrak{R}$, and $\mathbf{C}$, instead of N, creating many additional natural BRT settings, involving algebraic, topological, and analytic considerations.

The use of function spaces is also compelling. We mention (V,K), where V is the set of all bounded linear operators on L^2, and K is the set of all nontrivial closed subspaces of L^2. Then the famous invariant subspace problem for L^2 is expressed as the following instance of EBRT in A,fA on (V,K):

$$(\forall f \in V)(\exists A \in K)(fA = A).$$

We can obviously use other function spaces for BRT settings.

We also propose Topological BRT, where we use the continuous functions - and even the multivariate continuous functions - on various topological spaces, and the open subsets of the spaces.

It also makes sense to investigate those BRT statements that hold in the continuous functions and nonempty open sets, on all topological spaces obeying certain conditions.

Section 1.2 concludes with a back of the envelope calculation of the number of BRT settings presented there, that are suspected of having different BRT behavior. We count only those on N.

The estimate given there is 1,000,000 naturally described individual BRT settings with substantially different BRT behavior.

The book focuses on only five BRT settings (MF,INF), (ELG,INF), (SD,INF), (EVSD,INF), (ELG ∩ SD,INF), and only scratches the surface of very simple BRT fragments even in these settings. For the definition of all these settings in one place, see Appendix A. As indicated by the classifications in Chapter 2, incredible complexities are expected to always arise in passing from BRT fragments to even slightly richer BRT fragments - even on these five BRT settings. When considering the number 1,000,000 above, we see how vast and deep BRT is expected to be.

1.3. Complementation Theorems

This section focuses on aspects of the Complementation Theorem (CT). Recall the discussion at the beginning of section 1.1.

COMPLEMENTATION THEOREM. For all f ∈ SD there exists A ∈ INF such that fA = N\A.

COMPLEMENTATION THEOREM (with uniqueness). For all f ∈ SD there exists a unique A ⊆ N with fA = N\A. Moreover, A ∈ INF.

A few equivalent formulations of CT are given, as well as the simple inductive proof.

CT is then extended to strictly dominating functions on well founded relations. This extension is used in Chapter 4 to prove the Principal Exotic Case (Proposition A).

We also show that for irreflexive transitive relations with an upper bound condition, CT is equivalent to well foundedness.

In CT, we define the complementation of $f \in SD$ to be the unique $A \subseteq N$ with $fA = N\setminus A$.

There is the expectation that even for very simple $f \in SD$, the unique complementation A of f can be very complicated - and have an intricate structure well worth exploring.

We present some basic examples, where we calculate the unique complementation. In particular, we consider some cases where f is an affine transformation from N^k into N.

It is also very natural to consider affine $f:N^k \to Z$. Only here we need to use the following variant of CT. This requires use of the "upper image" of f on A, defined by

$$f_<A = \{f(x_1,\ldots,x_k): \\ f(x_1,\ldots,x_k) > \max(x_1,\ldots,x_k) \text{ and } x_1,\ldots,x_n \in A\}.$$

An upper complement of f is an $A \subseteq N$ with $f_<A = N\setminus A$.

UPPER COMPLEMENTATION THEOREM. Every $f:N^k \to Z$ has a unique upper complementation. This unique upper complement is infinite.

This formulation has the advantage that it applies to all $f:N^k \to Z$, without requiring that f obey any inequalities.

We then present some calculations of upper complementations.

We then view CT as a fixed point theorem, and present a more general BRT Fixed Point Theorem.

We also consider a version on the reals, and present a continuous complementation theorem.

The Complementation Theorem is closely related to an important development in digraph theory. These are the kernels and dominators of digraphs. Kernels are used in the recent work reported in section 0.14D.

1.4. Thin Set Theorems

This section focuses on aspects of the Thin Set Theorem (TST). Recall the discussion at the beginning of section 1.1.

THIN SET THEOREM. For all f ∈ MF there exists A ∈ INF such that fA ≠ N.

We begin by tracing the origins of the Thin Set Theorem back to the square bracket partition calculus in combinatorial set theory. There, one uses unordered tuples instead of ordered tuples. However, we give an equivalence proof in RCA_0 (see Theorem 1.4.2).

This is followed by a discussion of the metamathematical status of TST, which is only partially understood.

We then present a simple proof of TST using the infinite Ramsey theorem.

We give a strong form of TST where the codomain is [0,ot(k)], and establish its metamathematical status. We show that it is provably equivalent to ACA' over RCA_0.

We briefly consider TST with an infinite cardinal κ instead of N. We cite [To87], [BM90], and [Sh95] to obtain some results.

TST makes sense on any BRT setting. We explore TST on some BRT settings in real analysis.

We first consider 8 natural families of unary functions from $\mathfrak{R}$ to $\mathfrak{R}$, and 9 families of subsets of $\mathfrak{R}$, for a total of 72 BRT settings.

FCN($\mathfrak{R}$,$\mathfrak{R}$). All functions from $\mathfrak{R}$ to $\mathfrak{R}$.
BFCN($\mathfrak{R}$,$\mathfrak{R}$). All Borel functions from $\mathfrak{R}$ to $\mathfrak{R}$.
CFCN($\mathfrak{R}$,$\mathfrak{R}$). All continuous functions from $\mathfrak{R}$ to $\mathfrak{R}$.
C^1FCN($\mathfrak{R}$,$\mathfrak{R}$). All C^1 functions from $\mathfrak{R}$ to $\mathfrak{R}$.
C^∞FCN($\mathfrak{R}$,$\mathfrak{R}$). All C^∞ functions from $\mathfrak{R}$ to $\mathfrak{R}$.
RAFCN($\mathfrak{R}$,$\mathfrak{R}$). All real analytic functions from $\mathfrak{R}$ to $\mathfrak{R}$.
SAFCN($\mathfrak{R}$,$\mathfrak{R}$). All semialgebraic functions from $\mathfrak{R}$ to $\mathfrak{R}$.
CSAFCN($\mathfrak{R}$,$\mathfrak{R}$). All continuous semialgebraic functions from $\mathfrak{R}$ to $\mathfrak{R}$.

cSUB($\mathfrak{R}$). All subsets of $\mathfrak{R}$ of cardinality c.
UNCLSUB($\mathfrak{R}$). All uncountable closed subsets of $\mathfrak{R}$.
NOPSUB($\mathfrak{R}$). All nonempty open subsets of $\mathfrak{R}$.
UNOPSUB($\mathfrak{R}$). All unbounded open subsets of $\mathfrak{R}$.
DEOPSUB($\mathfrak{R}$). All open dense subsets of $\mathfrak{R}$.
FMOPESUB($\mathfrak{R}$). All open subsets of $\mathfrak{R}$ of full measure.
CCOPSUB($\mathfrak{R}$). All open subsets of $\mathfrak{R}$ whose complement is countable.

FCSUB($\Re$). All subsets of $\Re$ whose complement is finite.
≤1CSUB($\Re$). All subsets of $\Re$ whose complement has at most one element.

We determine the status of TST in all 72 BRT settings.

We then consider the corresponding 8 families of multivariate functions from $\Re$ to $\Re$. I.e., functions whose domain is some $\Re^n$ and whose range is a subset of $\Re$. We use the same 9 families of subsets of $\Re$.

FCN($\Re$*,$\Re$). All multivariate functions from $\Re$ to $\Re$.
BFCN($\Re$*,$\Re$). All multivariate Borel functions from $\Re$ to $\Re$.
CFCN($\Re$*,$\Re$). All multivariate continuous functions from $\Re$ to $\Re$.
C^1FCN($\Re$*,$\Re$). All multivariate C^1 functions from $\Re$ to $\Re$.
C^∞FCN($\Re$*,$\Re$). All multivariate C^∞ functions from $\Re$ to $\Re$.
RAFCN($\Re$*,$\Re$). All multivariate real analytic functions from $\Re$ to $\Re$.
SAFCN($\Re$*,$\Re$). All multivariate semialgebraic functions from $\Re$ to $\Re$.
CSAFCN($\Re$*,$\Re$). All multivariate continuous semialgebraic functions from $\Re$ to $\Re$.

We again determine the status of TST in all 72 BRT settings.

The status of TST in all 144 BRT settings is displayed in a table at the end of section 1.4.

Chapter 2 Classifications
2.1. Methodology

In Chapter 2, we focus on five BRT settings, falling naturally into three groups according to their observed BRT behavior.

(SD,INF), (ELG ∩ SD,INF).
(ELG,INF), (EVSD,INF).
(MF,INF).

The inclusion diagram for these five sets of multivariate functions is

ELG ∩ SD
SD ELG
EVSD
MF

(SD,INF), (ELG,INF), and (MF,INF) are the most natural of these five BRT settings. The remaining two BRT settings are closely related to these three, and serve to round out the theory.

In section 2.1, we present the treelike methodology for giving complete classifications for BRT fragments.

This treelike methodology is used in sections 2.4, 2.5, and the reader can absorb this methodology by looking at the physical layout of the classifications in those sections.

The formal treatment of the treelike methodology is given fully in section 2.1.

2.2. EBRT, IBRT in A,fA

In this section, we give a complete classification of EBRT in A,fA, and IBRT in A,fA, on our list of five basic BRT settings, (SD,INF), (ELG ∩ SD,INF), (ELG,INF), (EVSD,INF), (MF,INF).

The EBRT classifications are conducted entirely within RCA_0. The IBRT classifications are conducted entirely within ACA'.

This establishes that every instance of the EBRT fragments is provable or refutable in RCA_0, and every instance of the IBRT fragments is provable or refutable in ACA'.

Since there are only 16 instances for each of these simple BRT fragments, we can afford to simply list all of the A,fA elementary inclusions

$$A \cap fA = \emptyset.$$
$$A \cup fA = U.$$
$$A \subseteq fA.$$
$$fA \subseteq A.$$

and consider all of the 16 subsets, interpreted conjunctively. For EBRT in A,fA, if we reject a subset of the elementary inclusions, then we automatically reject any superset. So in order to save work, we can first list the subsets (A,fA formats) of cardinality 0, then list the subsets of cardinality 1, and so forth, through the subset of cardinality 4. But of course we don't have to list any subset where some proper subset has already been rejected.

This kind of classification is called a tabular classification. We give a tabular classification for EBRT in A,fA on (SD,INF), (ELG ∩ SD,INF), (ELG,INF), (EVSD,INF), (MF,INF), and present the results in a table that lists all sixteen of the A,fA formats.

For IBRT in A,fA on (SD,INF), we dualize, and thus put the assertions in the form

$$(\exists f \in V)(\forall A \in K)(\varphi)$$

where φ is an A,fA format interpreted conjunctively. Once again, if we reject a format, then we automatically reject any superset. So we also give a tabular classification of IBRT in A,fA on (SD,INF), (ELG ∩ SD,INF), (ELG,INF), (EVSD,INF), (MF,INf). We also present the results in a table listing all sixteen of the A,fA formats.

In the course of working out the classification on the IBRT side, we came across the following sharpening of the Thin Set Theorem, which we derive from TST.

THIN SET THEOREM (variant). For all f ∈ MF there exists A ∈ INF such that A ∪ fA ≠ N.

We conclude section 2.2 with a discussion of the effect of restricting the arity of the functions in the various classes.

The EBRT classifications are conducted in RCA_0, and the IBRT classifications are conducted in ACA'.

As a Corollary, all instances of EBRT in A,fA on these five BRT settings are provable or refutable in RCA_0, and all instances of IBRT in A,fA on these five BRT settings are provable or refutable in ACA'.

In fact, ACA' is used only in IBRT in A,fA on the setting (MF,INF), and not on the other four settings.

2.3. EBRT, IBRT in A,fA,fU

Here we redo section 2.2 for the signature A,fA,fU, with the same five BRT settings (SD,INF), (ELG ∩ SD,INF), (ELG,INF), (EVSD,INF), (MF,INF). Here U stands for the universal set, which in these five BRT settings, is N.

Now we have the 6 A,fA,fU elementary inclusions

$$A \cap fA = \emptyset.$$
$$A \cup fU = U.$$
$$A \subseteq fU.$$
$$fU \subseteq A \cup fA.$$
$$A \cap fU \subseteq fA.$$
$$fA \subseteq A.$$

There are 64 subsets of these 6 elementary inclusions. These are conveniently handled again by tabular classifications for both EBRT and IBRT.

Some interesting issues arise using N and fN, as presented in Theorems 2.3.2 and 2.3.3. We also examine the effect of arity on the class of functions, as in section 2.2.

As in section 2.2, the EBRT classifications are conducted in RCA_0, and the IBRT classifications are conducted in ACA'.

As a Corollary, all instances of EBRT in A,fA,fU on these five BRT settings are provable or refutable in RCA_0, and all instances of IBRT in A,fA,fU on these five BRT settings are provable or refutable in ACA'.

In fact, ACA' is used only in IBRT in A,fA,fU on (MF,INF), and not on the other four settings.

2.4. EBRT in A,B,fA,fB,⊆ on (SD,INF)
2.5. EBRT in A,B,fA,fB,⊆ on (ELG,INF)

Here we use the treelike classification method in order to give complete classifications of EBRT in A,B,fA,fB,⊆ on (SD,INF), (ELG ∩ SD,INF), (ELG,INF), and (EVSD,INF). EBRT on (MF,INF) is treated in section 2.6.

The classifications in sections 2.4, 2.5 are conducted in RCA_0. As a Corollary, all instances of these four BRT fragments are provable or refutable in RCA_0.

A substantial number of new issues arise in both of these classifications. The new issues can be seen from Lemmas 2.4.1 - 2.4.5, 2.5.1 - 2.5.14.

Both treelike classifications start with a listing of the 9 elementary inclusions in A,B,fA,fB,⊆.

$A \cap fA = \emptyset.$

B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
A ⊆ fB.
B ∩ fB ⊆ A ∪ fA.
fA ⊆ B.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.

Recall that the elementary inclusions originate from the 16 pre elementary inclusions through formal simplification using A ⊆ B.

The classifications provide a determination of the subsets S of the above nine inclusions for which

(∀f ∈ SD)(∃A ⊆ B from INF)(S)
(∀f ∈ ELG ∩ SD)(∃A ⊆ B from INF)(S)
(∀f ∈ ELG)(∃A ⊆ B from INF)(S)
(∀f ∈ EVSD)(∃A ⊆ B from INF)(S)

holds, where S is interpreted conjunctively.

We believe that obtaining complete classifications of EBRT in A,B,fA,fB on (SD,INF), (ELG ∩ SD,INF), (ELG,INF), and (EVSD,INF) is a manageable project, and can be completed within five years. The pre elementary inclusions in A,B,fA,fB number 16.

There needs to be a determination of the sets S of these sixteen inclusions for which

(∀f ∈ SD)(∃A ⊆ B from INF)(S)
(∀f ∈ ELG ∩ SD)(∃A ⊆ B from INF)(S)
(∀f ∈ ELG)(∃A ⊆ B from INF)(S)
(∀f ∈ EVSD)(∃A ⊆ B from INF)(S)

holds, where S is interpreted conjunctively.

The classifications are carried out entirely within RCA_0. Hence every instance of these classifications is provable or refutable in RCA_0.

2.6. EBRT in $A_1,...,A_k,fA_1,...,fA_k$,⊆ on (MF,INF)

Classifications in EBRT on (MF,INF) are substantially easier than on (SD,INF), (ELG ∩ SD,INF), (ELG,INF), and (EVSD,INF), at least under ⊆. Here we handle one function and k sets under $\subseteq$ on (MF,INF). Again, the classification is conducted in RCA_0, and so we see that every instance of this BRT fragment is provable or refutable in RCA_0.

We begin with a listing of the fifteen convenient types of elementary inclusions based on simple inequalities on the subscripts. Five of these are easily eliminated, leaving a sublist of ten. The conjunction of all of these is accepted.

Without $\subseteq$, we have an incomparably more difficult challenge, which we have not attempted.

2.7. IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$

In this section, we give a complete classification of IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (SD,INF), (ELG $\cap$ SD,INF), (ELG,INF), (EVSD,INF), and (MF,INF). We work entirely within RCA_0, except for the BRT setting (MF,INF), where we work within ACA'.

In fact, this classification for the first four of these BRT settings is seen to be trivial, and so section 2.7 focuses on the BRT setting (MF,INF).

We start with the $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ elementary inclusions, grouped into the same 15 categories based on simple inequalities of the subscripts that were used in section 2.6.

For each of these elementary inclusions, ρ, we will provide a useful description of the witness set for ρ, in the following sense: The set of all $f \in$ MF such that

$$(\forall A_1,...,A_k \in \text{INF})(A_1 \subseteq ... \subseteq A_k \rightarrow \rho).$$

We then calculate the witness sets for the sets of elementary inclusions by taking intersections.

It is easily seen that a format is correct if and only if this intersection is nonempty. Correctness of formats correspond to Boolean inequations. See item 4) just before Definition 1.1.40, with $n = 1$.

We completely determine the formats (sets of elementary inclusions) for which the intersection is nonempty.

Once again, without ⊆, we have an incomparably more difficult challenge, which we have not attempted.

Chapter 3 6561 Cases of Equational Boolean Relation Theory

3.1. Preliminaries

Recall that EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF) involves $2^9 = 512$ pre elementary inclusions, with 2^{512} statements. A complete classification is well beyond our capabilities. This is also true for EBRT in A,B,C,fA,fB,fC,gA,gB,gC,⊆ on (ELG,INF), although the number of elementary inclusions reduces to 64, with 2^{64} statements.

Here we completely classify a modest, but significant, part of EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF).

We use the notation A ∪. B from Definition 1.3.1. In particular,

$$A \cup. B \subseteq C \cup. D$$

means

$$A \cap B = \emptyset \wedge C \cap D = \emptyset \wedge A \cup B \subseteq C \cup D.$$

This is a very natural concept, and is illustrated by a diagram in section 3.1.

The part of EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF) treated here is given as follows.

TEMPLATE. For all f,g ∈ ELG there exist A,B,C ∈ INF such that

$$X \cup. fY \subseteq V \cup. gW$$
$$P \cup. fR \subseteq S \cup. gT.$$

Here X,Y,V,W,P,R,S,T are among the three letters A,B,C. We refer to the statements X ∪. fY ⊆ V ∪. gW, for X,Y,V,W ∈ {A,B,C}, as clauses.

In Chapter 3, we determine the truth values of all of these 6561 statements. We also read off a number of specific results about the Template. We do not know how to obtain these results without examining the classification.

In particular, every assertion in the Template is either provable or refutable in $SMAH^+$. In fact, there exist 12 assertions in the Template, which are obtained by permuting

A,B,C and interchanging the two clauses, so that the remaining 6549 assertions are each provable or refutable in RCA_0.

These 12 exceptional cases are called the Exotic Cases. The Principal Exotic Case is as follows.

PROPOSITION A. For all f,g ∈ ELG there exist A,B,C ∈ INF such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

In Chapter 4, we prove Proposition A in $SMAH^+$. In Chapter 5, we show that Proposition A is provably equivalent to 1-Con(SMAH) over ACA'.

We also show that every one of the 6561 assertions in the Template, other than the 12 Exotic Cases, are provably equivalent to the result of replacing ELG by any of ELG ∩ SD, SD, EVSD. All 12 Exotic Cases are refutable in RCA_0 if ELG is replaced by SD or EVSD (Theorem 6.3.5).

The 6561 cases are organized into 10 manageable groups according to the inner trace (quadruple) of letters used. I.e., the Principal Exotic Case above (Proposition A) has inner quadruple ACBC.

Lemma 3.1.6 establishes that we need only consider single clauses, of which there are 14 up to symmetry - and these ten inner traces:

1. AAAA. 20 up to symmetry.
2. AAAB. 81. No symmetries.
3. AABA. 81. No symmetries.
4. AABB. 45 up to symmetry.
5. AABC. 81. No symmetries.
6. ABAB. 36 up to symmetry.
7. ABAC. 45 up to symmetry.
8. ABBA. 45 up to symmetry.
9. ABBC. 81. No symmetries.
10. ACBC. 45 up to symmetry.

This adds up to a total of 574 ordered pairs up to equivalence (including the 14 duplicates or single clauses).

3.2. Some Useful Lemmas

In this section, five useful lemmas are established that are used extensively throughout Chapter 3.

The first of these lemmas provides f ∈ ELG ∩ SD such that whenever A is nonempty and fA ∩ 2N ⊆ A, we have fA is cofinite. This is useful for refuting instances of the Template, since if fA is cofinite then all instances of the Template in which fA appears must be false.

The second and fourth lemmas are variants of the first, also providing g ∈ ELG ∩ SD such that if g feeds any nontrivial A back into A, the gA is cofinite.

The third lemma decomposes any f ∈ ELG ∩ SD into a suitable composition of functions in ELG ∩ SD. It is used to prove the fourth lemma.

The fifth lemma says that if we have finitely many terms in a set variable A ⊆ N, built out of functions from EVSD, then we can find A ∈ INF which is disjoint from all of them. This is particularly straightforward.

3.3. Single Clauses (duplicates).

3.4. AAAA.

3.5. AAAB.

3.6. AABA.

3.7. AABB.

3.8. AABC.

3.9. ABAB.

3.10. ABAC.

3.11. ABBA.

3.12. ABBC.

3.13. ACBC.

In each section, every instance of the Template covered under the titles are either proved or refuted in RCA_0, with one exception. That exception is in section 3.13, and is the Principal Exotic Case (Proposition A). The Principal Exotic Case is treated in Chapters 4,5.

3.14. Annotated Table

Here we present a table of all of the results in sections 3.3 - 3.13.

The Template is based on INF. In sections 3.3 - 3.13, we also treat four alternatives to INF.

AL is "arbitrarily large", which includes infinite.

ALF is "arbitrarily large finite", which does not include infinite.

FIN is "finite".

NON is "nonempty".

The Annotated Table has 584 entries, each treating the five attributes INF, AL, ALF, FIN, NON. Every one of the 6561 instances is symmetric - and therefore trivially equivalent - to one of the 584.

Thus the Annotated Table lists a total of 574 × 5 = 2870 determinations.

3.15 Some Observations

In this final section of Chapter 3, we read off some striking information from examination of the Annotated Table from section 3.14.

The following asserts that ALF and INF come out the same in the Template.

BRT TRANSFER. Let X,Y,V,W,P,R,S,T be among the letters A,B,C. The following are equivalent.
i. for all f,g ∈ ELG and n ≥ 1, there exist finite A,B,C ⊆ N, each with at least n elements, such that X ∪. fY ⊆ V ∪. gW, P ∪. fR ⊆ S ∪. gT.
ii. for all f,g ∈ ELG, there exist infinite A,B,C ⊆ N, such that X ∪. fY ⊆ V ∪. gW, P ∪. fR ⊆ S ∪. gT.

Of course, BRT Transfer has, as a consequence, the Principal Exotic Case (Proposition A). In fact, it is clearly provably equivalent to the Principal Exotic Case over RCA_0.

BRT Transfer provides a way of stating a result in BRT for which it is necessary and sufficient to use large cardinals to prove, without having to give any particular BRT instance.

Chapter 4 Proof of Principal Exotic Case
4.1. Strongly Mahlo Cardinals of Finite Order

In this section, we introduce the large cardinals used to prove the Principal Exotic Case. These are the strongly Mahlo cardinals of finite order.

The relevant large cardinal combinatorics is developed in a self contained way using Erdös-Rado trees.

This large cardinal combinatorics first appeared in [Sc74]. We follow the treatment given in [HKS87].

We use $SMAH^+$ for ZFC + $(\forall n < \omega)(\exists\kappa)(\kappa$ is an n-Mahlo cardinal). We use SMAH for ZFC + $\{(\exists\kappa)(\kappa$ is a strongly n-Mahlo cardinal)$\}_{n<\omega}$.

The large cardinal combinatorics used in the book is given by the following. We give a self contained proof.

LEMMA 4.1.6. Let $n,m \geq 1$, κ a strongly n-Mahlo cardinal, and $A \subseteq \kappa$ unbounded. For all $i \in \omega$, let $f_i:A^{n+1} \to \kappa$, and let $g_i:A^m \to \omega$. There exists $E \subseteq \kappa$ of order type ω such that
i) for all $i \geq 1$, f_iE is either a finite subset of sup(E), or of order type ω with the same sup as E;
ii) for all $i \in \omega$, g_iE is finite.

4.2. Proof using Strongly Mahlo Cardinals

In this section, we prove the Principal Exotic Case (Proposition A) in $SMAH^+$. We actually prove the following sharp form of Proposition B.

PROPOSITION B. Let $f,g \in ELG$ and $n \geq 1$. There exist infinite sets $A_1 \subseteq \ldots \subseteq A_n \subseteq N$ such that
i) for all $1 \leq i < n$, $fA_i \subseteq A_{i+1} \cup. gA_{i+1}$;
ii) $A_1 \cap fA_n = \emptyset$.

We start with $f,g \in ELG$ and $n \geq 1$, with a cardinal κ that is strongly Mahlo of sufficiently high finite order.

We begin with the discrete linearly ordered semigroup with extra structure, $M = (N,<,0,1,+,f,g)$.

We first extend this structure to a countable structure

$$M^* = (N^*,<^*,0^*,1^*,+^*,f^*,g^*,c_0^*,\ldots)$$

generated by the atomic indiscernibles c_i^*, $i \in N$. This construction uses the infinite Ramsey theorem, infinitely iterated.

After verifying a number of properties of M*, we then extend transfinitely to

$$M^{**} = (N^{**},<^{**},0^{**},1^{**},+^{**},f^{**},g^{**},c_0^{**},\ldots,c_\alpha^{**},\ldots)$$

where the c**'s are indexed by the large cardinal κ. In particular, we verify that any partial substructure of M** boundedly generated by 0**, 1**, and a set of c**'s of order type ω, is embeddable back into M* and M.

We then apply then Complementation Theorem for well founded relations (Theorem 1.3.1) to obtain a unique set W of nonstandard elements of M** such that for all nonstandard x in M**,

$$x \in W \leftrightarrow x \notin g^{**}W.$$

We then build a Skolem hull construction of length ω consisting entirely of elements of W. The construction starts with the set of all c**'s. Witnesses are thrown in from W that verify that values of f** at elements thrown in at previous stages do not lie in W (provided they in fact do not lie in W). Only the first n stages of the construction will be used.

Every element of the n-th stage of the Skolem hull construction has a suitable name involving a bounded number of the c**'s.

At this crucial point, we then apply Lemma 4.1.6 to the large cardinal κ, in order to obtain a suitably indiscernible subset of the c**'s of order type ω, with respect to this naming system.

We can redo the length n Skolem hull construction starting with S. This is just a restriction of the original Skolem hull construction that started with all of the c**'s.

Because of the indiscernibility, we generate a subset of N** whose elements are given by terms of bounded length in c**'s of order type ω. This forms a suitable partial substructure of M**, so that it is embeddable back into M. The image of this embedding on the n stages of the Skolem hull construction will comprise the $A_1 \subseteq \ldots \subseteq A_n$ satisfying the conclusion of Proposition B.

This completes the proof of Proposition B in $SMAH^+$.

4.3. Some Existential Sentences

The proof of the Principal Exotic Case in section 4.2 from $SMAH^+$ is not optimal. Proposition B can, in fact, be proved in ACA' + 1-Con(SMAH). This is more delicate, and is proved in section 4.4. Section 4.3 provides a crucial Lemma for that proof.

The Lemma needed is Theorem 4.3.8, which gives a primitive recursive algorithm for determining the truth value of all sentences of the first form

$$(\exists \text{ infinite } B_1,\ldots,B_n \subseteq N^k)$$
$$(\forall i \in \{1,\ldots,n-1\})(\forall x_1,\ldots,x_m \in B_i)$$
$$(\exists y_1,\ldots,y_m \in B_{i+1})(R_i(x_1,\ldots,x_m,y_1,\ldots,y_m))$$

where $k,n,m \geq 1$, and $R_1,\ldots,R_{n-1} \subseteq N^{2km}$ are order invariant relations. Recall that order invariant sets of tuples are sets of tuples where membership depends only on the order type of a tuple. Furthermore, it is provable in ACA' that this algorithm is correct.

We start with the simpler set of sentences of the second form

$$(\exists \text{ infinite } B_1,\ldots,B_n \subseteq N^k)$$
$$(\forall i \in \{1,\ldots,n-1\})$$
$$(\forall x,y,z \in B_i)(\exists w \in B_{i+1})(R_i(x,y,z,w))$$

where $k,n \geq 1$, and $R_1,\ldots,R_{n-1} \subseteq N^{4k}$ are order invariant relations. We primitive recursively convert every sentence of the first form to a corresponding sentence of the second form, without changing the truth value.

We then consider sentences of the third form

$$(\exists f:N^p \to N)(\forall x_1,\ldots,x_q \in N)(\varphi)$$

where φ is a propositional combination of atomic formulas of the forms $x_i < x_j$, $f(y_1,\ldots,y_p) < f(z_1,\ldots,z_p)$, where $x_i,x_j,y_1,\ldots,y_p,z_1,\ldots,z_p$ are among the (distinct) variables $x_1,\ldots,x_q$. We primitive recursively convert every sentence of the second form to a corresponding sentence of the third form, without changing the truth value.

Sentences of the third form are analyzed using strong SOI's. It is shown that a sentence of the third form is true if and only if there is a small finite set of strong SOI's of a certain kind associated with the sentence.

4.4. Proof using 1-consistency

In this section we show that Proposition B - and hence the Principal Exotic Case - can be proved in ACA' + 1-Con(SMAH).

We first restate what is proved in section 4.2 in a different form with numerical parameters.

Recall that in section 4.2, we essentially proved in SMAH that for any suitable structure

$$M^* = (N^*,0^*,1^*,<^*,+^*,f^*,g^*,c_0^*,\ldots)$$

there exist $r \geq 1$ and infinite sets $D[1] \subseteq \ldots \subseteq D[n] \subseteq M^*[r]$ such that $D[1] \subseteq \{c_j^*: j \geq 0\}$, and for all $1 \leq i < n$, $f^*D[i] \subseteq D[i+1] \cup.\ g^*D[i+1]$. Here we assume that $n \geq 1$ and the arities p,q of f^*,g^*, and a bound b on the ELG inequalities, are given in advance. See Lemma 4.4.1.

Since for fixed parameters n,p,q,b, the set of such M* forms a compact space in an appropriate sense, we can choose r so large that it works even if the c*s are only indiscernible with respect to atomic formulas of bounded complexity.

So these considerations allow us formulate an assertion of the form $(\forall n)(\exists m)(\sigma(n,m))$ that implies Proposition B, where for each n, $(\exists m)(\sigma(n,m))$ is provable in SMAH.

Note that if $\sigma(n,m)$ were a primitive recursive equation, then $(\forall n)(\exists m)(\sigma(n,m))$ would be provable in ACA' + 1-Con(SMAH), and so would Proposition B, as required.

However, $\sigma(n,m)$ asserts the existence of a chain of infinite sets of length n satisfying some inclusion relations.

Now Theorem 4.3.8 comes to the rescue, telling us that $\sigma(n,m)$ can be put in primitive recursive form.

Chapter 5 Independence of Exotic Case

5.1 Proposition C and Length 3 Towers

Chapter 5 is devoted to a proof of 1-Con(SMAH) in ACA' + the Principal Exotic Case.

In fact, we use a specialization of the Principal Exotic Case, to a subset of ELG.

This subset is ELG ∩ SD ∩ BAF, where BAF is the countable set of functions given by terms in 0,1,+,-,•,↑,log. Here (see Definition 5.1.1),

1. Addition. x+y is the usual addition.
2. Subtraction. Since we are in N, x-y is defined by the usual x-y if x ≥ y; 0 otherwise.
3. Multiplication. x•y is the usual multiplication.
4. Base 2 exponentiation. x↑ is the usual base 2 exponentiation.
5. Base 2 logarithm. Since we are in N, log(x) is the floor of the usual base 2 logarithm, with log(0) = 0.

It is easier to work with EBAF (extended basic functions), defined in Definition 5.1.7. By Theorem 5.1.4, EBAF = BAF.

In Chapter 5, we give a proof of 1-Con(SMAH) in ACA' + Proposition C.

PROPOSITION C. For all f,g ∈ ELG ∩ SD ∩ BAF, there exist A,B,C ∈ INF such that

A ∪. fA ⊆ C ∪. gB
A ∪. fB ⊆ C ∪. gC.

Throughout Chapter 5, we assume Proposition C.

Note that Proposition C does not tell us that A ⊆ B ⊆ C. This is a very important condition to have, as we want to extend length 3 chains to chains of arbitrary finite length, and then apply compactness to get a single structure.

So in section 5.1, we obtain the badly needed chain of length 3 - but at the cost of degrading the two clauses in Proposition C. The tradeoff is well worth it - and needed.

Section 5.1 concludes with the following.

LEMMA 5.1.7. Let f,g ∈ ELG ∩ SD ∩ BAF and rng(g) ⊆ 6N. There exist infinite A ⊆ B ⊆ C ⊆ N\{0} such that
i) fA ∩ 6N ⊆ B ∪ gB;
ii) fB ∩ 6N ⊆ C ∪ gC;

iii) $fA \cap 2N+1 \subseteq B$;
iv) $fA \cap 3N+1 \subseteq B$;
v) $fB \cap 2N+1 \subseteq C$;
vi) $fB \cap 3N+1 \subseteq C$;
vii) $C \cap gC = \emptyset$;
viii) $A \cap fB = \emptyset$.

The remaining sections in Chapter 5 use only the last Lemma from the previous section, together with the previous definitions.

5.2. From length 3 towers to length n towers

In this section, we obtain a variant of Lemma 5.1.7 (Lemma 5.2.12) involving length n towers rather than length 3 towers.

However, we have to pay a serious cost. As opposed to Lemma 5.1.7, we will only have that the sets in the length n towers have at least r elements, for any given $r \geq 1$.

So it is important to make sure that the first sets in these towers be a suitable set of indiscernibles before we relinquish that the first sets be infinite.

In order to accomplish this, we first apply the infinite Ramsey theorem to shrink the infinite first sets coming from Lemma 5.1.7 to infinite subsets that are sets of indiscernibles of the right kind.

Section 5.2 concludes with the following.

LEMMA 5.2.12. Let $r \geq 3$ and $g \in ELG \cap SD \cap BAF$, where $rng(g) \subseteq 48N$. There exists $(D_1,\ldots,D_r)$ such that
i) $D_1 \subseteq \ldots \subseteq D_r \subseteq N\backslash\{0\}$;
ii) $|D_1| = r$ and D_r is finite;
iii) for all $x < y$ from D_1, $x\uparrow < y$;
iv) for all $1 \leq i \leq r-1$, $48\alpha(r,D_i;1,r) \subseteq D_{i+1} \cup gD_{i+1}$;
v) for all $1 \leq i \leq r-1$, $2\alpha(r,D_i;1,r)+1$, $3\alpha(r,D_i;1,r)+1 \subseteq D_{i+1}$;
vi) $D_r \cap gD_r = \emptyset$;
vii) $D_1 \cap \alpha(r,D_2;2,r) = \emptyset$;
viii) Let $1 \leq i \leq \beta(2r)$, $x_1,\ldots,x_{2r} \in D_1$, $y_1,\ldots,y_r \in \alpha(r,D_2)$, where $(x_1,\ldots,x_r)$ and $(x_{r+1},\ldots,x_{2r})$ have the same order type and min, and $y_1,\ldots,y_r \leq \min(x_1,\ldots,x_r)$. Then
$t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in D_3 \leftrightarrow$
$t[i,2r](x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \in D_3$.

Note the partial shift toward the language driven notions using α. These are carefully defined sets of nonnegative integers given by terms with arguments from sets. Also, note the use of t[i,2r].

5.3. Countable nonstandard models with limited indiscernibles

Our basic standard structure is (N,<,0,1,+,-,•,↑,log) that provides the operations that generate BAF (see section 5.1).

We use Lemma 5.2.12 to create, for each r ≥ 3, a structure (N,<,0,1,+,-,•,↑,log,E_1,...,E_r) with a related set of properties. This is Lemma 5.3.2, which frees us from any further consideration of BAF. Thus we no longer see the D ∪ gD construction, or the D ∩ gD = ∅ condition. See Lemma 5.3.2.

The next major step is to consolidate all of the structures given by Lemma 5.3.2 relative to each r ≥ 3, to a single countable nonstandard structure based on a single tower $E_1 \subseteq E_2 \subseteq$ ... of infinite sets of infinite length. Lemma 5.3.3 also has further simplifications.

One important point is the condition that the resulting single structure M is both a nonstandard model of some arithmetic - with primitives 0,1,+,-,•,↑,log - and also has the crucial tower of subsets $E_1 \subseteq E_2 \subseteq$ ..., acting like unary predicates. The arithmetic is simply the set of all true Π^0_1 sentences. This is important for obtaining 1-Con(SMAH), instead of just Con(SMAH).

A second point is that the elements of the tower are cofinal in the structure.

This consolidation into a single structure is obtained by two steps. The first step is the compactness argument, which arranges for all of the properties except that the E's are cofinal in the structure. The second step is to restrict this structure to the cut given by a subset of the first set in the tower that has order type ω. In fact, this subset of order type ω is just the interpretation of infinitely many constant symbols used in the compactness argument.

There is a considerable development of properties of M. One important development is internal finite sequence coding.

Because of the role of expansive linear growth - traces of which are carried through for several sections - we need the rather delicate way of handling coding provided by Definition 5.3.11.

Section 5.3 ends with the following.

LEMMA 5.3.18. There exists a countable structure M = $(A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,...)$ such that the following holds.
i) $(A,<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies $TR(\Pi^0{}_1,L)$;
ii) $E \subseteq A\backslash\{0\}$;
iii) The c_n, $n \geq 1$, form a strictly increasing sequence of nonstandard elements in $E\backslash\alpha(E;2,<\infty)$ with no upper bound in A;
iv) Let $r,n \geq 1$, $t(v_1,...,v_r)$ be a term of L, and $x_1,...,x_r \leq c_n$. Then $t(x_1,...,x_r) < c_{n+1}$;
v) $2\alpha(E;1,<\infty)+1$, $3\alpha(E;1,<\infty)+1 \subseteq E$;
vi) Let $r \geq 1$, $a,b \in N$, and $\varphi(v_1,...,v_r)$ be a quantifier free formula of L. There exist $d,e,f,g \in N\backslash\{0\}$ such that for all $x_1 \in \alpha(E;1,<\infty)$, $(\exists x_2,...,x_r \in E)(x_2,...,x_r \leq ax_1+b \wedge \varphi(x_1,...,x_r)) \leftrightarrow dx_1+e \notin E \leftrightarrow fx_1+g \in E$;
vii) Let $r \geq 1$, $p \geq 2$, and $\varphi(v_1,...,v_{2r})$ be a quantifier free formula of L. There exist $a,b,d,e \in N\backslash\{0\}$ such that the following holds. Let $n \geq 1$ and $x_1,....,x_r \in \alpha(E;1,<\infty) \cap [0,c_n]$. Then
$(\exists y_1,...,y_r \in E)(y_1,...,y_r \leq \uparrow p(|x_1,...,x_r|) \wedge \varphi(x_1,...,x_r,y_1,...,y_r)) \leftrightarrow$
$aCODE(c_{n+1};x_1,...,x_r)+b \notin E \leftrightarrow$
$dCODE(c_{n+1};x_1,...,x_r)+e \in E$. Here CODE is as defined just before Lemma 5.3.11;
viii) Let $k,n,m \geq 1$, and $x_1,...,x_k \leq c_n < c_m$, where $x_1,...,x_k \in \alpha(E;1,<\infty)$. Then $CODE(c_m;x_1,...,x_k) \in E$;
ix) Let $r \geq 1$ and $t(v_1,...,v_{2r})$ be a term of L. Let $i_1,...,i_{2r} \geq 1$ and $y_1,...,y_r \in E$, where $(i_1,...,i_r)$ and $(i_{r+1},...,i_{2r})$ have the same order type and min, and $y_1,...,y_r \leq \min(c_{i\_1},...,c_{i\_r})$. Then
$t(c_{i\_1},...,c_{i\_r},y_1,...,y_r) \in E \leftrightarrow$
$t(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r) \in E$.

Note that the infinite tower of sets from the M of Lemma 5.3.3 is removed in favor of a single subset E, and constants c_n, $n \geq 1$, enumerating the first term of the tower. The single set E is simply the union of the tower of E's from the M of Lemma 5.3.3. The E is cofinal in the structure.

5.4. Limited formulas, limited indiscernibles, Note that the M of Lemma 5.3.18 obeys two special forms of existential comprehension (clauses vi, vii), and one form of quantifier free indiscernibility (clause ix).

We upgrade these to a single form of comprehension for formulas with bounded quantifiers, and indiscernibility for formulas with bounded quantifiers. The range of this comprehension is E only, and the objects used in the indiscernibility are also only from E.

In fact, the bounded quantifier comprehension is given in terms of a normal form. I.e., every suitable k-ary relation on E is given by fixing 8 parameters from E in a fixed atomic formula with k+8 variables.

Section 5.4 ends with the following.

LEMMA 5.4.17. There exists a countable structure M = $(A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,...)$, and terms $t_1,t_2,...$ of L, where for all i, t_i has variables among $v_1,...,v_{i+8}$, such that the following holds.
i) $(A,<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies $TR(\Pi^0_1,L)$;
ii) $E \subseteq A\backslash\{0\}$;
iii) The c_n, $n \geq 1$, form a strictly increasing sequence of nonstandard elements in $E\backslash\alpha(E;2,<\infty)$ with no upper bound in A;
iv) Let $r,n \geq 1$ and $t(v_1,...,v_r)$ be a term of L, and $x_1,...,x_r \leq c_n$. Then $t(x_1,...,x_r) < c_{n+1}$;
v) $2\alpha(E;1,<\infty)+1$, $3\alpha(E;1,<\infty)+1 \subseteq E$;
vi) Let $k,n \geq 1$ and R be a c_n-definable k-ary relation. There exists $y_1,...,y_8 \in E \cap [0,c_{n+1}]$ such that R = $\{(x_1,...,x_k) \in E^k \cap [0,c_n]^k: t_k(x_1,...,x_k,y_1,...,y_8) \in E\}$;
vii) Let $r \geq 1$ and $\varphi(v_1,...,v_{2r})$ be a formula of L(E). Let $1 \leq i_1,...,i_{2r} < n$, where $(i_1,...,i_r)$ and $(i_{r+1},...,i_{2r})$ have the same order type and the same min. Let $y_1,...,y_r \in E$, $y_1,...,y_r \leq \min(c_{i\_1},...,c_{i\_r})$. Then $\varphi(c_{i\_1},...,c_{i\_r},y_1,...,y_r)^{c\_n} \leftrightarrow \varphi(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r)^{c\_n}$.

5.5. Comprehension, indiscernibles

Here we upgrade the bounded quantifier comprehension and indiscernibility to unbounded quantifier comprehension and indiscernibility. It is the indiscernibility itself that allows us to make this transition.

The comprehension produces bounded relations on E only.

A very robust and useful notion of internal relation emerges. These are the bounded relations on E that are definable with parameters from E and quantifiers ranging over E. See Lemma 5.5.4.

We pass to a second order structure where the internal relations are used to interpret the second order quantifiers.

We retain comprehension and indiscernibility in the appropriate forms.

Section 5.5 ends with the following.

LEMMA 5.5.8. There exists a countable structure $M^* = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,\ldots,X_1,X_2,\ldots)$, where for all $i \geq 1$, X_i is the set of all i-ary relations on A that are c_n-definable for some $n \geq 1$; and terms $t_1,t_2,\ldots$ of L, where for all i, t_i has variables among $x_1,\ldots,x_{i+8}$, such that the following holds.
i) $(A,<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies $TR(\Pi^0_1,L)$;
ii) $E \subseteq A\backslash\{0\}$;
iii) The c_n, $n \geq 1$, form a strictly increasing sequence of nonstandard elements of $E\backslash\alpha(E;2,<\infty)$ with no upper bound in A;
iv) For all $r,n \geq 1$, $\uparrow r(c_n) < c_{n+1}$;
v) $2\alpha(E;1,<\infty)+1$, $3\alpha(E;1,<\infty)+1 \subseteq E$;
vi) Let $k,n \geq 1$ and R be a c_n-definable k-ary relation. There exists $y_1,\ldots,y_8 \in E \cap [0,c_{n+1}]$ such that $R = \{(x_1,\ldots,x_k) \in E^k \cap [0,c_n]^k: t_k(x_1,\ldots,x_k,y_1,\ldots,y_8) \in E\}$;
vii) Let $k \geq 1$, $m \geq 0$, and φ be an E formula of $L^*(E)$ in which R is not free, where all first order variables free in φ are among $x_1,\ldots,x_{k+m+1}$. Then $x_{k+1},\ldots,x_{k+m+1} \in E \rightarrow (\exists R)(\forall x_1,\ldots,x_k \in E)(R(x_1,\ldots,x_k) \leftrightarrow (x_1,\ldots,x_k \leq x_{k+m+1} \wedge \varphi))$;
viii) Let $r \geq 1$, and $\varphi(x_1,\ldots,x_{2r})$ be an E formula of $L^*(E)$ with no free second order variables. Let $1 \leq i_1,\ldots,i_{2r}$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and the same min. Let $x_1,\ldots,x_r \in E$, $x_1,\ldots,x_r \leq \min(c_{i\_1},\ldots,c_{i\_r})$. Then $\varphi(c_{i\_1},\ldots,c_{i\_r},x_1,\ldots,x_r) \leftrightarrow \varphi(c_{i\_r+1},\ldots,c_{i\_2r},x_1,\ldots,x_r)$.

5.6. Π^0_1 correct internal arithmetic, simplification

The main focus of this section is the derivation of a suitable form of the axiom of infinity. This is the one place where it is essential to use that the c_n, $n \geq 1$, lie outside $\alpha(E;2,<\infty)$. This is from Lemma 5.5.8 iii).

The axiom of infinity takes the form of the existence of an internal set containing 1, and closed under $+2c_1$.

We then define I to be the intersection of all internal sets containing 1, and closed under $+2c_1$. The set I will serve as the internal natural numbers.

It is important to link the arithmetic operations that are uniquely defined, internally, on I, with the arithmetic operations given by the structure M* from Lemma 5.5.8. This is required in order to be able to use the fact that M* satisfies the true Π^0_1 sentences. It allows us to conclude that the internal arithmetic on I satisfies the true Π^0_1 sentences.

The required link is provided by Lemma 5.6.11.

LEMMA 5.6.11. Every element of I is of the form $2xc_1+1$, with $x \in E-E$. $x \in I \wedge x > 1 \rightarrow x-2c_1 \in I$.

Thus we link each $2xc_1+1 \in I$ with $x \in E-E$. This suggests that we can define $+,\bullet,-,\uparrow$,log on I by applying the $+,\bullet,-$ $,\uparrow$,log at relevant elements of E-E. But in order to do this, we need to know, e.g., that

$$2xc_1+1, 2yc_1+1 \in I \rightarrow 2xyc_1+1 \in I.$$

This is exactly what is established in Lemma 5.6.12.

So this defines the structure

$$M(I) = (I,<,0',1',+',-',\bullet',\uparrow',\log')$$

as in Definition 5.6.4, which is isomorphically embeddable in $(A,<,0,1,+,-,\bullet,\uparrow,\log)$.

Since $(A,<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies the true Π^0_1 sentences, we would like to conclude that M(I) also satisfies the true Π^0_1 sentences. However, because of the bounded quantifiers in Π^0_1 sentences, we can only conclude that M(I) satisfies the true Π^0_1 sentences with no bounded quantifiers allowed.

However, in the presence of PA, every Π^0_1 sentence is equivalent to a Π^0_1 sentence with no bounded quantifiers, using the Y. Matiyasevich solution to Hilbert's 10th problem (based on earlier work of J. Robinson, M. Davis, and H. Putnam). See [Da73], [Mat93].

By Lemma 5.6.13, M(I) satisfies PA. Therefore M(I) satisfies PA + the true Π^0_1 sentences.

We now introduce the linearly ordered set theory K(Π) in Definition 5.6.10. It has a linear ordering of the universe, full separation, an initial segment serving as the integers, with operations +,-,•,↑,log, obeying the true Π^0_1 sentences. There is also an infinite list of constants with axioms of indiscernibility.

A model of K(Π) is explicitly constructed using M* and M(I). We put I at the bottom, and E (without the initial segment of E determined by I) on top. The arithmetical operations on I are inherited from M(I). The c's, after c_1, serve as the indiscernibles. The $\in$ relation is interpreted using the normal form relation σ from Lemma 5.6.17.

Section 5.6 ends with the following.

LEMMA 5.6.20. There exists a countable structure M# = $(D,<,\in,NAT,0,1,+,-,\bullet,\uparrow,\log,d_1,d_2,\ldots)$ such that the following holds.
i) < is a linear ordering (irreflexive, transitive, connected);
ii) $x \in y \rightarrow x < y$;
iii) The d_n, $n \geq 1$, form a strictly increasing sequence of elements of D with no upper bound in D;
iv) Let φ be a formula of L# in which v_1 is not free. Then $(\exists v_1)(\forall v_2)(v_2 \in v_1 \leftrightarrow (v_2 \leq v_3 \wedge \varphi))$;
v) Let $r \geq 1$ and $\varphi(v_1,\ldots,v_{2r})$ be a formula of L#. Let $1 \leq i_1,\ldots,i_{2r}$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and min. Let $y_1,\ldots,y_r \leq \min(d_{i\_1},\ldots,d_{i\_r})$. Then $\varphi(d_{i\_1},\ldots,d_{i\_r},y_1,\ldots,y_r) \leftrightarrow \varphi(d_{i\_r+1},\ldots,d_{i\_2r},y_1,\ldots,y_r)$;
vi) NAT defines a nonempty initial segment under <, with no greatest element, and no limit point, where all points are $< d_1$, and whose first two elements are 0,1, respectively;
vii) $(\forall x)$(if x has an element obeying NAT then x has a < least element);
viii) Let $\varphi \in TR(\Pi^0_1,L)$. The relativization of φ to NAT holds.
ix) +,-,•,↑,log have the default value 0 in case one or more arguments lie outside NAT.

5.7. Transfinite induction, comprehension, indiscernibles, infinity, Π^0_1 correctness

In M#, the < may not be internally well ordered. Moreover, we may not have extensionality.

The focus of section 5.7 is on creating a structure corresponding to the M# of Lemma 5.6.20 with an internally well founded <. However, this new structure will not be a model of a set theory, but rather a second order structure. I.e., we will have a linearly ordered set of points, with a family of relations on the points of each arity.

We will obtain full second order separation (second order of course limited to these families of relations), and an initial segment corresponding to the natural numbers. We will also obtain an infinite sequence of indiscernibles as in Lemma 5.6.20, cofinal in the linear ordering.

The idea is to first develop a theory of pre well orderings (as binary relations) within M#. Every binary relation in M# is a point, since M# is a model of a set theory.

We use this theory of pre well orderings to place two closely related relations <#, ≤#, on points. See Definitions 5.7.21 and 5.7.22. These are, generally speaking, much stronger than the relations <, ≤. We define x =# y ↔ (x ≤# y ∧ y ≤# x).

By Lemma 5.7.18, we have the trichotomy

x <# y ∨ y <# x ∨ x =# y, with exclusive ∨.

The points in the desired structure with internal well foundedness are the equivalence classes under =#, each of which forms an interval of points in M*.

For the rest of the definition of the second order structure M^, see Definitions 5.7.26 - 5.7.34.

Section 5.7 ends with the following.

LEMMA 5.7.30. There exists a structure M^ = $(C,<,0,1,+,-,\bullet,\uparrow,\log,\omega,c_1,c_2,...,Y_1,Y_2,...)$ such that the following holds.
i) (C,<) is a linear ordering;
ii) {x: x < ω} forms an initial segment of (C,<);
iii) ({x: x < ω},<,0,1,+,-,•,↑,log) satisfies $TR(\Pi^0_1,L)$;
iv) For all x,y ∈ C, ¬(x < ω ∧ y < ω) → x+y = x•y = x-y = x↑ = log(x) = 0;

v) The c_n, $n \geq 1$, form a strictly increasing sequence of elements of C, all > ω, with no upper bound in C;
vi) For all $k \geq 1$, Y_k is a set of k-ary relations on C whose field is bounded above;
vii) Let $k \geq 1$, and φ be a formula of L^ in which the k-ary second order variable B^k_n is not free, and the variables B^m_r range over Y_r. Then $(\exists B^k_n \in Y_k)(\forall x_1,\ldots,x_k)(B^k_n(x_1,\ldots,x_k) \leftrightarrow (x_1,\ldots,x_k \leq y \wedge \varphi))$;
viii) Every nonempty M^ definable subset of C has a < least element;
ix) Let $r \geq 1$ and $\varphi(v_1,\ldots,v_{2r})$ be a formula of L^. Let $1 \leq i_1,\ldots,i_{2r}$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and the same min. Let $y_1,\ldots,y_r \in C$, $y_1,\ldots,y_r \leq \min(c_{i\_1},\ldots,c_{i\_r})$. Then $\varphi(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \leftrightarrow \varphi(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)$.

5.8. ZFC + V = L, indiscernibles, and Π^0_1 correct arithmetic

Now that we have a second order structure M^ from Lemma 5.7.30, we want to move back to a model of set theory. This time, the model will be of ZFC + V = L + the true Π^0_1 sentences, with an unbounded infinite sequence of ordinals with indiscernibility.

We need to build the constructible hierarchy in order to fully utilize the indiscernibility afforded by Lemma 5.7.30. In particular, the definable well ordering arising from L is needed in order to derive power set from indiscernibility.

Because of the internal well foundedness, the points in M^ already behave like ordinals. In M^, we can perform various transfinite recursions, resulting in second objects in M^. Sometimes in order to accomplish this, we make use of the indiscernibles in M^.

Extensionality, pairing, and union are verified in L by Lemma 5.8.24. Infinity is verified in L by Lemma 5.8.25. Foundation is verified in L by Lemma 5.8.26. Separation and Collection, both of which are schemes, are verified in L by Lemma 5.8.29.

We then show that power set holds in L with heavy use of indiscernibility.

It suffices to show that if, in L, every element of $x \in L$ is constructed before stage c_2, then $x < c_3$. (We can obtain such a strong conclusion because extensionality is built into the construction of L). This is Lemma 5.8.32.

If this is false, then by indiscernibility, for each $n \geq 3$, there is an $x \geq c_n$ such that every element of x in L is constructed before stage c_2.

Using the definable well ordering of L, we can set J(n) to be the < least $x \geq c_n$ such that every element of x in L is constructed before stage c_2.

But by indiscernibility, $J(4) < J(5)$ and J(4),J(5) will have the same elements in L. This is a contradiction. The treatment in section 5.8 is fully detailed. See Lemma 5.8.34.

We now obtain a model of ZF of the required kind. See Lemma 5.8.36. We can then relativize to L to obtain ZFC + V = L.

Section 5.8 ends with the following.

LEMMA 5.8.37. There exists a countable model M^+ of ZFC + V = L + TR(Π^0_1,L), with distinguished elements $d_1,d_2,\ldots$, such that
i) The d's are strictly increasing ordinals in the sense of M^+, without an upper bound;
ii) Let $r \geq 1$, and $i_1,\ldots,i_{2r} \geq 1$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and min. Let R be a 2r-ary relation M^+ definable without parameters. Let $\alpha_1,\ldots,\alpha_r \leq \min(d_{i\_1},\ldots,d_{i\_r})$. Then $R(d_{i\_1},\ldots,d_{i\_r},\alpha_1,\ldots,\alpha_r) \leftrightarrow R(d_{i\_r+1},\ldots,d_{i\_2r},\alpha_1,\ldots,\alpha_r)$.

5.9. ZFC + V = L + $\{(\exists\kappa)(\kappa$ is strongly k-Mahlo$)\}_k$ + TR(Π^0_1,L), and 1-Con(SMAH).

We first give a complete proof of a result in combinatorial set theory, of independent interest and not involving any developments in the book from sections 1.1 through 5.8. It is closely related to [Sc74] and the treatment is inspired by [HKS87]. The result is as follows.

THEOREM 5.9.5. The following is provable in ZFC. Let $k < \omega$ and α be an ordinal. Then $R(\alpha\backslash\omega,k+3,k+5)$ if and only if there is a strongly k-Mahlo cardinal $\leq \alpha$.

We then return to the model M^+ of ZFC + V = L + the true Π^0_1 sentences, given by Lemma 5.8.37.

We show that the indiscernibles themselves (the d's of M^+) essentially obey the relevant partition properties.

LEMMA 5.9.6. Let $k,r \geq 1$ be standard integers. Then $R(d_{r+2}+1\backslash\omega,k,r)$ holds in M^+.

This is proved by first assuming that it is false, and then taking the L least counterexample. We can do this since M^+ obeys V = L. Then apply the indiscernibility in M^+ from Lemma 5.8.37.

We then easily obtain that M^+ satisfies ZFC + V = L + $\{$there exists a strongly k-Mahlo cardinal$\}_k$ + the true Π^0_1 sentences. In fact, we conclude

THEOREM 5.9.11. ACA' proves the equivalence of each of Propositions A,B,C and 1-Con(MAH), 1-Con(SMAH).

The above is shown by checking that all of the relevant steps in Chapter 5 can be carried out within ACA', and quoting Theorem 4.4.11.

Chapter 5 ends with the following.

THEOREM 5.9.12. None of Propositions A,B,C are provable in any set of consequences of SMAH that is consistent with ACA'. The preceding claim is provable in RCA_0. For finite sets of consequences, the first claim is provable in EFA.

Chapter 6 Further Results

6.1. Propositions D-H

In section 6.1, we establish Theorem 5.9.11 for several variants of Propositions A,B,C. This requires various adaptations of Chapters 4 and 5.

The strongest proposition considered in this book that is proved from large cardinals is the following.

PROPOSITION D. Let $f \in LB \cap EVSD$, $g \in EXPN$, $E \subseteq N$ be infinite, and $n \geq 1$. There exist infinite $A_1 \subseteq \ldots \subseteq A_n \subseteq N$ such that

i) for all $1 \leq i < n$, $fA_i \subseteq A_{i+1} \cup. gA_{i+1}$;
ii) $A_1 \cap fA_n = \emptyset$;
iii) $A_1 \subseteq E$.

Proposition D immediately implies Proposition B. We then adapt Chapter 4 to derive Proposition D in ACA' + 1-Con(SMAH).

We then consider the remaining main variants of Propositions A,B,C in section 6.1.

PROPOSITION E. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A ⊆ B ⊆ C ⊆ N, each containing infinitely many powers of 2, such that

fA ⊆ B ∪. gB
fB ⊆ C ∪. gC.

PROPOSITION F. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A ⊆ B ⊆ C ⊆ N, each containing infinitely many powers of 2, such that

fA ⊆ C ∪. gB
fB ⊆ C ∪. gC.

PROPOSITION G. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A,B,C ⊆ N, whose intersection contains infinitely many powers of 2, such that

fA ⊆ C ∪. gB
fB ⊆ C ∪. gC.

PROPOSITION H. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A,B,C ⊆ N, where A ∩ B contains infinitely many powers of 2, such that

fA ⊆ C ∪. gB
fB ⊆ C ∪. gC.

We first observe that in RCA_0, D → E → F → G → H. See Lemma 6.1.5.

Section 6.1 ends with an adaptation of part of Chapter 5 in order to resolve the status of Propositions E-H. I.e., ACA' proves Propositions E-H are equivalent to Con(SMAH). See Theorem 6.1.10.

6.2. Effectivity

Section 6.2 begins with a straightforward proof that Propositions A-H hold in the arithmetic sets. The proof is conducted in ACA^+. See Definition 6.2.1.

Next in section 6.2, we show that Propositions C,E-H hold in the recursive sets (and even in the sets with primitive recursive enumeration functions). We also show that this result is provably equivalent to 1-Con(SMAH) over ACA'.

We don't know if any or all of Propositions A,B,D hold in the recursive sets. We conjecture that they do not.

Recall that in the proofs of Propositions C,E-H coming out of Chapter 4, we rely on an infinite set of indiscernibles for functions in BAF. These sets of indiscernibles are given by applying the infinite Ramsey theorem, and so go up the arithmetic hierarchy, and are far from being recursive.

A key idea of section 6.2 is the development of appropriate infinite sets of indiscernibles for functions in BAF that are recursive - and even primitive recursive or better.

This relies on properties of the structure (N,+,↑), or base 2 exponential Presburger arithmetic. It has a primitive recursive decision procedure going back to [Se80], [Se83]. A modern treatment of quantifier elimination for this structure (with additional predicates) appears in [CP85], and also a more recent version appears as Appendix B in this book, authored by F. Point.

The required infinite sets of indiscernibles are given by Lemma 6.2.17.

Section 6.2 continues with an adaptation of sections 4.3 and 4.4 primitive recursively. This culminates with Theorem 6.2.20.

6.3. A Refutation

Section 6.3 is devoted to a refutation of the following.

PROPOSITION α. For all f,g ∈ SD ∩ BAF there exist A,B,C ∈ INF such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

Note that this shows the need for using ELG in Propositions A,B,C. In fact, section 6.3 contains a refutation of the following.

PROPOSITION β. Let f,g ∈ SD ∩ BAF. There exist A,B,C ⊆ N, |A| ≥ 4, such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

The proof proceeds by assuming Proposition β, and first adapting Lemma 5.1.8. See Lemma 5.1.8'. This is followed by a combinatorial construction that provides the required contradiction.

0.16. Some Open Problems.

1. Is the set of all true instances of EBRT (or IBRT) in $A_1,...,A_k,f_1A_1,...,f_1A_m,...,f_nA_1,...,f_nA_m$ on (MF,INF) (or (SD,INF), (ELG,INF), (EVSD,INF)) recursive? Here n,m are not fixed. We expect a positive result to be hugely intractable, and so we are raising the possibility of a negative result.

2. PBRT was introduced in section 1.1, but not investigated in this book. It is spectacularly more complex than EBRT and IBRT. See Definition 1.1.26, and the brief discussion of PBRT right after the proof of Theorem 1.1.2. What can we say about PBRT in A,fA on (MF,INF) (or (SD,INF), (ELG,INF), (EVSD,INF))? What about question 1 for PBRT?

3. Does the behavior of BRT fragments in the various BRT settings presented in section 1.2 depend very delicately on the choice of BRT setting, as we believe? Give some precise formulations of this question and determine whether they hold.

4. This concerns the Upper Complementation Theorem of section 1.3. Is there a decision procedure for determining whether, given two affine functions $f:N^k \to Z$, whether their unique upper complementations are equal? What if the two functions are quadratics? Polynomials? For any given affine f, what can we say about the computational complexity of its unique upper complementation?

5. Every instance of EBRT in $A,B,fA,fB,\subseteq$ on (SD,INF), (ELG,INF), (EVSD,INF) is provable or refutable in RCA_0. This is shown in sections 2.4, 2.5. Is every instance of EBRT in A,B,fA,fB on (SD,INF), (ELG $\cap$ SD,INF), (ELG,INF), (EVSD,INF) provable or refutable in RCA_0? As a presumably smaller step, what about using $A,B,fA,fB,fU,\subseteq$?

6. Every instance of EBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (MF,INF) is provable or refutable in RCA_0. This is shown in section 2.6. Is every instance of EBRT in $A_1,...,A_k,fA_1,...,fA_k$ on (MF,INF) provable or refutable in RCA_0? What if k = 2?

7. What about question 5 for IBRT in light of section 2.7?

Recall the Template of Chapter 3:

TEMPLATE. For all f,g ∈ ELG there exist A,B,C ∈ INF such that

$$X \cup. fY \subseteq V \cup. gW$$
$$P \cup. fR \subseteq S \cup. gT.$$

Consider two richer Templates.

TEMPLATE'. For all f,g ∈ ELG there exist A,B,C ∈ INF such that

$$X \cup. fY \subseteq V \cup. gW$$
$$P \cup. fR \subseteq S \cup. gT.$$
$$D \cup. fE \subseteq J \cup. gK.$$

TEMPLATE ''. For all f,g ∈ ELG there exist A,B,C ∈ INF such that

$$X \cup. \alpha Y \subseteq V \cup. \beta W$$
$$P \cup. \gamma R \subseteq S \cup. \delta T.$$

where $\alpha,\beta,\gamma,\delta$ are among the letters f,g.

8. Every instance of the above Template is provable or refutable in $SMAH^+$. This is shown in Chapter 3. Is this true for Template'? Is this true for Template''?

9. The Principal Exotic Case (Proposition A) universally quantifies over eight numerical parameters. The upper and lower rational constant factors for f ∈ ELG, the lower and upper rational constant factors for g ∈ ELG, constants for sufficiently large associated with each of these four rational constant factors, the arity of f, and the arity of g. In the case of Proposition B, there is an additional parameter, namely the length of the tower. In section 4.2, we proved Proposition B by fixing p,n ≥ 1, where p is the arity of f, and n is the length of the tower. We used a strongly p^{n-1}-Mahlo cardinal. This amounts to using a strongly p^2-Mahlo cardinal to prove the Principal Exotic Case (Proposition A). What is the least order of strong Mahloness needed here? Also, what is the metamathematical status of Propositions A (B) if we fix various combinations of the eight (nine) parameters and let the others vary? For some combinations, we expect to get independent statements, and for other combinations we expect to get Σ^0_1 statements,

which are, of course provable. But do we get length of proof results corresponding to the provably recursive functions of SMAH?

10. The Principal Exotic Case, is an instance of EBRT in A,C,fA,fB,gB,gC on (ELG,INF). The Principal Exotic Case with $A \subseteq B \subseteq C$ is an instance of EBRT in A,C,fA,fB,gB,gC,$\subseteq$ on (ELG,INF). They are both provable in $SMAH^+$ but not in SMAH. This is shown in section 4.2 and in Chapter 5. Is every instance of EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF) provable or refutable in $SMAH^+$? What about in A,B,C,fA,fB,fC,gA,gB,gC,$\subseteq$, A,C,fA,fB,gB,gC, or A,C,fA,fB,gB,gC,$\subseteq$?

11. ACA' proves that Propositions A-H are each equivalent to 1-Con(SMAH). This is shown in section 6.1. For which of these Propositions, can ACA' be replaced by RCA_0, or by WKL_0 in either the forward or the reverse direction of the equivalence?

12. Propositions A-H hold in the arithmetic sets. This is shown in section 6.2. Does the Principal Exotic Case (Proposition A) hold in the recursive sets? What about Propositions B,D?

13. Propositions C,E-H hold in the recursive sets, and even in the sets with primitive recursive enumeration functions. This is shown in section 6.2. Do Propositions C,E-H hold in the sets with superexponential enumeration functions as discussed at the end of section 6.2?

14. What is the status of Proposition D[5] presented in section 6.1? What is the status of Proposition G[1], also presented in section 6.1?

0.17. Concreteness in the Hilbert Problem List.

We now discuss the levels of Concreteness associated with Hilbert's famous list of 23 problems, 1900. See [Br76], and http://en.wikipedia.org/wiki/Hilbert's_problems#Table_of_problems

[Br76] includes a reprint of Hilbert's article. For ready web access, see

http://aleph0.clarku.edu/~djoyce/hilbert/toc.html
http://aleph0.clarku.edu/~djoyce/hilbert/problems.html

It is important to distinguish between two quite different but overlapping projects. We use HP for "Hilbert's Problems".

HP PROOF THEORY. An analysis of levels of Concreteness in the **proofs of theorems** surrounding the Hilbert problem list.

HP STATEMENT THEORY. An analysis of levels of Concreteness in the **statements of propositions** surrounding the Hilbert problem list.

In this section, we focus entirely on HP Statement Theory. We view it as preliminary to a systematic development of HP Proof Theory.

There is a very limited amount of work in HP Proof Theory. We view HP Proof Theory as part of a wider Mathematical Proof Theory limited to theorems surrounding the Hilbert problem list. Here Mathematical Proof Theory is the systematic study of Concreteness in mathematical proofs, generally in the sense of Reverse Mathematics and Strict Reverse Mathematics as discussed in section 0.4.

We view HP Statement Theory as part of a wider Mathematical Statement Theory limited to propositions (which may or may not be theorems) surrounding the Hilbert problem list. HP Mathematical Statement Theory is the systematic study of Concreteness in mathematical statements. We make full use of the basic framework laid out in section 0.3, consisting of the categories of sentences

$$\Pi^0_n,\ \Sigma^0_n,\ \Pi^1_n,\ \Sigma^1_n,\ 0 \leq n \leq \infty$$

discussed there. In Mathematical Statement Theory, we begin with a mathematical proposition P, and proceed as follows.

a. We first examine a fully detailed statement of P and find the lowest category in which it resides, without significant reformulation of P. We say that P is literally Π^i_j (or Σ^i_j).

b. We then find a reformulation P' of P, so that we can prove the equivalence P $\leftrightarrow$ P', where P' is in the lowest category of sentences above that we can find. We say that P is essentially Π^i_j (or Σ^i_j).

c. If P has already been proved (or refuted), then b) is not to be taken literally, because we can always take P' to be 0 = 0 (or 1 = 0), and declare any P to be essentially Π^0_0. In other words, if we just follow b) uncritically, then Mathematical Statement Theory does not apply to theorems - only to propositions of unknown status.

d. In case P has already been proved (or refuted), we demand that the proof of the equivalence P ↔ P' be based on generally applicable principles, and not involve substantial ideas from the proof (or refutation) of P.

e. Of special note in the theory are implications P' → P, where P' is in the lowest category we can find, and P' is interesting. I.e., P' is a strengthening of P. If P is not (yet) a theorem, then we want P' to represent a reasonable path toward proving P. If P is a theorem, then we want the proof of the implication P' → P to not involve substantial ideas from the proof of P, and ideally, P' should also be a theorem. This often occurs when one discovers the "combinatorial essence" of a proof. P' is based on the combinatorial essence of P.

We acknowledge the informal nature of d), but submit that in practice, d) is rather objective. To a lesser extent, there are fuzzy issues regarding a) as well. In fact, a) and d) appear to be sufficiently objective in practice to support the viability of Mathematical Statement Theory.

Coming back to HP Proof Theory, the principal tool used for analyzing levels of Concreteness in proofs is our Reverse Mathematics program (RM). The RM program was discussed in detail in section 0.3.

However, not much of the work surrounding the Hilbert problems falls under the scope of RM. One reason is that so much of the work on these problems falls below the radar screen of RM - the proof is already carried out (or easily seen to be carried out) in the base theory, RCA_0, of RM.

As discussed in section 0.3, our Strict Reverse Mathematics program (SRM), which was conceived of even before RM, has a far more ambitious scope than RM. However, SRM is at a very early stage of development, having been effectively launched only with the recent [Fr09], [Fr09a] - and only there in certain limited directions. Yet more substantial work needs to be done in order to bring SRM to anything like the level of development RM even decades ago.

It would seem premature to apply SRM to HP Proof Theory at this point, although such a venture will be a great test for the SRM program.

It would be of great interest to investigate Smale Problems Statement Theory, and Clay Problems Statement Theory, based on the 18 Smale problems, 1998, and the 7 Clay Millennium Prize Problems, 2000. See [Sm00] and [http://www.claymath.org].

There are many gaps in our limited discussion of HP Statement Theory. We view the treatment below as a good starting point for an intensive and systematic investigation. This, in turn, should serve as a prototype for Mathematical Statement Theory.

However, it must be said that it is not yet clear just what the most fruitful and illuminating frameworks are for a suitable discussion of Concreteness and Abstraction in mathematics. Even though the framework of Mathematical Statement Theory needs to be solidified and amplified, we expect it will remain an integral part of subsequent formulations.

H1. Cantor's problem of the cardinal number of the continuum

This well known problem of Cantor in abstract set theory - called the continuum hypothesis - can be conveniently stated as follows. Every infinite set of real numbers is in one-one correspondence with the integers of the real numbers. Assuming ZFC is consistent, this statement is not provable in ZFC ([Co63,64]), and not refutable in ZFC ([Go38], [Go86-03]). The use of all sets of real numbers (and functions onto the reals) means that it is a statement of Abstract Mathematics as opposed to Concrete Mathematics.

Furthermore, it is well known that the Continuum Hypothesis is not provably equivalent, over ZFC, to any Π^1_n sentence, n $\geq$ 1, and hence lies essentially ouside of Concrete Mathematics.

The easiest way to prove this claim is to start with a countable model M of ZFC + $2^\omega = \omega_2$. Let M' be a generic extension of M obtained by collapsing ω_2 to ω_1 using countable functions from ω_1 into ω_2. Then $2^\omega = \omega_1$ holds in M', yet M and M' have the same real numbers.

The continuum hypothesis has well known specializations to (more) concrete mathematical objects. For instance, it is provable in ZFC that every infinite Borel set of real numbers is in one-one correspondence with the integers or the real numbers.

To be fully coherent, we also need to treat the maps. It is also provable in ZFC that every infinite Borel set of real numbers is in Borel one-one correspondence with the integers or the real numbers. In fact, we can replace Borel by "Borel of finite rank".

This Borel form of the continuum hypothesis follows easily from the classic theorem of Alexandrov and Hausdorff that every Borel set of real numbers is either countable or contains a Cantor set, and the obvious Borel form of the Cantor-Bernstein theorem. See [Ke95], p. 83, and [Je78,06].

H2. The compatibility of the arithmetical axioms

This is properly viewed as a metamathematical problem as opposed to a mathematical problem. However, it did generate a considerable amount of work on formal systems and their relationships, beginning, most notably, with [Pr29] and [Go31].

These formal investigations generally give rise to formal problems in classes Π^0_1, Σ^0_1, Π^0_2, and Σ^0_2, and theorems in classes Π^0_1, Π^0_2.

For instance, consistency of an effectively presented formal system is a Π^0_1 sentence; interpretability of one finitely axiomatized system in another is a Σ^0_1 sentence; 1-consistency of an effectively presented formal system is a Π^0_2 sentence; interpretability of one effectively presented formal system in another is a Σ^0_3 sentence. In each specific example, the relevant theorems witness the outermost existential quantifiers with particular interpretations.

H3. The equality of two volumes of two tetrahedra of equal bases and equal altitudes

Hilbert asks whether there exists

two tetrahedra of equal bases and equal altitudes which can in no way be split up into congruent tetrahedra, and which cannot be combined with congruent tetrahedra to form two polyhedra which themselves could be split up into congruent tetrahedral.

The dissections are normally required to be polyhedra, in the sense of a 3 dimensional solid consisting of a collection of polygons, joined at their edges.

The problem is literally $\Sigma^1{}_2$ as stated. This is a rather high complexity class, given that so much mathematics is $\Pi^0{}_\infty$.

Suppose two tetrahedra are given, as well as an integer bound on the number of complementary tetrahedra allowed, the number of pieces in the dissections allowed, and the number of points in the polyhedra allowed. Then the statement of impossibility can be expressed as a first order formula in the ordered field of reals. Thus the formula is subject to Tarski's elimination of quantifiers for real closed fields, [Ta51], and is quantifier free in the language of ordered fields.

These considerations show that H3 is essentially $\Sigma^1{}_1$. The outermost second order existential quantifiers correspond to the tetrahedral, which are followed by a universal quantifier(s) over integers, corresponding to the bound.

Can further uses of Tarski's elimination and some general principles further reduce the essentially complexity? E.g., from $\Sigma^1{}_1$ to $\Pi^0{}_2$ or even $\Pi^0{}_1$?

As is widely known, the problem was solved negatively in [Dehn01] using Dehn invariants. The counterexample given by Dehn provides many specific natural examples α,β.

For any of these specific natural examples (using algebraic points), the Tarski elimination yields a $\Pi^0{}_1$ sentence, since the outermost second order quantifiers are replaced by specific algebraic numbers.

Thus H3 is immediately implied by a $\Pi^0{}_1$ sentence. The proof of this implication does not involve [Dehn01].

H4. Problem of the straight line as the shortest distance between two points

It would be very interesting to have clear formulations of this problem, and subject them to logical analysis.

H5. Lie's concept of a continuous group of transformations without the assumption of the differentiability of the functions defining the group

The modern formulation of this problem is:

Are continuous groups automatically differentiable groups?

A topological group (continuous group) G is a topological space and group such that the group operations of product and inverse are continuous.

A continuous group is a topological group where the topological space is locally Euclidean.

The problem asks whether it follows that the group operations of product and inverse are (continuously) differentiable.

It is clear that we can assume without loss of generality that the space is separable.

Additional considerations show that the problem is essentially in class Π^1_1. Do the positive solutions by Gleason, Montgomery, Zippin provide a stronger assertion that is essentially Π^0_2, or even essentially Π^0_1?

H6. Mathematical Treatment of the Axioms of Physics

The investigations on the foundations of geometry suggest the problem: To treat in the same manner, by means of axioms, those physical sciences in which already today mathematics plays an important part; in the first rank are the theory of probabilities and mechanics.

Although very substantial mathematics is needed to begin seriously treating this problem, the problem itself is not a mathematical problem in the sense meant here.

H7. Irrationality and transcendence of certain numbers

Hilbert's seventh problem is answered by the Gelfond-Schneider theorem, which states that

If α and β are algebraic numbers with $\alpha \neq 0,1$ and if β is not a rational number, then any value of $\alpha^\beta = \exp(\beta \log \alpha)$ is a transcendental number.

There are three main types of such problems. The first is where we present a particular interesting number, and ask if it is irrational or if it is transcendental. In this case, invariably we have an effective means of approximating the number, α.

It follows that "α is irrational" is a Π^0_2 sentence, and that "α is transcendental" is also a Π^0_2 sentence.

A particularly famous example is $e + \pi$. It is not known if $e + \pi$ is rational or if $e + \pi$ is transcendental. The transcendence, or irrationality, is in Π^0_2.

Many expect that not only is $e + \pi$ irrational, but there is a reasonable function f such that

$$(\forall a,b \geq 1)(|e + \pi - a/b| > 1/f(a,b))$$

thereby creating a stronger form of the assertion, that is Π^0_1.

The second is statements that all interesting combinations of a countable family of numbers - typically algebraic numbers - are irrational, or transcendental. Such statements are also generally Π^0_2. The Gelfond-Schneider theorem is obviously of this second type.

Does the proof of the Gelfond-Schneider theorem give a stronger theorem that is much more concrete? E.g., Π^0_2 or even Π^0_1?

The third type concerns relationships between interesting combinations of arbitrary real or complex numbers. Such statements are generally Π^1_1. We expect that they are generally implied by interesting statements of far lower complexity - e.g., Π^0_2 or even Π^0_1.

Schanuel's Conjecture is in the third type, and is wide open. So Schanuel's Conjecture is literally Π^1_1. Is there a reasonable stronger conjecture that is much more concrete? E.g., Π^0_2, or even Π^0_1?

H8. Problems of prime numbers

Here Hilbert poses the following problems.

The Riemann hypothesis (the real part of any non-trivial zero of the Riemann zeta function is 1/2), Goldbach's conjecture (every even number greater than 2 can be written as the sum of two prime numbers), and the Twin Prime conjecture (there are infinitely many primes p such that p+2 is prime).

Let

$$\delta(x) = \prod_{n<x}\prod_{j\leq n} \eta(j)$$

where $\eta(j) = 1$ unless j is a prime power, and $\eta(p^k) = p$.

LEMMA. RH is equivalent to the following. For all integers $n \geq 1$, $(\sum_{k\leq\delta(n)} 1/k - n^2/2)^2 < 36 n^3$.

Proof: See [DMR76]], p. 335. QED

The above equivalence to RH can be straightforwardly expressed in Π^0_1 form, and so RH is essentially Π^0_1.

It is obvious that Goldbach's conjecture and Fermat's Last Theorem are Π^0_1. The latter was proved by Wiles.

The Twin Prime conjecture asserts that for all $n \geq 0$ there exists $p > n$ such that p and p+2 are prime. Hence the Twin Prime conjecture is Π^0_2.

It is expected that the Twin Prime conjecture is true and a stronger result will be obtained in the form

$$(\forall n)(\exists p)(p,p+2 \text{ are prime and } p \leq f(n))$$

for some reasonable function f. This strong form will obviously be Π^0_1.

Mordell's conjecture (proved by Faltings) is Π^0_3. It asserts that certain Diophantine equations have at most finitely many solutions. I.e., this takes the form

$$(\forall n)(\exists m)(\forall r)(h(n,m,r) \text{ is not a solution})$$

which is Π^0_3. (Here h is a specific primitive recursive function required in the classification scheme.)

Many expect this result to be improved with an upper bound for m as a reasonable function of n:

$$(\forall n)(\exists m \leq f(n))(\forall r)(h(n,m,r) \text{ is not a solution})$$

which is Π^0_1 (after some quantifier manipulation).

H9. Proof of the most general law of reciprocity in any number field

A number field is a finite degree field extension of the field of rational numbers. The residue fields are all finite, and so these kinds of problems about solving equations mod primes are all Π^0_1.

This problem led to far reaching developments in algebraic number theory, and ultimately to the Langlands program. It would be interesting to see what these developments mean from the point of view of Mathematical Statement Theory.

H10. Determination of the solvability of a diophantine equation

The most commonly cited interpretation of Hilbert's tenth problem is the following.

Is there an algorithm for determining whether a given polynomial of several variables with integer coefficients has a zero in the integers?

This has the form

$$(\exists \text{ algorithm } \alpha)(\forall \text{ integral polynomials } P)(P \text{ has a zero} \rightarrow \alpha(P) = 1 \wedge P \text{ does not have a zero} \rightarrow \alpha(P) = 0)$$

which is Σ^0_3 (after some quantifier manipulation). The negation

$$(\forall \text{ algorithm } \alpha)(\exists \text{ integral polynomial } P)(\neg(P \text{ has a zero} \wedge \alpha(P) = 1 \wedge P \text{ does not have a zero} \rightarrow \alpha(P) = 0))$$

is therefore Π^0_3, and was proved in [Mat70] building on earlier work of M. Davis, H. Putnam, and J. Robinson. See [Da73], [DMR76]], [Mat93].

Actually, what is proved is stronger, and results in a Σ^0_2 sentence. A rather complicated algorithm γ is provided with the following Π^0_1 property.

Given any algorithm α, $\gamma(\alpha)$ quickly produces
an integral polynomial P
and an integral vector x such that either
$P(x) = 0$ and $\alpha(x)$ does not compute 1, or

P(x) has no integral zero and α(x) does not compute 0.

If we ask for real or complex zeros, then there is an algorithm by [Ta51]. The problem is open for rational zeros.

There has been considerable interest in this problem over number fields. It is known that if the Shafarevich-Tate conjecture holds, then Hilbert's Tenth Problem has a negative answer over the ring of integers of every number field. See [MR10].

We use the solution to H10 in section 5.6 as a technical tool.

H11. Quadratic forms with any algebraic numerical coefficients

A quadratic form over a number field F is a quadratic in several variables over F, all of whose terms have degree 2. Two quadratic forms over F are considered equivalent over F if and only if one form can be transformed to the other by a linear transformation with coefficients from F.

The Hasse Minkowski theorem is most often cited in connection with H11. It asserts that two quadratic forms over a number field are equivalent if and only if they are equivalent over every completion of the field (which may be real, complex, or p-adic).

This theorem takes the form

($\forall$ number fields F)($\forall$ quadratic forms α,β over F)
(α,β are equivalent over F $\leftrightarrow$ ($\forall$ completions F' of F)
(α,β are equivalent over F')).

It would appear that using standard techniques, this can be put into Π^0_∞ form. Can it be put into Π^0_2 or even Π^0_1? If there a stronger theorem that is in Π^0_1?

H12. Extension of Kronecker's theorem on Abelian fields to any algebraic realm of rationality

The modern interpretation of this problem is to extend the Kronecker-Weber theorem on Abelian extensions of the rational numbers to any base number field.

The Kronecker-Weber theorem states that every finite extension of Q whose Galois group over Q is Abelian, is a subfield of a cyclotomic field; i.e., a field obtained by adjoining a root of unity to Q. This takes the form

(∀ finite extensions F of Q)(Gal(F/Q) is Abelian →
(∃ cyclotomic G over Q)(F is a subfield of G))

which is Π^0_3. It would appear that this can be put into Π^0_2 form. If there a stronger form that is Π^0_1?

The same issues occur with related statements over any base number field.

H13. Impossibility of the solution of the general equation of the 7-th degree by means of functions of only two arguments

In modern terms, Hilbert considered the general seventh-degree equation

$$x^7 + ax^3 + bx^2 + cx + 1 = 0$$

and asked whether its solution, x, a function of the three coefficients a,b,c, can be expressed using a finite number of two variable functions.

A more general question is: can every continuous function of three variables be expressed as a composition of finitely many continuous functions of two variables?

V.I. Arnold proved a much stronger statement: every continuous function of three variables be expressed as a composition of finitely many continuous functions of two variables? See [Ar59,62].

Arnold's statement is in Π^1_2 form, using standard coding techniques from mathematical logic. Is there a yet stronger version that is much more concrete? E.g., Π^0_2 or Π^0_1?

H14. Proof of the finiteness of certain complete systems of functions

In modern terms, Hilbert asks the following question.

Let F be a field, and K be a subfield of $F(x_1,...,x_n)$. Is the ring $K \cap F[x_1,...,x_n]$ finitely generated over F?

Here $F(x_1,...,x_n)$ and $F[x_1,...,x_n]$ are the ring of rational functions over F and the ring of polynomial functions over F, in n variables.

On the face of it, this question is even less concrete than H1, the continuum hypothesis! This is because the question involves absolutely all fields F.

Is there a way of separating the abstract set theory from the intended mathematical content? More specifically, is there a way of showing, e.g., that if the statement holds for all countable fields, then it holds for all fields?

The answer is yes by a simple construction. Let F,K be a counterexample. Build an appropriate infinite sequence from F and from K, and use the subfield of F generated by the infinite sequence from F.

Consequently, we consider the following statement.

Let F be a countable field, and K be a subfield of $F(x_1,...,x_n)$. Is the ring $K \cap F[x_1,...,x_n]$ finitely generated over F?

This is a Π^1_1 sentence. Can we put it in Π^0_∞ form using basic algebraic principles? What about Π^0_2 or even Π^0_1?

Nagata gave a negative answer to H14 in [Na59].

[CT06] gives the following formulation of Hilbert's 14th problem:

If an algebraic group G acts linearly on a polynomial algebra S, is the algebra of invariants S^G finitely generated?

According to [CT06], this has been proved for reductive G in [Hil1890], and for certain nonreductive groups in [Wei32]. Can this theorems, and related open questions, be put into Π^0_∞, or even Π^0_2 or Π^0_1 form? Are they implied by Π^0_1 statements?

H15. Rigorous foundation of Schubert's enumerative calculus

Hermann Schubert claimed some spectacular counts on the number of geometric objects satisfying certain conditions, using methods that were not rigorous even by 1900 standards. Many of his claims have not been confirmed or denied.

Hilbert asked for a rigorous foundation for Schubert's enumerative calculus. Independently of the search for foundations here, many, if not all, of his counts, when given rigorous treatments, fit into the framework of Tarski's decision procedure for the field of real numbers, [Ta51].

As an example, it follows (based on work subsequent to Tarski), that there is an algorithm that takes any $S \subseteq \Re^n \times \Re^m$ presented with rational coefficients, and produces a number $0,1,\ldots,\infty$, which counts the number of distinct cross sections of S (obtained by fixing the first argument, from $\Re^n$). This can be applied in the many situations where one wants to count the number of nice objects satisfying some nice condition.

This can be used to put various statements in Π^0_1 form, or even in quantifier free form.

H16. Problem of the topology of algebraic curves and surfaces

In modern terms: describe relative positions of ovals originating from a real algebraic curve and as limit cycles of a polynomial vector field on the plane.

Here a limit cycle of a polynomial vector field in the plane is a periodic orbit which can be separated from all other periodic orbits by placing a tube around it. Here it is understood that periodic orbits consist of more than one point.

It has been shown in [Il91] and [Ec92] (or at least claimed) that every polynomial vector field in the plane has at most finitely many limit cycles.

We can put this in the form

$$(\forall P)(\exists n)(\forall x_1,\ldots,x_n)(x_1,\ldots,x_n \text{ do not generate different limit cycles})$$

which, unless some interesting mathematics comes to bear, is going to be Π^1_3 and maybe a lot higher. Can we use perhaps even some elementary mathematics to reduce this very sharply? Does the proof yield a stronger statement that is far more concrete? Perhaps Π^0_2 or even Π^0_1?

A principal open question is whether there is a uniform bound on the number of limit cycles of a polynomial vector field in the plane that depends only on the degree of the polynomial. This takes the form

$$(\forall d)(\exists n)(\forall P \text{ of degree} \leq d)(\exists x_1,...,x_n)$$
$$(\forall y)(\text{if } y \text{ is not on a limit cycle then } x_1,...,x_n \text{ are on it})$$

which also looks Π^1_3 and maybe a lot higher, unless some interesting (perhaps elementary) mathematics is used to reduce the complexity.

H17. Expression of definite forms by squares

In modern terms, is every polynomial of several variables over the reals that assumes no negative values a sum of squares of rational functions?

Emil Artin proved the assertion in [Art27]. The theorem takes the form

$$(\forall \text{ polynomials } P)(\text{if } P \text{ assumes no negative value then}$$
$$(\exists \text{ rational functions } R_1,...,R_k)(P = R_1^2 + ... + R_k^2 \text{ holds everywhere}))$$

which is Π^1_3 with no mathematical considerations. However, much sharper results have been proved which are much more concrete.

Specifically, it is known that for each d,n, there exists r such that

for all polynomials of degree ≤ d in n variables,
if P assumes no negative value then
P is the sum of at most r rational functions
of degrees at most r.

See [Day61], [Kre60], [Rob55], [Rob56], [DGL92]. In fact, a primitive recursive bound on r as a function of d,n is given in the first two references.

Note that the displayed statement above is a sentence in the language of the field of real numbers, primitive recursively obtained from d,n. Using Tarski's decision procedure for the field of real numbers, [Ta51], we now see that this stronger result is Π^0_2. In fact, given the above mentioned upper bound on r, we see that the strong form of this stronger result is in fact Π^0_1.

H18. Building up of space from congruent polyhedra

In modern terms, there are three parts to the problem.

The first part asks whether there are only finitely many essentially different space groups in *n*-dimensional Euclidean space.

More formally, let E(n) be the group of all isometries of $\mathfrak{R}^n$. We look for discrete subgroups $\Gamma \subseteq$ E(n) such that there is a compact region D $\subseteq \mathfrak{R}^n$ where the various congruent copies of D cover $\mathfrak{R}^n$ and have only boundary points in common.

Ludwig Bieberbach answered this question affirmatively by showing that there are only finitely many such Γ up to isomorphism. See [Bi11], [Bi12].

The theorem takes the form: for some t, if

if $G_1,\ldots,G_t$ are discrete in E(n), and
$D_1,\ldots,D_t \subseteq \mathfrak{R}^n$ are compact and congruent copies of D_i under G_i
that cover $\mathfrak{R}^n$ and have only boundary points in common,
then there exists $i \neq j$ such that G_i and G_j are isomorphic.

Using quantifier manipulations and a small dose of mathematics, we see that this is Π^1_3. We expect that with some additional mathematics, this can be reduced to Π^1_1. We also expect that from Bieberbach's work, we can find a stronger statement which is considerably more concrete. Possibly Π^0_2 or even Π^0_1.

The second part of the problem asks whether there exists a polyhedron which tiles 3-dimensional Euclidean space but is not the fundamental region of any space group. Such tiles are called anisohedral.

It is now known that there is an anisohedral tiling of even 2-dimensional Euclidean space. See Heinrich Heesch's Tiling, http://www.spsu.edu/math/tiling/17.html

The problem is in the form

(∃ polyhedon P)(P is not the fundamental region of any space group ∧ P tiles the plane)

which appears to be around Σ^1_2 with only simple mathematical considerations. But consider the stronger statement

(∃ polyhedron P)(P is not the fundamental region of any space group ∧ P tiles the plane periodically).

We can put this in the form: there exists r such that

∃ polyhedron P with r sides)(P is not the fundamental region of any space group ∧ P tiles the plane periodically).

We expect that the displayed property of r can be viewed as a sentence in the theory of the field of reals, so that we can apply Tarski's decision procedure [Ta51]. This results in a Σ^0_1 sentence.

The third part of the problem asks for the best way to pack congruent solids of a given form. In particular, spheres of equal radius in $\mathfrak{R}^3$.

The Kepler Conjecture is the case of sphere packing: the usual way of packing spheres of equal size in $\mathfrak{R}^3$ is the best.

Appropriate use of Tarski's decision procedure for the field of real numbers will show that the Kepler Conjecture - in various fully rigorous forms - is essentially Π^0_1.

Of course, Hales has reduced Kepler's Conjecture to a specific large computation, which is Π^0_0. But that involves deep insights into the problem itself, and is not a generic reduction in the sense of using the decision procedure for the real numbers.

H19. Are solutions of regular problems in the calculus of variations always necessarily analytic?

H20. The general problem of boundary values

H21. Proof of the existence of linear differential equations having a prescribed monodromic group

H22. Uniformization of analytic relations by means of automorphic functions

H23. Further development of the methods of the calculus of variations

H19-H23 involve statements of the following rough form (and sometimes simpler):

($\forall$ continuous objects α)(if there exist continuous objects β such that $P(\alpha,\beta)$, then there exist continuous objects γ such that $Q(\alpha,\gamma)$, which is unique with respect to some equivalence relation R).

Generally speaking, it is clear that statements of this kind are Π^1_2. There is the opportunity for reduction from Π^1_2 using some significant mathematics not presupposing the proof or refutation, if any exist at this time. But far more likely is that if such a statement is proved or refuted, then an interesting stronger statement is really what is proved or refuted, and that the interesting stronger statement is considerably more concrete - perhaps even Π^0_2 or Π^0_1.

We may encounter statements with an additional logical complication:

($\forall$ continuous objects α)(if there exist continuous objects β such that $P(\alpha,\beta)$, then there exist continuous objects γ such that $Q(\alpha,\gamma)$, which is related to all continuous objects γ' such that $Q(\alpha,\gamma)$ by some relation R).

Because R may not be an equivalence relation (it may, for example, be a maximality condition), such a statement may be only Π^1_3 or higher. Again, there are opportunities for reduction from Π^1_3 (or higher), and particularly so in terms of finding an interesting stronger statement that is far more concrete.

The many issues that arise in terms of a logical analysis of H19 - H23 are too varied and delicate to be appropriately dealt with here.

CHAPTER 1
INTRODUCTION TO BRT

1.1. General Formulation.

Before presenting the precise formulation of Boolean Relation Theory (BRT), we give two examples of assertions in BRT that are of special importance for the theory.

DEFINITION 1.1.1. N is the set of all nonnegative integers. $A\backslash B = \{x: x \in A \wedge x \notin B\}$. For $x \in N^k$, we let max(x) be the maximum coordinate of x.

THIN SET THEOREM. Let $k \geq 1$ and $f:N^k \to N$. There exists an infinite set $A \subseteq N$ such that $f[A^k] \neq N$.

COMPLEMENTATION THEOREM. Let $k \geq 1$ and $f:N^k \to N$. Suppose that for all $x \in N^k$, $f(x) > \max(x)$. There exists an infinite set $A \subseteq N$ such that $f[A^k] = N\backslash A$.

These two theorems are assertions in BRT. In fact, the complementation theorem has the following sharper form.

COMPLEMENTATION THEOREM (with uniqueness). Let $k \geq 1$ and $f:N^k \to N$. Suppose that for all $x \in N^k$, $f(x) > \max(x)$. There exists a unique set $A \subseteq N$ such that $f[A^k] = N \setminus A$. Furthermore, A is infinite.

We will explore the Thin Set Theorem and the Complementation Theorem in sections 1.3, 1.4. At this point we analyze their logical structure.

DEFINITION 1.1.2. A multivariate function on N is a function whose domain is some N^k and whose range is a subset of N. A strictly dominating function on N is a multivariate function on N such that for all $x \in N^k$, $f(x) > \max(x)$. We define MF as the set of all multivariate functions on N, SD as the set of all strictly dominating functions on N, and INF as the set of all infinite subsets of N.

DEFINITION 1.1.3. Let $f \in MF$, where $dom(f) = N^k$. For $A \subseteq N$, we define $fA = f[A^k]$.

The notation fA is very convenient. It avoids the unnecessary use of explicit mention of arity or dimension. It is used throughout this book.

Using this notation, we can restate our two theorems as follows.

THIN SET THEOREM. For all $f \in MF$ there exists $A \in INF$ such that $fA \neq N$.

COMPLEMENTATION THEOREM. For all $f \in SD$ there exists $A \in INF$ such that $fA = N \setminus A$.

Note that in the Thin Set Theorem, we use the family of multivariate functions MF, and the family of sets INF. In the Complementation Theorem, we use the family of multivariate functions SD, and the family of sets INF.

In BRT terminology this will be expressed by saying that the Thin Set Theorem is an instance of IBRT (inequational BRT) on the BRT setting (MF,INF), and the Complementation Theorem is an instance of EBRT (equational BRT) on the BRT setting (SD,INF).

Note that we can regard the condition fA ≠ N as a Boolean inequation in fA,N. We also regard the condition fA = N\A as a Boolean equation in fA,N.

Here N plays the role of the universal set in Boolean algebra. From this perspective, fA ≠ N is a Boolean inequation in fA, and fA = N\A is a Boolean equation in A,fA.

The fact that N should play the role of the universal set can be read off from the BRT settings (MF,INF) and (SD,INF). See "Full BRT Semantics" below.

EBRT stands for "equational Boolean relation theory". IBRT stands for "inequational Boolean relation theory".

Thus we say that

i. The Thin Set Theorem is an instance of: IBRT in fA on (MF,INF).
ii. The Complementation Theorem is an instance of: EBRT in A,fA on (SD,INF).

We now fully explain what we mean by such phrases as "IBRT in fA on (MF,INF)" and "EBRT in A,fA on (SD,INF)".

The principal BRT environments are

IBRT
EBRT

defined below. We will mention one other (much richer) BRT environment below (PBRT), but in this book we stay within the environments IBRT and EBRT.

We call the lists

fA
A,fA

BRT signatures. In general, the BRT signatures will be substantially richer than the above two examples.

We have already called the pairs

(MF,INF)
(SD,INF)

BRT settings. One other BRT setting plays a particularly important role in this book. This is the BRT setting (ELG,INF). See Definition 2.1.

We are now prepared for the formal presentation of BRT.

FULL BRT SYNTAX

DEFINITION 1.1.4. The BRT set variables are the symbols $A_1,A_2,\ldots$. The BRT function variables are the symbols $f_1,f_2,\ldots$.

In practice, we will use appropriate upper case and lower case letters without subscripts for these BRT variables.

DEFINITION 1.1.5. The BRT terms are defined by

i) every BRT set variable is a term;
ii) $\emptyset$,U are BRT terms (U represents the universal set);
iii) if s,t are BRT terms then $(s \cup t),(s \cap t),(s\backslash t)$ are BRT terms;
iv) if f is a BRT function variable and t is a BRT term then ft is a BRT term.

DEFINITION 1.1.6. The BRT equations are of the form s = t, where s,t are BRT terms. The BRT inequations are of the form $s \neq t$, where s,t are BRT terms. The BRT inclusions are of the form $s \subseteq t$, where s,t are BRT terms.

DEFINITION 1.1.7. The BRT formulas are defined by

i) every BRT equation is a BRT formula;
ii) if φ,ψ are BRT formulas then $(\neg\varphi),(\varphi \vee \psi),(\varphi \wedge \psi),(\varphi \rightarrow \psi),(\varphi \leftrightarrow \psi)$ are BRT formulas.

We routinely omit parentheses when no ambiguity arises. We also adhere to the usual precedence table

$$\neg$$
$$\vee \quad \wedge$$
$$\rightarrow \quad \leftrightarrow$$

FULL BRT SEMANTICS

DEFINITION 1.1.8. A multivariate function is a pair (f,k), where

i) f is a function in the standard sense of a univalent set of ordered pairs;
ii) if $k \geq 2$, then every element of dom(f) is a k-tuple.

DEFINITION 1.1.9. We say that the arity of (f,k) is k. The domain of (f,k) is taken to be dom(f).

We rely on the fact that for all $1 < i < j$, no i-tuple is a j-tuple.

Let f be a function (in the standard sense). Note that if f is empty then for all $k \geq 1$, (f,k) is a multivariate function. Also, if f is nonempty then

i) (f,1) is a multivariate function;
ii) there is at most one $k \geq 2$ such that (f,k) is a multivariate function.

The explicit mention of k is intended to avoid the following type of ambiguity. A function $f:N^2 \to N$ could be viewed as either a 1-ary multivariate function with domain N^2, or a 2-ary multivariate function with domain N^2. In our notation, the former would be written (f,1), and the latter would be written (f,2). Note that (f,3) is not a multivariate function.

In practice, the intended arity k of functions is clear from context, and we generally ignore the above definition of multivariate function. However, we need the above definition for full rigor.

DEFINITION 1.1.10. Let f = (f,k) be a multivariate function and E be a set. We define $fE = f[E^k]) = \{f(x_1,\ldots,x_k): x_1,\ldots,x_k \in E\} = \{y: (\exists x_1,\ldots,x_k \in E)(y = f(x_1,\ldots,x_k)\}$.

DEFINITION 1.1.11. A BRT setting is a pair (V,K), where V is a nonempty set of multivariate functions and K is a nonempty family of sets.

DEFINITION 1.1.12. The BRT assertions are the assertions of the form $(\forall g_1,\ldots,g_n \in V)(\exists B_1,\ldots,B_m \in K)(\varphi)$

where $n,m \geq 1$, $B_1,\ldots,B_m$ are distinct BRT set variables, $g_1,\ldots,g_n$ are distinct BRT function variables, and φ is a BRT formula involving at most the variables $B_1,\ldots,B_m,g_1,\ldots,g_n$.

Every BRT assertion gives rise to an actual mathematical statement provided we are also given a BRT setting (V,K). Specifically,

DEFINITION 1.1.13. ∩ is interpreted as intersection, ∪ as union, \ as set theoretic difference, and ∅ as the empty set. ft is interpreted as the image of f on the interpretation of t, using Definition 1.10. U is interpreted as the least set U such that

i) for all A ∈ K, A ⊆ U;
ii) for all f ∈ V, fU ⊆ U.

Note that U may or may not lie in K.

An important special kind of BRT is obtained by requiring that the relevant sets form a tower under inclusion. Specifically,

DEFINITION 1.1.14. The BRT,⊆ assertions are the assertions of the form
$(\forall g_1,\ldots,g_n \in V)(\exists B_1 \subseteq \ldots \subseteq B_m \in K)(\varphi)$

where $n,m \geq 1$, $B_1,\ldots,B_m$ are distinct BRT set variables, $g_1,\ldots,g_n$ are distinct BRT function variables, and φ is a BRT formula involving at most the variables $B_1,\ldots,B_m,g_1,\ldots,g_n$.

Here $B_1 \subseteq \ldots \subseteq B_m \in K$ means

$$B_1 \subseteq \ldots \subseteq B_m \wedge B_1,\ldots,B_m \in K.$$

DEFINITION 1.1.15. We say that a BRT formula is BRT valid if and only if it is true on all BRT settings (V,K) under any assignment of elements of V to the function variables, and any assignment of elements of K to the set variables.

DEFINITION 1.1.16. We say that a BRT formula is BRT,⊆ valid if and only if it is true on all BRT settings (V,K) under any assignment of elements of V to the function variables, and any assignment of elements of K to the set variables such that for all $i \leq j$, the assignment to A_i is a subset of the assignment to A_j.

DEFINITION 1.1.17. Let φ,ψ be BRT formulas. We say that φ,ψ are BRT (BRT,⊆) equivalent if and only if $\varphi \leftrightarrow \psi$ is BRT (BRT,⊆) valid. This definition is extended to sets of BRT formulas in the obvious way.

BRT FRAGMENTS

Obviously there are infinitely many BRT formulas. Results concerning all BRT formulas, even in very basic BRT settings, have been entirely inaccessible to us. The book will only be concerned with very modest fragments of BRT.

DEFINITION 1.1.18. The BRT fragments are written

[Environment] in [Signature] on [Setting].

It remains to say what the BRT Environments and Signatures are. The BRT Settings have already been defined.

DEFINITION 1.1.19. There are three BRT environments:

i) EBRT (equational BRT);
ii) IBRT (inequational BRT);
iii) PBRT (propositional BRT).

DEFINITION 1.1.20. A core BRT term is a BRT term that is either a BRT set variable or begins with a BRT function variable. For example, $f_3(A_1 \cup A_4)$ is a core BRT term, and $A_1 \cup A_4$ is not a core BRT term.

DEFINITION 1.1.21. A BRT signature is

i) a finite list of one or more distinct core BRT terms; or
ii) a finite list of one or more distinct core BRT terms, followed by the symbol $\subseteq$.

DEFINITION 1.1.22. The entries of a BRT signature are just its core BRT terms.

Let α be a BRT fragment. I.e., let α = "[Environment] in σ on [Setting]" be a BRT fragment, where σ is a BRT signature.

DEFINITION 1.1.23. The signature of α is σ. The α terms are defined by

i) every entry of σ is an α term;
ii) $U,\emptyset$ are α terms;
iii) if s,t are α terms then $(s \cup t),(s \cap t),(s\setminus t)$ are α terms.

The α terms are to be distinguished from the entries of σ, since we are closing the entries of σ under Boolean operations.

DEFINITION 1.1.24. The α equations are the equations between α terms. The α inequations are the inequations ($\neq$) between α terms. The α inclusions are the inclusions between α terms.

DEFINITION 1.1.25. The α formulas are inductively defined by

i) every α equation is an α formula;
ii) if φ,ψ are α formulas, then $(\neg\varphi),(\varphi \vee \psi),(\varphi \wedge \psi),(\varphi \rightarrow \psi),(\varphi \leftrightarrow \psi)$ are α formulas.

DEFINITION 1.1.26. The α basics are the α equations if the environment of α is EBRT; the α inequations if the environment of α is IBRT; the α formulas if the environment of α is PBRT.

Suppose first that the signature σ of α does not end with $\subseteq$. Let the BRT setting of α be (V,K).

DEFINITION 1.1.27. An α assignment is an assignment of an element of V to each function variable appearing in σ, and an element of K to each set variable appearing in σ.

DEFINITION 1.1.28. The α assertions are assertions of the form

$$(\forall g_1,\ldots,g_n \in V)(\exists B_1,\ldots,B_m \in K)(\varphi)$$

where $n,m \geq 1$, $B_1,\ldots,B_m$ are the BRT set variables mentioned in σ with strictly increasing subscripts, $g_1,\ldots,g_n$ are the BRT function variables mentioned in σ with strictly increasing subscripts, and φ is an α basic.

Now assume that σ ends with $\subseteq$.

DEFINITION 1.1.29. An α assignment is an assignment of an element of V to each function variable appearing in σ, and an element of K to each set variable appearing in σ, where if A_i,A_j appear in σ and $1 \leq i \leq j$, then the set assigned to A_i is included in the set assigned to A_j.

DEFINITION 1.1.30. The α assertions are assertions of the form

$$(\forall g_1,\ldots,g_n \in V)(\exists B_1 \subseteq \ldots \subseteq B_m \in K)(\varphi)$$

where $n,m \geq 1$, $B_1,\ldots,B_m$ are the BRT set variables mentioned in σ with strictly increasing subscripts, $g_1,\ldots,g_n$ are the BRT function variables mentioned in σ with strictly increasing subscripts, and φ is an α basic.

Thus if the environment of α is EBRT, then the α assertions are based on α equations φ. If the environment of α is IBRT, then the α assertions are based on α inequations φ. If the environment of α is PBRT, then the α assertions are based on α formulas φ. These hold regardless of whether the signature of α ends with $\subseteq$.

DEFINITION 1.1.31. We say that an α formula is α valid if and only if it holds for all α assignments.

DEFINITION 1.1.32. Let φ,ψ be α formulas. We say that φ,ψ are α equivalent if and only if $\varphi \leftrightarrow \psi$ is α valid. This definition is extended to sets of α formulas in the obvious way.

This concludes the definition of BRT fragments, and their assertions.

The above treatment of BRT fragments, α =

[Environment] in [Signature] on [Setting]

fully explains the titles of the Classification sections 2.4 - 2.7.

DEFINITION 1.1.33. The standard BRT signatures have the form

$$A_1,\ldots,A_n,f_1A_1,\ldots,f_1A_n,\ldots,f_mA_1,\ldots,f_mA_n$$
$$A_1,\ldots,A_n,f_1A_1,\ldots,f_1A_n,\ldots,f_mA_1,\ldots,f_mA_n,\subseteq$$

and are referred to as

m functions and n sets.
m functions and n sets/$\subseteq$.

where $n,m \geq 1$. A flat BRT signature is a BRT signature where every entry is either some A_i, or some f_iA_j, or some f_iU.

DEFINITION 1.1.34. A standard BRT fragment is a BRT fragment whose environment is EBRT or IBRT, and whose signature is a standard BRT signature. A flat BRT fragment is a BRT fragment, with environment EBRT or IBRT, whose signature is flat.

The BRT fragments considered in sections 2.2, 2.4-2.7, and Chapter 3, are all standard. In section 2.3, we work with the flat signature A,fA,fU. In Chapter 3, we are successful in analyzing a small part of the standard BRT fragment (see Definition 2.1)

EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF).

For example, in this book we do not consider such interesting BRT signatures as

A,fA,ffA.
A,fA,f(U\A).
A,B,fA,fB,f(A∪B),⊆.

none of which are flat.

Let α be a standard BRT fragment with m functions and n sets, whose signature does not end with ⊆. Then the number of entries of the signature is n(m+1). So the number of α terms is $2^{2^{\wedge}n(m+1)}$ up to Boolean identities. Therefore the number of α basics is also $2^{2^{\wedge}n(m+1)}$ up to formal Boolean equivalence. This is also the number of α assertions up to formal Boolean equivalence.

The number of α assertions, up to formal Boolean equivalence, grows very rapidly. For 1 function and 1 set, we have $2^{2^{\wedge}2}$ = 16. For 1 function and 2 sets, we have $2^{2^{\wedge}4}$ = 2^{16} = 65,536. For 1 function and 3 sets, we have $2^{2^{\wedge}6}$ = 2^{64}. For 2 functions and 2 sets, we have $2^{2^{\wedge}6}$ = 2^{64}. For the second, third, and fourth of these cases, we do not know if the α assertions on the basic BRT settings considered here include assertions independent of ZFC. We believe that they do not.

The number of α assertions grows less rapidly, up to BRT equivalence, if the signature ends with ⊆. This reduction of complexity allows us to work successfully with EBRT in A,B,fA,fB,⊆ on various basic settings, in Chapter 2.

For standard BRT fragments with 2 functions and 3 sets, without ⊆ in the signature, we have $2^{2^{\wedge}9}$ = 2^{512} assertions.

The so called Principal Exotic Case lives in EBRT in the standard signature with 2 functions and 3 sets, on the BRT setting (ELG,INF). The Principal Exotic Case is Proposition A from Appendix A, and is the focus of Chapters 4 and 5 where it is shown to be independent of ZFC (assuming SMAH = ZFC augmented with the existence of strongly Mahlo cardinals of each finite order, is consistent).

The Principal Exotic Case lies formally in the standard BRT fragment

EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF).

In fact, the Principal Exotic Case lives in the considerably reduced flat BRT fragment

EBRT in A,C,fA,fB,gB,gC on (ELG,INF).

In fact, we can strengthen the Principal Exotic Case with $A \subseteq B \subseteq C$, which now lives in the further reduced flat BRT fragment

EBRT in A,C,fA,fB,gB,gC,$\subseteq$ on (ELG,INF).

In Chapters 4 and 5, we show that both of these statements are provable using large cardinals, but not in ZFC (assuming ZFC is consistent).

It is important to have a useful format for presenting BRT assertions. For the purposes of Chapter 2, this amounts to creating a useful format for presenting BRT equations. The most useful format is a set of pre elementary inclusions, or a set of elementary inclusions, defined below.

Let α be a flat BRT fragment, with signature σ.

DEFINITION 1.1.35. The α pre elementary inclusions are of the form

i) $t_1 \cap \ldots \cap t_n = \emptyset$, where $n \geq 1$, $t_1,\ldots,t_n$ are the entries of σ, in order of their appearance in σ;
ii) $t_1 \cup \ldots \cup t_n = U$, where $n \geq 1$, $t_1,\ldots,t_n$ are the entries of σ, in order of their appearance in σ;
iii) $r_1 \cap \ldots \cap r_p \subseteq s_1 \cup \ldots \cup s_q$, where $p,q \geq 1$, and $r_1,\ldots,r_p,s_1,\ldots,s_q$ are a listing of all of the entries of σ without repetition, and $r_1,\ldots,r_p$ and $s_1,\ldots,s_q$ are both in order of their appearance in σ.

Note that if there are n entries of σ, then there are 2^n α pre elementary inclusions.

DEFINITION 1.1.36. Suppose σ does not end with $\subseteq$. The α elementary inclusions are obtained from the σ pre elementary inclusions in the following way. If fU and some fA_i appears in an intersection, then remove fU there. If fU appears in a union, then remove all fA_i there. In order to be an elementary inclusion, we require that for every fA on the left, fU must not be on the right.

Note that if fU is not an entry of the signature of α, then the elementary inclusions are just the pre elementary inclusions.

Now suppose the signature of α ends with $\subseteq$.

DEFINITION 1.1.37. Suppose σ ends with $\subseteq$. The α elementary inclusions are obtained from the α pre elementary inclusions in the following way. For any A appearing in an intersection, retain only the A_i where i is least. For any A appearing in a union, retain only the A_i where i is greatest. For any f appearing in an intersection, retain only the fA_i where i is least (if only fU appears, then retain fU). For any f appearing in a union, retain the fA_i where i is greatest (if fU appears, then retain only fU). In order to be an elementary inclusion, we require that for every fA_i on the left, fU must not be on the right, and every fA_j, $j \geq i$, must not be on the right.

DEFINITION 1.1.38. An α format is a set of α elementary inclusions.

In case σ does not end with $\subseteq$, our α formats take advantage of the fact that $fA_i \subseteq fU$. In case σ ends with $\subseteq$, our α formats take advantage of the fact that $A_i \subseteq A_j$ and $fA_i \subseteq fA_j \subseteq fU$, for $i < j$.

We need to verify that our reduction to α formats is valid; i.e., covers what we want. This amounts to verifying that every α equation is α equivalent to an α format. In fact, we show that every set of α inclusions is α equivalent to an α format.

THEOREM 1.1.1. Let α be a flat BRT fragment. Every α inclusion is α equivalent to an α format. Every set of α inclusions is α equivalent to an α format. Every α format is α equivalent to an α inclusion, and an α equation.

Proof: We first assume that the signature of α does not end with $\subseteq$.

For the first claim, let $s \subseteq t$ be an α inclusion. Using standard Boolean algebra, write s as a union of intersections of entries and complements of entries of the signature σ. Write t as an intersection of unions of entries and complements of entries of σ. Here the complements are taken with respect to the universal set U. We allow the degenerate case where s is $\emptyset$,U, and t is $\emptyset$,U. Of course, intersections and unions of cardinality 1 are also allowed.

We then obtain a set of inclusions $s' \subseteq t'$, where the s' are intersections of entries and complements of entries from σ, and the t' are unions of entries and complements of entries of σ. Again, we allow the degenerate case of s',t' = $\emptyset$,U. We can remove all such degenerate cases except $U \subseteq \emptyset$.

We can now arrange for each of these inclusions to be of the forms

$$\pm s_1 \cap \ldots \cap \pm s_n \subseteq \pm t_1 \cup \ldots \cup \pm t_m.$$
$$U \subseteq \pm t_1 \cup \ldots \cup \pm t_m.$$
$$\pm s_1 \cap \ldots \cap \pm s_n \subseteq \emptyset.$$
$$U \subseteq \emptyset.$$

And then of the forms

$$\pm s_1 \cap \ldots \cap \pm s_n \subseteq \pm t_1 \cup \ldots \cup \pm t_m.$$
$$\pm t_1 \cup \ldots \cup \pm t_m = U$$
$$\pm s_1 \cap \ldots \cap \pm s_n = \emptyset.$$
$$U = \emptyset.$$

Here $n,m \geq 1$, and the s's and t's are entries in σ. We write +t for t and −t for U\t. We must allow for the possibility that there are no inclusions. This corresponds to the case where we have only U = U.

We can also require that in each of these clauses, each s_i can appear only once, each $-s_i$ can appear only once, and we cannot have s_i and $-s_i$ appear. This is because of the Boolean equivalence

$$X \cap Y \subseteq Z \cup -Y \leftrightarrow X \cap Y \subseteq Z.$$

We now replace each of the above five forms with an equivalent set of inclusions in which all entries of σ appear (or their complement). Thus suppose

$$\pm s_1 \cap \ldots \cap \pm s_n \subseteq \pm t_1 \cup \ldots \cup \pm t_m$$

is missing $\pm r_1,\ldots,\pm r_k$. Then replace it with the set of all

$$\pm s_1 \cap \ldots \cap \pm s_n \subseteq \pm t_1 \cup \ldots \cup \pm t_m \cup \beta_1 \cup \ldots \cup \beta_k$$

where each β_i is r_i or $-r_i$.

Suppose

$$\pm t_1 \cup \ldots \cup \pm t_m = U$$

is missing entries $\pm r_1,\ldots,\pm r_k$. Then replace it with the set of all

$$\pm t_1 \cup \ldots \cup \pm t_m \cup \beta_1 \cup \ldots \cup \beta_k = U$$

where each β_i is r_i or $-r_i$.

Suppose

$$\pm s_1 \cap \ldots \cap \pm s_n = \emptyset.$$

is missing entries $\pm r_1,\ldots,\pm r_k$. Then replace it with the set of all

$$\pm s_1 \cap \ldots \cap \pm s_n \subseteq \beta_1 \cup \ldots \cup \beta_k$$

where each β_i is r_i or $-r_i$.

Replace $U = \emptyset$ with

$$\beta_1 \cup \ldots \cup \beta_k = U$$

where each $\beta_i = r_i$ or $-r_i$ and $r_1,\ldots,r_k$ is a list without repetition of all entries of σ.

We now have a set of what would be α pre elementary inclusions except for the fact that complements are present. However, we can eliminate the complements by shifting from one side to the other according to the following Boolean equivalences.

$$X \subseteq Y \cup U\backslash Z \leftrightarrow X \cap Z \subseteq Y.$$

$$X \cap U\backslash Y \subseteq Z \leftrightarrow X \subseteq Y \cup Z.$$
$$X \subseteq U\backslash Z \leftrightarrow X \cap Z = \emptyset.$$
$$U\backslash Y \subseteq Z \leftrightarrow Y \cup Z = U.$$

Thus we are left with a set (possibly empty) of α pre elementary inclusions.

Recall the process of converting any α pre elementary inclusion to an α elementary inclusion. The given α pre elementary inclusion is obviously α equivalent to the resulting α elementary inclusion. Thus we are left with an α format.

This establishes the first claim. The second claim follows immediately from the first claim since a finite set of α inclusions can be written as a single α inclusion.

For the final claim, let $\{s_1 \subseteq t_1,\ldots,s_n \subseteq t_n\}$ be an α format, $n \geq 0$. If $n = 0$, then take $A \subseteq A$, $A = A$, where A is an entry of σ. Suppose $n > 0$. Then use the Boolean equivalence

$$s_1 \subseteq t_1 \wedge \ldots \wedge s_n \subseteq t_n \leftrightarrow$$
$$s_1\backslash t_1 \cup \ldots \cup s_n\backslash t_n = \emptyset \leftrightarrow$$
$$s_1\backslash t_1 \cup \ldots \cup s_n\backslash t_n \subseteq \emptyset.$$

We now assume that the signature of α does end with $\subseteq$. Let α be $\alpha'\subseteq$. For the first claim, let $s \subseteq t$ be an α inclusion. As before, we obtain an equivalent set of pre elementary inclusions for α'. At this point, we perform the reductions that create an equivalent set of pre elementary inclusions for α. We then proceed as above to create an equivalent set of elementary inclusions for α.

The second and third claims are proved as before. QED

We will use Theorem 1.1.1 as follows. Let α be a flat BRT fragment with signature σ and BRT setting (V,K).

Suppose the environment of α is EBRT, and α does not end with $\subseteq$. By Theorem 1.1.1, the α assertions can be put into the form

$$(\forall g_1,\ldots,g_n \in V)(\exists B_1,\ldots,B_m \in K)(S)$$

where $n,m \geq 1$, $B_1,\ldots,B_m$ are the BRT set variables mentioned in σ with strictly increasing subscripts, $g_1,\ldots,g_n$ are the BRT function variables mentioned in σ with strictly increasing subscripts, and S is an α format, interpreted conjunctively.

Suppose the environment of α is EBRT, and σ ends with $\subseteq$. By Theorem 1.1.1, the α assertions can be put into the form

$$(\forall g_1,\ldots,g_n \in V)(\exists B_1 \subseteq \ldots \subseteq B_m \in K)(S)$$

where $n,m \geq 1$, $B_1,\ldots,B_m$ are the BRT set variables mentioned in σ with strictly increasing subscripts, $g_1,\ldots,g_n$ are the BRT function variables mentioned in σ with strictly increasing subscripts, and S is an α format, interpreted conjunctively.

Suppose the environment of α is IBRT, and σ does not end with $\subseteq$. To avoid considering the very awkward negated formats, we work with the dual. Thus the inequation becomes an equation, so that we can apply Theorem 1.1.1. By Theorem 1.1.1, the α assertions can be put into the form

$$\neg(\exists g_1,\ldots,g_n \in V)(\forall B_1,\ldots,B_m \in K)(S)$$

where $n,m \geq 1$, $B_1,\ldots,B_m$ are the BRT set variables mentioned in σ with strictly increasing subscripts, $g_1,\ldots,g_n$ are the BRT function variables mentioned in σ with strictly increasing subscripts, and S is an α format, interpreted conjunctively.

Suppose the environment of α is IBRT, and σ does end with $\subseteq$. By Theorem 1.1.1, the α assertions can be put into the form

$$\neg(\exists g_1,\ldots,g_n \in V)(\forall B_1 \subseteq \ldots \subseteq B_m \in K)(S)$$

where $n,m \geq 1$, $B_1,\ldots,B_m$ are the BRT set variables mentioned in σ with strictly increasing subscripts, $g_1,\ldots,g_n$ are the BRT function variables mentioned in σ with strictly increasing subscripts, and S is an α format, interpreted conjunctively.

As indicated above, Theorem 1.1.1 tells us that we need only work with

1) $(\forall g_1,\ldots,g_n \in V)(\exists B_1,\ldots,B_m \in K)(S)$.
2) $(\forall g_1,\ldots,g_n \in V)(\exists B_1 \subseteq \ldots \subseteq B_m \in K)(S)$.
3) $(\exists g_1,\ldots,g_n \in V)(\forall B_1,\ldots,B_m \in K)(S)$.
4) $(\exists g_1,\ldots,g_n \in V)(\forall B_1 \subseteq \ldots \subseteq B_m \in K)(S)$.

where the g's and B's are as indicated earlier, and S is an α format. It will be seen to be very convenient to drop the negation signs in front of the last two of the above.

DEFINITION 1.1.39. Let α be a flat BRT fragment. The α statements (rather than the α assertions) are statements of form 1) above if the environment of α is EBRT and the signature of α does not end with $\subseteq$; 2) above if the environment of α is EBRT and the signature of α ends with $\subseteq$; 3) above if the environment of α is IBRT and the signature of α does not end with $\subseteq$; 4) above if the environment of α is IBRT and the signature of α ends with $\subseteq$.

DEFINITION 1.1.40. Let α be a flat BRT fragment. An α format S is said to be correct if and only if the α statement using S is true; incorrect otherwise.

Informally speaking, a classification of a BRT fragment α amounts to a determination of all α correct α formats.

As discussed earlier, the number of pre elementary inclusions in the standard signature

$$A_1,\ldots,A_n,f_1A_1,\ldots,f_1A_n,\ldots,f_mA_1,\ldots,f_mA_n$$

with m functions and n sets is $2^{n(m+1)}$, and the number of formats is therefore $2^{2\wedge n(m+1)}$.

THEOREM 1.1.2. The number of elementary inclusions in $A_1,\ldots,A_n,f_1A_1,\ldots,f_1A_n,\ldots,f_mA_1,\ldots,f_mA_n,\subseteq$ is $(n+1)^{m+1}$. Therefore the number of formats (or statements) is $2^{(n+1)\wedge m+1}$. In the case of A,B,C,fA,fB,fC,gA,gB,gC,$\subseteq$, we have 64 and 2^{64}. In the case of A,C,fA,fB,gB,gC,$\subseteq$, we have 27 and 2^{27}. In the case of A,B,fA,fB,$\subseteq$, we have 9 and 2^9.

Proof: Let us first focus on the pattern of A's in elementary inclusions. Recall that the elementary inclusions are the immediate simplifications of the pre elementary inclusions, using $A_1 \subseteq \ldots \subseteq A_n$.

i. A_i on left, A_{i-1} on right.
ii. A_1 on left, no A_j on right.
iii. No A_i on left, A_n on right.

There are n+1 among i-iii. The same count holds for the other m groups. So we obtain a total of $(n+1)^{m+1}$ elementary inclusions. QED

For PBRT in σ on (V,K), where σ is based on m functions and n sets, we cannot specify the assertions by a single format. Instead, what is relevant is the number of all α formulas up to propositional and Boolean equivalence. The number of α equations, up to Boolean equivalence, is 2^2^n(m+1), and so the number of α formulas up to propositional and Boolean equivalence is 2^2^2^2^n(m+1). This quantity is quite frightening. Even in one function and one set, this is 2^2^2^2^2 = $2^{65,536}$. For one function and two sets, this is 2^2^2^2^4 = $2^{2^{65,636}}$. These numbers do not address, say, two functions and three sets. We do not tackle PBRT in this book.

In Chapter 2, we focus on the five basic BRT settings, (SD,INF), (ELG ∩ SD,INF), (ELG,INF), (EVSD,INF), and (MF,INF).

In section 2.2, we classify EBRT/IBRT in A,fA on the five basic BRT settings, where the number of assertions is 2^{2^2} = 16. This is of course completely manageable, but still turns out to be substantial. Already, the significant Thin Set Theorem and Complementation Theorem appear among the 16.

In section 2.3, we classify EBRT/IBRT in A,fA,fU on the five basic BRT settings, where the number of statements is 2^{2^3} = 256, with considerable duplication due to equivalence on all BRT settings. This is still manageable.

For EBRT/IBRT in A,B,fA,fB, the number of statements is 2^{2^4} = 2^{16} = 65,536. This is rather daunting, but within manageability with a few years of effort. This optimism is based on the expectation that there will be a large proportion of trivial cases, and lots of relations between cases. This has been the experience with sections 2.4 and 2.5.

In sections 2.4 and 2.5, we classify EBRT in A,B,fA,fB,⊆ on the five basic settings excluding (MF,INF), where the number of statements is 2^9 = 512 (according to Theorem 1.1.2). As can be seen from sections 2.6 and 2.7, we can go much further in the fifth basic BRT setting, (MF,INF), as well as in IBRT on all five basic settings.

In sections 2.2 and 2.3, we make a brute force enumeration of cases. However, in sections 2.4 - 2.7, we prefer to use a treelike methodology. This treelike methodology is presented in section 2.1, where we also develop the relevant theory.

We see that all of the BRT statements that arise from the EBRT classifications in Chapter 2 are decided in RCA_0, and all of the BRT statements that arise from the IBRT classifications in Chapter 2 are decided in ACA'.

ZFC incompleteness arises somewhat later in the development of BRT, with EBRT in A,B,C,fA,fB,fC,gA,gB,gC on the BRT setting (ELG,INF). The Principal Exotic Case, also known as Proposition A in this book, lies within this BRT fragment (see Appendix A). Here we have $2^{2^9} = 2^{512}$ statements. This is entirely unmanageable. It would take several major new ideas to make this manageable in any sense of the word. The same is true even for A,B,C,fA,fB,fC,gA,gB,gC,⊆, since by Theorem 1.1.2, this involves 2^{64} statements. There is a lot of simplification coming from ⊆, but there does not seem to be nearly enough for manageability.

However, the Principal Exotic Case lies within the much smaller fragment EBRT in A,C,fA,fB,gB,gC,⊆ on (ELG,INF). We expect to get enough substantive simplification from ⊆ to make A,C,fA,fB,gB,gC,⊆ as a manageable decade long project. According to Theorem 1.1.2, the relevant count is 2^{27} before substantive simplifications.

In section 3, we give a classification for a very restricted subclass of the statements for EBRT in A,B,C,fA,fB,fC,gA,gB,gC on the BRT setting (ELG,INF). The Principal Exotic Case lies within this very restricted subclass with $3^8 = 6561$ statements.

The Principal Exotic Case is shown in Chapters 4,5 to be provable using strongly Mahlo cardinals of all finite orders, yet not provable in ZFC (assuming ZFC is consistent).

We have given only an informal account of what we mean by a classification for a BRT fragment. We now seek to be more formal.

DEFINITION 1.1.41. Let α be a BRT fragment. A tabular classification for α is a table of the correct α formats.

However, this definition does not take into account the background theory needed to document the table, which is of importance for BRT.

Let T be a formal system with an adequate definition of the BRT fragment α.

DEFINITION 1.1.42. We say that an α format S is α,T correct if and only if the α statement using S is provable in T. We say that S is α,T incorrect if and only if the α statement using S is refutable in T.

DEFINITION 1.1.43. We say that α is T secure if and only if every α format is α,T correct or α,T incorrect.

DEFINITION 1.1.44. A tabular α,T classification consists of a table of all α formats, together with a proof or refutation of each of the corresponding α statements, within T. This is a rather direct demonstration that α is T secure.

In sections 2.2, 2.3, we provide what amounts to a tabular α,T classification for some simple BRT fragments α, where T is RCA_0 or a weak extension of RCA_0.

In Chapter 3, we provide what amounts to a tabular α,$SMAH^+$ classification for a very limited subclass of the EBRT formats α in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF). (For $SMAH^+$, see Appendix A).

But for some α, it is not reasonable to present such large tables. How do we show that α is T secure? What then do we mean by a classification of the α statements in T?

In sections 2.4 - 2.7, we do not present tables, but instead use a treelike methodology. In section 2.1, we develop the theory of this methodology, showing how the analyses in sections 2.4 - 2.7 demonstrate that α is T secure, for various α,T.

To give a classification of the α statements in T, it suffices to give a listing of the maximally α,T correct α formats; i.e., the α,T correct α formats that are not properly included in any other α,T correct format.

In section 2.1, we define the T classifications, TREE, for α. We prove that there is a T classification for α if and only if α is T secure. We also give an algorithm for generating the maximally α,T correct α formats from TREE. We show that the number of maximally α,T correct α formats is at most the number of vertices in TREE.

In sections 2.4 - 2.7, T classifications for the relevant α are actually given in a style prescribed in section 2.1, where T = RCA_0 and ACA'.

The classifications given in Chapters 2 and 3 are rather limited in scope. For instance, we conjecture that

i. EBRT in A,B,fA,fB,fN on any of the five basic BRT settings is RCA_0 secure.

ii. IBRT in A,B,fA,fB,fN on any of the five basic BRT settings is ACA’ secure.

iii. EBRT/IBRT in A,B,C,fA,fB,fC,gA,gB,gC,fN,gN on any of the five basic BRT settings is $SMAH^+$ secure.

These conjectures are wide open. In fact, we have not even established any of i-iii for A,B,fA,fB. We have established i-iii for A,B,fA,fB,$\subseteq$.

1.2. Some BRT settings.

The BRT settings were defined in Definition 1.11.

Most areas of mathematics have a naturally associated family of (multivariate) functions and sets. This usually forms a natural and interesting BRT setting.

This book focuses on five basic BRT settings, as noted in section 1.1. These are formally introduced in Chapter 2. In fact, we have only been able to scratch the surface of BRT even on these basic BRT settings.

In this section, we survey a huge range of mathematically interesting BRT settings. This will give the reader a sense of the unusual scope of BRT and a glimpse of what can be expected in the future development of BRT.

We provide a plausible estimate that at least 1,000,000 of these mathematically interesting BRT settings represent significantly different BRT phenomena. Any substantial probing of BRT on these settings is beyond the scope of this book.

In sections 1.3 and 1.4, we will investigate the status of the Complementation Theorem and the Thin Set Theorem in some very modest sampling of the BRT settings presented in this section. This will give a modest indication as to the depth of BRT and its sensitivity to the choice of BRT setting.

I. On N.

We now consider a number of natural conditions on functions in MF. These conditions are of three kinds.

1. Bounding conditions.
2. Regularity conditions.
3. Choice of norm.

We propose the following basic lower bound conditions on f ∈ MF.

i. There exist c,d such that c op i, d op’ j, and for all x ∈ dom(f), $c|x|^d$ op’’ f(x). Here op,op’ ∈ {<,>,≤,≥,=}, op’’ ∈ {<,≤}, i,j ∈ {0,1/2,1,3/2,2}, and | | is the l_∞ norm, the l_1 norm, or the l_2 norm.

We propose the following basic upper bound conditions on f ∈ MF.

ii. There exist c,d such that c op i, d op’ j, such that for all x ∈ dom(f), $c|x|^d$ op’’ f(x). Here op,op’ ∈ {<,>,≤,≥,=}, op’’ ∈ {>,≥}, i,j ∈ {0,1/2,1,3/2,2}, and | | is the l_∞ norm, the l_1 norm, or the l_2 norm.

Each of these conditions in i,ii above results from the choice of 6 parameters: op,op',op'',i,j,| |. Note that some of the choices of parameters result in degenerate conditions.

Each of these basic lower bound conditions and basic upper bound conditions can be modified by using “for all but finitely many x” instead of “for all x”. This doubles the number of lower and upper conditions, and the resulting conditions are called the lower bound conditions and the upper bound conditions.

The bounding conditions consist of a conjunction of zero or more conditions, each of which is either a basic lower bound condition or a basic upper bound condition.

The five basic BRT settings formally introduced in Chapter 2 are examples of classes of functions obeying bounding conditions.

The basic regularity conditions that we propose on f ∈ MF are as follows.

i. f is a linear function.
ii. f is a polynomial of degree op d with integer (or rational) coefficients. Here op ∈ {=,≤,≥} and d ∈ {1,2,3,4}.
iii. f is a polynomial with integer (or rational) coefficients.
iv. f is given by an expression in some chosen subset of the operations 0,1,+,-,•,÷,↑,log,exp.
v. f is a Presburger function; i.e., definable in (N,+).
vi. f is a primitive recursive function.
vii. f is a recursive function.
viii. f is an arithmetic function.
ix. f is a hyperarithmetic function.

The class of functions BAF = EBAF introduced in section 5.1 is an example of a set of functions obeying a basic regularity condition (see iv above). In Definition 5.1.1, we define 0,1,+,-,•,↑,log used in iv above. Here exp(n,m) = n^m, where exp(n,0) = 1. Also x÷y is the floor of (x divided by y), where x÷0 is taken to be 0.

We place two modifiers on the basic regularity conditions. One is that we allow finitely many exceptions in conditions i - iv above. The second is that we allow conditions i - iv above to merely hold piecewise. I.e., we modify each of conditions i - iv above, to assert only that the function obeys the condition on each of finitely many pieces, where each piece is given by a finite set of inequalities involving functions obeying that same condition. Note that these modifiers have no effect on conditions v - ix above.

Finally, the conditions on f ∈ MF that we propose consist of the conjunction of zero or more conditions, each of which are either a bounding condition, or a regularity condition (perhaps modified).

We now come to the proposed conditions on A ∈ INF.

Firstly, we have the density conditions.

i. A has (upper, lower) density d ∈ ‘a,b’, where a ≤ b, a,b ∈ {0,1/3,1/2,2/3,1}, and ‘ is (or [, and ’ is) or].

Secondly, we have the arithmetic and geometric progression conditions.

ii. A is (contains, is contained in, excludes) an arithmetic (geometric) progression.
iii. Same as ii) with "eventually".
iv. A meets every arithmetic (geometric) progression.
v. A contains infinitely many even (odd) elements.
vi. A has arbitrarily long consecutive runs.

Thirdly, we have the regularity conditions.

vii. A is a Presburger set.
viii. A is a primitive recursive set.
ix. A is a recursive set.
x. A is an arithmetic set.
xi. A is a hyperarithmetic set.

Finally, the conditions on A ∈ INF that we propose consist of zero or more conditions, each of which is either a density condition, an arithmetic/geometric progression condition, or a regularity condition.

The BRT settings that we propose on N are the (V,K), where V is the set of all f ∈ MF obeying a condition in this part I, and K is the set of all A ∈ INF obeying a condition in this part I.

II. On **Z**.

The conditions on functions proposed in part I on functions from MF have natural counterparts as conditions on functions from MF(**Z**) = the class of all multivariate functions from **Z** into **Z**. Specifically, in the bounding conditions, we use |f(x)| instead of f(x). The basic regularity conditions extend to MF(**Z**) in obvious natural ways.

Let INF(**Z**) be the set of all infinite subsets of **Z**. Every pair of conditions α,β on INF from part I generates conditions on A ∈ INF(**Z**) as follows.

i. α holds of A ∩ N.
ii. β holds of −A ∩ N.
iii. α holds of A ∩ N and β holds of −A ∩ N.

Here are three particularly natural examples of such conditions on A ∈ INF(**Z**).

i. No condition. I.e., A ∈ INF(**Z**).
ii. A^+ is infinite.
iii. A^+ and A^- are infinite.

III. On **Q**.

We lift the conditions on **Z** to **Q**. We can additionally use "for all arguments of sufficiently large norm", in addition to "for all but finitely many".

We can also place Lipshitz conditions everywhere, or merely for all arguments of sufficiently large norm. We can restrict attention to Lipshitz conditions involving $c|x-y|^d$, where the constants c,d are treated in a manner similar to the way c,d were treated in connection with lower (and upper) bounds in A above.

In the regularity conditions on functions, Presburger can be replaced by "definable in the ordered additive group of rationals", or "definable in the ordered additive group of rationals with a predicate for the integers".

The density and arithmetic/geometric progression conditions on sets can be replaced by conditions involving the Jordan content of the subset of Q.

IV. On $\mathfrak{R}$.

We can lift the conditions on **Q** to $\mathfrak{R}$. We can additionally add pointwise continuity, uniform continuity, differentiability, and real analyticity conditions on the functions.

We can use semialgebraic as a regularity condition on sets. We can also use open, closed, F_σ, and G_δ as regularity conditions. We can use Lebesgue measure instead of Jordan content.

V. On **C**.

We can of course treat the complex plane **C** like $\mathfrak{R}^2$ and lift the conditions on $\mathfrak{R}$ to conditions on **C**. But it is interesting to use analyticity and other important notions from complex analysis as regularity conditions.

VI. On L^2.

Here we should focus attention on the set V of all bounded linear operators on L^2, and the set K of all nontrivial closed subspaces of L^2. The invariant subspace problem for L^2 is expressed as the followings instance of EBRT in A,fA on (V,K):

$$(\forall f \in V)(\exists A \in K)(fA = A).$$

We can obviously use other function spaces for BRT settings.

VII. Topological BRT.

Here we can extend the conditions used on $\Re$ above to various specific topological spaces. Being nonempty and open is a particularly natural condition on sets.

It also makes sense to investigate those BRT statements that hold in the continuous functions and nonempty open sets, on all topological spaces obeying certain conditions.

The above gives a mere indication of just some of the wide ranging natural BRT settings throughout mathematics.

We believe that the truth value of BRT statements depend very delicately on the choice of BRT setting. In fact, we believe that this delicate relationship already manifests itself in EBRT and IBRT in A,B,C,fA,fB,fC,gA,gB,gC.

Indications of this sensitivity are already present in our classifications of Chapter 2 as well as our results in section 1.4.

In particular, we expect that for many pairs of settings presented in parts I-VII, both the EBRT and the IBRT statements in A,B,C,fA,fB,fC,gA,gB,gC differ. In fact, we suspect that this is true even for small fragments of A,B,C,fA,fB,fC,gA,gB,gC.

We now give a very crude lower estimate on the number of settings presented in parts I-VII above, that we suspect have different BRT behavior. Note that we have been fully precise only in part I above concerning BRT settings on N. So we will only make a rough lower estimate of the number of specific BRT settings proposed on N.

This will not take into account the greater richness that comes with working on other underlying sets, which are generally endowed with various structure, as in parts II-VII above.

In the basic lower bound conditions, there are 5 choices of op, 5 choices of op', 2 choices of op'', 5 choices of i, 5 choices of j, and 3 choices of norm. This results in 5 x 5 x 2 x 5 x 5 x 3 = 3750.

A conservative lower estimate as to the number of these lower bound conditions that are substantially different for BRT purposes is sqrt(3750), which is approximately 60.

Analogously, a conservative lower estimate for basic upper bound conditions is also 60.

The choice of going from "for all x" to "for all but finitely many x" should double these numbers to 120. Conjuncting lower bound conditions and upper bound conditions could result in at least 120 x 120 = 14400 bounding conditions. The interactions between the lower and upper bound conditions might not be all that strong, and so a conservative lower estimate for the bounding conditions for our purposes is 1000.

There are 24 basic regularity conditions under ii above, in addition to 8 others. For BRT significance, we use the conservative estimate of 10.

We have the two modifiers - finitely many exceptions and piecewiseness. This replaces 10 by 20, from a conservative point of view.

Finally, the interaction of bounding conditions and regularity conditions should conservatively result in an estimate of 10,000 families of multivariate functions on N which are substantially different for BRT purposes.

We now take the conditions on subsets of N into consideration.

The density conditions have the upper/lower parameter, 15 pairs a,b, and 4 choices of kinds of intervals. This results in 2 x 15 x 4 = 120 possibilities. Conservatively, we use the lower estimate of 25 for our purposes.

In the arithmetic and geometric progression conditions, items ii and iii each have 6 possibilities, items iv,v each have 2 possibilities, and one for vi, for a total of 17. We use the lower estimate of 8 for our purposes.

There are 5 regularity conditions on sets. We conservatively estimate that 2 have substantial BRT significance.

This results in a triple product 25 x 8 x 2 = 400. We use the conservative lower estimate of 100 for conditions on sets with substantial BRT significance.

We have been sufficiently conservative and believe that our lower estimates for the conditions on multivariate functions, and conditions on sets, are rather lean and mean. Hence for our final estimate, we will simply multiply 10,000 by 100. Thus our lower estimate on the number of interesting BRT settings on N that have been presented, that are BRT different in A,B,C,fA,fB,fC,gA,gB,gC, is 1,000,000.

It is beyond the scope of this book to provide substantive justification for this conjectured lower estimate.

1.3. Complementation Theorems.

Recall the Complementation Theorem from section 1.1. It first appeared in print in [Fr92], Theorem 3, p. 82, (in a slightly different form), where we presented some precursors of BRT.

The Complementation Theorem is closely related to the standard Contraction Mapping Theorem. We discuss the connection below.

The Complementation Theorem is also closely related to a well known theorem, due to von Neumann in [VM44], and subsequent developments in graph theory. We discuss this at the end of this section.

COMPLEMENTATION THEOREM. For all f ∈ SD there exists A ∈ INF such that fA = N\A.

COMPLEMENTATION THEOREM (with uniqueness). For all f ∈ SD there exists a unique A ⊆ N with fA = N\A. Moreover, A ∈ INF.

Before giving the proof of the Complementation Theorem (with uniqueness), we discuss some alternative formulations.

The Complementation Theorem (without uniqueness) is written above as a statement of EBRT in A,fA on (SD,INF). Strictly speaking, we cannot express the uniqueness within BRT.

DEFINITION 1.3.1. $A \cup. B$ is the disjoint union of A and B, and is defined as $A \cup B$ if A,B are disjoint; undefined otherwise. E.g., $A \cup. B = C$ if and only if $A \cup B = C \wedge A \cap B = \emptyset$.

Note that there are other equivalent ways of writing $fA = N\backslash A$. E.g., we can write

$$fA = N\backslash A.$$
$$A = N\backslash fA.$$
$$A \cup. fA = N.$$

The first evaluates the action of f on A.

The second asserts that A is a fixed point (of the operator that sends each B to $N\backslash fB$.

The third asserts that N is partitioned into A and fA.

Proof: Let $f \in SD$. Note that for all $A \subseteq N$, $n \in fA$ if and only if $n \in f(A \cap [0,n))$.

We inductively define a set $A \subseteq N$ as follows. Suppose $n \geq 0$ and we have defined membership in A for all $0 \leq i < n$. We then define $n \in A$ if and only if $n \notin f(A \cap [0,n))$. Since $f \in SD$, we have for all n, $n \in A \leftrightarrow n \notin fA$ as required.

Now suppose $fB = N\backslash B$. Let m be least such that A,B differ. Then $m \in B \leftrightarrow m \notin fB \leftrightarrow m \notin f(B \cap [0,m))$, and $m \in A \leftrightarrow m \notin f(A \cap [0,m))$. Since $A \cap [0,m) = B \cap [0,m)$, we have $m \in A \leftrightarrow m \in B$. This is a contradiction. Hence A = B.

If A is finite then fA is finite and $N\backslash A$ is infinite. Hence A is infinite. QED

It will be convenient to use the following terminology. Let $f:X^k \to X$.

DEFINITION 1.3.2. Let f be a multivariate function with domain X (see Definitions 1.1.8 - 1.10). A complementation of f is a set A ⊆ X such that fA = X\A.

Thus we can restate the Complementation theorem (with uniqueness) as follows.

COMPLEMENTATION THEOREM (with uniqueness). Every f ∈ SD has a unique complementation.

Note that we have proved the Complementation Theorem (with uniqueness) within the base theory RCA_0 of Reverse Mathematics. See [Si99].

The Complementation Theorem is obviously a particularly simple way of encapsulating the essence of recursion along the natural numbers. It appears to have significant educational value.

We now state a Complementation Theorem for well founded relations. We will be using this generalization in section 4.2.

DEFINITION 1.3.3. A binary relation is a set R of ordered pairs. We place no restriction on the coordinates of the elements of R. We write fld(R) = {x: (∃y ∈ R)(x is a coordinate of y)}.

DEFINITION 1.3.4. We say that a binary relation R is well founded if and only if for all nonempty S ⊆ fld(R), there exists y ∈ S such that for all x ∈ S, (x,y) ∉ R. Thus well founded relations are irreflexive.

DEFINITION 1.3.5. We say that $f:fld(R)^k \rightarrow fld(R)$ is strictly dominating if and only if for all $x \in fld(R)^k$, $(x_1,f(x)),\ldots,(x_k,f(x)) \in R$.

DEFINITION 1.3.6. We write SD(R) for the set of all strictly dominating functions whose domain is a Cartesian power of fld(R) and whose range is a subset of fld(R).

THEOREM 1.3.1. COMPLEMENTATION THEOREM (for well founded relations, with uniqueness). If R is a well founded relation, then every f ∈ SD(R) has a unique complementation.

Proof: We want to be particularly careful because we are not assuming that R is transitive. Let the arity of f be $k \geq 1$.

For all $b \in fld(R)$, define b^* to be the set of all x which ends a backward R chain of length ≥ 1 that starts with b. Thus $b \in b^*$.

We first make a coherence claim. Let $b,b' \in fld(R)$, and $S,T \subseteq fld(R)$, where

$$S \subseteq b^* \wedge (\forall c \in b^*)(c \in S \leftrightarrow c \notin fS).$$
$$T \subseteq b'^* \wedge (\forall c \in b'^*)(c \in T \leftrightarrow c \notin fT).$$

Then

$$(\forall c \in b^* \cap b'^*)(c \in S \leftrightarrow c \in T).$$

Suppose this is false. By well foundedness, fix c such that

$$c \in b^* \cap b'^* \wedge (c \in S \leftrightarrow c \notin T)$$
$$(\forall d)(R(d,c) \rightarrow \neg(d \in b^* \cap b'^* \wedge (d \in S \leftrightarrow d \in T)))$$

and obtain a contradiction.

We now claim that $c \in fS \leftrightarrow c \in fT$. For the forward direction, let $c = f(d_1,...,d_k)$, $d_1,...,d_k \in S$. By $f \in SD(R)$, we have $R(d_1,c),...,R(d_k,c)$. Hence $d_1,...,d_k \in T$, and so $c \in fT$. The reverse direction is proved in the same way.

Since $c \in S \leftrightarrow c \notin T$, we have $c \notin fS \leftrightarrow c \in fT$. This contradicts the above claim, and the coherence claim is established.

We now claim that for all $b \in fld(R)$, there exists $S_b \subseteq b^*$ such that $(\forall c \in b^*)(c \in S_b \leftrightarrow c \notin f(S_b))$. To see this, suppose this is false, and fix $b \in fld(R)$ such that

$$(\forall x)(R(x,b) \rightarrow (\exists S \subseteq x^*)(\forall c \in x^*)(c \in S \leftrightarrow c \notin fS)).$$
$$\neg(\exists S \subseteq b^*)(\forall c \in b^*)(c \in S \leftrightarrow c \notin fS).$$

By the coherence claim, for each x such that $R(x,b)$, there is a unique set $S_x \subseteq x^*$ such that $(\forall c \in x^*)(c \in S_x \leftrightarrow c \notin f(S_x))$.

Furthermore, by the coherence claim, we have

$$(\forall x,y)((R(x,b) \wedge R(y,b)) \rightarrow$$

$$(\forall c \in x^* \cap y^*)(c \in S_x \leftrightarrow c \in S_y)).$$

Let V be the union of the S_x such that R(x,b). We claim that

$$(\forall c \in b^*\backslash\{b\})(c \in V \leftrightarrow c \notin fV).$$

To see this, let $c \in b^*\backslash\{b\}$. First assume $c \in V$, $c \in fV$. Fix x such that $c \in S_x$, R(x,b). Let $c = f(d_1,...,d_k)$, $d_1,...,d_k \in V$. Then $R(d_1,c),...,R(d_k,c)$. Hence $d_1,...,d_k \in x^*$. By coherence, $d_1,...,d_k \in S_x$, since $d_1,...,d_k \in V$. Hence $c \in S_x$, $c \in f(S_x)$, which contradicts the definition of S_x.

Now assume $c \notin fV$. Since $c \in b^*\backslash\{b\}$, let $c \in x^*$, R(x,b). Then $c \in S_x \leftrightarrow c \notin f(S_x)$. Now $c \notin f(S_x)$. Hence $c \in S_x$. Therefore $c \in V$.

The set V is not quite the same as the set S_b that we are looking for. We let $S_b = V$ if $b \in fV$; $V \cup \{b\}$ otherwise. Then

$$\neg(\exists S \subseteq b^*)(\forall c \in b^*)(c \in S \leftrightarrow c \notin fS).$$

and so we have a contradiction. Hence the claim is established.

To complete the proof, let S be the union of all S_b, $b \in$ fld(R). By the same argument, we see that

$$(\forall c \in fld(R))(c \in S \leftrightarrow c \notin fS).$$

and so S is a complementation of f. S is unique by the argument given above for the coherence claim. QED

DEFINITION 1.3.7. Let (V,K) be a BRT setting (see Definition 1.11). The Complementation Theorem for (V,K) asserts that $(\forall f \in V)(\exists A \in K)(fA = U\backslash A)$. The Complementation Theorem for (V,K) (with uniqueness) asserts that $(\forall f \in V)(\exists! A \in K)(fA = U\backslash A)$.

We use POW(E) for the power set of E.

Let $<$ be a binary relation. Then (SD($<$),POW(fld($<$))) is a BRT setting, and its universal set U = fld($<$). See Definition 1.13 for the definition of U.

THEOREM 1.3.2. Let $<$ be an irreflexive transitive relation with the upper bound condition $(\forall x,y)(\exists z)(x,y < z)$. The following are equivalent.

1. The Complementation Theorem holds on (SD(<),POW(fld(<))).
2. The Complementation Theorem (with uniqueness) holds on (SD(<),POW(fld(<))).
3. < is well founded

Proof: Obviously 3 → 2 → 1 follows immediately from Theorem 1.3.1, even for arbitrary relations <. Thus we have only to assume that < is non well founded, and give a counterexample to 1.

Since < is irreflexive and transitive, < has no cycles. Since < is non well founded, < must have an infinite descending sequence.

Let $x_1 > x_2 > x_3 > \ldots$ be an infinite descending sequence. Let f ∈ SD(<) have arity 2, where for all 0 < i < j, $f(x_{2i},x_{2j-1}) = x_{2i-1}$. For all other pairs y,z ∈ fld(<), let $f(y,z) > x_1,y,z$. Then f ∈ SD(<). Let A ⊆ fld(<), fA = fld(<)\A.

Clearly each $x_{2i} \notin fA$, and so each $x_{2i} \in A$. Hence for all i > 0, $x_{2i-1} \in fA \leftrightarrow (\exists j > i)(x_{2j-1} \in A)$. Hence for all i > 0, $x_{2i-1} \in A \leftrightarrow (\forall j > i)(x_{2j-1} \notin A)$.

Let i > 0. Suppose $(\forall j > i)(x_{2j-1} \notin A)$. Then $(\forall j > i+1)(x_{2j-1} \notin A)$, and so $x_{2i+1} \in A$. This is a contradiction, using j = i+1.

Hence for all i > 0, $x_{2i-1} \notin A$. But then $x_1 \notin fA$, $x_1 \in A$. This is a contradiction. Hence fA ≠ fld(<)\A. QED

Transitivity cannot be removed from the hypotheses of Theorem 1.3.2, as indicated by the following example.

THEOREM 1.3.3. Let R be the non well founded irreflexive binary relation on Z with the upper bound condition, given by $x\ R\ y \leftrightarrow (x+1 = y \vee (x < y \wedge y \geq 0))$. Then every f ∈ SD(R) has a complementation.

Proof: Let f ∈ SD(R). We first define $A \cap Z^-$ as follows. Let $B = Z^-\backslash rng(f)$. We first put B ⊆ A.

Now define membership in A in the open interval between any two numerically successive elements of B by induction. I.e., if n < m are two numerically successive elements of B, then for all 1 ≤ i ≤ m-n-1, put n+i in A if and only if n+i $\notin$ fA. This is well defined because the truth value of n+i $\in$ fA depends only on the truth value of n+i-1 $\in$ A.

If max(B) < 0 then define membership in A in the open interval between max(B) and 0 by induction in the same way.

Now suppose that B has a least element, t. Put t-1 $\notin$ A, t-2 $\in$ A, t-3 $\notin$ A, ..., alternating in the obvious way. If B = $\emptyset$, put -1 $\notin$ A, -2 $\in$ A, -3 $\notin$ A, ...

This completes the definition of A $\cap$ Z^-. Note that for all n < 0, n $\in$ A $\leftrightarrow$ n $\notin$ fA.

We can now define A $\cap$ N recursively as follows. For n $\in$ N, take n $\in$ A if and only if n $\notin$ fA. Then for all n $\geq$ 0, n $\in$ A $\leftrightarrow$ n $\notin$ fA. Since for all n < 0, n $\in$ A $\leftrightarrow$ n $\notin$ fA, A is a complementation of f. QED

We now consider the structure of the unique complementations, for various simple f $\in$ SD.

From examination of the construction of the unique complementation A, given in the proof of the Complementation Theorem above, we see that as more numbers are placed in A, more numbers appear in fA, and so fewer numbers are placed in A later. And as fewer numbers are placed in A later, fewer numbers appear in fA, and so more numbers are placed in A latter. So there is a tension between numbers going in and numbers staying out.

There is the expectation that even for very simple f $\in$ SD, the unique complementation A of f can be very complicated - and have an intricate structure well worth exploring.

Let us consider some very basic examples.

DEFINITION 1.3.8. We define Res(n,m) as the residue of n modulo m $\geq$ 1.

THEOREM 1.3.4. Let $f:N^k \to N$ be given by $f(n_1,...,n_k) = n_1+...+n_k+c$, where c is a constant $\geq$ 1. Then the complementation of f is {n $\geq$ 0: Res(n,k(c-1)+c+1) < c}. Thus A is periodic with period k(c-1)+c+1.

Proof: Let k,f,c be as given. Let A = {n $\geq$ 0: Res(n,k(c-1)+c+1) < c}. Suppose $n_1,...,n_k \in$ A. Then $Res(n_1,k(c-1)+c+1),...,Res(n_k,k(c-1)+c+1)$ < c. Hence $Res(n_1+...+n_k+c,k(c-1)+c+1) \in [c,k(c-1)+c]$, because when we add the residues of n1,...,nk,c, we stay below the modulus k(c-1)+c+1. Therefore $n_1+...+n_k+c \notin A$.

Suppose $n \notin A$, $n \geq 0$. Then p = Res(n,k(c-1)+c+1) ∈ [c,k(c-1)+c] and $n \geq c$. Hence p-c ∈ [0,k(c-1)], and so write p-c as a sum of k elements of [0,c-1]. Hence write p = $t_1+...+t_k+c$, where $t_1,...,t_k \in [0,c-1]$. Write n = $(n-p+t_1)+t_2+...+t_k+c$.

By the definition of p, we have $p \leq n$, and so $n-p+t_1 \geq 0$ and Res($n-p+t_1$,k(c-1)+c+1),Res(t_1,k(c-1)+c+1),...,Res(t_k,k(c-1)+c+1) ∈ [0,c-1]. Hence $n-p+t_1,t_2,...,t_k \in A$. QED

We now come to a basic example where the function is unary and one-one. This is a very special case, and it lends itself to a general result of independent interest.

Let f:X → X be one-one and k be an integer. For $k \geq 0$ and x ∈ X, let $f^k(x)$ = f...f(x), where there are k f's. Let $f^{-k}(x)$ be the unique y such that $f^k(y) = x$, if y exists; undefined otherwise.

LEMMA 1.3.5. Let f:X → X be one-one. Assume that for all x ∈ X there exists $k \geq 1$ such that $f^{-k}(x)$ does not exist. Then the unique complementation of f is $X\backslash fX \cup f^2(X\backslash fX) \cup f^4(X\backslash fX) \cup ...$.

Proof: Let f be as given. We first claim that every x ∈ X can be written as $f^i(y)$, where $i \geq 0$ and $y \in X\backslash fX$. Suppose this is false for x. We show that by induction on $i \geq 1$ that for all $i \geq 1$, $f^{-i}(x)$ exists, contrary to the hypothesis on f. Clearly x ∈ fX, and so the case i = 1 is verified.

Suppose $f^{-i}(x)$ exists. If $f^{-i-1}(x)$ does not exist then $f^{-i}(x) \in X\backslash fX$, and so $x \in f^i(X\backslash fX)$. This is a contradiction. Hence $f^{-i-1}(x)$ exists, completing the induction argument.

We next claim that X is partitioned by the infinite disjoint union

1) $X\backslash fX \cup. f(X\backslash fX) \cup. f^2(X\backslash fX) \cup. ...$.

We have just shown that the union is X. To see that these sets are disjoint, let $f^i(x) = f^j(y)$, where $0 \leq i < j$, and $x,y \in X\backslash fX$. Since f is one-one, we have $x = f^{j-i}(y)$, and so x ∈ fX. This is a contradiction.

We now see that X is partitioned by the two disjoint sets

$$X\backslash fX \cup. f^2(X\backslash fX) \cup. f^4(X\backslash fX) \cup. \ldots .$$
$$f(X\backslash fX) \cup. f^3(X\backslash fX) \cup. f^5(X\backslash fX) \cup. \ldots .$$

Also note that the forward image of f on the first set is the second set. Therefore the first set is a complementation of f.

For uniqueness, suppose E is a complementation of f. Then obviously $X\backslash fX \subseteq E$. Hence $f(X\backslash fX) \subseteq X\backslash E$. Therefore $f^2(X\backslash fX) \subseteq X$. Continue in this way. This determines membership in X for all of 1), which is all of X. QED

THEOREM 1.3.6. Let $f:N \to N$ be given by $f(n) = an+b$, where $a \geq 2$ and $0 < b < a$. Then the unique complementation of f is a finite union of ranges of two variable expressions involving addition, subtraction, multiplication, unnested base a exponentiation, and constants. In particular, the unique complementation of f is $\{(an+k)a^{2i} + b(a^{2i}-1)/(a-1): n,i \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}$.

Proof: Let f,a,b be as given. Note that f is one-one. We apply Lemma 1.3.5.

Let $S = N\backslash fN$. Note that $S = \{an+k: n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}$.

We claim that for all $i \geq 0$,

$$f^iS = \{(an+k)a^i + b(a^i-1)/(a-1): n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}.$$

We prove this by induction. For $i = 0$, we must verify that

$$f^0S = S = \{an+k: n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}$$

which is obvious. Suppose

$$f^iS = \{(an+k)a^i + b(a^i-1)/(a-1): n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}.$$

Then

$$f^{i+1}S = \{a[(an+k)a^i + b(a^i-1)/(a-1)] + b: n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\} =$$

$$\{(an+k)a^{i+1} + ab(a^i-1)/(a-1) + b: n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\} =$$

$$\{(an+k)a^{i+1} + b(a(a^i-1)/(a-1) + 1): n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\} =$$

$$\{(an+k)a^{i+1} + b(a^{i+1}-1)/(a-1): n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}.$$

Obviously, the first disjoint union from Lemma 1.3.5, which is the unique complementation of f, is

$$\{(an+k)a^i + b(a^i-1)/(a-1): n \geq 0 \wedge k \in [0,a-1]\backslash\{b\} \wedge i \in 2N\} =$$

$$\{(an+k)a^{2i} + b(a^{2i}-1)/(a-1): n,i \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}.$$

QED

We would like to consider any affine function f from a Cartesian power of N into N. The problem is that affine functions may not be in SD.

DEFINITION 1.3.9. Let f be a multivariate function and A be a set. We define the "upper image" of f on A by

$$f_{<}A = \{f(x_1,\ldots,x_k): f(x_1,\ldots,x_k) > \max(x_1,\ldots,x_k) \text{ and } x_1,\ldots,x_n \in A\}$$

where f has arity k. Obviously, if f ∈ SD then $f_{<}A$ = fA.

DEFINITION 1.3.10. Let < be a binary relation and f be a multivariate function with domain fld(R). An upper complementation of f is a set A ⊆ X such that $f_{<}A$ = fld(R)\A.

For upper complementations of f ∈ MF, it is understood that < is the usual ordering on N.

UPPER COMPLEMENTATION THEOREM. Every $f:N^k \to Z$ has a unique upper complementation. This unique upper complement is infinite.

In fact, this was the first form of the Complementation Theorem in print. See [Fr92], Theorem 3, p. 82.

We continue with two more examples.

THEOREM 1.3.7. Let $f:N^k \to N$ be given by $f(n_1,...,n_k) = n_1+...+n_k$, $k \geq 2$. Then the unique upper complementation of f is $\{n \geq 0: Res(n,k) = 1\} \cup \{0\}$. Thus the unique upper complementation is periodic with period k. If k = 1 then the unique upper complementation is N.

Proof: Let k,f be as given. Let $A = \{n \geq 0: Res(n,k) = 1\} \cup \{0\}$. Let $n = f_<(n_1,...,n_k)$, $n_1,...,n_k \in A$. Then $Res(n_1+...+n_k,k) = 0$, and so $n = f_<(n_1,...,n_k)$ has residue 0 mod k and is > 0 if defined. Hence $n \notin A$ if defined.

Suppose $n \notin A$, $n \geq 0$. Then n > 1. Let p be largest such that p < n and Res(p,k) = 1. Since $Res(n,k) \neq 1$, we have $0 < n-p \leq k-1$. Let $n_1,...,n_{k-1} \in \{0,1\}$ be such that $n_1 + ... + n_{k-1} = n-p$. Then $n = p + n_1 + ... + n_{k-1}$, and $p,n_1,...,n_{k-1} \in A$. Also $n > p,n_1,...,n_{k-1}$. Hence $n \in f_<(p,n_1,...,n_k)$. Therefore $n \in f_<A$. QED

Robert Lubarsky considered the case of binary multiplication (private communication). Here is his result.

THEOREM 1.3.8. Let $f:N^2 \to N$ be given by f(n,m) = nm. Then the unique upper complementation of f is $\{n: n = 0 \vee n = 1 \vee n$ is the product of an odd number of primes$\}$.

Proof: Let f be as given. Let $A = \{n: n = 0 \vee n = 1 \vee n$ is the product of an odd number of primes$\}$. Let $n \in A$, $n \in f_<A$. Write n = mr, $m,r \in A$, n > m,r. Then $m,r \geq 2$, and so m,r are each the product of an odd number of primes. Therefore n = mr is the product of an even number of primes, and hence $n = mr \notin A$. This establishes that $(\forall n \in N)(n \in f_<A \to n \notin A)$.

Now let $n \notin A$, $n \geq 0$. Then $n \geq 2$ and n is not the product of an odd number of primes. Hence n is the product of an even number, 2t, of primes, $t \geq 1$. We can obviously write n = mr, where m,r are each the product of t primes. Hence we have written n = mr, where $m,r \in A$, and $m,r \geq 2$. Therefore $n \in f_<A$. QED

To understand the complementation of a function like nm+1 appears to be difficult.

A challenge would be to understand the structure of the unique upper complementation of every affine function $f:N^k \to Z$ with integer coefficients. In particular, can we estimate the number of elements below n of these unique upper complementations? Can we algorithmically determine whether there are arbitrarily long blocks?

Can we algorithmically determine the cardinalities of all finite Boolean combinations of the unique upper complementations of these f's?

We now wish to generalize the Complementation Theorem (for SD) in a different direction that will be used in section 2.4. Recall the definition of BRT term in Definition 1.1.5.

Note that one of the three forms of fA = N\A is A = N\fA, which converts the Complementation Theorem into a fixed point theorem.

BRT FIXED POINT THEOREM. Let t be a BRT term in several set variables and several function variables, in which all occurrences of the set variable A lie within the scope of a function variable. Let us assume that the function variables have been assigned elements of SD, and the set variables other than A have been assigned subsets of N. Then there is a unique set A ⊆ N such that the BRT equation A = t holds.

Proof: We first claim that if t is any BRT term, and an assignment for t is as stated, and A,A' ⊆ N agree on [0,n), then n ∈ t(A) ↔ n ∈ t(A'). This claim is proved by induction on the BRT term t. We now follow the proof given above of the Complementation Theorem, building sets $A_0 \subseteq A_1 \subseteq \ldots$ by induction, and setting $A = \bigcup_n A_n$. We use the claim to verify that A = t holds. Uniqueness is easily verified as before. QED

The BRT fixed point theorem is closely associated with the standard contraction mapping theorem.

CONTRACTION MAPPING THEOREM. Let (X,d) be a compact metric space, c ∈ [0,1), and T:X → X be continuous. Assume that for all x,y ∈ X, d(T(x),T(y)) ≤ c•d(x,y). Then T has a unique fixed point.

We can apply the Contraction Mapping Theorem to prove the BRT Fixed Point Theorem, using the usual compact metric space on POW(N). This metric is given by

$$d(B,C) = 2^{-\min(B\Delta C)} \text{ if } B \neq C;\ 0 \text{ otherwise.}$$

The claim in the proof of the BRT Fixed Point Theorem establishes the required inequality for the mapping t(A) with constant c = 1/2.

We now present a useful sufficient condition on $f:X^k \to X$ so that f has a unique complementation. The sufficiency of the criterion follows immediately from the Complementation Theorem (for well founded relations, with uniqueness) proved earlier in this section.

DEFINITION 1.3.11. Define the relation R(f) on X by

R(f)(x,y) if and only if
y is the value of f at some arguments that include x.

THEOREM 1.3.9. Every $f:X^k \to X$, where R(f) is well founded, has a unique complementation.

Proof: Let $f:X^k \to X$, where R(f) is well founded. We claim that $f \in SD(R)$. To see this, note that for all $1 \le i \le k$, $f(x_1,...,x_k)$ is the value of f at some arguments that include x_i. Hence f has a unique complementation by Theorem 1.3.1. QED

Note that in Lemma 1.3.5, the f has a (very) well founded R(f). Hence the existence of a unique complementation in Lemma 1.3.5 follows immediately from Theorem 1.3.9.

We now prove a Continuous Complementation Theorem.

We say that $f:E^k \to \Re$, $E \subseteq \Re$, is strictly dominating if and only if for all $x \in E^k$, $|f(x)| > |x|$. Here we take | | to be the sup norm.

CONTINUOUS COMPLEMENTATION THEOREM (with uniqueness). Every strictly dominating continuous $f:E^k \to E$, where $E \subseteq \Re$ is closed, has a unique complementation.

Proof: Let f be as given. By Theorem 1.3.9 it suffices to prove that R(f) is well founded. Let ... x_3 R(f) x_2 R(f) x_1 be an infinite backwards chain living in E. Then $|x_1| > |x_2| > ...$. Let $w_1,w_2,... \in E^k$, where for all $i \ge 1$, $x_i = f(w_i)$ and x_{i+1} is a coordinate of w_i. Then for all $i \ge 1$, $|x_i| > |w_i| \ge |x_{i+1}|$. In particular, $|w_1| > |w_2| > ...$. Note that the $|x_i| = |f(w_i)|$ and the $|w_i|$ are both strictly decreasing and have the same inf, α. Note that α is the unique limit point of the $|f(w_i)|$ and of the $|w_i|$. Since the w_i are bounded, let w be a limit point of the w_i. Since E is closed, $w \in E^k$. Clearly $|w| = \alpha$. By continuity, $f(w)$ is a limit point of the $f(w_i)$. Hence $|f(w)|$ is a limit point of the $|f(w_i)|$. Therefore $|f(w)| = \alpha$. I.e., $|f(w)| = |w| = \alpha$. This violates that f is strictly dominating. QED

If we strengthen strictly dominating, then we no longer need continuity.

DEFINITION 1.3.12. We say that $f:E^k \to \Re$, $E \subseteq \Re$, is shift dominating if and only if there exists a constant $c > 0$ such that for all $x \in E^k$, $|f(x)| > |x| + c$.

SHIFT DOMINATING COMPLEMENTATION THEOREM (with uniqueness). Every shift dominating $f:E^k \to E$, $E \subseteq \Re$, has a unique complementation.

Proof: Let f be as given. A backwards chain in R(f) creates vectors $x_1,x_2,\ldots$ such that each $|x_i| > |x_{i+1}| + c$. This is obviously impossible. Hence R(f) is well founded. Apply Theorem 1.3.9. QED

The Complementation Theorem is closely related to an important development in digraph theory.

DEFINITION 1.3.13. A digraph (directed graph) is a pair $G = (V,E)$, where $V = V(G)$ is a set of vertices and $E = E(G)$ is a set of edges. $E(G) \subseteq V^2$ is required. We say that x is G connected to y if and only if $(x,y) \in E(G)$.

The key definition is that of a kernel (see [Be85]) and its dual notion, dominator.

DEFINITION 1.3.14. A kernel K of G is a subset of V(G) such that

i. There is no edge connecting any two elements of K. In particular, there is no loop with vertex from K.
ii. Every element of $V(G)\setminus K$ is G connected to an element of K.

DEFINITION 1.3.15. A dominator D of G is a subset of V(G) such that

i. There is no edge connecting any two elements of D. In particular, there is no loop with vertex from D.
ii. Every element of D is G connected to an element of $V(G)\setminus D$.

It is obvious that K is a kernel of G if and only if the following holds:

$x \in K$ if and only if
x is not G connected to any element of K.

Also D is a dominator of G if and only if the following holds:

$x \in D$ if and only if
no element of D is G connected to x.

Also let G be a digraph and G* be the dual of G; i.e., the same digraph with the arrows reversed. Then the kernels of G are the same as the dominators of G*, and the dominators of G are the same as the kernels of G*.

Dominators are explicitly connected with the Complementation Theorem in the unary case $f:X \to X$. We can think of f as a graph G whose vertex set is X and whose edges are the (x,f(x)). Then the complementations of f are the same as the dominators of G.

DEFINITION 1.3.16. A dag is a directed acyclic graph. I.e., a digraph with no cycles. A cycle (in a digraph) is a finite path which starts and ends at the same place.

The following is due to von Neumann in [VM44]. Also see [Be85].

THEOREM 1.3.10. Every finite dag has a unique kernel and a unique dominator.

Proof: Since the dual of an acyclic graph is acyclic, it suffices to prove that there is a unique kernel.

Let (V,G) be a finite dag. We can assume that V(G) is nonempty. We inductively define $V_0,V_1,V_2,\ldots$, where for every i, V_i is the set of vertices outside $V_0 \cup \ldots \cup V_{i-1}$ which G connect only to vertices in $V_0 \cup \ldots \cup V_{i-1}$. In particular, V_0 is the set of vertices that do not G connect to any vertex. Since G is a dag, V_0 is nonempty. Obviously the V's are eventually empty, and are pairwise disjoint. So we write $V_0,V_1,\ldots,V_n$, $n \geq 0$, where these V's are nonempty and $V_{n+1} = \emptyset$.

We claim that $V(G) = V_0 \cup \ldots \cup V_n$. Otherwise, let $x \notin V_0 \cup \ldots \cup V_n$. Since $x \notin V_{n+1}$, x G connects to some $y \notin V_0 \cup \ldots$

$\cup V_n$. We can continue this process, obtaining an infinite chain of G connections. This contradicts that V(G) is finite.

Now define $K \cap V_i$ by induction on i = 0,...,n. Take $x \in K \cap V_i$ if and only if x is not G connected to any element of $V_0 \cup \ldots \cup V_{i-1}$. By the construction of the V's, we see that $x \in K$ if and only if x is not G connected to any element of K. QED

This is not true for arbitrary dag's (as is well known).

THEOREM 1.3.11. There is a countable dag without a kernel and without a dominator.

Proof: We first construct a countable dag G without a kernel.

Let G be the digraph with V(G) = N and whose edges are the (n,m) where $n < m$. Let K be a kernel of G. We have $n \in K \leftrightarrow$ n is not connected to any element of $K \leftrightarrow$ K has no element $>$ n. If K is empty then $0 \in K$. Hence K is nonempty. Let $n \in K$. Then K has no elements $> n$. In particular, $n+1 \notin K$. Hence n+1 is G connected to some element of K. Therefore K has an element $> n+1$. This is a contradiction.

For the final claim, let G* be the dual of G. Then G* has no dominator. Let H be the disjoint union of G and G*. I.e., $V(H) = V(G) \cup V(G^*)$ and $E(H) = E(G) \cup E(G^*)$, where we assume $V(G) \cap V(G^*) = \emptyset$. Then any kernel of H intersected with G is a kernel of G, and any dominator of H intersected with G* is a dominator of G. Therefore H is a countable dag without a kernel and without a dominator. QED

We mention an old but rather striking result of [Ri46].

THEOREM 1.3.12. Every finite graph without cycles of odd length has a kernel and a dominator.

Here we do not have uniqueness since the two vertex digraph with each vertex connected to the other, has no cycles of odd length, and two obvious kernels - the singletons – which are also dominators.

The book [HHS98a] has an extensive bibliography that includes many papers on kernels in graphs. Also see [HHS98b], [GLP98].

Theorem 1.3.10 has the following known extension to infinite digraphs.

THEOREM 1.3.13. Every digraph without an infinite walk $x_0 \rightarrow x_1 \rightarrow \ldots$ has a unique kernel.

Proof: We can either give a proof analogous to that of Theorem 1.3.1 (as a referee has done), or we can conveniently derive this from Theorem 1.3.1. Let G be a digraph with no infinite walk $x_0 \rightarrow x_1 \rightarrow \ldots$. Let R be the binary relation $R(x,y) \leftrightarrow (y,x) \in E(G)$; i.e., $y \rightarrow x$ in G. Then R is well founded.

In fact, we need to use an extension R' of R. We introduce a new copy of every vertex in G, and make all of these copies R' predecessors of every vertex in G. These copies have no R' predecessors. Also introduce new points $\infty,\infty+1,\infty+2,\ldots$, each an R' predecessor of the next, all of which are R' successors of all vertices in G and their copies. Note that any two elements of fld(R') have a common successor.

Define $f:\text{fld}(R')^2 \rightarrow V(G)$ by cases.

case 1. $x \in V(G)$, y is a copy of some $z \in V(G)$ with $R(x,z)$. Then define $f(x,y) = z$.

case 2. otherwise. Define f(x,y) to be any R' successor of x,y.

By Theorem 1.3.1, let A be a complementation of f. Note that all of the copies of vertices in G lie in A. Hence if x is G connected to an element of A then $x \in fA$, $x \notin A$.

On the other hand, suppose $x \in V(G)$ is not G connected to any element of A. Then $x \notin fA$, $x \in A$. This establishes that $A \cap V(G)$ is a kernel of G.

To show that all kernels of G are the same, let K,K' be kernels of G. Assume that $K \Delta K'$ is nonempty, and choose $x \in K \Delta K'$ such that x is not G connected to any element of $K \Delta K'$. By symmetry, we can assume that $x \in K$, $x \notin K'$. Then x is not G connected to any element of K, and x is G connected to some element y of K'. Clearly $y \notin K \Delta K'$, $y \in K$. This is a contradiction. QED

1.4. Thin Set Theorems.

Recall the Thin Set Theorem from section 1.1.

THIN SET THEOREM. For all f ∈ MF there exists A ∈ INF such that fA ≠ N.

The Thin Set Theorem as written above is a statement of IBRT in A,fA on (MF,INF). This specific statement is due to the present author, who studied it for its significance for Reverse Mathematics and recursion theory.

A variant of this statement was already introduced much earlier in the literature on the (square bracket) partition calculus in combinatorial set theory, in [EHR65]. In their language, the Thin Set Theorem reads

$$(\forall n < \omega)(\omega \rightarrow [\omega]^n_\omega).$$

The n indicates a coloring of the unordered n-tuples from the ω to the left of →, the lower ω indicates the number of colors, and the ω in [ ] indicates the cardinality of the "homogenous" set. But here [ ] indicates a weak form of homogeneity - that at least one color is omitted.

The mathematical difference between this square bracket partition relation statement and the Thin Set Theorem is that the former involves unordered tuples, whereas the latter involves ordered tuples. However, see Theorem 1.4.2 below for an equivalence proof in RCA_0. Also see [EHMR84], Theorem 54.1. It was immediately recognized that this square bracket partition relation follows from the usual infinite Ramsey theorem, which is written in terms of the round parenthesis partition relation

$$(\forall n,m < \omega)(\omega \rightarrow (\omega)^n_m).$$

Experience reveals that when the Thin Set Theorem is stated exactly in our formulation above (with ordered n tuples), mathematicians who are not experts in the partition calculus, do not recognize the Thin Set Theorem's connection with the partition calculus and combinatorial set theory. They are struck by its fundamental character, and will not be able to prove it in short order. They apparently would have to rediscover the infinite Ramsey theorem, and in our experience, long before they invest that kind of effort, they demand a proof from us.
The Thin Set Theorem - as an object of study in the foundations of mathematics - first appeared publicly in

[Fr00], and in print in [FS00], p. 139. There we remark that it trivially follows from the following well known Free Set Theorem for N.

FREE SET THEOREM. Let $k \geq 1$ and $f:N^k \to N$. There exists infinite $A \subseteq N$ such that for all $x \in A^k$, $f(x_1,\ldots,x_k) \in A \to f(x_1,\ldots,x_k) \in \{x_1,\ldots,x_k\}$.

The implication is merely the observation that if A obeys the conclusion of the Free Set Theorem, then $A\backslash\{\min(A)\}$ obeys the conclusion of the Thin Set Theorem ($\min(A)$ is not a value of f on $(A\backslash\{\min(A)\})^k$).

The Free Set Theorem is easily obtained from the infinite Ramsey theorem in a well known way. Choose infinite $A \subseteq N$ such that the truth value of $f(x_1,\ldots,x_k) = y$ depends only on the order type of $x_1,\ldots,x_k,y$, provided $x_1,\ldots,x_k,y \in A$. If $f(x_1,\ldots,x_k) = y \notin \{x_1,\ldots,x_k\}$, where $x_1,\ldots,x_k,y \in A$, then we can move $x_1,\ldots,x_k,y$ around in A so that we have

$$f(x_1,\ldots,x_k) = y$$
$$f(x_1,\ldots,x_k) = y'$$

where y' is the element of A right after y. This is a contradiction.

In [FS00], p. 139-140, we presented our proof that the Thin Set Theorem is not provable in ACA_0. A proof of our result that the Thin Set Theorem for binary functions cannot be proved in WKL_0 appears in [CGHJ05]. [CGHJ05] also contains an exposition of our proof that the Thin Set Theorem is not provable in ACA_0. It is easy to see that the Free Set Theorem, and hence the Thin Set Theorem, for arity 1, is provable in RCA_0.

The metamathematical status of the Thin Set Theorem and the Free Set Theorem are not known.

This is in sharp contrast to the well known status of the infinite Ramsey theorem. The infinite Ramsey theorem for any fixed exponent $n \geq 3$ is provably equivalent to ACA_0 over RCA_0. The infinite Ramsey theorem stated for all exponents is provably equivalent to a system ACA′ over RCA_0, defined as follows.

DEFINITION 1.4.1. The system ACA′ is the system ACA_0 together with $(\forall n)(\forall x \subseteq \omega)$(the n-th Turing jump of x exists). This is logically equivalent to RCA_0 + $(\forall n)(\forall x \subseteq \omega)$(the n-th Turing jump of x exists).

It is well known that ACA′ is a fragment of the system ACA, which is ACA_0 together with full induction. See [Si99] for a discussion of ACA_0 and other subsystems of second order arithmetic, including RCA_0 (used throughout this book).

We originally introduced ACA′ around the time we set up Reverse Mathematics (but after we introduced $RCA_0, ACA_0, WKL_0, ATR_0, \Pi^1_1\text{-}CA_0$), in order to analyze the usual infinite Ramsey theorem. We straightforwardly adapted part of the recursion theoretic treatment due to Carl Jockusch of Ramsey theorem to show that RT is provably equivalent to ACA′ over RCA_0.

It must be mentioned that the metamathematical status of the infinite Ramsey theorem for exponent 2 is not known, although there has been considerable progress on this. See [CJS01].

The main metamathematical open questions concerning the Thin Set Theorem and the Free Set Theorem are these. Do they imply ACA_0 over RCA_0 for fixed exponents? Do they imply Ramsey's theorem (when stated for arbitrary exponents)? By the previous remarks, these questions are equivalent to the following. For fixed exponents, are they equivalent to ACA_0 over RCA_0? Are they equivalent to ACA′ over RCA_0 (or over ACA_0)? It is possible that the Free Set Theorem is stronger than the Thin Set Theorem over RCA_0.

We now present a proof of our Thin Set Theorem privately communicated to us by Jeff Remmel, that does not pass through the Free Set Theorem.

DEFINITION 1.4.2. Let $f:N^k \to N$. We define ot(k) to be the number of order types of k tuples from N.

We now define a coloring of the k-tuples x from N according to the value f(x). Specifically, the color f(x) is assigned to x if $f(x) \in [1,ot(k)]$, and the color 0 is assigned to x otherwise.

By the usual infinite Ramsey theorem for k tuples, we obtain $A \in INF$ such that for all $m \in [0,ot(k)]$,

$$(\forall x,y \in A^k)(\text{if } x,y \text{ have the same order type then } f(x) = m \leftrightarrow f(y) = m).$$

It is clear that the $x \in A^k$ of any given order type can only map to at most one element of [0,ot(k)]. Hence $rng(f|A^k) \cap$ [0,ot(k)] has at most ot(k) elements. Therefore $rng(f|A^k)$ omits at least one element of [0,ot(k)].

From this proof, we can conclude the following strong form of the Thin Set Theorem.

THIN SET THEOREM ([0,ot(k)]). For all $f:N^k \to [0,ot(k)]$ there exists infinite $A \subseteq N$ such that $fA \neq [0,ot(k)]$.

The function ot(k) has been well studied in the literature. Let ot(k) be the number of order types of elements of N^k. It is obvious that $ot(k) \leq k^k$ (every element on N^k has the same order type as an element of $[k]^k$), and a straightforward inductive argument shows that $ot(k) \leq 2k(k!)$. In [Gr62] it is shown that ot(k) is asymptotic to $(k!/2) \ln^{k+1}2$.

The metamathematical status of this form of the Thin Set Theorem can be easily determined as follows.

THEOREM 1.4.1. Thin Set Theorem ([0,ot(k)]), for fixed exponents, or for exponent 3, is provably equivalent to ACA_0 over RCA_0. Thin Set Theorem ([0,ot(k)]) is provably equivalent to ACA' over RCA_0. RCA_0 refutes Thin Set Theorem ([1,ot(k)]) in every exponent k.

Proof: Evidently, Thin Set Theorem ([0,ot(k)]) for fixed exponent k is provable in ACA_0. For general exponents k (as a free variable), it is provable from the infinite Ramsey theorem, and therefore in ACA'.

We now argue in RCA_0. Let $k \geq 2$ (as a free variable). Assume the Thin Set theorem ([0,ot(k)]). We derive the infinite Ramsey theorem for exponent k and $ot(k) \geq 2$ colors, as follows. Let $f:[N]^k \to \{0,1\}$, where $[A]^k$ is the set of all subsets of A of cardinality k. Let $\alpha_1,\ldots,\alpha_{ot(k)}$ be an enumeration of all of the order types of k-tuples from N, where α_1 is the order type of 1,2,...,k. We now define $g:N^k \to [0,ot(k)]$ as follows.

case 1. $x_1 < \ldots < x_k$. Set $g(x_1,\ldots,x_k) = f(\{x_1,\ldots,x_k\})$.

case 2. Otherwise. Let the order type of $x_1,\ldots,x_k$ be α_i, and set $g(x_1,\ldots,x_k) = i \geq 2$.

Let $A \subseteq N$ be infinite, where gA does not contain [0,ot(k)]. Clearly gA contains [2,ot(k)]. Since gA does not contain both 0,1, we see that f is constant on $[A]^k$.

If we fix k = 3 then we obtain the infinite Ramsey theorem for exponent 3 with 2 colors, and hence ACA_0, over RCA_0.

If we use k as a free variable, then we obtain the infinite Ramsey theorem, and hence ACA', over RCA_0.

For the final claim, use $f:N^k \to [1,ot(k)]$ by $f(x_1,...,x_k) = i$, where the order type of $(x_1,...,x_k)$ is the i-th order type of elements of N^k. QED

What if we use another, simpler, function of k?

THIN SET THEOREM ($[1,k^k]$). For all $f:N^k \to [1,k^k]$ there exists infinite $A \subseteq N$ such that $fA \neq [0,k^k]$.

We do not know the status of THIN SET THEOREM ($[1,k^k]$). It obviously follows from THIN SET THEOREM ([1,ot(k)]), exponent by exponent.

From the point of view of the partition calculus, it is more natural to use $[N]^k$ instead of N^k. Here $[N]^k$ is the set of all subsets of N of cardinality k. The square bracket partition relation

$$\omega \to [\omega]^k_\omega$$

can be stated as follows. Let $[A]^k$ be the set of all subsets of A of cardinality k.

THIN SET THEOREM (unordered tuples). For all $f:[N]^k \to N$ there exists infinite $A \subseteq N$ such that $f[[A]^k] \neq N$.

THEOREM 1.4.2. The Thin Set Theorem and the Thin Set Theorem (unordered tuples) are provably equivalent in RCA_0.

Proof: The forward direction is obvious. Now assume the Thin Set Theorem (unordered tuples). Let $f:N^k \to N$, $k \geq 1$. We will prove the existence of an infinite $A \subseteq N$ such that $fA \neq N$.

We can assume that Ramsey's theorem for two colors fails (arbitrary exponents), since otherwise we conclude the Thin Set Theorem. Let $g:[N]^r \to \{0,1\}$ be a counterexample to Ramsey's theorem. We construct a function $h:[N]^{k+r\cdot ot(k)} \to N$

such that for all infinite $A \subseteq N$, $fA \subseteq h[[A]^{k+r\bullet ot(k)}]$. So if $h[[A]^{k+r\bullet ot(k)}] \neq N$ then $fA \neq N$.

Define $h:[N]^{k+r\bullet ot(k)} \to N$ as follows. Let $x_1 < \ldots x_k < y_1 < \ldots y_{r\bullet ot(k)}$ be given. Apply g to the ot(k) successive blocks of length r in $y_1,\ldots,y_{r\bullet ot(k)}$ to obtain ot(k) bits. Let t be the position of the first one of these bits that is 0. If they are all 1's, then set t = 1. Clearly $1 \leq t \leq ot(k)$. Let α be the t-th order type of length k, in some prearranged listing of order types of elements of N^k. Let $y \in \{x_1,\ldots,x_k\}^k$ be minimum (have minimum max) of order type α. Set $h(\{x_1,\ldots,x_k,y_1,\ldots,y_{r\bullet ot(k)}\}) = f(y)$. By the Thin Set Theorem (unordered tuples), let $A \in INF$ be such that $h[[A]^{k+r\bullet ot(k)}] \neq N$. Since g is a counterexample to Ramsey's theorem, all ot(k) length bit sequences appear in the construction of hA. Hence all length k order types are used. Therefore $fA \subseteq h[[A]^{k+r\bullet ot(k)}] \neq N$. QED

We now discuss some other kinds of strengthenings of the Thin Set Theorem. Let $W \subseteq POW(N)$.

THIN SET PROPERTY FOR W. For all $f \in MF$ there exists $A \in W$ such that $fA \neq N$.

DEFINITION 1.4.3. The upper density of $A \subseteq N$ is given by

$$\limsup_{n\to\infty}|A \cap [0,n)|/n.$$

DEFINITION 1.4.4. The upper logarithmic density of $A \subseteq N$ is given by

$$\limsup_{n\to\infty}\log|A \cap [0,n)|/n.$$

THEOREM 1.4.3. The Thin Set Property fails for positive upper density. In fact, it fails for arity 3.

Proof: Let $f:N^3 \to N$ be defined by

$$f(a,b,c) = (c-a)/(b-a) - 2 \text{ if this lies in } N; \quad 0 \text{ otherwise.}$$

Let $A \subseteq N$ have positive upper density. Szemeredi's theorem, [Gow01], asserts that every set of positive upper density contains arbitrarily long arithmetic progressions. Let $p \geq 2$ and $a,a+b,\ldots,a+pb$ be an arithmetic progression in A of length p+1, where $a \geq 0$ and $b \geq 1$. Then $f(a,a+b,a+pb) = (pb)/b - 2 = p-2$. Hence $fA = N$. QED

We do not know if Theorem 1.4.3 can be improved to arity 2, and we do not know if the Thin Set Property holds for upper logarithmic density. We do not know any interesting necessary or sufficient conditions on W so that the Thin Set Property holds for W.

DEFINITION 1.4.5. Let κ be an infinite cardinal. The Thin Set Property for κ asserts the following. For all $f:\kappa^n \to \kappa$, there exists $A \subseteq \kappa$ of cardinality κ such that $fA \neq \kappa$.

THEOREM 1.4.4. [To87], Theorem 5.2. The Thin Set Property fails for the successor of any regular cardinal. In fact, it fails even for unordered 2-tuples. In particular, it fails for unordered 2-tuples in the case of ω_1.

The Thin Set Property is well known to hold of all weakly compact cardinals, since it follows from $\kappa \to \kappa^n{}_m$. In fact, the Thin Set Property holds for weakly compact cardinals in the strong [0,ot(k)] form. For more on the Thin Set Property, see [BM90], Theorem 4.12, and [EHMR84], Theorem 54.1. Also see [Sh95].

The Thin Set Theorem makes perfectly good sense in any BRT setting (V,K). It simply asserts that for all $f \in V$, there exists $A \in K$, such that $fA \neq U$. Here U is the universal set associated with the BRT setting (V,K), as defined in section 1.1.

We now explore the Thin Set Theorem on some BRT settings in real analysis. There have no intention of exhausting anything like a fully representative sample of all interesting BRT settings in real analysis. We only present a very limited sample.

We will see that the Thin Set Theorem, which is the simplest nontrivial statement in all of BRT, depends very much on the choice of BRT setting. We expect that the same is true for a huge variety of statements in BRT, in a rather deep way.

We first consider only unary functions from $\Re$ to $\Re$. It is natural to extend the investigation to incorporate families of functions whose domains are of various kinds (open, semialgebraic, etc.). This is beyond the scope of this book.

We now restrict attention to 8 families of functions from $\Re$ into $\Re$, and 9 families of subsets of $\Re$.

FCN(ℜ,ℜ). All functions from ℜ to ℜ.
BFCN(ℜ,ℜ). All Borel functions from ℜ to ℜ.
CFCN(ℜ,ℜ). All continuous functions from ℜ to ℜ.
C^1FCN(ℜ,ℜ). All C^1 functions from ℜ to ℜ.
C^∞FCN(ℜ,ℜ). All C^∞ functions from ℜ to ℜ.
RAFCN(ℜ,ℜ). All real analytic functions from ℜ to ℜ.
SAFCN(ℜ,ℜ). All semialgebraic functions from ℜ to ℜ.
CSAFCN(ℜ,ℜ). All continuous semialgebraic functions from ℜ to ℜ.

cSUB(ℜ). All subsets of ℜ of cardinality c.
UNCLSUB(ℜ). All uncountable closed subsets of ℜ.
NOPSUB(ℜ). All nonempty open subsets of ℜ.
UNOPSUB(ℜ). All unbounded open subsets of ℜ.
DEOPSUB(ℜ). All open dense subsets of ℜ.
FMOPESUB(ℜ). All open subsets of ℜ of full measure.
CCOPSUB(ℜ). All open subsets of ℜ whose complement is countable.
FCSUB(ℜ). All subsets of ℜ whose complement is finite.
≤1CSUB(ℜ). All subsets of ℜ whose complement has at most one element.

These two lists alone provide 8•9 = 72 BRT settings. We conjecture that there are substantial BRT differences between these 72, except that perhaps C^1FCN(ℜ,ℜ) and C^∞FCN(ℜ,ℜ) have the same BRT behavior. We won't venture an opinion on that.

Note that here we only focus on just one statement of IBRT in one function and one set: the Thin Set Theorem.

THEOREM 1.4.5. The Thin Set Theorem holds on (FCN(ℜ,ℜ),cSUB(ℜ)), (BFCN(ℜ,ℜ),UNCLSUB(ℜ)), (CFCN(ℜ,ℜ),FMOPSUB(ℜ)), (C^1FCN(ℜ,ℜ),CCOPSUB(ℜ)), (SAFCN(ℜ,ℜ),FCSUB(ℜ)), (CSAFCN(ℜ,ℜ),≤1CSUB(ℜ)).

Proof: Let f:ℜ → ℜ. We can assume that rng(f) = ℜ. Let A = f^{-1}[0,1]. Then A has cardinality c and fA = [0,1] ≠ ℜ.

Let f:ℜ → ℜ be Borel. According to [Ke94], exercise 19.8, there exists a nowhere dense perfect set P ⊆ ℜ such that f is either 1-1 continuous on P, or f is constant on P. In either case, fP is nowhere dense, and so fP ≠ ℜ. See Theorem 1.4.7 for the sharper multivariate form of this result.

Let $f:\Re \to \Re$ be continuous. Then there exists $x \in \Re$ such that $f^{-1}(x)$ is a closed set of measure 0. Let $A = \Re\backslash f^{-1}(x)$. Then A is an open subset of $\Re$ of full measure, and $fA \neq \Re$.

Let $f:\Re \to \Re$ be C^1. By Sard's theorem, $S = \{f(x): f'(x) = 0\}$ has measure zero. Suppose $f^{-1}(x)$ is uncountable. Then $f^{-1}(x)$ contains a limit u, where obviously $f'(u) = 0$. Hence $f(u) \in S$, and so $x \in S$. Thus $\{x: f^{-1}(x)$ is uncountable$\} \subseteq S$. Since S has measure zero, let x be such that $f^{-1}(x)$ is countable. Then $\Re\backslash f^{-1}(x)$ is an open subset A of $\Re$ whose complement is countable, and $fA \neq \Re$. (The use of Sard's theorem here was suggested to the author by Gerald Edgar.)

Let $f:\Re \to \Re$ be semialgebraic. Every $f^{-1}(x)$ is finite or contains a nonempty open interval. Hence some $f^{-1}(x)$ is finite. Let $A = \Re\backslash f^{-1}(x)$. Then A is a subset of $\Re$ whose complement is finite, and $fA \neq \Re$.

Let $f:\Re \to \Re$ be continuous and semialgebraic. We can assume that $rng(f) = \Re$. Hence there exists $x > 0$ such that

$f:[x,\infty) \to [f(x),\infty)$ is strictly increasing and onto, and $f:(-\infty,-x] \to (-\infty,f(-x)]$ is strictly increasing and onto; or

$f:[x,\infty) \to (-\infty,f(x)]$ is strictly decreasing and onto, and $f:(-\infty,-x] \to [f(-x),\infty)$ is strictly decreasing and onto.

This can be proved using the well known structural properties of semialgebraic $f:\Re \to \Re$ as treated in [Dr98], Chapter 1.
In the first case, choose $y > \max(f[(-\infty,x]])$, so that the value y is attained only on $[x,\infty)$, in which case $f^{-1}(y)$ has exactly one element. In the second case, choose $y < \min(f[(-\infty,x]])$, so that the value y is also attained only on $[x,\infty)$, in which case $f^{-1}(y)$ has exactly one element. In both cases, we can find y by the continuity of f. Let $A = \Re\backslash f^{-1}(y)$. Then A is a subset of $\Re$ whose complement has cardinality 1, where $fA \neq \Re$. QED

THEOREM 1.4.6. The Thin Set Theorem fails on (FCN($\Re,\Re$),UNCLSUB($\Re$)), (BFCN($\Re,\Re$),NOPSUB($\Re$)), (CFCN($\Re,\Re$),CCOPSUB($\Re$)), (RAFCN($\Re,\Re$),FCSUB($\Re$)), (SAFCN($\Re,\Re$),≤1CSUB($\Re$)).

Proof: We first construct a function α which maps every uncountable closed subset of $\Re$ to a subset of cardinality c, such that $A \neq B \to \alpha(A) \cap \alpha(B) = \emptyset$. This is done by a transfinite construction of length c. We use an enumeration of the uncountable closed subsets of $\mathfrak{R}$ of length c.

At any stage, we have a function β which maps every uncountable closed subsets of $\mathfrak{R}$ to a subset of cardinality < c, where < c uncountable closed subsets are assigned a nonempty subset. At the next stage, we can add one more point to each of the nonempty subsets thus far, and assign a subset of cardinality 1 to the first uncountable closed subset of $\mathfrak{R}$ that was previously assigned $\emptyset$. Since uncountable closed subsets of $\mathfrak{R}$ are of cardinality c, there is no problem making sure that the sets assigned are pairwise disjoint.

For each uncountable closed A, map $\alpha(A) \subseteq A$ onto $\mathfrak{R}$. By the disjointness of the $\alpha(A)$, we can take the union of these functions, and then extend this union arbitrary to $f:\mathfrak{R} \to \mathfrak{R}$. Clearly for all uncountable closed A, we have $fA = \mathfrak{R}$. This establishes the first claim.

It is well known that there exists a continuous $f:\mathfrak{R} \to \mathfrak{R}$ such that each $f^{-1}(x)$ is uncountable. E.g., start with a continuous $g:K \to K$ such that each $f^{-1}(x)$, $x \in K$, is uncountable, where K is the Cantor set. (Take g(x) to be the real number whose base 3 expansion is digits number 1,3,5,7,... in the base 3 expansion of x). Compose with a continuous map from K onto [0,1] to obtain a continuous $h:K \to [0,1]$ such that each $h^{-1}(x)$, $x \in [0,1]$, is uncountable. Then extend to a continuous $J:[0,1] \to [0,1]$ with this property. Then paste copies of the functions J+n, $n \in Z$, together with some filler, to obtain $f:\mathfrak{R} \to \mathfrak{R}$ such that each $f^{-1}(x)$ is uncountable. Let $A \subseteq \mathfrak{R}$ have countable complement. Then A must meet each $f^{-1}(x)$. Hence $fA = \mathfrak{R}$.

It is obvious that there exists real analytic $f:\mathfrak{R} \to \mathfrak{R}$ such that each $f^{-1}(x)$ is infinite - e.g., xsin(x). Let $A \subseteq \mathfrak{R}$ have finite complement. Then A must meet each $f^{-1}(x)$. Hence $fA = \mathfrak{R}$.

It is obvious that there are semialgebraic $f:\mathfrak{R} \to \mathfrak{R}$ such that each $f^{-1}(x)$ has at least 2 elements. Let $A \subseteq \mathfrak{R}$ omit at most one real number. Then A must meet each $f^{-1}(x)$. Hence $fA = \mathfrak{R}$.

It remains to treat (BFCN($\mathfrak{R}$,$\mathfrak{R}$),NOPSUB($\mathfrak{R}$)). We define $f:[0,1] \to [0,1]$ and $g:[0,1] \to Z$ as follows. Let $x \in [0,1]$ and let $b_1,b_2,...$ be the base 2 expansion of x. Let x* be greatest $m \geq 1$ such that $b_1,b_2,...,b_m$ =

$b\_8^m+1, b\_8^m+3, \ldots, b\_8^m+2m-1$. If m does not exist, set f(x) = 0. If m exists, set f(x) to be the real number $b_{4m}, b_{4m+4}, b_{4m+8}, \ldots$. Set |g(x)| to be the least i ≥ 0 such that $b_{4m+4i+6} = 0$ if it exists; 0 otherwise. Choose the sign of g(x) according to the bit b_{4m+2}.

We claim that for all nonempty open A ⊆ [0,1] and y ∈ [0,1] and k ∈ Z, there exists x ∈ A such that f(x) = y and g(x) = k.

To see this, let A,y,k be as given. Let (p,q) ⊆ A be nondegenerate, where p,q are dyadic rationals, 0 ≤ p < q ≤ 1. Let $b_1, \ldots, b_n, 0,0,0, \ldots$ be the base 2 expansion of p and $c_1, \ldots, c_n, 0,0,0, \ldots$ be the base 2 expansion of q. By continuing the base 2 expansion $b_1, \ldots, b_n$, we can arrange that x* = m exists, m > n, without committing ourselves to any of the base 2 digits beyond b_n in even positions. We then arrange $b_{4m}, b_{4m+4}, b_{4m+8}, \ldots$ to be a binary expansion of y. We have thus arranged f(x) = y. We can also arrange g(x) = k.

Finally, we define h:ℜ → ℜ by h(x) = f(x-⌊x⌋)+g(x-⌊x⌋). Here ⌊x⌋ is the floor of x, which is the greatest integer ≤ x.

Now let A ⊆ ℜ be a nonempty open subset of ℜ and y ∈ ℜ. Let (p,q) + k be an open interval contained in A, where 0 < p < q < 1. We can find x ∈ (p,q) such that f(x) = y−⌊y⌋ and g(x) = ⌊y⌋. Then h(x+⌊y⌋) = f(x)+g(x) = y as required. QED

Note that in the above development, we have not come across a distinction between C^1FCN(ℜ,ℜ), C^∞FCN(ℜ,ℜ), and RAFCN(ℜ,ℜ). We suspect that important distinctions will arise as we go deeper into BRT.

We now consider the corresponding 8 families of multivariate functions from ℜ to ℜ. I.e., functions whose domain is some $ℜ^n$ and whose range is a subset of ℜ. We use the same 9 families of subsets of ℜ.

FCN(ℜ*,ℜ). All multivariate functions from ℜ to ℜ.
BFCN(ℜ*,ℜ). All multivariate Borel functions from ℜ to ℜ.
CFCN(ℜ*,ℜ). All multivariate continuous functions from ℜ to ℜ.
C^1FCN(ℜ*,ℜ). All multivariate C^1 functions from ℜ to ℜ.
C^∞FCN(ℜ*,ℜ). All multivariate C^∞ functions from ℜ to ℜ.
RAFCN(ℜ*,ℜ). All multivariate real analytic functions from ℜ to ℜ.

SAFCN($\Re^*,\Re$). All multivariate semialgebraic functions from $\Re$ to $\Re$.
CSAFCN($\Re^*,\Re$). All multivariate continuous semialgebraic functions from $\Re$ to $\Re$.

Here the domains of all functions considered are Cartesian powers of $\Re$, and the ranges are all subsets of $\Re$.

THEOREM 1.4.7. The Thin Set Theorem holds on (BFCN($\Re^*,\Re$),UNCLSUB($\Re$)), (CFCN($\Re^*,\Re$),NOPSUB($\Re$)). If c is a real valued measurable cardinal then the Thin Set Theorem holds on (FCN($\Re^*,\Re$),cSUB($\Re$)). If κ is a weakly compact cardinal internal to a countable transitive model M of ZFC, and we force over M with finite partial functions from κ into {0,1} under inclusion, then the Thin Set Theorem holds on (FCN($\Re^*,\Re$),cSUB($\Re$)) in the generic extension.

Proof: We start with the first claim. It is convenient to prove a somewhat stronger result: that the Thin Set Theorem holds on BFCN($\Re^*,\Re$) with the uncountable closed subsets of $\Re$ that are unbounded.

We will rely on the well known adaptation of forcing technology for such applications. Let K be the usual Cantor space $\{0,1\}^N$. We first show the following.

#) Let $\alpha_0,\alpha_1,\ldots$ be Borel functions from K^n into K. There exists a perfect $K' \subseteq K$ such that each $\alpha_i[K'^{n\neq}]$ is nowhere dense in K, where $K'^{n\neq}$ is the set of all n-tuples of distinct elements of K'.

We fix a countable admissible set X containing a sequence of codes for the Borel functions $\alpha_0,\alpha_1,\ldots$. We will freely use forcing over X.

We write $\{0,1\}^{<N} = \cup\{\{0,1\}^i: i \geq 0\}$. Here $\{0,1\}^i$ is the set of functions from i into {0,1}, where i = {0,...,i-1}.

We use $(f_1,\ldots,f_n)$ as the name of an undetermined generic element of K^n. The statements we will force are of the form

$$\alpha_i(f_1,\ldots,f_n)(k) = j,$$

where $i,k \geq 0$ and $j \in \{0,1\}$. Forcing will be defined as usual over X for conditions $p = (x_1,\ldots,x_n) \in (\{0,1\}^{<N})^n$. The notion of generic $(g_1,\ldots,g_n) \in K^n$ is defined as usual using dense sets of conditions lying in X.

A 1-condition is an element of $\{0,1\}^{<N}$. The conditions are of course n-tuples of 1-conditions.

We will now build a perfect finite sequence tree T of conditions. The root is the empty sequence of conditions. The vertices will have the form $<p_1,...,p_b>$, $p \geq 0$, where $p_1 \subseteq ... \subseteq p_b$ are 1-conditions. Here b is the length of the vertex.

At every level i in T, the 2^i vertices will all have a common structure in that they will all have the form $<p_1,...,p_i>$, and any two of them, $<p_1,...,p_i> \neq <p_1',...,p_i'>$, will have

$$lth(p_1) = lth(p_1').$$
$$...$$
$$lth(p_i) = lth(p_i').$$
$$p_i \neq p_i'.$$

Here $p_1,...,p_i$ are 1-conditions with $p_1 \subseteq ... \subseteq p_i$.

Let $D_1,D_2,...$ be an enumeration of the dense sets of conditions lying in X, which are closed upward. Let $w_1,...,w_n$ be the last terms of n distinct vertices at level i of T. These w's are 1-conditions. We require that the condition $(w_1,...,w_n)$ lie in $D_1 \cap ... \cap D_i$. This will guarantee that any sequence of n distinct infinite paths through T will be a generic element of K^n (when flattened out in the obvious way).

Suppose we have constructed the i-th level of T, $i \geq 0$. We now show how to construct the i+1-st level of T. Let $w_1,...,w_{2^i}$ be the last terms of the vertices of T at the i-th level. Recall that the w's are distinct 1-conditions of the same lengths.

Let $i' >> i$. Before doing any splitting, first extend the w's to $w_1^*,...,w_{2^i}^*$ so that every sequence of distinct elements $u_1,...,u_n$ of $\{w_1^*,...,w_{2^i}^*\}$ decides all forcing statements

$$\alpha_s(f_1,...,f_n)(t) = 0,\ 0 \leq s,t < i'.$$

This will ensure that for all $s \geq 1$, the number of possible first i' bits of values of α_s, at the n-tuples of distinct infinite paths through T, will be smaller than, say, the square root of $2^{i'}$. This will guarantee the desired nowhere density of the set of all values of α_s, at the n-tuples of distinct infinite paths through T.

There is no problem meeting the earlier requirements by further extensions and by 2 splitting. This establishes #). We now sharpen #).

##) Let $\alpha_0,\alpha_1,...$ be Borel functions from K^n into K. There exists a perfect $K' \subseteq K$ such that each $\alpha_i K'$ is nowhere dense in K. In particular, $\cup\{\alpha_i K': i \geq 0\} \neq K$.

Let the α's be as given. For each $i \geq 0$ and $1 \leq j_1,...,j_n \leq n$, put the function

$$\beta(x_1,...,x_n) = \alpha_i(x_{j1},...,x_{jn})$$

in a new list, and apply #) to these β's. Let K' be given by #). Then each $\alpha_i K'$ is a finite union of the various $\beta[K'^{n\neq}]$, and is therefore nowhere dense in K.

The final part of ##) is by the Baire category theorem for K.

Now let $f:\mathfrak{R}^n \rightarrow \mathfrak{R}$ be Borel. We now think of $K \subseteq \mathfrak{R}$ by viewing each element of K as a base 3 expansion with only 0's and 2's. Let $h:\mathfrak{R} \rightarrow K$ be a Borel bijection.

For all $\delta \in N^n$, let $g_\delta:K^n \rightarrow K$ be defined by

$$g_\delta(x) = h(f(x+\delta)).$$

By ##), let $K' \subseteq K$ be a perfect set such that $\cup\{g_\delta K': \delta \in N^n\} \neq K$. We claim that

$$A = \cup\{K'+i: i \geq 0\} \subseteq \mathfrak{R}$$

is uncountable, closed, and unbounded.

$$fA \neq \mathfrak{R}.$$

Since $K' \subseteq [0,1]$ is uncountable and closed, clearly, A is uncountable, closed, and unbounded.

Let $u \in K\backslash\cup\{g_\delta K': \delta \in N^n\}$. Then for all $\delta \in N^n$, $u \notin g_\delta K'$. Hence for all $\delta \in N^n$ and $x \in K'$, $u \neq g_\delta x = h(f(x+\delta))$. Clearly, for all $\delta \in N^n$ and $x \in K'$, $h^{-1}u \neq f(x+\delta)$. Hence for all $i \geq 0$, $h^{-1}u \notin f(K+i)$. Hence $h^{-1}u \notin fA$.

For the second claim of the Theorem, let $f:\Re^k \to \Re$ be continuous. Then $f([0,1]) = f([0,1]^k)$ is compact, and therefore not $\Re$.

The real valued measurable claim is proved in [So71], Lemma 14, page 406.

For the final claim, let M be a countable transitive model of ZFC with the internal weakly compact cardinal κ. We force to create a generic set $a \subseteq \kappa$ using finite conditions. It is convenient to write this generic set as mutually generic subsets of ω, $\{a_\alpha \subseteq \omega: \alpha < \kappa\}$.

Fix a generic extension $M^* = M[\{a_\alpha \subseteq \omega: \alpha < \kappa\}]$ using this notion of forcing. It suffices to show that in M*, for every $f:\wp(\omega)^n \to \wp(\omega)$ there exists $A \subseteq \wp(\omega)$ of cardinality κ such that $fA \neq \wp(\omega)$.

Let τ be a forcing term representing f in M*. Let p force $\tau:\wp(\omega)^n \to \wp(\omega)$, where the condition p is compatible with the generic object.

Since κ is a weakly compact cardinal in M, κ is strongly inaccessible, and $\kappa \to \kappa^n{}_\omega$ in M. Let σ be one of the finitely many possible order types of tuples $(\alpha_1,\ldots,\alpha_n,\gamma)$ with $\gamma \neq \alpha_1,\ldots,\alpha_n$. Let $E \in M$, $E \subseteq \kappa$, E unbounded, be such that

for all $\alpha_1,\ldots,\alpha_n,\gamma < \kappa$, $(\alpha_1,\ldots,\alpha_n,\gamma)$ of type σ, $\tau(a_{\alpha 1},\ldots,a_{\alpha n}) = a_\gamma$ is not forced by any extension of p; or

for all $\alpha_1,\ldots,\alpha_n\ \gamma < \kappa$, $(\alpha_1,\ldots,\alpha_n,\gamma)$ of type σ, $\tau(a_{\alpha 1},\ldots,a_{\alpha n}) = a_\gamma$ is forced by some extension of p.

Suppose that the latter holds. Let $\alpha_1,\ldots,\alpha_n,\gamma$ be of type σ, where there are uncountably many γ' such that $(\alpha_1,\ldots,\alpha_n,\gamma')$ has type σ. Then the corresponding extensions of p must be incompatible. This violates the fact that this notion of forcing has the countable chain condition in M.

Hence we have

for all $\alpha_1,\ldots,\alpha_n,\gamma < \kappa$, $(\alpha_1,\ldots,\alpha_n,\gamma)$ of type σ, $\tau(a_{\alpha 1},\ldots,a_{\alpha n}) = a_\gamma$ is not forced by any extension of p

assuming that σ is an order type with last term different than all earlier terms. Hence for all $\alpha_1,\ldots,\alpha_n,\gamma < \kappa$, if $\gamma \neq \alpha_1,\ldots,\alpha_n$ then $\tau(a_{\alpha\_1},\ldots,a_{\alpha\_n}) = a_\gamma$ is not forced by any extension of p.

In M*,

for all $\alpha_1,\ldots,\alpha_n < \kappa$, $f(a_{\alpha\_1},\ldots,a_{\alpha\_n}) \neq a_{\alpha\_1},\ldots,a_{\alpha\_n} \rightarrow (\forall\gamma \neq \alpha_1,\ldots,\alpha_n)(f(a_{\alpha\_1},\ldots,a_{\alpha\_n}) \neq a_\gamma)$.

Let $A = \{a_\alpha: \alpha \in E\}$. Then in M*, $|A| = \kappa$, and

for all $x_1,\ldots,x_n < \kappa$, $f(x_1,\ldots x_n) \neq x_1,\ldots,x_n \rightarrow f(x_1,\ldots,x_n) \notin A$.

Clearly $\min(A) \notin f(A\backslash\{\min(A)\})$. QED

THEOREM 1.4.8. The Thin Set Theorem fails on $(SAFCN(\Re^3,\Re),NOPSUB(\Re))$, $(CSAFCN(\Re^3,\Re),UNOPSUB(\Re))$. If the continuum hypothesis holds then the Thin Set Theorem fails on $(FCN(\Re^2,\Re),cSUB(\Re))$.

Proof: Let $f:\Re^3 \rightarrow \Re$ be given by $f(x,y,z) = 1/(x-y) + 1/(x-z)$ if defined; 0 otherwise. Then f is semialgebraic. Let $a,b \in \Re$, $a < b$. We claim that $f[(a,b)] = \Re$. To see this, let $u \in \Re$. Fix $x \in (a,b)$. We can find $y,z \in (a,b)$ such that $1/(x-y)$ and $1/(x-z)$ are any two reals with sufficiently large absolute values. Hence we can find $y,z \in (a,b)$ such that $f(x,y,z) = u$.

Let $f:\Re^3 \rightarrow \Re$ be given by $x(y-z)$. Then f is continuous and semialgebraic. Let A be an unbounded open subset of $\Re$. We claim that $fS = \Re$. To see this, let $u \in \Re$. Let $(a,b) \subseteq A$, where $a < b$. Choose $z \in A$ such that $|z| > |u/(b-a)|$. Then $|u/z| < b-a$. Let $x,y \in (a,b)$, where $x-y = u/z$. Then $f(x,y,z) = u$.

The final claim is by Theorem 1.4.4. QED

Note that the counterexamples above are in 3 dimensions.

THEOREM 1.4.9. The Thin Set Theorem holds on $(SAFCN(\Re^2,\Re),UNOPSUB(\Re))$. The Thin Set Theorem fails on $(CSAFCN(\Re^2,\Re),DEOPSUB(\Re))$ and $(RAFCN(\Re^2,\Re),UNOPSUB(\Re))$.

Proof: Let $E \subseteq \Re^2$ be semialgebraic. We say that $A \subseteq \Re^2$ is small if and only if $(\forall x >> 0)(\forall y >> x)((x,y) \notin A)$. We claim that for any disjoint semialgebraic $A,B \subseteq \Re^2$, A is small or B is small.

To see this, let A,B $\subseteq \Re^2$ be pairwise disjoint semiaglebraic sets, where A,B are not small. Then

$$\neg(\forall x >> 0)(\forall y >> x)((x,y) \notin A).$$
$$\neg(\forall x >> 0)(\forall y >> x)((x,y) \notin B).$$

By the o-minimality of the field of real numbers,

$$(\forall x >> 0)\neg(\forall y >> x)((x,y) \notin A).$$
$$(\forall x >> 0)\neg(\forall y >> x)((x,y) \notin B).$$

Again by o-minimality,

$$(\forall x >> 0)(\forall y >> x)((x,y) \in A).$$
$$(\forall x >> 0)(\forall y >> x)((x,y) \in B).$$

This violates $A \cap B = \emptyset$.

For $A \subseteq \Re^2$, let $rev(A) = \{(x,y): (y,x) \in A\}$.

We now claim that for any three pairwise disjoint semialgebraic A,B,C $\subseteq \Re^2$,

A and rev(A) is small; or
B and rev(B) is small; or
C and rev(C) is small.

To see this, by the previous claim, among every pair of sets drawn from A,B,C, at least one is small. Hence at least two among A,B,C are small. By symmetry, assume A,B are small. Note that rev(A),rev(B) are disjoint and semialgebraic. Hence rev(A) is small or rev(B) is small. This establishes the claim.

For the first claim of the Theorem, let $f:\Re^2 \rightarrow \Re$ be semialgebraic. Consider $f^{-1}(0),f^{-1}(1),\ldots$. These sets are semialgebraic and pairwise disjoint. By the above, we see that there exist infinitely many i such that $f^{-1}(i)$ and $rev(f^{-1}(i))$ are small.

Also note that for all $i \geq 0$, $f^{-1}(i)$ contains all (x,x), x sufficiently large, or excludes all (x,x), x sufficiently large. Because of mutual disjointness, all but at most one $f^{-1}(i)$ has the property that it excludes all (x,x), x sufficiently large.

It is now clear that we can fix i such that

$$f^{-1}(i) \text{ is small.}$$
$$\mathrm{rev}(f^{-1}(i)) \text{ is small.}$$
$$f^{-1}(i) \text{ excludes } (x,x),\ x \text{ sufficiently large.}$$

Let $B = f^{-1}(i)$. We now construct an unbounded open $A \subseteq \Re$ which is disjoint from B.

We have

$$(\forall x >> 0)(\forall y >> x)$$
$$(x,y) \notin B \wedge (y,x) \notin B \wedge (x,x) \notin B.$$

Fix $b > 0$ such that

$$(\forall x \geq b)(\forall y >> x)$$
$$(x,y) \notin B \wedge (y,x) \notin B \wedge (x,x) \notin B.$$

Let $f:(b,\infty) \to \Re$ be semialgebraic such that

$$1)\ (\forall x \geq b)(\forall y \geq f(x))$$
$$(x,y) \notin B \wedge (y,x) \notin B \wedge (x,x) \notin B \wedge f(x) > x.$$

Then f is eventually strictly increasing. Let f be strictly increasing on $[c,\infty)$, $c > b$.

We now define real numbers $c = c_0 < c_1 < \ldots$ as follows.

Define $c_0 = c$. Suppose $c_0 < \ldots < c_i$ have been defined, $i \geq 0$. Define $c_{i+1} = f(c_i)+1$.

For all $i \geq 0$, let $\varepsilon(i) \in (0,1)$ be so small that $B \cap (c_i,c_i+\varepsilon(i))^2 = \emptyset$. We can find $\varepsilon(i)$ since the ordered pair $(c_i,c_i) \notin B$ and B is closed.

By 1), for all $0 \leq i < j$ and $x \in (c_i,c_i+1)$, $y \in (c_j,c_j+1)$, we have $(x,y) \notin B \wedge (y,x) \notin B \wedge (y,y) \notin B$. Hence B is disjoint from A^2, where $A = (c_0,c_0+\varepsilon(0)) \cup (c_1,c1+\varepsilon(1)) \cup \ldots$ is an unbounded open set.

For the second claim of the Theorem, let A be a dense open subset of $\Re$. It suffices to show that $A-A = \Re$. Let $x \in \Re$ and $[a,b] \subseteq A$, $a < b$. Since A is dense, let $y \in [a+x,b+x]$, $y \in A$. Then $y-x \in [a,b]$, and so $y-x \in A$. Hence $x = y-(y-x)$ demonstrates that $x \in A-A$.

For the final claim of the Theorem, let $f:\Re^2 \to \Re$ be given by $f(x,y) = x \sin(xy)$. Then f is real analytic. Let A be an unbounded open subset of $\Re$ and $z \in \Re$. Let $(a,b) \subseteq A$, $a <$

b. Choose x ∈ A with |x| > |z| so large that (xa,xb) ∪ (xb,xa) contains a closed interval of length 2π. Then as y varies in (a,b), the quantity sin(xy) takes on any value from −1 to 1. Hence as y varies in (a,b), x sin(xy) takes on any value from -|x| to |x|. In particular, it takes on the value z. Therefore fA = ℜ. QED

Note that in the above development, no distinction between BFCN*(ℜ*,ℜ) and SAFCN(ℜ*,ℜ) has arisen. Also no distinction between C^1FCN(ℜ*,ℜ), C^∞FCN(ℜ*,ℜ), RAFCN(ℜ,ℜ), and CSAFCN(ℜ*,ℜ) has arisen. We suspect that important distinctions will arise as BRT is further developed.

We provide a tabular display of the results in Theorems 1.4.5-1.4.9. We first transcribed the information contained there, where + means that the Thin Set Theorem holds, - means that the Thin Set Theorem fails, and ? means that the Thin Set Theorem is independent of ZFC. We then filled in the remaining entries by immediate inference using obvious inclusion relations between the various classes of functions and the various classes of sets.

	cSUB	UNCLSUB	NOPSUB	UNOPSUB	DEOPSUB	FMOPESUB	CCOPSUB	FCSUB	≤1CSUB
FCN(ℜ,ℜ)	+	−	−	−	−	−	−	−	−
BFCN(ℜ,ℜ)	+	+	−	−	−	−	−	−	−
CFCN(ℜ,ℜ)	+	+	+	+	+	+	−	−	−
C^1FCN(ℜ,ℜ)	+	+	+	+	+	+	+	−	−
C^∞FCN(ℜ,ℜ)	+	+	+	+	+	+	+	−	−
RAFCN(ℜ,ℜ)	+	+	+	+	+	+	+	−	−
SAFCN(ℜ,ℜ)	+	+	+	+	+	+	+	+	−
CSAFCN(ℜ,ℜ)	+	+	+	+	+	+	+	+	+
FCN(ℜ*,ℜ)	?	−	−	−	−	−	−	−	−
FCN($\mathfrak{R}^2$,ℜ)	?	−	−	−	−	−	−	−	−
BFCN(ℜ*,ℜ)	+	+	−	−	−	−	−	−	−
CFCN(ℜ*,ℜ)	+	+	+	−	−	−	−	−	−
C^1FCN(ℜ*,ℜ)	+	+	+	−	−	−	−	−	−
C^∞FCN(ℜ*,ℜ)	+	+	+	−	−	−	−	−	−
RAFCN(ℜ*,ℜ)	+	+	+	−	−	−	−	−	−
RAFCN($\mathfrak{R}^2$,ℜ)	+	+	+	−	−	−	−	−	−
SAFCN(ℜ*,ℜ)	+	+	−	−	−	−	−	−	−
SAFCN($\mathfrak{R}^3$,ℜ)	+	+	−	−	−	−	−	−	−
SAFCN($\mathfrak{R}^2$,ℜ)	+	+	+	+	−	−	−	−	−
CSAFCN(ℜ*,ℜ)	+	+	+	−	−	−	−	−	−
CSAFCN($\mathfrak{R}^3$,ℜ)	+	+	+	−	−	−	−	−	−
CSAFCN($\mathfrak{R}^2$,ℜ)	+	+	+	+	−	−	−	−	−

CHAPTER 2
CLASSIFICATIONS

In this Chapter, we treat several significant BRT fragments. For most of these BRT fragments, we show that every statement is either provable or refutable in RCA_0.

For the remainder of these BRT fragments, we show that every statement is either provable in RCA_0, refutable in RCA_0, or provably equivalent to the Thin Set Theorem of section 1.4 over RCA_0.

Thus in this Chapter, we do not run into any independence results from ZFC. In the classification of Chapter 3, we do run into a statement independent of ZFC, called the Principal Exotic Case, which is the focus of the remainder of the book.

In this Chapter, we focus on five BRT settings (see Definition 1.1.11). These fall naturally, in terms of their observed BRT behavior, into three groups (see Definitions 1.1.2, and 2.1):

(SD,INF), (ELG ∩ SD,INF).
(ELG,INF), (EVSD,INF).
(MF,INF).

The inclusion diagram for these five sets of multivariate functions is

ELG ∩ SD
SD ELG
EVSD
MF

Here each item in any row is properly contained in any item in any lower row. Multiple items on any row are incomparable under inclusion.

(SD,INF), (ELG,INF), and (MF,INF) are the most natural of these five BRT settings. The remaining two BRT settings are closely associated, and serve to round out the theory.

MF (multivariate functions), SD (strictly dominating), and INF (infinite) were defined in section 1.1 in connection with the Complementation Theorem and the Thin Set Theorem.

DEFINITION 2.1. Let f ∈ MF. We say that f is of expansive linear growth if and only if there exist rational constants c,d > 1 such that for all but finitely many x ∈ dom(f),

$$c|x| \leq f(x) \leq d|x|$$

where |x| is the maximum coordinate of the tuple x. Let ELG be the set of all f ∈ MF of expansive linear growth.

DEFINITION 2.2. Let f ∈ MF. We say that f is eventually strictly dominating if and only if for all but finitely many x ∈ dom(f), f(x) > |x|. We write EVSD for the set of all f ∈ MF that are eventually strictly dominating.

In this Chapter, the two asymptotic BRT settings (ELG,INF), (EVSD,INF), have the same behavior, whereas the two non asymptotic BRT settings (SD,INF), (ELG ∩ SD,INF), also have the same behavior. In this Chapter, the behavior of (ELG,INF), (EVSD,INF) differs from the behavior of (SD,INF), (ELG ∩ SD,INF). In this Chapter, (MF,INF) behaves differently from the other four settings.

2.1. Methodology.

In this section, we use notation and terminology that was introduced in section 1.1.

Recall the definitions of

BRT fragment. Definition 1.1.18.
BRT environment. Definition 1.1.19.
BRT signature. Definition 1.1.21.
flat BRT fragment. Definition 1.1.34.

In Definition 1.1.39, the flat BRT fragments were divided into these four mutually disjoint categories:

1) EBRT in σ on (V,K), where σ does not end with $\subseteq$.
2) EBRT in σ on (V,K), where σ ends with $\subseteq$.
3) IBRT in σ on (V,K), where σ does not end with $\subseteq$.
4) IBRT in σ on (V,K), where σ ends with $\subseteq$.

Let α be a flat BRT fragment, and let S be an α format; i.e., a set of α elementary inclusions. According to Definition 1.39, we say that S is α correct if and only if

1’) $(\forall g_1,...,g_n \in V)(\exists B_1,...,B_m \in K)(S)$.
2’) $(\forall g_1,...,g_n \in V)(\exists B_1 \subseteq ... \subseteq B_m \in K)(S)$.
3’) $(\exists g_1,...,g_n \in V)(\forall B_1,...,B_m \in K)(S)$.
4’) $(\exists g_1,...,g_n \in V)(\forall B_1 \subseteq ... \subseteq B_m \in K)(S)$.

where we use 1’),2’),3’),4’) according to whether α is in category 1),2),3),4).

For example, the Thin Set Theorem is the negation of a statement of the form 3').

In the case of EBRT and IBRT in A,fA on any given setting, there are 16 formats, and hence 16 statements of forms 1',3', respectively, that have to be considered. This is such a small number that we can profitably list all of these statements, and determine their truth values. We do this in section 2.2.

In the case of EBRT and IBRT on A,fA,fU on any given setting, there are 256 formats, and hence at most 256 statements that have to be considered. Actually, a closer look shows that there are only 6 elementary inclusions, generating only 2^6 = 64 formats. In section 2.3, we list these formats in order of increasing cardinality. This avoids considerable duplication of work. This method of compilation is seen to be perfectly manageable in section 2.3.

In the case of EBRT and IBRT on A,B,fA,fB, there are 2^{16} = 65,536 formats, and hence 65,536 statements that have to be considered. We do not attempt to work with A,B,fA,fB here.

In sections 2.4 - 2.7, we instead work with A,B,fA,fB,$\subseteq$. There are 9 elementary inclusions, and so 2^9 = 512 formats need be considered. This is considerably less than 65,536. Here a treelike methodology is preferable to the enumeration procedure used in section 2.3. We expect the treelike methodology to be the method of choice when analyzing richer BRT fragments.

We treat EBRT in A,B,fA,fB,⊆ on (SD,INF), (ELG,INF) in sections 2.4, 2.5. We treat EBRT in $A_1,...,A_k,fA_1,...,fA_k$,⊆ on (MF,INF) in section 2.6. We treat IBRT in $A_1,...,A_k,fA_1,...,fA_k$,⊆ on (SD,INF), (ELG,INF), (MF,INF) in section 2.7.

The most substantial uses of the treelike methodology are in sections 2.4 and 2.5. We believe that EBRT in A,B,fA,fB on (MF,INF), (SD,INF), (ELG,INF) can be treated using this treelike methodology, but with considerably more effort.

In this section, we rigorously present this treelike methodology and establish some important facts about it.

Fix a flat BRT fragment α. Let S be an α format. Let 1 ≤ i ≤ 4 be such that α is in category i) above. We also fix a true formal system T that includes RCA_0. We assume that α is given a description in T.

According to Definition 1.1.42, we say that S is α,T correct if and only if T proves that S is α correct. We say that S is α,T incorrect if and only if T refutes that S is α correct.

According to Definition 1.43, we say that α is T secure if and only if every α format is α,T correct or α,T incorrect.

The goal of the treelike methodology is

a) to show that α is T secure.
b) to list all maximal α,T correct formats; i.e., α,T correct α formats that are not properly included in any α,T correct α format.

Note the following obvious but crucial property of α,T correct/incorrect α formats:

Every subset of an α,T correct α format is α,T correct.
Every α format that contains an α,T incorrect format is α,T incorrect.

Goal b) is preferable to listing all α,T correct α formats, as the latter may be uncomfortably numerous, or even impractically enormous, whereas the former may be very manageable in size.

The challenge is to show that our treelike methodology does in fact rigorously justify the claim that we have actually established a) and done b). In other words, we need to justify that

i. The α formats listed under b) are indeed α,T correct, and are incomparable under inclusion.
ii. Any α format not included in any of those listed under b) is α,T incorrect.

Some readers may be content with examining the classifications made in sections 2.4, 2.5, and absorbing the methodology from the displays. When the significance of some features are not apparent, the reader can look at the formal treatment of the methodology presented below.

Let α be a flat BRT fragment with BRT setting (V,K). Recall the definition of α formulas (Definition 1.1.25).

DEFINITION 2.1.1. We say that an α formula is α,T valid if and only if, it is provable in T that it holds for all values of the function variables from V and all values of the set variables from K. In case the signature of α ends with $\subseteq$, the values of the set variables, in increasing order of subscripts, are assumed to form a tower under inclusion.

DEFINITION 2.1.2. An α worklist is a two part finite sequence

$$(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$$

where $r,s \geq 0$, and $\varphi_1,\ldots,\varphi_r,\psi_1,\ldots,\psi_s$ are α inclusions.

DEFINITION 2.1.3. The formats of an α worklist are the α formats that include $\{\varphi_1,\ldots,\varphi_r\}$ and are included in $\{\varphi_1,\ldots,\varphi_r,\psi_1,\ldots,\psi_s)$.

DEFINITION 2.1.4. We say that a worklist $(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$ is α,T secure if and only if for all $\{\varphi_1,\ldots,\varphi_r\} \subseteq S \subseteq \{\varphi_1,\ldots,\varphi_r,\psi_1,\ldots,\psi_s\}$, S is α,T correct or α,T incorrect.

Informally, the goal of an α worklist is to constructively verify that it is α,T secure, in the sense of determining the α,T correctness or α,T incorrectness of all α formats.

Sometimes we want to replace one worklist with a simpler worklist, without altering its goal. Here are some reduction operations that are very useful.

Let W = $\{\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$.

i. We can replace $\varphi_1,\ldots,\varphi_r$ with any $\varphi_1',\ldots,\varphi_p'$ such that $(\varphi_1 \wedge \ldots \wedge \varphi_r) \leftrightarrow (\varphi_1' \wedge \ldots \varphi_p')$ is α,T valid.

ii. We can replace any ψ_i by ψ_i', where $(\varphi_1 \wedge \ldots \wedge \varphi_r) \rightarrow (\psi_i \leftrightarrow \psi_i')$ is α,T valid.

iii. We can remove any ψ_i such that $(\varphi_1 \wedge \ldots \wedge \varphi_r) \rightarrow \psi_i$ is α,T valid.

iv. We can remove any ψ_i such that $(\varphi_1,\ldots,\varphi_r;\psi_i)$ is α,T-incorrect.

v. We can remove duplicates among $\psi_1,\ldots,\psi_s$.

vi. We can permute the $\psi_1,\ldots,\psi_s$.

DEFINITION 2.1.5. α,T reduction consists of performing any finite number of the above operations in succession.

This notion of α,T reduction corresponds to what happens in the classifications in sections 2.4, 2.5. For instance, consider LIST 1.2.1 in section 2.4.

Here the BRT fragment α is EBRT in A,B,fA,fB,$\subseteq$ on (SD,INF), and T is RCA_0. This displays the worklist (A $\cap$ fA = $\emptyset$, A $\cap$ fB = $\emptyset$, fA $\subseteq$ B; B $\cup$ fB = N, B $\subseteq$ A $\cup$ fB, fB $\subseteq$ B $\cup$ fA, B $\cap$ fB $\subseteq$ A $\cup$ fA). This gets reduced to the worklist displayed by LIST 1.2.1.*, which is the worklist (A $\cap$ fA = $\emptyset$, A $\cap$ fB = $\emptyset$, fA $\subseteq$ B; B $\cup$ fB = N, B $\subseteq$ A $\cup$ fB, B $\cap$ fB $\subseteq$ fA).

Here we have merely eliminated fB $\subseteq$ B $\cup$ fA from the second half of LIST 1.2.1, since Lemma 2.4.4 tells us that (A $\cap$ fB = $\emptyset$; fB $\subseteq$ B $\cup$ fA) is α,T incorrect.

LEMMA 2.1.1. Let α be a flat BRT fragment, and T be a true theory with a presentation of α. Suppose W = $(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$ α,T reduces to W' =

$(\varphi_1',...,\varphi_p';\psi_1',...,\psi_q')$. Then W is α,T secure if and only if W' is α,T secure.

Proof: It suffices to show that α,T security is preserved under each of the operations i-vi. Let one of the operations send worklist W to worklist W'. In cases i,ii,iii,v,vi, evidently every α format for W is α,T equivalent to some α format for W', and vice versa.

It remains to consider operation iv. We have W = $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$, W' = $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_{i-1},\psi_{i+1},...,\psi_s)$, where W' is α,T secure. Let $\{\varphi_1,...,\varphi_r\} \subseteq S \subseteq \{\varphi_1,...,\varphi_r,\psi_1,...,\psi_s\}$. If $\psi_i \in S$ then S is α,T incorrect. If $\psi_i \notin S$ then S is a format for W_i', and so S is α,T correct or α,T incorrect. QED

It is simpler to use sequences instead of sets. Accordingly, let W = $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$ be an α worklist.

DEFINITION 2.1.6. A subsequence for W is a subsequence of the sequence $(\varphi_1,...,\varphi_r,\psi_1,...,\psi_s)$ that begins with $\varphi_1,...,\varphi_r$, and which includes the underlying subsequence of positions 1,...,r,...,r+s. This is very useful for handling all sorts of repetitions in worklists.

DEFINITION 2.1.7. A finite sequence of α elementary inclusions is said to be α,T correct (α,T incorrect) if and only if its set of terms is α,T-correct (α,T incorrect).

LEMMA 2.1.2. Let α be a flat BRT fragment, and T be a true theory with a presentation of α. Let an α,T reduction of W = $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$ to W' = $(\varphi_1',...,\varphi_p';\psi_1,...,\psi_q')$ be given. Let the list of maximal α,T correct subsequences for W' be given (together with proofs in T). We can efficiently generate the list of maximal α,T correct subsequences for W (together with proofs in T). Furthermore, these two lists have the same number of sequences.

Proof: We can assume that we have W = $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$ that is α,T reduced to W' = $(\varphi_1',...,\varphi_p';\psi_1',...,\psi_q')$ by any one of the reductions i-v.

case i. Here we have W = $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$ and W' = $(\varphi_1',...,\varphi_p';\psi_1,...,\psi_s)$. Let f be the obvious one-one correspondence between subsequences for W and subsequences for W'. Then for every α sequence τ for W, τ and f(τ) are α,T equivalent. It is now evident that τ is α,T correct if and only if f(τ) is α,T correct. It is then evident that τ

is maximally α,T correct for W if and only if $f(\tau)$ is maximally α,T correct for W'.

case ii. Here we have $W = (\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$ and $W' = (\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_{i-1},\psi_i',\psi_{i+1},\ldots,\psi_s)$. Let f be the obvious one-one correspondence between subsequences for W and subsequences for W', based on corresponding positions. Then for every α sequence τ for W, τ and $f(\tau)$ are α,T equivalent. As in case i, τ is maximally α,T correct for W if and only if $f(\tau)$ is maximally α,T correct for W'.

case iii. Here we have $W = (\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$, $W' = (\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_{i-1},\psi_{i+1},\ldots,\psi_s)$. Let f be the obvious map from subsequences for W to subsequences for W' defined by ignoring ψ_i; i.e., as position r+i. Note that f is not one-one. However, the restriction g of f to the τ with ψ_i (as position r+i) is one-one, and for all $\tau \in \mathrm{dom}(g)$, τ and $g(\tau)$ are α,T equivalent. Since $(\varphi_1 \wedge \ldots \wedge \varphi_r) \rightarrow \psi_i$ is α,T valid, all maximal α,T correct subsequences for W have ψ_i (as position r+i). It is now evident that g is a one-one correspondence between the maximal α,T correct subsequences for W and the maximal α,T correct subsequences for W'.

case iv. Here we have $W = (\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$, $W' = (\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_{i-1},\psi_{i+1},\ldots,\psi_s)$. Note that the α,T correct subsequences for W are identical to the α,T correct subsequences for W', since ψ_i cannot be present.

cases v-vi. Left to the reader.

QED

LEMMA 2.1.3. Let α be a flat BRT fragment, and T be a true theory with a presentation of α. Let an α,T reduction of $W = (\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$ to $W' = (\varphi_1',\ldots,\varphi_p';\psi_1,\ldots,\psi_q')$ be given. Let the list of maximal α,T correct formats for W' be given (together with proofs in T). We can efficiently generate the list of maximal α,T correct formats for W (together with proofs in T). Furthermore, these two lists have the same number of formats. W is α,T secure if and only if W' is α,T secure.

Proof: This is the same as Lemma 2.1.2, except that we are using subsets (formats) instead of subsequences. It suffices to observe that the maximal α,T correct sequences for W are exactly the subsequences for W whose set of terms is an α,T correct format for W. The last claim is by Lemma 2.1.2. QED

DEFINITION 2.1.8. The starred α worklists are the α worklists with a * appended at the end.

DEFINITION 2.1.9. We say that TREE is a T classification for α if and only if α is a flat BRT fragment, T is a true theory extending RCA_0 which adequately defines the BRT setting of α, and TREE is a finite labeled tree with the properties given below.

1. The root of TREE is labeled by an α worklist $(;\delta_1,...,\delta_t)$, where the δ's list all α elementary inclusions without repetition.

2. Suppose a vertex v is labeled $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$, where v is not terminal. Then v has exactly one son w. The label of w is some $(\varphi_1',...,\varphi_p';\psi_1',...,\psi_q')^*$, where

$(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$ is α,T reducible to $(\varphi_1',...,\varphi_p';\psi_1',...,\psi_q')$.
$\varphi_1',...,\varphi_p',\psi_1',...,\psi_q'$ are distinct.

In sections 2.4, 2.5, note that the worklists whose names don't end with * are immediately followed by those which do, and the succeeding worklists with * are obtained by α,T reduction.

3. Suppose a vertex v is labeled $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)^*$, where v is not terminal. Then there exists $1 \leq i \leq s$ such that v has exactly i sons $w_1,...,w_i$, with labels

$$(\varphi_1,...,\varphi_r,\psi_1;\psi_2,...,\psi_s)$$
$$(\varphi_1,...,\varphi_r,\psi_2;\psi_3,...,\psi_s)$$
$$...$$
$$(\varphi_1,...,\varphi_r,\psi_i;\psi_{i+1},...,\psi_s)$$

respectively, where w_i is terminal, and $w_1,...,w_{i-1}$ are not terminal.

4. Suppose the vertex v is terminal, with label $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$ or $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)^*$. Then $\{\varphi_1,...,\varphi_r,\psi_1,...,\psi_s\}$ is α,T correct.

This completes Definition 2.1.7.

We want to show that if we have a T classification for α, then α is T secure.

LEMMA 2.1.4. Let TREE be a T classification for α. Then α is T secure and the number of maximally α,T correct α formats is at most the number of terminal vertices of T.

Proof: We prove the following by induction on TREE. Let v be a vertex of TREE whose label is the worklist W (or W*). Then W is α,T secure, and the number of maximal α,T correct formats for W is the number of terminal vertices from v; i.e., the number of terminal vertices that descend from v, including v.

case 1. v is a terminal vertex of TREE. Let the label of v be $(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$ or $(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)^*$. Then $(\varphi_1,\ldots,\varphi_r,\psi_1,\ldots,\psi_s)$ is α,T correct. Hence $\{\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$ is α,T secure. The number of maximal α,T correct formats for $(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$ is 1.

case 2. Suppose v has label $(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$, and is nonterminal. Then v has exactly one son, w, labeled $(\varphi_1',\ldots,\varphi_p';\psi_1',\ldots,\psi_q')^*$. Suppose $(\varphi_1',\ldots,\varphi_p';\psi_1',\ldots,\psi_q')$ is α,T secure. Suppose the number of maximal α,T correct formats for $(\varphi_1',\ldots,\varphi_p';\psi_1',\ldots,\psi_q')$ is at most the number of terminal vertices from w. The label of w is some $(\varphi_1',\ldots,\varphi_p';\psi_1',\ldots,\psi_q')^*$, where

$$(\varphi_1',\ldots,\varphi_p';\psi_1',\ldots,\psi_q') \text{ is an } \alpha\text{,T reduction of } (\varphi_1,\ldots,\varphi_r;\varphi_1,\ldots,\varphi_s).$$

By the induction hypothesis, $(\varphi_1',\ldots,\varphi_p';\psi_1',\ldots,\psi_q')$ is α,T secure. Hence by Lemma 2.1.3, $(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$ is α,T secure. Also by Lemma 2.1.3, the number of maximal α,T correct formats is preserved.

case 3. Suppose v has label $(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)^*$, where v is not terminal. Let $1 \leq i \leq s$, where v has exactly i sons, $w_1,\ldots,w_i$, with labels

$$(\varphi_1,\ldots,\varphi_r,\psi_1;\psi_2,\ldots,\psi_s)$$
$$(\varphi_1,\ldots,\varphi_r,\psi_2;\psi_3,\ldots,\psi_s)$$
$$\ldots$$
$$(\varphi_1,\ldots,\varphi_r,\psi_i;\psi_{i+1},\ldots,\psi_s)$$

respectively, where w_i is terminal. Suppose each of these labels is α,T secure. Suppose for each $1 \leq j \leq i$, the number of maximal α,T correct formats for $(\varphi_1,...,\varphi_r,\psi_j;\psi_{j+1},...,\psi_s)$ is the number of terminal vertices from w_j.

Note that $\{\varphi_1,...,\varphi_r,\psi_i;\psi i+1,...,\psi_s\}$ is α,T correct, and so automatically α,T secure. Also note that $\varphi_1,...,\varphi_r,\psi_1,...,\psi_s$ are distinct.

Let $\{\varphi_1,...,\varphi_r\} \subseteq S \subseteq \{\varphi_1,...,\varphi_r,\psi_1,...,\psi_s\}$. Suppose first that $S \cap \{\psi_1,...,\psi_i\} \neq \emptyset$. Let $1 \leq j \leq i$ be least such that $\psi_j \in S$. Then $\{\varphi_1,...,\varphi_r,\psi_j\} \subseteq S \subseteq \{\varphi_1,...,\varphi_r,\psi_{j+1},...,\psi_s\}$. By the induction hypothesis, $(\varphi_1,...,\varphi_r,\psi_j;\psi_{j+1},...,\psi_s)$ is α,T secure. Hence S is α,T correct or α,T incorrect.

Now suppose that $S \cap \{\psi_1,...,\psi_i\} = \emptyset$. Then $S \subseteq \{\varphi_1,...,\varphi_r,\psi_{i+1},...,\psi_s\}$. Hence S is α,T correct.

Now let S be maximal so that $\{\varphi_1,...,\varphi_r\} \subseteq S \subseteq \{\varphi_1,...,\varphi_r,\psi_1,...,\psi_s\}$ and S is α,T correct. Suppose first that $S \cap \{\psi_1,...,\psi_i\} \neq \emptyset$. Let $1 \leq j \leq i$ be least such that $\psi_j \in S$. Then $\{\varphi_1,...,\varphi_r,\psi_j\} \subseteq S \subseteq \{\varphi_1,...,\varphi_r,\psi_{j+1},...,\psi_s\}$. In fact, S is maximal such that $\{\varphi_1,...,\varphi_r,\psi_j\} \subseteq S \subseteq \{\varphi_1,...,\varphi_r,\psi_{j+1},...,\psi_s\}$.

Now suppose that $S \cap \{\psi_1,...,\psi_i\} = \emptyset$. Then $S \subseteq \{\varphi_1,...,\varphi_r,\psi_{i+1},...,\psi_s\}$. Hence $S = \{\varphi_1,...,\varphi_r,\varphi_{i+1},...,\psi_s\}$.

Hence the number of maximal α,T correct formats for $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$ is at most the sum over $1 \leq j \leq i$ of the number of maximal α,T correct formats for the label of w_j. By the induction hypothesis, the number of maximal α,T correct formats for the label of w_j is at most the number of terminal vertices from w_j. Hence the number of maximal α,T correct formats for $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$ is at most the number of terminal vertices from v.

This concludes the induction argument. Now apply the result to the label of the root. QED

THEOREM 2.1.5. Let α be a flat BRT fragment, and T be a true theory with a presentation of α. Then α is T secure if and only if there is a T classification for α. Let TREE be a T classification for α. The number of maximally α,T correct α formats is at most the number of terminal vertices of T.

Proof: Let α,T be as given. By Lemma 2.1.4, we need only show that if α is T secure, then there is a T classification for α.

Assume α is T secure. We build TREE as follows. The construction will be such that any vertex whose label is starred is not terminal.

Create the root of T, with label $(;\delta_1,...,\delta_r)$, where $\delta_1,...,\delta_r$ is a listing, without repetition, of the α elementary inclusions.

Suppose we have constructed the vertex v of TREE with label $W = (\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$. If $\{\varphi_1,...,\varphi_r,\psi_1,...,\psi_s\}$ is α,T correct, then v is terminal. Otherwise, we apply α,T reductions iii,iv,v to W, as much as possible, as well as removing duplicates among $\varphi_1,...,\varphi_r$. Let the result be the worklist W'. We create the single son w of v, with label W*. Clearly W' is not α,T correct.

Suppose we have constructed the vertex v of TREE with label $W^* = (\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)^*$. If $\{\varphi_1,...,\varphi_r,\psi_1,...,\psi_s\}$ is α,T correct then v is terminal. Suppose $\{\varphi_1,...,\varphi_r,\psi_1,...,\psi_s\}$ is not α,T correct. Then v is not α,T correct. Clearly $\{\varphi_1,...,\varphi_r,\psi_s\}$ is α,T correct, since otherwise we could apply reduction operation iv to $(\varphi_1,...,\varphi_r;\psi_1,...,\psi_s)$, contrary to W* being a label of a vertex in TREE.

Let $2 \leq i \leq s$ be smallest such that $\{\varphi_1,...,\varphi_r,\psi_i,...,\psi_s\}$ is α,T correct. Create i sons with labels

$$(\varphi_1,...,\varphi_r,\psi_1;\psi_2,...,\psi_s)$$
$$(\varphi_1,...,\varphi_r,\psi_2;\psi_3,...,\psi_s)$$
$$...$$
$$(\varphi_1,...,\varphi_r,\psi_i;\psi_{i+1},...,\psi_s)$$

respectively, where w_i is terminal. Vertices $w_1,...,w_{i-1}$ are not terminal.

This construction must terminate since

a. The clause applying to non starred vertices that are not terminal, creates a single son whose label has the same number of entries to the right of the semicolon.

b. The clause applying to starred vertices v that are not terminal, creates sons $w_1,...,w_i$, where for all j, the number of entries to the right of the label of w_j is less than the number of entries to the right of the label of v.

QED

THEOREM 2.1.6. Let α be a flat BRT fragment, and T be a true theory with a presentation of α. Let TREE be a T classification for α. We can efficiency list all of the maximal α,T correct formats.

Proof: Let α,T,TREE be as given. For each worklist for vertices in TREE, $(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$, we construct a list of the maximal α,T correct formats S with $\{\varphi_1,\ldots,\varphi_r\} \subseteq S \subseteq \{\varphi_1,\ldots,\varphi_r,\psi_1,\ldots,\psi_s\}$. We do this by recursion, starting at the terminal vertices, towards the root, ending at the root. At terminal vertices, there is exactly one maximal α,T correct S. At nonterminal non starred vertices, apply the procedure from Lemma 2.1.3.

Now let $(\varphi_1,\ldots,\varphi_r;\psi_1,\ldots,\psi_s)$ be the worklist at a nonterminal starred vertex. Let $1 \leq i \leq s$ be such that the vertex has the i sons with labels

$$(\varphi_1,\ldots,\varphi_r,\psi_1;\psi_2,\ldots,\psi_s)$$
$$(\varphi_1,\ldots,\varphi_r,\psi_2;\psi_3,\ldots,\psi_s)$$
$$\ldots$$
$$(\varphi_1,\ldots,\varphi_r,\psi_i;\psi_{i+1},\ldots,\psi_s)$$

respectively, where w_i is terminal. Vertices $w_1,\ldots,w_{i-1}$ are not terminal.

We already have the i lists of maximal α formats associated with each of the above i worklists. Clearly every maximal α,T correct format S with $\{\varphi_1,\ldots,\varphi_r\} \subseteq S \subseteq \{\varphi_1,\ldots,\varphi_r,\psi_1,\ldots,\psi_s\}$ must appear in at least one of these lists. So we can simply merge these lists of α formats, and take their maximal elements. QED

The tree methodology we have presented here is applicable to situations that do not involve BRT.

An important application of this tree methodology occurs in section 2.7 (see Witness Set List), where we start with a list of sets $V_1,V_2,\ldots,V_k$, and we want to determine which subsets of $\{V_1,\ldots,V_k\}$ have nonempty intersection. Thus the notion of "correctness" of subsets of $\{V_1,\ldots,V_k\}$ here is "having a nonempty intersection".

But what takes the place of the notion of reduction used in case 2? In the application in section 2.7, we only use the elimination of terms, from the second part of a worklist, that is disjoint from the intersection of the terms from the first part of that worklist.

This rather pure form of our tree methodology is used to prove Theorems 2.7.25 - 2.7.27.

2.2. EBRT, IBRT in A,fA.

This section is intended to be a particularly gentle introduction to BRT classification theory. It is wholly subsumed by section 2.3.

Recall the five main BRT settings introduced at the beginning of this Chapter: (SD,INF), (ELG,INF), (MF,INF), (ELG ∩ SD,INF), (EVSD,INF).

We begin with the BRT fragments α =

EBRT in A,fA on these five BRT settings.

As discussed in sections 1.1 and 2.1, classification of these BRT fragments amounts to a determination of the true α assertions, which take the form

1) $(\forall f \in V)(\exists A \in K)(\varphi)$

where φ is an α equation (since we are in the environment EBRT).

As discussed in sections 1.1 and 2.1, we work, equivalently, with the α statements, which take the form

1’) $(\forall f \in V)(\exists A \in K)(S)$

where S is an α format, interpreted conjunctively.

Recall that in EBRT, S is correct if and only if 1') holds. S is incorrect if and only if 1') fails.

In this case of EBRT in A,fA, the number of elementary inclusions is 4, and the number of formats is 16.

Since 16 is so small, we might as well list all of the formats S. It is most convenient to list the formats S in increasing order of their cardinality - which is 0-4.

The four A,fA elementary inclusions are as follows. See Definition 1.1.36. (These do not depend on the BRT environment or BRT setting).

$$A \cap fA = \emptyset.$$
$$A \cup fA = U.$$
$$A \subseteq fA.$$
$$fA \subseteq A.$$

According to Definition 1.1.13 of the universal set U in BRT settings, we see that on our five BRT settings, U is N.

Before beginning this tabular EBRT classification, we organize the nontrivial mathematical facts that we will use.

THEOREM 2.2.1. Let $f \in EVSD$ and $E \subseteq A \subseteq N$, where E is finite, A is infinite, and $E \cap fE = \emptyset$. Also let $D \subseteq N$ be infinite. There exists infinite B such that $E \subseteq B \subseteq A$, $B \cap fB = \emptyset$, and neither A nor D are subsets of $B \cup fB$. Moreover, this is provable in RCA_0.

Proof: Let f,E,A,D be as given. Let $n \in D$ be such that $n > \max(E \cup fE)$, and $|x| \geq n \rightarrow f(x) > |x|$. Let $t > n$, $t \in A$. We define an infinite strictly increasing sequence $n_1 < n_2 \ldots$ by induction as follows.

Define $n_1 = \min\{m \in A: m > t\}$. Suppose $n_1 < \ldots < n_k$ have been defined, $k \geq 1$. Define n_{k+1} to be the least element of A that is greater than n_k and all elements of $f(E \cup \{n_1,\ldots,n_k\})$.

Let $B = E \cup \{n_1,n_2,\ldots\} \subseteq A$. Clearly $B \cap fB = \emptyset$. Also $n,t \notin B$, and so A,D are not subsets of $B \cup fB$. QED

In the applications of Theorem 2.2.1 to the tabular EBRT classification below, we can ignore E,A,D. We just use that for all $f \in EVSD$, there exists infinite $B \subseteq N$ such that $B \cap fB = \emptyset$.

Here is the other fact that we need.

COMPLEMENTATION THEOREM. For all $f \in SD$ there exists $A \in INF$ such that $fA = N\setminus A$.

We proved the Complementation Theorem in section 1.3 within RCA_0.

A,fA FORMAT OF CARDINALIY 0
EBRT

The empty format is obviously correct, on all five BRT settings.

A,fA FORMATS OF CARDINALITY 1
EBRT

1.1. $A \cap fA = \emptyset$.
1.2. $A \cup fA = U$. Correct on all five. Set $A = N$.
1.3. $A \subseteq fA$. Incorrect on all five. Set $f(x) = 2x+1$.
1.4. $fA \subseteq A$. Correct on all five. Set $A = N$.

A,fA FORMATS OF CARDINALITY 2
EBRT

2.1. $A \cap fA = \emptyset$, $A \cup fA = U$. Equivalent to $fA = U\backslash A$ on all five.
2.2. $A \cap fA = \emptyset$, $A \subseteq fA$. Incorrect on all five. Contains 1.3.
2.3. $A \cap fA = \emptyset$, $fA \subseteq A$. Incorrect on all five.
2.4. $A \cup fA = U$, $A \subseteq fA$. Incorrect on all five. Contains 1.3.
2.5. $A \cup fA = U$, $fA \subseteq A$. Correct on all five. Set $A = U$.
2.6. $A \subseteq fA$, $fA \subseteq A$. Incorrect on all five. Contains 1.3.

A,fA FORMATS OF CARDINALITY 3
EBRT

3.1. $A \cap fA = \emptyset$, $A \cup fA = U$, $A \subseteq fA$. Incorrect on all five. Contains 1.3.
3.2. $A \cap fA = \emptyset$, $A \cup fA = U$, $fA \subseteq A$. Incorrect on all five. Contains 2.3.
3.3. $A \cap fA = \emptyset$, $A \subseteq fA$, $fA \subseteq A$. Incorrect on all five. Contains 1.3.
3.4. $A \cup fA = U$, $A \subseteq fA$, $fA \subseteq A$. Incorrect on all five. Contains 1.3.

A,fA FORMAT OF CARDINALITY 4
EBRT

4.1. $A \cap fA = \emptyset$, $A \cup fA = U$, $A \subseteq fA$, $fA \subseteq A$. Incorrect on all five. Contains 1.3.

We now list all of the formats whose status has not been determined. We use any stated equivalences that hold on all five.

1.1. A ∩ fA = ∅.
2.1. fA = U\A.

We now indicate the status of 1.1, 1.2, for EBRT in A,fA on each of our five main BRT settings.

We heavily use the fact that every function in our five main BRT settings, with the exception of MF, has infinite range.

EBRT in A,fA on (SD,INF)/(ELG ∩ SD,INF)

1.1. A ∩ fA = ∅. Correct on both. See Theorem 2.2.1.
2.1. fA = U\A. Correct on both. The Complementation Theorem.

EBRT in A,fA on (ELG,INF)/(EVSD,INF)

1.1. A ∩ fA = ∅. Correct on both. See Theorem 2.2.1.
2.1. fA = U\A. Incorrect on both. Let f(x) = 0 if x = 0; 2x+1 otherwise.

EBRT in A,fA on (MF,INF)

1.1. A ∩ fA = ∅. Incorrect. Let f(x) = x.
2.1. fA = U\A. Incorrect. Let f(x) = x.

We now make a table from our findings. + indicates that the format along left column is α correct, where α is EBRT in A,fA on the setting across the top row. - indicates otherwise.

EBRT in A,fA on:	(SD,INF)	(ELG ∩ SD,INF)	(ELG,INF)	(EVSD,INF)	(MF,INF)
∅	+	+	+	+	+
A ∩ fA = ∅	+	+	+	+	-
A ∪ fA = U	+	+	+	+	+
A ⊆ fA	-	-	-	-	-
fA ⊆ A	+	+	+	+	+
A ∩ fA = ∅, A ∪ fA = U	+	+	-	-	-
A ∩ fA = ∅, A ⊆ fA	-	-	-	-	-
A ∩ fA = ∅, fA ⊆ A	-	-	-	-	-
A ∪ fA = U, A ⊆ fA	-	-	-	-	-
A ∪ fA = U, fA ⊆ A	+	+	+	+	+
A ⊆ fA, fA ⊆ A	-	-	-	-	-
A ∩ fA = ∅, A ∪ fA = U, A ⊆ fA	-	-	-	-	-
A ∩ fA = ∅, A ∪ fA = U, fA ⊆ A	-	-	-	-	-
A ∩ fA = ∅, A ⊆ fA, fA ⊆ A	-	-	-	-	-
A ∪ fA = U, A ⊆ fA, fA ⊆ A	-	-	-	-	-
A ∩ fA = ∅,A ∪ fA = U,A ⊆ fA,fA ⊆ A	-	-	-	-	-

THEOREM 2.2.2. EBRT in A,fA on (SD,INF),(ELG ∩ SD,INF) have the same correct formats (or, equivalently, true statements, or true assertions). So do EBRT in A,fA on (ELG,INF),(EVSD,INF). This is not true of EBRT in A,fA on any distinct pair of settings among (SD,INF),(ELG,INF),(MF,INF). EBRT in A,fA on all five settings, is RCA_0 secure.

Proof: Immediate from the above tabular classifications and their documentation. This uses the observation that Theorem 2.2.1 and the Complementation Theorem are provable in RCA_0. The counterexamples are very explicit. QED

We now come to IBRT in A,fA on the same five BRT settings. We investigate the assertions

$$2)\ (\forall f \in V)(\exists A \in K)(\varphi)$$

where φ is an α inequation (since we are in the environment IBRT).

As discussed in sections 1.1 and 2.1, we work, equivalently, with the α statements, which take the form

$$2')\ (\exists f \in V)(\forall A \in K)(S)$$

where S is an α format, interpreted conjunctively.

Recall that in IBRT, S is correct if and only if 2') holds. S is incorrect if and only if 2') fails.

We again start with the same four A,fA elementary inclusions, as these do not depend on the environment.

Before beginning this tabular EBRT classification, we organize the nontrivial facts that we will use. Recall the Thin Set Theorem from section 1.4.

THIN SET THEOREM. For all f ∈ MF there exists A ∈ INF such that fA ≠ N.

We also need the following variant.

THIN SET THEOREM (variant). For all f ∈ MF there exists A ∈ INF such that A ∪ fA ≠ N.

Proof: We derive this variant from the Thin Set Theorem (over RCA_0). Let $f:N^k \to N$. Define $g:N^{k+1} \to N$ by

$g(x_1,...,x_{k+1}) = f(x_1,...,x_k)$ if $x_k \neq x_{k+1}$; x_k otherwise. By the Thin Set Theorem, let A ∈ INF, gA ≠ N. Then gA = A ∪ fA ≠ N. QED

By the above proof, it is clear that the Thin Set Theorem and the Thin Set Theorem (variant) are provably equivalent in RCA_0.

The system ACA' (see Definition 1.4.1) is sufficient to prove the Thin Set Theorem. Here are the four A,fA elementary inclusions.

A ∩ fA = ∅.
A ∪ fA = U.
A ⊆ fA.
fA ⊆ A.

A,fA FORMAT OF CARDINALIY 0
IBRT

The empty format is obviously correct, on all five BRT settings.

A,fA FORMATS OF CARDINALITY 1
IBRT

1.1. A ∩ fA = ∅. Incorrect on all five. Set A = N.
1.2. A ∪ fA = U. Incorrect on all five. Thin Set Theorem (variant).
1.3. A ⊆ fA.
1.4. fA ⊆ A.

A,fA FORMATS OF CARDINALITY 2
IBRT

2.1. A ∩ fA = ∅, A ∪ fA = U. Incorrect on all five. Contains 1.1.
2.2. A ∩ fA = ∅, A ⊆ fA. Incorrect on all five. Contains 1.1.
2.3. A ∩ fA = ∅, fA ⊆ A. Incorrect on all five. Contains 1.1
2.4. A ∪ fA = U, A ⊆ fA. Incorrect on all five. Contains 1.2.
2.5. A ∪ fA = U, fA ⊆ A. Incorrect on all five. Contains 1.2.
2.6. A ⊆ fA, fA ⊆ A. Equivalent to fA = A on all five.

A,fA FORMATS OF CARDINALITY 3

IBRT

3.1. A ∩ fA = ∅, A ∪ fA = U, A ⊆ fA. Incorrect on all five. Contains 1.1.
3.2. A ∩ fA = ∅, A ∪ fA = U, fA ⊆ A. Incorrect on all five. Contains 1.1.
3.3. A ∩ fA = ∅, A ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
3.4. A ∪ fA = U, A ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.2.

A,fA FORMAT OF CARDINALITY 4
IBRT

A ∩ fA = ∅, A ∪ fA = U, A ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.

These are the only formats whose status has not been determined. We use equivalences that hold on all five.

1.3. A ⊆ fA.
1.4. fA ⊆ A.
2.6. fA = A.

We now indicate the status of 1.3, 1.4, 1.6, for IBRT in A,fA on each of our five main BRT settings.

IBRT in A,fA on (SD,INF),(ELG ∩ SD,INF),(ELG,INF),(EVSD,INF)

1.3. A ⊆ fA. Incorrect on all four. Theorem 2.2.1.
1.4. fA ⊆ A. Incorrect on all four. Theorem 2.2.1.
2.6. fA = A. Incorrect on all four. Theorem 2.2.1.

IBRT in A,fA on (MF,INF)

1.3. A ⊆ fA. Correct. Set f(x) = x.
1.4. fA ⊆ A. Correct. Set f(x) = x.
2.6. fA = A. Correct. Set f(x) = x.

Recall that the instances of 2’) are in dual form. I.e., they are the negations of the IBRT in A,fA assertions. In particular, the Thin Set Theorem and the Thin Set Theorem (variant) are assertions in IBRT in A,fA on (MF,INF), and therefore negations of statements in IBRT in A,fA on (MF,INF).

We now make a table from our findings. + indicates that the format along left column is α correct, where α is IBRT in A,fA on the setting across the top row. – indicates otherwise.

IBRT in A,fA on:	(SD,INF)	(ELG ∩ SD,INF)	(ELG,INF)	(EVSD,INF)	(MF,INF)
∅	+	+	+	+	+
A ∩ fA = ∅	-	-	-	-	-
A ∪ fA = U	-	-	-	-	-
A ⊆ fA	-	-	-	-	+
fA ⊆ A	-	-	-	-	+
A ∩ fA = ∅, A ∪ fA = U	-	-	-	-	-
A ∩ fA = ∅, A ⊆ fA	-	-	-	-	-
A ∩ fA = ∅, fA ⊆ A	-	-	-	-	-
A ∪ fA = U, A ⊆ fA	-	-	-	-	-
A ∪ fA = U, fA ⊆ A	-	-	-	-	-
A ⊆ fA, fA ⊆ A	-	-	-	-	+
A ∩ fA = ∅, A ∪ fA = U, A ⊆ fA	-	-	-	-	-
A ∩ fA = ∅, A ∪ fA = U, fA ⊆ A	-	-	-	-	-
A ∩ fA = ∅, A ⊆ fA, fA ⊆ A	-	-	-	-	-
A ∪ fA = U, A ⊆ fA, fA ⊆ A	-	-	-	-	-
A ∩ fA = ∅,A ∪ fA = U,A ⊆ fA,fA ⊆ A	-	-	-	-	-

THEOREM 2.2.3. For IBRT in A,fA on (SD,INF),(ELG ∩ SD,INF), (ELG,INF),(EVSD,INF), the only correct format is ∅. This is not true of IBRT in A,fA on (MF,INF). IBRT in A,fA on each of (SD,INF),(ELG ∩ SD,INF),(ELG,INF),(EVSD,INF) is RCA_0 secure. IBRT in A,fA on (MF,INF) is ACA' secure, but not ACA_0 secure. Every correct format in A,fA on (MF,INF) is RCA_0 correct. We can replace ACA' here by RCA_0 + Thin Set Theorem.

Proof: The first two claims are immediate from the given tabular classifications. For the third claim, it suffices to verify that the incorrectness of 1.1,1.2,1.3,1.4,2.6 on these four settings is provable in RCA_0. For 1.1, this is trivial. For 1.3, 1.4, 2.6, this is from the provability of Theorem 2.2.1 in RCA_0. For 1.2, this is also from the provability of Theorem 2.2.1 in RCA_0.

For the fourth claim, note that all correctness determinations in IBRT in A,fA on (MF,INF) were given in RCA_0, and all incorrectness determinations in α = IBRT in A,fA on (MF,INF) were given in RCA_0 + Thin Set Theorem (variant). Thus α is RCA_0 + Thin Set Theorem (variant) secure, and hence ACA' secure. Since the incorrectness of 1.2 in α is equivalent, over RCA_0, to Thin Set Theorem (variant), α is not ACA_0 secure. This is because of the unprovability of the Thin Set Theorem in ACA_0 (see [FS00], [CGHJ05]).

For the fifth claim, α is RCA_0 + Thin Set Theorem secure, because of the proof given above of Thin Set Theorem (variant) from Thin Set Theorem (over RCA_0). QED

An interesting issue is the effect of the arity of the functions. The classes SD, ELG ∩ SD, ELG, EVSD, and MF use functions of every arity k ≥ 1.

LEMMA 2.2.4. The Thin Set Theorem (variant) for exponent 1 is provable in RCA_0.

Proof: Let f:N → N. If {n: f(n) = 0} is infinite then set A = {n: f(n) = 0}. If not, let n > 0 be such that f is nonzero on [n,∞). Set A = [n,∞). Then A ∪ fA ≠ N. QED

DEFINITION 2.2.1. For k ≥ 1, let SD[k], (ELG ∩ SD)[k], ELG[k], EVSD[k], MF[k] be the restrictions of SD, ELG ∩ SD, ELG, EVSD, MF to functions whose domain is N^k.

THEOREM 2.2.5. Let k ≥ 1. EBRT in A,fA on SD[k], (ELG ∩ SD)[k], ELG[k], EVSD[k], MF[k], and IBRT in A,fA on SD[k], (ELG ∩ SD)[k], ELG[k], EVSD[k], are RCA_0 secure. IBRT in A,fA on MF[k] is ACA_0 secure. IBRT in A,fA on MF[1] is RCA_0 secure. EBRT and IBRT in A,fA on SD[k], (ELG ∩ SD)[k], ELG[k], EVSD[k], MF[k] have the same correct formats as EBRT and IBRT in SD, ELG ∩ SD, ELG, EVSD, MF, respectively.

Proof: An examination of the arguments immediately reveals that all of the incorrectness determinations given for EBRT involve unary functions only, and all of the correctness determinations given for IBRT also involve unary functions only. We can obviously pad these unary functions as k-ary functions. IBRT in A,fA on MF[k] is ACA_0 secure since the Thin Set Theorem (variant) is provable in ACA_0 for k-ary functions, using the infinite Ramsey theorem for k-tuples. By Lemma 2.2.4, IBRT in A,fA on MF[1] is RCA_0 secure. QED

2.3. EBRT, IBRT in A,fA,fU.

We redo section 2.2 for the signature A,fA,fU, with the same five BRT settings (SD,INF), (ELG ∩ SD,INF), (ELG,INF), (EVSD,INF), (MF,INF).

After we treat these five BRT settings, we then treat the five corresponding unary BRT settings (SD[1],INF), (ELG[1] ∩ SD[1],INF), (ELG[1],INF), (EVSD[1],INF), (MF[1],INF). These are the same except that we restrict to the 1-ary functions only. There is quite a lot of difference between the unary settings and the multivariate settings; this was not the case in section 2.2, with just A,fA.

We begin with EBRT in A,fA,fU. The 8 A,fA,fU pre elementary inclusions are as follows (see Definition 1.1.35).

A ∩ fA ∩ fU = ∅.
A ∪ fA ∪ fU = U.
A ⊆ fA ∪ fU.
fA ⊆ A ∪ fU.
fU ⊆ A ∪ fA.
A ∩ fA ⊆ fU.
A ∩ fU ⊆ fA.
fA ∩ fU ⊆ A.

The 6 A,fA,fU elementary inclusions are as follows (see Definition 1.1.36).

A ∩ fA = ∅.
A ∪ fU = U.
A ⊆ fU.
fU ⊆ A ∪ fA.
A ∩ fU ⊆ fA.
fA ⊆ A.

We will use Theorem 2.2.1, and the Complementation Theorem from section 1.3. In fact, we need the following strengthening of the Complementation Theorem.

THEOREM 2.3.1. Let f ∈ SD and B ∈ INF. There exists A ∈ INF, A ⊆ B, such that A ∩ fA = ∅ and B ⊆ A ∪ fA. Moreover, this is provable in RCA_0.

Proof: Let f,B be as given. We inductively define A ⊆ B as follows. Suppose the elements of A from 0,1,...,n-1 have been defined, n ≥ 0. We put n in A if and only if n ∈ B and n is not the value of f at arguments from A less than n. Then A is as required, using f ∈ SD. QED

THEOREM 2.3.2. For all f ∈ EVSD there exists A ∈ INF such that A ∩ fA = ∅, A ∪ fN = N. Moreover, this is provable in RCA_0.

Proof: Let f ∈ EVSD be k-ary. Let n be such that |x| ≥ n → f(x) ≥ |x|. We define A inductively. First put [0,n]\fN in A. For m > n, put m in A if and only if m = f(x) for no |x| < m. Then [n+1,∞) ⊆ A ∪ fA. Also [0,n] ⊆ A ∪ fA. Hence A ∪

fN = N. Suppose m ∈ A ∩ fA. If m ≤ n then by construction, m ∈ [0,n]\fN, contradicting m ∈ fA. Hence m > n. Let m = f(x), x ∈ A^k. If |x| ≥ m then f(x) > |x| ≥ m, which is a contradiction. Hence |x| < m, and so m ∉ A by construction. This contradicts m ∈ A. QED

THEOREM 2.3.3. Let k ≥ 2. There exists k-ary f ∈ ELG ∩ SD such that N\fN = {0}. There exists k-ary f ∈ ELG such that fN = N.

Proof: For all n ≥ 1, let $f_n:[2^n,2^{n+1})^k \rightarrow [2^{n+1},2^{n+2})$ be onto. Let f be the union of the f_n extended as follows. For x not yet defined, set f(x) = 1 if |x| = 0; 2 if |x| = 1; 3 if |x| = 2; 2|x| if |x| ≥ 3. Then fN = N\{0} and f ∈ ELG ∩ SD. Let g be the union of the f_n extended as follows. For x not yet defined, set f(x) = 0 if |x| = 0; 1 if |x| = 1; 2 if |x| = 2; 3 if |x| = 3; 2|x| if |x| ≥ 4. Then fN = N and f ∈ ELG. QED

SETTINGS: (SD,INF), (ELG ∩ SD,INF),
(ELG,INF), (EVSD,INF), (MF,INF).

A,fA,fU FORMAT OF CARDINALITY 0
EBRT

The empty format is obviously correct, for all five BRT settings.

A,fA,fU FORMATS OF CARDINALITY 1
EBRT

1.1. A ∩ fA = ∅.
1.2. A ∪ fU = U. Correct on all five. Set A = N.
1.3. A ⊆ fU.
1.4. fU ⊆ A ∪ fA. Correct on all five. Set A = N.
1.5. A ∩ fU ⊆ fA. Correct on all five. Set A = N.
1.6. fA ⊆ A. Correct on all five. Set A = N.

A,fA,fU FORMATS OF CARDINALITY 2
EBRT

2.1. A ∩ fA = ∅, A ∪ fU = U.
2.2. A ∩ fA = ∅, A ⊆ fU.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA.
2.4. A ∩ fA = ∅, A ∩ fU ⊆ fA. Equivalent on all five to A ∩ fU = ∅. Incorrect on all five. Theorem 2.3.3.
2.5. A ∩ fA = ∅, fA ⊆ A. Equivalent on all five to fA = ∅. Incorrect on all five using any f.

2.6. A ∪ fU = U, A ⊆ fU. Equivalent on all five to fU = U. Incorrect on all five. Set rng(f) ≠ N.
2.7. A ∪ fU = U, fU ⊆ A ∪ fA. Correct on all five. Set A = N.
2.8. A ∪ fU = U, A ∩ fU ⊆ fA. Correct on all five. Set A = N.
2.9. A ∪ fU = U, fA ⊆ A. Correct on all five. Set A = N.
2.10. A ⊆ fU, fU ⊆ A ∪ fA.
2.11. A ⊆ fU, A ∩ fU ⊆ fA. Equivalent on all five to A ⊆ fA. Incorrect on all five. Set f(x) = 2x+1.
2.12. A ⊆ fU, fA ⊆ A.
2.13. fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Correct on all five. Set A = N.
2.14. fU ⊆ A ∪ fA, fA ⊆ A. Correct on all five. Set A = N.
2.15. A ∩ fU ⊆ fA, fA ⊆ A. Correct on all five. Set A = N.

A,fA,fU FORMATS OF CARDINALITY 3
EBRT

3.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU. Incorrect on all five. Contains 2.6.
3.2. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA. Equivalent to A ∩ fA = ∅, A ∪ fA = U on all five.
3.3. A ∩ fA = ∅, A ∪ fU = U, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.4.
3.4. A ∩ fA = ∅, A ∪ fU = U, fA ⊆ A. Incorrect on all five. Contains 2.5.
3.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA.
3.6. A ∩ fA = ∅, A ⊆ fU, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.11.
3.7. A ∩ fA = ∅, A ⊆ fU, fA ⊆ A. Incorrect on all five. Contains 2.5.
3.8. A ∩ fA = ∅, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.4.
3.9. A ∩ fA = ∅, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
3.10. A ∩ fA = ∅, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
3.11. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA. Incorrect on all five. Contains 2.6.
3.12. A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.6.
3.13. A ∪ fU = U, A ⊆ fU, fA ⊆ A. Incorrect on all five. Contains 2.6.
3.14. A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Correct on all five. Set A = N.
3.15. A ∪ fU = U, fU ⊆ A ∪ fA, fA ⊆ A. Correct on all five. Set A = N.

3.16. A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A. Correct on all five. Set A = N.
3.17. A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.11.
3.18. A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A.
3.19. A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.11.
3.20. fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Correct on all five. Set A = N.

A,fA,fU FORMATS OF CARDINALITY 4
EBRT

4.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA. Incorrect on all five. Contains 2.6.
4.2. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.6.
4.3. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.4. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.4.
4.5. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.6. A ∩ fA = ∅, A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.7. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.11.
4.8. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.9. A ∩ fA = ∅, A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.10. A ∩ fA = ∅, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.11. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.6.
4.12. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.6.
4.13. A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.6.
4.14. A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Correct on all five. Set A = N.
4.15. A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.11.

A,fA,fU FORMATS OF CARDINALITY 5
EBRT

5.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.6.
5.2. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
5.3. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
5.4. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
5.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
5.6. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.6.

A,fA,fU FORMATS OF CARDINALITY 6
EBRT

6.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.

We now list all of the formats whose status has not been determined. We use any stated equivalences that hold on all five.

1.1. A ∩ fA = ∅.
1.3. A ⊆ fU.
2.1. A ∩ fA = ∅, A ∪ fU = U.
2.2. A ∩ fA = ∅, A ⊆ fU.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA.
2.10. A ⊆ fU, fU ⊆ A ∪ fA.
2.12. A ⊆ fU, fA ⊆ A.
3.2. A ∩ fA = ∅, A ∪ fA = U.
3.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA.
3.18. A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A.

We now settle the status of each of these formats on the various settings.

EBRT in A,fA,fU on (SD,INF),(ELG ∩ SD,INF)

1.1. A ∩ fA = ∅. Correct on both. See Theorem 2.2.1.
1.3. A ⊆ fU. Correct on both. Set A = fN.
2.1. A ∩ fA = ∅, A ∪ fU = U. Correct on both. The Complementation Theorem (section 1.3).
2.2. A ∩ fA = ∅, A ⊆ fU. Correct on both. Theorem 2.2.1.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA. Correct on both. The Complementation Theorem.
2.10. A ⊆ fU, fU ⊆ A ∪ fA. Correct on both. Set A = fN.
2.12. A ⊆ fU, fA ⊆ A. Correct on both. Set A = fN.

3.2. A ∩ fA = ∅, A ∪ fA = U. Correct on both. Complementation Theorem.
3.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA. Correct on both. Theorem 2.3.1 with B = fU.
3.18. A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Correct on both. Set A = fN.

EBRT in A,fA,fU on (ELG,INF),(EVSD,INF)

1.1. A ∩ fA = ∅. Correct on both. See Theorem 2.2.1.
1.3. A ⊆ fU. Correct on both. Set A = fN.
2.1. A ∩ fA = ∅, A ∪ fU = U. Correct on both. Theorem 2.3.2.
2.2. A ∩ fA = ∅, A ⊆ fU. Correct on both. Theorem 2.2.1.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA. Incorrect on both. Set f(x) = 2x.
2.10. A ⊆ fU, fU ⊆ A ∪ fA. Correct on both. Set A = fN.
2.12. A ⊆ fU, fA ⊆ A. Correct on both. Set A = fN.
3.2. A ∩ fA = ∅, A ∪ fA = U. Incorrect on both. Set f(x) = 2x.
3.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA. Incorrect on both. Set f(x) = 2x.
3.18. A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Correct on both. Set A = fN.

From the above, we see a difference between (SD,INF) and (EVSD,INF) with regard to 2.3, 3.2, 3.5.

EBRT in A,fA,fU on (MF,INF)

1.1. A ∩ fA = ∅. Incorrect. Set f(x) = x.
1.3. A ⊆ fU. Incorrect. Set f(x) = 0.
2.1. A ∩ fA = ∅, A ∪ fU = U. Incorrect. Set f(x) = x.
2.2. A ∩ fA = ∅, A ⊆ fU. Incorrect. Set f(x) = x.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA. Incorrect. Set f(x) = x.
2.10. A ⊆ fU, fU ⊆ A ∪ fA. Incorrect. Set f(x) = 0.
2.12. A ⊆ fU, fA ⊆ A. Correct on both. Set A = fN. Incorrect. Set f(x) = 0.
3.2. A ∩ fA = ∅, A ∪ fA = U. Incorrect. Set f(x) = x.
3.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA. Incorrect. Set f(x) = x.
3.18. A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect. Set f(x) = 0.

THEOREM 2.3.4. EBRT in A,fA,fU on (SD,INF),(ELG ∩ SD,INF) have the same correct formats. So do EBRT in A,fA,fU on (ELG,INF),(EVSD,INF). This is not true of EBRT in A,fA,fU on any distinct pair of settings among

(SD,INF),(ELG,INF),(MF,INF). EBRT in A,fA on all five settings, is RCA_0 secure.

Proof: Immediate from the above tabular classifications and their documentation. Format 2.3 provides a difference between A,fA,fU on (SD[1],INF) and (ELG[1],INF), and on (SD,INF) and (MF,INF). Format 1.3 proves a difference between A,fA,fU on (ELG,INF) and (MF,INF). QED

We now turn to IBRT in A,fA,fU on the same five BRT settings.

We will use the Thin Set Theorem (variant) from section 2.2, as well as Theorem 2.2.1, and previous results of this section.

SETTINGS: (SD,INF), (ELG ∩ SD,INF),
(ELG,INF), (EVSD,INF), (MF,INF).

A,fA,fU FORMAT OF CARDINALITY 0
IBRT

The empty format is obviously correct, for all five BRT settings.

A,fA,fU FORMATS OF CARDINALITY 1
IBRT

1.1. A ∩ fA = ∅. Incorrect on all five. Set A = N.
1.2. A ∪ fU = U.
1.3. A ⊆ fU.
1.4. fU ⊆ A ∪ fA.
1.5. A ∩ fU ⊆ fA.
1.6. fA ⊆ A.

A,fA,fU FORMATS OF CARDINALITY 2
IBRT

2.1. A ∩ fA = ∅, A ∪ fU = U. Incorrect on all five. Contains 1.1.
2.2. A ∩ fA = ∅, A ⊆ fU. Incorrect on all five. Contains 1.1.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA. Incorrect on all five. Contains 1.1.
2.4. A ∩ fA = ∅, A ∩ fU ⊆ fA. Incorrect on all five. Contains 1.1.
2.5. A ∩ fA = ∅, fA ⊆ A. Incorrect on all five. Contains 1.1.

2.6. A ∪ fU = U, A ⊆ fU. Equivalent on all five to fU = U.
2.7. A ∪ fU = U, fU ⊆ A ∪ fA. Equivalent on all five to A ∪ fA = U. Incorrect on all five. Thin Set Theorem (variant).
2.8. A ∪ fU = U, A ∩ fU ⊆ fA.
2.9. A ∪ fU = U, fA ⊆ A.
2.10. A ⊆ fU, fU ⊆ A ∪ fA. Incorrect on all five. Suppose fN ≠ N. Set A = N. Suppose fN = N. Thin Set Theorem (variant).
2.11. A ⊆ fU, A ∩ fU ⊆ fA. Equivalent on all five to A ⊆ fA.
2.12. A ⊆ fU, fA ⊆ A.
2.13. fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Equivalent on all five to fU = fA.
2.14. fU ⊆ A ∪ fA, fA ⊆ A. Equivalent on all five to fU ⊆ A. Incorrect on all five.
2.15. A ∩ fU ⊆ fA, fA ⊆ A.

A,fA,fU FORMATS OF CARDINALITY 3
IBRT

3.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU. Incorrect on all five. Contains 1.1.
3.2. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA. Incorrect on all five. Contains 1.1.
3.3. A ∩ fA = ∅, A ∪ fU = U, A ∩ fU ⊆ fA. Incorrect on all five. Contains 1.1.
3.4. A ∩ fA = ∅, A ∪ fU = U, fA ⊆ A. Incorrect on all five. Contains 1.1.
3.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA. Incorrect on all five. Contains 1.1.
3.6. A ∩ fA = ∅, A ⊆ fU, A ∩ fU ⊆ fA. Incorrect on all five. Contains 1.1.
3.7. A ∩ fA = ∅, A ⊆ fU, fA ⊆ A. Incorrect on all five. Contains 1.1.
3.8. A ∩ fA = ∅, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 1.1.
3.9. A ∩ fA = ∅, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
3.10. A ∩ fA = ∅, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
3.11. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA. Incorrect on all five. Contains 2.7.
3.12. A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA. Equivalent on all five to fU = U, A ⊆ fA.
3.13. A ∪ fU = U, A ⊆ fU, fA ⊆ A. Equivalent on all five to fU = U, fA ⊆ A.

3.14. A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.7.
3.15. A ∪ fU = U, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.7.
3.16. A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A.
3.17. A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.10.
3.18. A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.10.
3.19. A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Equivalent on all five to fA = A.
3.20. fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.14.

A,fA,fU FORMATS OF CARDINALITY 4
IBRT

4.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA. Incorrect on all five. Contains 1.1.
4.2. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA. Incorrect on all five. Contains 1.1.
4.3. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fA ⊆ A. Incorrect on all five. Contains 1.1.
4.4. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 1.1.
4.5. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
4.6. A ∩ fA = ∅, A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
4.7. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 1.1.
4.8. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
4.9. A ∩ fA = ∅, A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
4.10. A ∩ fA = ∅, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
4.11. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.7.
4.12. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.7.
4.13. A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Equivalent on all five to fU = U, fA = A.
4.14. A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.7.
4.15. A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.10.

A,fA,fU FORMATS OF CARDINALITY 5
IBRT

5.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 1.1.
5.2. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
5.3. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
5.4. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
5.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.
5.6. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.7.

A,fA,fU FORMATS OF CARDINALITY 6
IBRT

6.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 1.1.

We now list all of the formats whose status has not been determined. We use any stated equivalences that hold on all five.

1.2. A ∪ fU = U.
1.3. A ⊆ fU.
1.4. fU ⊆ A ∪ fA.
1.5. A ∩ fU ⊆ fA.
1.6. fA ⊆ A.
2.6. fU = U.
2.8. A ∪ fU = U, A ∩ fU ⊆ fA.
2.9. A ∪ fU = U, fA ⊆ A.
2.11. A ⊆ fA.
2.12. A ⊆ fU, fA ⊆ A.
2.13. fU = fA.
2.15. A ∩ fU ⊆ fA, fA ⊆ A.
3.12. fU = U, A ⊆ fA.
3.13. fU = U, fA ⊆ A.
3.16. A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A.
3.19. fA = A.
4.13. fU = U, fA = A.

We now determine the status of the above formats on the five settings.

IBRT in A,fA,fU on (SD,INF),(ELG ∩ SD,INF)

1.2. A ∪ fU = U. Incorrect on both. Set A = N\{0}.
1.3. A ⊆ fU. Incorrect on both. Set A = N.
1.4. fU ⊆ A ∪ fA. Incorrect on both. Theorem 2.2.1.
1.5. A ∩ fU ⊆ fA. Incorrect on both. Set A = [min(fU),∞).
1.6. fA ⊆ A. Incorrect on both. Theorem 2.2.1.
2.6. fU = U. Incorrect on both.
2.8. A ∪ fU = U, A ∩ fU ⊆ fA. Incorrect on both. Contains 1.2.
2.9. A ∪ fU = U, fA ⊆ A. Incorrect on both. Contains 1.6.
2.11. A ⊆ fA. Incorrect on both. Set A = N.
2.12. A ⊆ fU, fA ⊆ A. Incorrect on both. Contains 1.3.
2.13. fU = fA. Incorrect on both. See 1.4.
2.15. A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on both. Contains 1.6.
3.12. fU = U, A ⊆ fA. Incorrect on both. Contains 2.6.
3.13. fU = U, fA ⊆ A. Incorrect on both. Contains 2.6.
3.16. A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on both. Contains 1.6.
3.19. fA = A. Incorrect on both. See 1.6.
4.13. fU = U, fA = A. Incorrect on both. Contains 2.6.

IBRT in A,fA,fU on (ELG,INF),(EVSD,INF)

1.2. A ∪ fU = U. Correct on both. Theorem 2.3.3.
1.3. A ⊆ fU. Correct on both. Theorem 2.3.3.
1.4. fU ⊆ A ∪ fA. Incorrect on both. Theorem 2.2.1.
1.5. A ∩ fU ⊆ fA. Incorrect on both. Set A = [n,∞), where n is a sufficiently large element of fU.
1.6. fA ⊆ A. Incorrect on both. Theorem 2.2.1.
2.6. fU = U. Correct on both. Theorem 2.3.3.
2.8. A ∪ fU = U, A ∩ fU ⊆ fA. Incorrect on both. Contains 1.5.
2.9. A ∪ fU = U, fA ⊆ A. Incorrect on both. Contains 1.6.
2.11. A ⊆ fA. Incorrect on both. Theorem 2.2.1.
2.12. A ⊆ fU, fA ⊆ A. Incorrect on both. Contains 1.6.
2.13. fU = fA. Incorrect on both. Use Theorem 2.2.1 with D = fN. Obtain infinite A where fN ¬⊆ A ∪ fA.
2.15. A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on both. Contains 1.6.
3.12. fU = U, A ⊆ fA. Incorrect for both. Contains 2.11.
3.13. fU = U, fA ⊆ A. Incorrect for both. Contains 1.6.
3.16. A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect for both. Contains 1.6.
3.19. fA = A. Incorrect for both. See 1.6.
4.13. fU = U, fA = A. Incorrect for both. See 1.6.

Note the difference between (SD,INF) and (ELG,INF). E.g., 1.3 is incorrect on (SD,INF) but correct on (ELG,INF).

IBRT in A,fA,fU on (MF,INF)

1.2. A ∪ fU = U. Correct. Set f(x) = x.
1.3. A ⊆ fU. Correct. Set f(x) = x.
1.4. fU ⊆ A ∪ fA. Correct. Set f(x) = 0.
1.5. A ∩ fU ⊆ fA. Correct. Set f(x) = x.
1.6. fA ⊆ A. Correct. Set f(x) = x.
2.6. fU = U. Correct. Set f(x) = x.
2.8. A ∪ fU = U, A ∩ fU ⊆ fA. Correct. Set f(x) = x.
2.9. A ∪ fU = U, fA ⊆ A. Correct. Set f(x) = x.
2.11. A ⊆ fA. Correct. Set f(x) = x.
2.12. A ⊆ fU, fA ⊆ A. Correct. Set f(x) = x.
2.13. fU = fA. Correct. Set f(x) = 0.
2.15. A ∩ fU ⊆ fA, fA ⊆ A. Correct. Set f(x) = x.
3.12. fU = U, A ⊆ fA. Correct. Set f(x) = x.
3.13. fU = U, fA ⊆ A. Correct. Set f(x) = x.
3.16. A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A. Correct. Set f(x) = x.
3.19. fA = A. Correct. Set f(x) = x.
4.13. fU = U, fA = A. Correct. Set f(x) = x.

THEOREM 2.3.5. For IBRT in A,fA,fU on (SD,INF) and (ELG ∩ SD,INF), the only correct format is ∅. This is not true of IBRT in A,fA on (ELG,INF),(EVSD,INF),(MF,INF). IBRT in A,fA,fU on (ELG,INF) and (EVSD,INF) have the same correct formats. IBRT in A,fA,fU on (ELG,INF) and on (MF,INF) have different correct formats. IBRT in A,fA,fU on each of (SD,INF),(ELG ∩ SD,INF),(ELG,INF),(EVSD,INF) is RCA_0 secure. IBRT in A,fA,fU on (MF,INF) is ACA' secure, but not ACA_0 secure. Every correct format in A,fA,fU on (MF,INF) is RCA_0 correct. We can replace ACA' here by RCA_0 + Thin Set Theorem.

Proof: The first four claims are immediate from the given tabular classifications. For the fifth claim, it suffices to verify that the incorrectness of formats 2.7,2.10,3.11,3.14,3.15,3.17,3.18, 4.11,4.12,4.14,4.15,5.6 on these four settings is provable in RCA_0. These are the places where we have used Thin Set Theorem. In fact, it suffices to show incorrectness of 2.7 and 2.10 only, within RCA_0. But 2.7 and 2.10 each contain 1.4, which was shown to be incorrect in all four settings by Theorem 2.2.1. IBRT in A,fA,fU on (MF,INF) is ACA' secure since we only use the Thin Set Theorem (variant), which is provable in ACA'. Note that all arguments for IBRT correctness in these settings are very explicit, easily conducted in RCA_0.The last claim is by Theorem 2.2.3. QED

THEOREM 2.3.6. Let k ≥ 2. EBRT in A,fA,fU on SD[k], (ELG ∩ SD)[k], ELG[k], EVSD[k], MF[k], and IBRT in A,fA,fU on SD[k], (ELG ∩ SD)[k], ELG[k], EVSD[k], are RCA_0 secure. IBRT in A,fA,fU on MF[k] is ACA_0 secure. EBRT and IBRT in A,fA on SD[k], (ELG ∩ SD)[k], ELG[k], EVSD[k], MF[k] have the same correct formats as EBRT and IBRT in SD, ELG ∩ SD, ELG, EVSD, MF, respectively.

Proof: An examination of the arguments immediately reveals that all of the incorrectness determinations given for EBRT, and all of the correctness determinations given for IBRT, involve unary and binary functions only. We can obviously pad these unary functions as k-ary functions. It is clear that the Thin Set Theorem (variant) for any fixed k ≥ 1 is provable in ACA_0, since it relies on Ramsey's theorem for a fixed exponent. QED

We now classify EBRT and IBRT in A,fA,fU on (SD[1],INF), (ELG[1] ∩ SD[1],INF), (ELG[1],INF), (EVSD[1],INF), (MF[1],INF). Much of the work is the same, but there are substantial differences that are embodied in the following results.

THEOREM 2.3.7. Let f ∈ ELG[1]. Then N\fN is infinite.

Proof: Let c be a real constant > 1. Let t ≥ 1 be such that for all n ≥ t, f(n) ≥ cn. We show that N\fN is infinite. Note that we are using only the lower bound provided by membership in ELG.

Let r ≥ 0 and s > (r+t+1)/(1 - 1/c). Then $f^{-1}[r,s] \subseteq [0,s/c] \cup [0,t]$. Hence $f^{-1}[r,s]$ has at most s/c + 1+t+1 = t+2 + s/c elements. Hence f assumes at most t+2 + s/c values in [r,s]. But by elementary algebra, t+2 + s/c < s-r+1. Hence f must assume fewer than s-r+1 values in [r,s]. Hence f omits a value in [r,s]. Since r is arbitrary and s can be taken to be a function of r (t,c are fixed), we see that f omits infinitely many values. QED

Contrast Theorem 2.3.7 with Theorem 2.3.3.

LEMMA 2.3.8. No element of EVSD[1] is surjective.

Proof: Let f ∈ EVSD. Let n be such that f is strictly dominating on [n,∞). Then $f^{-1}[0,n] \subseteq [0,n-1]$. By counting, there exists 0 ≤ i ≤ n such that i ∉ fN. QED

Contrast Lemma 2.3.8 with Theorem 2.3.3.

SETTINGS: (SD[1],INF), (ELG[1] ∩ SD[1],INF), (ELG[1],INF), (EVSD[1],INF), (MF[1],INF).

A,fA,fU FORMAT OF CARDINALITY 0
EBRT

The empty format is obviously correct, on all five.

A,fA,fU FORMATS OF CARDINALITY 1
EBRT

1.1. A ∩ fA = ∅.
1.2. A ∪ fU = U. Correct on all five. Set A = N.
1.3. A ⊆ fU.
1.4. fU ⊆ A ∪ fA. Correct on all five. Set A = N.
1.5. A ∩ fU ⊆ fA. Correct on all five. Set A = N.
1.6. fA ⊆ A. Correct on all five. Set A = N.

A,fA,fU FORMATS OF CARDINALITY 2
EBRT

2.1. A ∩ fA = ∅, A ∪ fU = U.
2.2. A ∩ fA = ∅, A ⊆ fU.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA.
2.4. A ∩ fA = ∅, A ∩ fU ⊆ fA. Equivalent on all five to A ∩ fU = ∅.
2.5. A ∩ fA = ∅, fA ⊆ A. Equivalent on all five to fA = ∅. Incorrect on all five. Use any f.
2.6. A ∪ fU = U, A ⊆ fU. Equivalent on all five to fU = U. Incorrect on all five. Set rng(f) ≠ N.
2.7. A ∪ fU = U, fU ⊆ A ∪ fA. Correct on all five. Set A = N.
2.8. A ∪ fU = U, A ∩ fU ⊆ fA. Correct on all five. Set A = N.
2.9. A ∪ fU = U, fA ⊆ A. Correct on all five. Set A = N.
2.10. A ⊆ fU, fU ⊆ A ∪ fA.
2.11. A ⊆ fU, A ∩ fU ⊆ fA. Equivalent on all five to A ⊆ fA. Incorrect on all five. Set f(x) = 2x+1.
2.12. A ⊆ fU, fA ⊆ A.
2.13. fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Correct on all five. Set A = N.
2.14. fU ⊆ A ∪ fA, fA ⊆ A. Correct on all five. Set A = N.

2.15. $A \cap fU \subseteq fA$, $fA \subseteq A$. Correct on all five. Set A = N.

A,fA,fU FORMATS OF CARDINALITY 3
EBRT

3.1. $A \cap fA = \emptyset$, $A \cup fU = U$, $A \subseteq fU$. Incorrect on all five. Contains 2.6.
3.2. $A \cap fA = \emptyset$, $A \cup fU = U$, $fU \subseteq A \cup fA$. Equivalent to $A \cap fA = \emptyset$, $A \cup fA = U$ on all five.
3.3. $A \cap fA = \emptyset$, $A \cup fU = U$, $A \cap fU \subseteq fA$. Equivalent to $A \cap fU = \emptyset$, $A \cup fU = U$ on all five. Equivalent to $A = U\backslash fU$ on all five.
3.4. $A \cap fA = \emptyset$, $A \cup fU = U$, $fA \subseteq A$. Incorrect on all five. Contains 2.5.
3.5. $A \cap fA = \emptyset$, $A \subseteq fU$, $fU \subseteq A \cup fA$.
3.6. $A \cap fA = \emptyset$, $A \subseteq fU$, $A \cap fU \subseteq fA$. Incorrect on all five. Contains 2.11.
3.7. $A \cap fA = \emptyset$, $A \subseteq fU$, $fA \subseteq A$. Incorrect on all five. Contains 2.5.
3.8. $A \cap fA = \emptyset$, $fU \subseteq A \cup fA$, $A \cap fU \subseteq fA$. Equivalent to $A \cap fA = \emptyset$, $fU \subseteq fA$, $A \cap fU = \emptyset$. Incorrect on all five. Set $f(x) = 2x+1$.
3.9. $A \cap fA = \emptyset$, $fU \subseteq A \cup fA$, $fA \subseteq A$. Incorrect on all five. Contains 2.5.
3.10. $A \cap fA = \emptyset$, $A \cap fU \subseteq fA$, $fA \subseteq A$. Incorrect on all five. Contains 2.5.
3.11. $A \cup fU = U$, $A \subseteq fU$, $fU \subseteq A \cup fA$. Incorrect on all five. Contains 2.6.
3.12. $A \cup fU = U$, $A \subseteq fU$, $A \cap fU \subseteq fA$. Incorrect on all five. Contains 2.6.
3.13. $A \cup fU = U$, $A \subseteq fU$, $fA \subseteq A$. Incorrect on all five. Contains 2.6.
3.14. $A \cup fU = U$, $fU \subseteq A \cup fA$, $A \cap fU \subseteq fA$. Correct on all five. Set A = N.
3.15. $A \cup fU = U$, $fU \subseteq A \cup fA$, $fA \subseteq A$. Correct on all five. Set A = N.
3.16. $A \cup fU = U$, $A \cap fU \subseteq fA$, $fA \subseteq A$. Correct on all five. Set A = N.
3.17. $A \subseteq fU$, $fU \subseteq A \cup fA$, $A \cap fU \subseteq fA$. Incorrect on all five. Contains 2.11.
3.18. $A \subseteq fU$, $fU \subseteq A \cup fA$, $fA \subseteq A$.
3.19. $A \subseteq fU$, $A \cap fU \subseteq fA$, $fA \subseteq A$. Incorrect on all five. Contains 2.11.
3.20. $fU \subseteq A \cup fA$, $A \cap fU \subseteq fA$, $fA \subseteq A$. Correct on all five. Set A = N.

A,fA,fU FORMATS OF CARDINALITY 4

EBRT

4.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA. Incorrect on all five. Contains 2.6.
4.2. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.6.
4.3. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.4. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Equivalent to A = U\fU on all five. Same as 3.3 on all five.
4.5. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.6. A ∩ fA = ∅, A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.7. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.11.
4.8. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.9. A ∩ fA = ∅, A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.10. A ∩ fA = ∅, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
4.11. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.6.
4.12. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.6.
4.13. A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.6.
4.14. A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Correct on all five. Set A = N.
4.15. A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.11.

A,fA,fU FORMATS OF CARDINALITY 5
EBRT

5.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA. Incorrect on all five. Contains 2.6.
5.2. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
5.3. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
5.4. A ∩ fA = ∅, A ∪ fU = U, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.
5.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.

5.6. A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.6.

A,fA,fU FORMATS OF CARDINALITY 6
EBRT

6.1. A ∩ fA = ∅, A ∪ fU = U, A ⊆ fU, fU ⊆ A ∪ fA, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on all five. Contains 2.5.

We now list all of the formats whose status has not been determined. We use any stated equivalences that hold on all five.

1.1. A ∩ fA = ∅.
1.3. A ⊆ fU.
2.1. A ∩ fA = ∅, A ∪ fU = U.
2.2. A ∩ fA = ∅, A ⊆ fU.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA.
2.4. A ∩ fU = ∅.
2.12. A ⊆ fU, fA ⊆ A.
3.2. A ∩ fA = ∅, A ∪ fA = U.
3.3. A = U\fU.
3.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA.
3.18. A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A.

We now settle the status of each of these formats on the various settings.

EBRT in A,fA,fU on (SD[1],INF),(ELG[1] ∩ SD[1],INF)

1.1. A ∩ fA = ∅. Correct on both. Theorem 2.2.1.
1.3. A ⊆ fU. Correct on both. Set A = fN.
2.1. A ∩ fA = ∅, A ∪ fU = U. Correct on both. Complementation Theorem.
2.2. A ∩ fA = ∅, A ⊆ fU. Correct on both. Theorem 2.2.1.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA. Correct on both. Complementation Theorem.
2.4. A ∩ fU = ∅. Incorrect on (SD[1],INF). Set f(x) = x+1. Correct on (ELG[1] ∩ SD[1],INF). Theorem 2.3.7.
2.12. A ⊆ fU, fA ⊆ A. Correct on both. Set A = fN.
3.2. A ∩ fA = ∅, A ∪ fA = U. Correct on both. Complementation Theorem.
3.3. A = U\fU. Incorrect on (SD[1],INF). Set f(x) = x+1. Correct on (ELG[1] ∩ SD[1],INF). Theorem 2.3.7.
3.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA. Correct on both. Theorem 2.3.1 with B = fN.

EBRT in A,fA,fU on (ELG[1],INF),(EVSD[1],INF)

1.1. A ∩ fA = ∅. Correct on both. Theorem 2.2.1.
1.3. A ⊆ fU. Correct on both. Set A = fN.
2.1. A ∩ fA = ∅, A ∪ fU = U. Correct on both. Theorem 2.3.2.
2.2. A ∩ fA = ∅, A ⊆ fU. Correct on both. Theorem 2.2.1.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA. Incorrect on both. Set f(x) = 2x.
2.4. A ∩ fU = ∅. Incorrect on (EVSD[1],INF). Set f(x) = x+1. Correct on (ELG[1],INF). Theorem 2.3.7.
3.2. A ∩ fA = ∅, A ∪ fA = U. Incorrect on both. Set f(x) = 2x.
3.3. A = N\fU. Incorrect on (EVSD[1],INF). Set f(x) = x+1. Correct on (ELG[1],INF). Theorem 2.3.7.
3.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA. Incorrect on both. Set f(x) = 2x.
3.18. A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Correct on both. Set A = fN.

EBRT in A,fA,fU on (MF[1],INF)

1.1. A ∩ fA = ∅. Incorrect. Set f(x) = x.
1.3. A ⊆ fU. Incorrect. Set f(x) = 0.
2.1. A ∩ fA = ∅, A ∪ fU = U. Incorrect. Set f(x) = x.
2.2. A ∩ fA = ∅, A ⊆ fU. Incorrect. Set f(x) = x.
2.3. A ∩ fA = ∅, fU ⊆ A ∪ fA. Incorrect. Set f(x) = x.
2.4. A ∩ fU = ∅. Incorrect. Set f(x) = x.
2.12. A ⊆ fU, fA ⊆ A. Incorrect. Set f(x) = 0.
3.2. A ∩ fA = ∅, A ∪ fA = U. Incorrect. Set f(x) = x.
3.3. A = N\fU. Incorrect. Set f(x) = x.
3.5. A ∩ fA = ∅, A ⊆ fU, fU ⊆ A ∪ fA. Incorrect. Set f(x) = x.
3.18. A ⊆ fU, fU ⊆ A ∪ fA, fA ⊆ A. Incorrect. Set f(x) = 0.

THEOREM 2.3.9. EBRT in A,fA,fU on the ten BRT settings (SD,INF), (ELG ∩ SD,INF), (ELG,INF), (EVSD,INF), (MF,INF). (SD[1],INF), (ELG[1] ∩ SD[1],INF), (ELG[1],INF), (EVSD[1],INF), (MF[1],INF), are RCA_0 secure. They also have different correct formats, with the following exceptions. (SD,INF), (ELG ∩ SD,INF), (SD[1],INF) have the same; (ELG,INF), (EVSD,INF), (EVSD[1],INF) have the same; (MF,INF), (MF[1],INF) have the same. In particular, (SD[1],INF), (ELG[1] ∩ SD[1],INF), (ELG[1],INF), (EVSD[1],INF), (MF[1],INF), all differ on EBRT in A,fA,fU.

Proof: Our entire analysis of EBRT in this section takes place in RCA_0. To compare the multivariate settings with the unary settings, we have only to examine where we use a function that is not unary for an incorrectness determination in the multivariate setting.

(SD,INF), (SD[1],INF). In 2.4, 3.3, 4.4, we use Theorem 2.3.3, which involves functions that are not unary. However, we can instead use f(x) = x+1, which lies in SD[1].

(EVSD,INF), (EVSD[1],INF). In 2.4, 3.3, 4.4, we use Theorem 2.3.3, which involves functions that are not unary. However, we can instead use f(x) = x+1, which lies in EVSD[1].

(MF,INF), (MF[1],INF). In 2.4, 3.3, 4.4, we use Theorem 2.3.3, which involves functions that are not unary. However, we can instead use f(x) = x+1, which lies in MF[1].

It suffices to verify that EBRT in A,fA,fU pairwise differ on

(SD,INF).
(ELG,INF).
(MF,INF).
(ELG[1] ∩ SD[1],INF).
(ELG[1],INF)

(ELG[1] ∩ SD[1],INF) and (ELG[1],INF) both differ from (SD,INF), (ELG,INF), (MF,INF) at 2.4. (ELG[1] ∩ SD[1],INF) and (ELG[1],INF) differ at 2.3. From Theorem 2.3.4, we know that (SD,INF), (ELG,INF), (MF,INF) differ. QED

We now come to IBRT in the five unary settings. First note that in the earlier table of formats of cardinalities 0-6 on IBRT in A,fA,fU, compiled earlier, the only determinations were of incorrectness. Obviously those determinations still apply. So we can jump ahead to where we list the formats that remain undetermined:

1.2. A ∪ fU = U.
1.3. A ⊆ fU.
1.4. fU ⊆ A ∪ fA.
1.5. A ∩ fU ⊆ fA.
1.6. fA ⊆ A.
2.6. fU = U.
2.8. A ∪ fU = U, A ∩ fU ⊆ fA.
2.9. A ∪ fU = U, fA ⊆ A.
2.11. A ⊆ fA.

2.12. A ⊆ fU, fA ⊆ A.
2.13. fU = fA.
2.15. A ∩ fU ⊆ fA, fA ⊆ A.
3.12. fU = U, A ⊆ fA.
3.13. fU = U, fA ⊆ A.
3.16. A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A.
3.19. fA = A.
4.13. fU = U, fA = A.

We now determine the status of the above formats on the five unary settings.

IBRT in A,fA,fU on (SD[1],INF),(ELG[1] ∩ SD[1],INF)

Since the only correct format for IBRT in A,fA,fU on (SD[1],INF), (ELG[1] ∩ SD[1],INF) is ∅, the only correct format for IBRT in A,fA,fU on (SD,INF), (ELG ∩ SD,INF) is ∅.

IBRT in A,fA,fU on (ELG[1],INF),(EVSD[1],INF)

1.2. A ∪ fU = U. Incorrect on both. Lemma 2.3.8.
1.3. A ⊆ fU. Incorrect on both. Lemma 2.3.8.
1.4. fU ⊆ A ∪ fA. Incorrect on both. Theorem 2.2.1.
1.5. A ∩ fU ⊆ fA. Incorrect on both. FIX!!! Use Theorem 2.2.1 with D = fN. Obtain infinite A disjoint from fA, where fN ¬⊆ A ∪ fA. If A ∩ fN ⊆ fA then fN ⊆ fA.
1.6. fA ⊆ A. Incorrect on both. Theorem 2.2.1.
2.6. fU = U. Incorrect on both. Lemma 2.3.8.
2.8. A ∪ fU = U, A ∩ fU ⊆ fA. Incorrect on both. Contains 1.5.
2.9. A ∪ fU = U, fA ⊆ A. Incorrect on both. Contains 1.6.
2.11. A ⊆ fA. Incorrect on both. Theorem 2.2.1.
2.12. A ⊆ fU, fA ⊆ A. Incorrect on both. Contains 1.6.
2.13. fU = fA. Incorrect on both. Use Theorem 2.2.1 with D = fU.
2.15. A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on both. Contains 1.6.
3.12. fU = U, A ⊆ fA. Incorrect on both. Contains 2.11.
3.13. fU = U, fA ⊆ A. Incorrect on both. Contains 1.6.
3.16. A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A. Incorrect on both. Contains 1.6.
3.19. fA = A. Incorrect on both. See 1.6.
4.13. fU = U, fA = A. Incorrect on both. See 1.6.

We now see that in IBRT on SD[1],INF), (ELG[1] ∩ SD[1],INF), (ELG[1],INF), (EVSD[1],INF), every format is incorrect.

IBRT in A,fA,fU on (MF[1],INF)

1.2. A ∪ fU = U. Correct. Set f(x) = x.
1.3. A ⊆ fU. Correct. Set f(x) = x.
1.4. fU ⊆ A ∪ fA. Correct. Set f(x) = 0.
1.5. A ∩ fU ⊆ fA. Correct. Set f(x) = x.
1.6. fA ⊆ A. Correct. Set f(x) = x.
2.6. fU = U. Correct. Set f(x) = x.
2.8. A ∪ fU = U, A ∩ fU ⊆ fA. Correct. Set f(x) = x.
2.9. A ∪ fU = U, fA ⊆ A. Correct. Set f(x) = x.
2.11. A ⊆ fA. Correct. Set f(x) = x.
2.12. A ⊆ fU, fA ⊆ A. Correct. Set f(x) = x.
2.13. fU = fA. Correct. Set f(x) = 0.
2.15. A ∩ fU ⊆ fA, fA ⊆ A. Correct. Set f(x) = x.
3.12. fU = U, A ⊆ fA. Correct. Set f(x) = x.
3.13. fU = U, fA ⊆ A. Correct. Set f(x) = x.
3.16. A ∪ fU = U, A ∩ fU ⊆ fA, fA ⊆ A. Correct. Set f(x) = x.
3.19. fA = A. Correct. Set f(x) = x.
4.13. fU = U, fA = A. Correct. Set f(x) = x.

THEOREM 2.3.10. IBRT in A,fA,fU on (SD,INF), (ELG ∩ SD,INF), (SD[1],INF),(ELG[1] ∩ SD[1],INF), (ELG[1],INF), (EVSD[1],INF), (SD[1],INF), (ELG[1] ∩ SD[1],INF) have only the correct format ∅. IBRT in A,fA,fU on (MF,INF) and (MF[1],INF) have the same correct formats. IBRT in A,fA,fU on (SD[1],INF), (ELG[1] ∩ SD[1],INF), (ELG[1],INF), (EVSD[1],INF), (MF[1],INF) are RCA_0 secure.

Proof: By inspection. Also, Thin Set Theorem (variant) is provable in RCA_0 by Lemma 2.2.4 QED

Note that by Theorem 2.3.10, there are exactly five different behaviors of the ten BRT settings (SD,INF), (ELG ∩ SD,INF), (ELG,INF), (EVSD,INF), (MF,INF). (SD[1],INF), (ELG[1] ∩ SD[1],INF), (ELG[1],INF), (EVSD[1],INF), (MF[1],INF) under EBRT in A,fA,fU. By Theorem 2.3.10, there are three under IBRT in A,fA,fU.

2.4. EBRT in A,B,fA,fB,⊆ on (SD,INF).

In this section, we use the tree methodology described in section 2.1 to classify EBRT in A,B,fA,fB,⊆ on (SD,INF) and (ELG ∩ SD,INF). We handle both BRT settings at once, as they behave the same way for EBRT in A,B,fA,fB,⊆. In particular, we show that they are RCA_0 secure (see Definition 1.1.43).

We begin with a list of five Lemmas that we will need for documenting the classification.

LEMMA 2.4.1. Let f ∈ SD. There exist infinite A ⊆ B ⊆ N such that B ∪. fA = N and A = B ∩ fB.

Proof: By the BRT Fixed Point Theorem, section 1.3, let A be the unique A ⊆ N such that A = N\fA ∩ f(N\fA). Let B = N\fA. Clearly A ⊆ B and B ∪. fA = N. Also B ∩ fB = N\fA ∩ f(N\fA) = A.

Suppose A is finite. Then N\fA is cofinite and f(N\fA) is infinite. Hence their intersection is infinite, and so A is infinite. So we conclude that A is infinite. QED

LEMMA 2.4.2. Let f ∈ SD. There exist infinite A ⊆ B ⊆ N such that A ∪. fB = N, fA ⊆ B, and B ∩ fB ⊆ fA.

Proof: By the BRT Fixed Point Theorem, section 1.3, let B be the unique B ⊆ N such that B = N\fB ∪ f(N\fB). Let A = N\fB. Then A ⊆ B, fA ⊆ B. Now B ∩ fB = (N\fB ∪ f(N\fB)) ∩ fB = f(N\fB) ∩ fB ⊆ fA. Suppose A is finite. Then B = A ∪ fA is finite. Hence N\fB = A is infinite, which is a contradiction. Hence A is infinite. Therefore fA,B are infinite. QED

The following is a sharpening of the Complementation Theorem.

LEMMA 2.4.3. Let f ∈ SD and X ⊆ N. There exists a unique A such that A ⊆ X ⊆ A ∪. fA.

Proof: We will give a direct argument from scratch. Let f,X be as given. Define membership in A inductively as follows. Suppose membership in A for 0,...,n-1 has been defined. Define n ∈ A if and only if n ∈ X and n ∉ fA thus far. The construction is unique. QED

LEMMA 2.4.4. The following is false. For all f ∈ ELG ∩ SD there exist infinite A ⊆ B ⊆ N such that A ∩ fB = ∅ and fB ⊆ B.

Proof: Let f be given by Lemma 3.2.1, and let A ⊆ B ⊆ N, A ∩ fB = ∅, and fB ⊆ B, where A is infinite. Just using fB ⊆

B, B ≠ ∅, we see that fB is cofinite, and hence A is finite. This is the desired contradiction. QED

LEMMA 2.4.5. Let f ∈ SD. There is no nonempty A ⊆ N such that A ⊆ fA.

Proof: Let n be the least element of A. Then n ∉ fA. QED

Note that in the proofs of Lemmas 2.4.1, 2.4.2, 2.4.3, 2.4.5, we never used the fact that f is everywhere defined. Hence these Lemmas hold even for partially defined f. We will use Lemma 2.4.2 for partial f in section 2.5.

The 16 A,B,fA,fB pre elementary inclusions are as follows (see Definition 1.1.35).

A ∩ B ∩ fA ∩ fB = ∅.
A ∪ B ∪ fA ∪ fB = N.
A ⊆ B ∪ fA ∪ fB.
B ⊆ A ∪ fA ∪ fB.
fA ⊆ A ∪ B ∪ fB.
fB ⊆ A ∪ B ∪ fA.
A ∩ B ⊆ fA ∪ fB.
A ∩ fA ⊆ B ∪ fB.
A ∩ fB ⊆ B ∪ fA.
B ∩ fA ⊆ A ∪ fB.
B ∩ fB ⊆ A ∪ fA.
fA ∩ fB ⊆ A ∪ B.
A ∩ B ∩ fA ⊆ fB.
A ∩ B ∩ fB ⊆ fA.
A ∩ fA ∩ fB ⊆ B.
B ∩ fA ∩ fB ⊆ A.

The 9 A,B,fA,fB,⊆ elementary inclusions are as follows (see Definition 1.1.37).

A ∩ fA = ∅.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
A ⊆ fB.
B ∩ fB ⊆ A ∪ fA.
fA ⊆ B.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.

Our classification provides a determination of the subsets S of the above nine inclusions for which

$(\forall f \in SD)(\exists A \subseteq B$ from $INF)(S)$
$(\forall f \in ELG \cap SD)(\exists A \subseteq B$ from $INF)(S)$

holds, where S is interpreted conjunctively.

We now build an RCA_0 classification for α (see Definition 2.1.9), where α is the BRT fragment: EBRT in A,B,fA,fB,$\subseteq$ on (SD,INF).

Recall that RCA_0 classifications for α are trees whose vertices are labeled with worklists. Our presentation of such trees in text, presents each vertex with a numerical label and the worklist label. (There are two special exceptions to this - see two paragraphs down).

The numerical label consists of finite sequences of small positive integers, in lexicographic order, reflecting the tree structure. The worklist label is presented as a list of elementary inclusions, where the items in the first part of the worklist end with colons, and the items in the second part of the worklist end with periods.

We begin with the presentation of the root of the classification tree, which does not have a numerical label, but instead has a label stating the BRT fragment(s) we are classifying. Its worklist label is a list of the elementary inclusions. It is immediately followed by the unique son of the root, with the same non numerical label appending with *, and its worklist label is a permutation of the list of the elementary inclusions. Note that these elementary inclusions end with periods because the first part of the worklist is empty.

If a presented vertex is terminal, then it must be documented that it is entirely α,T correct, in the sense that the format obtained by ignoring the colons of the worklist is α,T correct.

If a worklist has numerical label $n_1.n_2. \ldots n_k.$, then either this worklist is terminal (no sons), or it has a unique son labeled $n_1.n_2. \ldots n_k.*$. In the latter case, there is a documented α,RCA_0 reduction from the former's worklist to the latter's worklist (see Definition 2.1.5).

If a worklist is labeled $n_1.n_2. \ldots n_k.*$, then it is either terminal, or has one or more sons, none of which end with *. The worklist of the last son is terminal.

The symbols # k that appear right under the label of a vertex with a starred label indicates the number of sons. These # k are placed under the numerical label.

We begin with the root worklist. It consists of the 9 A,B,fA,fB,⊆ elementary inclusions above.

The root worklist is followed by an α,RCA_0 reduction, which permutes the entries in a perhaps strategic way. This starred worklist has five sons, as indicated by # 5.

EBRT in A,B,fA,fB,⊆ on (SD,INF), (ELG ∩ SD,INF).

A ∩ fA = ∅.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
A ⊆ fB.
B ∩ fB ⊆ A ∪ fA.
fA ⊆ B.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.

EBRT in A,B,fA,fB,⊆ on (SD,INF), (ELG ∩ SD,INF).*
5

A ∩ fA = ∅.
B ∪ fB = N.
fA ⊆ B.
A ⊆ fB.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 1.

A ∩ fA = ∅:
B ∪ fB = N.
fA ⊆ B.
A ⊆ fB.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA. A ∩ fB = ∅.
B ∩ fA ⊆ A. B ∩ fA = ∅.
B ∩ fB ⊆ A ∪ fA.

LIST 1*.
5

A ∩ fA = ∅:
B ∩ fA = ∅.
A ∩ fB = ∅.
fA ⊆ B.
A ⊆ fB.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA.

LIST 1.1.

A ∩ fA = ∅:
B ∩ fA = ∅:
A ∩ fB = ∅.
fA ⊆ B. B ∩ fA = fA = ∅. No.
A ⊆ fB.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA. B ∩ fB ⊆ A.

LIST 1.1.*
3

A ∩ fA = ∅:
B ∩ fA = ∅:
A ∩ fB = ∅.
A ⊆ fB.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A.

LIST 1.1.1.

A ∩ fA = ∅:
B ∩ fA = ∅:
A ∩ fB = ∅:
A ⊆ fB. No.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A. B ∩ fB = ∅.

LIST 1.1.1.*
0

A ∩ fA = ∅:
B ∩ fA = ∅:
A ∩ fB = ∅:
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB = ∅.

Entirely RCA_0 correct. By the Complementation Theorem, let A ∪. fA = N. Set B = A.

LIST 1.1.2.

A ∩ fA = ∅:
B ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N.
B ⊆ A ∪ fB. B ⊆ fB. No. Lemma 2.4.5.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A.

LIST 1.1.2.*
0

A ∩ fA = ∅:
B ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A.

Entirely RCA_0 correct. By Lemma 2.4.1, let A ⊆ B ⊆ N, B ∪. fA = N, A = B ∩ fB.

LIST 1.1.3.

A ∩ fA = ∅:
B ∩ fA = ∅:
B ∪ fB = N:
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A.

Entirely RCA_0 correct. By the Complementation Theorem, let A ∪. fA = N. Set B = A.

LIST 1.2.

A ∩ fA = ∅:
A ∩ fB = ∅:
fA ⊆ B.
A ⊆ fB. No.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA. B ∩ fB ⊆ fA.

LIST 1.2.*
2

A ∩ fA = ∅:
A ∩ fB = ∅:
fA ⊆ B.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ fA.

LIST 1.2.1.

A ∩ fA = ∅:
A ∩ fB = ∅:
fA ⊆ B:
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA. fB ⊆ B. No. Lemma 2.4.4.
B ∩ fB ⊆ fA.

LIST 1.2.1.*
0

A ∩ fA = ∅:
A ∩ fB = ∅:
fA ⊆ B:
B ∪ fB = N.
B ⊆ A ∪ fB.
B ∩ fB ⊆ fA.

Entirely RCA_0 correct. By Lemma 2.4.2, let A ⊆ B ⊆ N, A ∪. fB = N, fA ⊆ B, B ∩ fB ⊆ fA.

LIST 1.2.2.

A ∩ fA = ∅:
A ∩ fB = ∅:
B ∪ fB = N:
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ fA.

Entirely RCA_0 correct. By the Complementation Theorem, let A ∪. fA = N. Set B = A.

LIST 1.3.

A ∩ fA = ∅:
fA ⊆ B:
A ⊆ fB.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA. fB ⊆ B.
B ∩ fB ⊆ A ∪ fA.

LIST 1.3.*
2

A ∩ fA = ∅:
fA ⊆ B:
A ⊆ fB.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B.
B ∩ fB ⊆ A ∪ fA.

LIST 1.3.1.

A ∩ fA = ∅:
fA ⊆ B:
A ⊆ fB:
B ∪ fB = N.
B ⊆ A ∪ fB. B ⊆ fB. No. Lemma 2.4.5.
fB ⊆ B.
B ∩ fB ⊆ A ∪ fA.

LIST 1.3.1.*
0

A ∩ fA = ∅:
fA ⊆ B:

A ⊆ fB:
B ∪ fB = N.
fB ⊆ B.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. By Lemma 2.4.3, let A ⊆ fN ⊆ A ∪. fA. Set B = N.

LIST 1.3.2.

A ∩ fA = ∅:
fA ⊆ B:
B ∪ fB = N:
B ⊆ A ∪ fB.
fB ⊆ B.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. By the Complementation Theorem, let A ∪. fA = N. Set B = N.

LIST 1.4.

A ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N.
B ⊆ A ∪ fB. B ⊆ fB. No. Lemma 2.4.5.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA.

LIST 1.4.*
0

A ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. By Lemma 2.4.3, let A ⊆ fN ⊆ A ∪. fA. Set B = N.

LIST 1.5.

A ∩ fA = ∅:
B ∪ fB = N:
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. By the Complementation Theorem, let A ∪. fA = N. Set B = A.

LIST 2.

B ∪ fB = N:
fA ⊆ B.
A ⊆ fB.
B ⊆ A ∪ fB. A ∪ fB = N.
fB ⊆ B ∪ fA. B ∪ fA = N.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.*
2

B ∪ fB = N:
A ⊆ fB.
fA ⊆ B.
A ∪ fB = N.
B ∪ fA = N.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.1.

B ∪ fB = N:
A ⊆ fB:
fA ⊆ B.
A ∪ fB = N. fB = N. No. Lemma 2.4.5.
B ∪ fA = N.
A ∩ fB ⊆ fA. A ⊆ fA. No. Lemma 2.4.5.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.1.*
2

B ∪ fB = N:
A ⊆ fB:
fA ⊆ B.
B ∪ fA = N.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.1.1.

B ∪ fB = N:
A ⊆ fB:
fA ⊆ B:
B ∪ fA = N. B = N.
B ∩ fA ⊆ A. fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.1.1.*
0

B ∪ fB = N:
A ⊆ fB:
fA ⊆ B:
B = N.
fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = fN, B = N.

LIST 2.1.2.

B ∪ fB = N:
A ⊆ fB:
B ∪ fA = N:
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Let B = N, A = fN.

LIST 2.2.

B ∪ fB = N:
fA ⊆ B:
A ∪ fB = N.
B ∪ fA = N.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = B = N.

LIST 3.

fA ⊆ B:
A ⊆ fB.
B ⊆ A ∪ fB.

fB ⊆ B ∪ fA. fB ⊆ B.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A. fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 3*.
3

fA ⊆ B:
fA ⊆ A.
A ⊆ fB.
B ⊆ A ∪ fB.
fB ⊆ B.
A ∩ fB ⊆ fA.
B ∩ fB ⊆ A ∪ fA.

LIST 3.1.

fA ⊆ B:
fA ⊆ A:
A ⊆ fB.
B ⊆ A ∪ fB.
fB ⊆ B.
A ∩ fB ⊆ fA.
B ∩ fB ⊆ A ∪ fA. B ∩ fB ⊆ A.

LIST 3.1.*
2

fA ⊆ B:
fA ⊆ A:
A ⊆ fB.
B ⊆ A ∪ fB.
fB ⊆ B.
A ∩ fB ⊆ fA.
B ∩ fB ⊆ A.

LIST 3.1.1.

fA ⊆ B:
fA ⊆ A:
A ⊆ fB:
B ⊆ A ∪ fB. B ⊆ fB. No. Lemma 2.4.5.
fB ⊆ B.
A ∩ fB ⊆ fA. A ⊆ fA. No. Lemma 2.4.5.
B ∩ fB ⊆ A.

LIST 3.1.1.*

0

fA ⊆ B:
fA ⊆ A:
A ⊆ fB:
fB ⊆ B.
B ∩ fB ⊆ A.

Entirely RCA_0 correct. Set A = fN, B = N.

LIST 3.1.2.

fA ⊆ B:
fA ⊆ A:
B ⊆ A ∪ fB:
fB ⊆ B.
A ∩ fB ⊆ fA.
B ∩ fB ⊆ A.

Entirely RCA_0 correct. Set A = B = N.

LIST 3.2.

fA ⊆ B:
A ⊆ fB:
B ⊆ A ∪ fB. B ⊆ fB. No. Lemma 2.4.5.
fB ⊆ B.
A ∩ fB ⊆ fA. A ⊆ fA. No. Lemma 2.4.5.
B ∩ fB ⊆ A ∪ fA.

LIST 3.2.*
0

fA ⊆ B:
A ⊆ fB:
fB ⊆ B.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = fN, B = N.

LIST 3.3.

fA ⊆ B:
B ⊆ A ∪ fB:
fB ⊆ B.
A ∩ fB ⊆ fA.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = B = N.

LIST 4.

A ⊆ fB:
B ⊆ A ∪ fB. B ⊆ fB. No. Lemma 2.4.5.
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA. A ⊆ fA. No. Lemma 2.4.5.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 4.*
0

A ⊆ fB:
fB ⊆ B ∪ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = fN, B = N.

LIST 5.

B ⊆ A ∪ fB:
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = B = N.

THEOREM 2.4.6. EBRT in A,B,fA,fB,⊆ on (SD,INF) and (ELG ∩ SD,INF) have the same correct formats. EBRT in A,B,fA,fB,⊆ on (SD,INF) and (ELG ∩ SD,INF) are RCA_0 secure.

Proof: We have presented an RCA_0 classification of EBRT in A,B,fA,fB,⊆ on (SD,INF), (ELG ∩ SD,INF) in the sense of the tree methodology of section 2.1. All of the documentation works equally well on (SD,INF) and (ELG ∩ SD,INF), and we have remained within RCA_0. QED

THEOREM 2.4.7. There are at most 18 maximally α correct α formats, where α is EBRT in A,B,fA,fB,⊆ on (SD,INF), (ELG ∩ SD,INF).

Proof: Here is the list of numerical labels of terminal vertices in the RCA_0 classification of EBRT in A,B,fA,fB,⊆ on (SD,INF), (ELG ∩ SD,INF) given above:

1.1.1.*
1.1.2.*
1.1.3.
1.2.1.*
1.2.2.
1.3.1.*
1.3.2.
1.4.*
1.5.
2.1.1.*
2.1.2.
2.2.
3.1.1.*
3.1.2.
3.2.*
3.3.
4.*
5.
The count is 18. Apply Theorem 2.1.5. QED

2.5. EBRT in A,B,fA,fB,⊆ on (ELG,INF).

In this section, we use the tree methodology described in section 2.1 to analyze EBRT in A,B,fA,fB,⊆ on (ELG,INF) and (EVSD,INF). We handle both BRT settings at once, as they behave the same way for EBRT in A,B,fA,fB,⊆. In particular, we show that they are RCA_0 secure (see Definition 1.1.43).

Some of this treatment is the same as for EBRT in A,B,fA,fB,⊆ on (SD,INF) given in section 2.4. However, many new features appear that makes this section considerably more involved than section 2.4.

A key difference between EBRT in A,B,fA,fB,⊆ on (SD,INF) and on (ELG,INF) is that the Compelmentation Theorem holds on (SD,INF), yet fails on (ELG,INF). E.g., it fails for f(x) = 2x.

Let $f:N^k \to N$ be partial. Define the following series of sets by induction i ≥ 1.

$$S_1 = N.$$
$$S_{i+1} = N\setminus fS_i.$$

LEMMA 2.5.1. $S_2 \subseteq S_4 \subseteq S_6 \subseteq \ldots \subseteq \ldots \subseteq S_5 \subseteq S_3 \subseteq S_1$. I.e., for all i ≥ 1, $S_{2i} \subseteq S_{2i+2} \subseteq S_{2i+1} \subseteq S_{2i-1}$.

Proof: We argue by induction on $i \geq 1$. The basis case is

$$S_2 \subseteq S_4 \subseteq S_3 \subseteq S_1.$$

To see this, clearly

$S_3 \subseteq S_1$.
$N\backslash S_1 \subseteq N\backslash S_3$.
$S_2 \subseteq S_4$.
$S_2 \subseteq S_1$.
$N\backslash S_1 \subseteq N\backslash S_2$.
$S_2 \subseteq S_3$.
$fS_2 \subseteq fS_3$.
$N\backslash fS_3 \subseteq N\backslash fS_2$.
$S_4 \subseteq S_3$.

Now assume the induction hypothesis

$$S_{2i} \subseteq S_{2i+2} \subseteq S_{2i+1} \subseteq S_{2i-1}.$$

Then

$$fS_{2i} \subseteq fS_{2i+2} \subseteq fS_{2i+1} \subseteq fS_{2i-1}.$$
$$N\backslash fS_{2i-1} \subseteq N\backslash fS_{2i+1} \subseteq N\backslash fS_{2i+2} \subseteq N\backslash fS_{2i}.$$
$$S_{2i} \subseteq S_{2i+2} \subseteq S_{2i+3} \subseteq S_{2i+1}.$$
$$fS_{2i} \subseteq fS_{2i+2} \subseteq fS_{2i+3} \subseteq fS_{2i+1}.$$
$$N\backslash fS_{2i+1} \subseteq N\backslash fS_{2i+3} \subseteq N\backslash fS_{2i+2} \subseteq N\backslash fS_{2i}.$$
$$S_{2i+2} \subseteq S_{2i+4} \subseteq S_{2i+3} \subseteq S_{2i+1}.$$

QED

LEMMA 2.5.2. Let $f:N^k \to N$ be partial, where each $f^{-1}(n)$ is finite. Let $A = S_2 \cup S_4 \cup \ldots$, and $B = S_1 \cap S_3 \cap \ldots$. Then $A \subseteq B$, $A = N\backslash fB$, $B = N\backslash fA$.

Proof: Let A,B be as given. By Lemma 2.5.1, $A \subseteq B$.

Fix $i \geq 1$. S2i = N\fS2i-1, S2i $\cap$ fS2i-1 = $\emptyset$, S2i $\cap$ fB = $\emptyset$. Since $i \geq 1$ is arbitrary, $A \cap fB = \emptyset$. I.e., $A \subseteq N\backslash fB$.

Since $S_{2i+1} = N\backslash fS_{2i}$, we see that for all $j \geq i$, $S_{2i+1} \cap fS_{2j} = \emptyset$. Hence $S_{2i+1} \cap fA = \emptyset$. Since $i \geq 1$ is arbitrary, $B \cap fA = \emptyset$. I.e., $B \subseteq N\backslash fA$.

Now let $n \in N\backslash fB$. We claim that for some $j \geq 0$, $n \notin fS_{2j+1}$. Suppose that for all $j \geq 0$, $n \in fS_{2j+1}$. Since $f^{-1}(n)$ is finite, there exists $x \in f^{-1}(n)$ which lies in infinitely many S_{2j+1}. Hence there exists $x \in f^{-1}(n)$ such that $x \in B$. Therefore $n \in fB$. This establishes the claim. Fix $j \geq 0$ such that $n \notin fS_{2j+1}$. Then $n \in S_{2j+2}$, and so $n \in A$. This establishes that $A = N\backslash fB$.

Finally, let $n \in N\backslash fA$. Then for all i, $n \notin fS_{2i}$. Hence for all j, $n \in S_{2j+1}$. Therefore $n \in B$. This estabslihes that $B = N\backslash fA$. QED

LEMMA 2.5.3. Let $f:[0,n]^k \to [0,n]$ be partial, $n \geq 0$. There exist $A \subseteq B \subseteq [0,n]$ such that $A = [0,n]\backslash fB$ and $B = [0,n]\backslash fA$.

Proof: Let n,f be as given. Obviously f:Nk → N is partial, and each f-1(n) is finite. By Lemma 2.5.2, let $A = S_2 \cup S_4 \cup \ldots$, and $B = S_1 \cap S_3 \cap \ldots$. Then $A \subseteq B$, $A = N\backslash fB$, $B = N\backslash fA$. Note that $A \cap [0,n] \subseteq B \cap [0,n]$, $A \cap [0,n] = [0,n]\backslash fB$, $B \cap [0,n]\backslash fA$. QED

LEMMA 2.5.4. For all $f \in$ EVSD there exist infinite $A \subseteq B \subseteq N$ such that $B \cup. fA = A \cup fB = N$.

Proof: Let $f \in$ EVSD. Let $n \geq 1$ be such that $|x| \geq n \to f(x) > |x|$. Let f′ be the restriction of f to those elements of $[0,n-1]^k$ whose value lies in $[0,n-1]$. Then $f':[0,n-1]^k \to [0,n-1]$ is partial.

By Lemma 2.5.3, let $A' \subseteq B' \subseteq [0,n-1]$, where $A' = [0,n-1]\backslash f'B'$ and $B' = [0,n-1]\backslash f'A'$.

We now define the required A,B by induction. Membership in A,B for $m < n$ is just membership in A′,B′. Thus for all $m < n$,

$$m \in B \leftrightarrow m \in B' \leftrightarrow m \notin f'A' \leftrightarrow m \notin fA.$$
$$m \in A \leftrightarrow m \in A' \leftrightarrow m \notin f'B' \leftrightarrow m \notin fB.$$

Now suppose membership in A,B has been defined for all $0 \leq i < m$, where $m \geq n$, and we have $A \subseteq B$ thus far.

case 1. $m \notin fA$ thus far. Put $m \in A,B$.
case 2. $m \in fA$ thus far. Put $m \notin A,B$.

This defines membership of m in A,B. NOte that we still have $A \subseteq B$.

Now let A,B be the result of this inductive construction. Note that by the choice of n, all of the “thus far” remain true of the actual A,B, where $m \geq n$. Thus we have for all $m \geq n$,

$$A \subseteq B.$$
$$m \notin fA \leftrightarrow m \in A \leftrightarrow m \in B.$$
$$m \notin A \rightarrow m \in fA \rightarrow m \in fB.$$

Hence for all $m \geq n$, $m \in B \cup. fA$ and $m \in A \cup fB$. Since this also holds for $m < n$, this holds for all $m \in N$.

Finally, suppose A is finite. Then fA is finite, and so eventually all m are placed in A. Thus A is infinite. Hence A is infinite. QED

LEMMA 2.5.5. For all $f \in EVSD$ there exist infinite $A \subseteq B \subseteq N$ such that $A \cup. fB = N$ and $B \cap fA = \emptyset$.

Proof: Let $f \in EVSD$. Let n,A',B' be as in the first paragraph of the proof of Lemma 2.5.4.

We now define the required A,B by induction. Membership in A,B for $m < n$ is just membership in A',B'. Thus for all $m < n$,

$$m \in B \leftrightarrow m \in B' \leftrightarrow m \notin f'A' \leftrightarrow m \notin fA.$$
$$m \in A \leftrightarrow m \in A' \leftrightarrow m \notin f'B' \leftrightarrow m \notin fB.$$

Now suppose membership in A,B has been defined for all $i < m$, where $m \geq n$, and we have $A \subseteq B$ thus far.

case 1. $m \notin fB$ thus far. Put $m \in A,B$.
case 2. $m \in fB$ thus far. Put $m \notin A,B$.

This defines membership of m in A,B. Note that we still have $A \subseteq B$.

Now let A,B be the result of this inductive construction. Note that by the choice of n, all of the "thus far" remain true of the actual A,B, where $m \geq n$. Thus we have for all $m \geq n$,

$$A \subseteq B.$$
$$m \notin fB \leftrightarrow m \in A \leftrightarrow m \in B.$$
$$m \in B \rightarrow m \notin fB \rightarrow m \notin fA.$$

Hence for all $m \geq n$, $m \in A \cup. fB$ and $m \notin B \cap fA$. Since this also holds for $m < n$, this holds for all $m \in N$.

Finally, suppose A is finite. Then eventually all m are placed in fB. Hence eventually all m are placed outside B. Hence B is finite. So fB is finite. Then eventually all m are put in A,B. This is a contradiction. QED

LEMMA 2.5.6. There exists f ∈ ELG such that $f^{-1}(0)$ = {(0,...,0)}, f(N\{0}) ⊆ 2N+1, and for all A ⊆ N containing 0, fA ∩ 2N ⊆ A → fA is cofinite.

Proof: Let g ∈ ELG ∩ SD be given by Lemma 3.2.1. We define 4-ary f ∈ ELG as follows. f(0,0,0,0) = 0. f(0,n,m,r) = g(n,m,r) if (n,m,r) ≠ (0,0,0). f(t,n,m,r) = 2|t,n,m,r|+1 if t ≠ 0. Obviously f ∈ ELG ∩ SD, f(N\{0}) ⊆ 2N+1, and $f^{-1}(0)$ = {(0,0,0,0)}.

Now let A ⊆ N, 0 ∈ A, where fA ∩ 2N ⊆ A. Since gA ⊆ fA, we have gA ∩ 2N ⊆ A, and so by Lemma 3.2.1, gA is cofinite. Hence fA is cofinite. QED

LEMMA 2.5.7. The following is false. For all f ∈ ELG there exist infinite A ⊆ B ⊆ N such that A ∩ fB = ∅, B ∪ fB = N, and fB ⊆ B ∪ fA.

Proof: Let f ∈ ELG be given by Lemma 2.5.6. Let A ∩ fB = ∅, B ∪ fB = N, and fB ⊆ B ∪ fA, where A is infinite. Now 0 ∈ B v 0 ∈ fB. Since
$f^{-1}(0)$ = {(0,0,0,0)}, we have 0 ∈ B, 0 ∈ fB, 0 ∉ A. Therefore fA ⊆ 2N+1. Since fB ⊆ B ∪ fA, we have fB ∩ 2N ⊆ B. Therefore fB is cofinite. This contradicts A ∩ fB = ∅. QED

LEMMA 2.5.8. The following is false. For all f ∈ ELG there exist infinite A ⊆ B ⊆ N such that B ∪. fA = N and A ∩ fB = ∅.

Proof: Let f be as given by Lemma 2.5.6. Let A ⊆ B ⊆ N, B ∪. fA = N, A ∩ fB = ∅, where A is infnite. Since 0 ∈ B ∪. fA, we have 0 ∈ B v 0 ∈ fA. If 0 ∈ fA then 0 ∈ A,B, because $f^{-1}(0)$ = {(0,0,0,0)}. Hence 0 ∉ fA, 0 ∉ A. Therefore fA ⊆ 2N+1. Since B ∪ fA = N, we have 2N ⊆ B. By Lemma 3.2.1, fB is cofinite. By A ∩ fB = ∅, A is finite. But A is infinite. QED

LEMMA 2.5.9. For all f ∈ EVSD there exist infinite A ⊆ B ⊆ N such that B ∪. fA = N and A ⊆ fB.

Proof: Let n be such that |x| ≥ n → f(x) > |x|. We can use Lemma 2.4.1 with N replaced by [n,∞). Let A,B ⊆ [n,∞), A ⊆

B, B ∪. fA = [n,∞) and A = B ∩ fB, where A is infinite. Then B ∪. fA = [n,∞), A ⊆ fB. Replace B with B ∪ [0,n-1]. QED

LEMMA 2.5.10. The following is false. For all f ∈ ELG there exist infinite A ⊆ B ⊆ N such that A ∩ fA = ∅, B ∪ fB = N, B ∩ fB ⊆ A ∪ fA.

Proof: Let f be as given by Lemma 2.5.6. Let A ⊆ B ⊆ N such that A ∩ fA = ∅, B ∪ fB = N, B ∩ fB ⊆ A ∪ fA, where A,B are infinite. Then 0 ∈ B ∪ fB, and so 0 ∈ B ∩ fB. Hence 0 ∈ A ∪ fA, in which case 0 ∈ A ∩ fA. QED

LEMMA 2.5.11. For all f ∈ EVSD there exist infinite A ⊆ B ⊆ N such that A ∪. fB = N and fA ⊆ B.

Proof: Let f' be the restriction of f to {x: f(x) > |x|}. Then f' is defined at all but finitely many elements of dom(f). As remarked right after Lemma 2.4.5, Lemma 2.4.2 holds even for partial functions, and so in particular for f'. Let A ⊆ B ⊆ N, where A ∪. f'B = N and f'A ⊆ B and A is infinite. Let A' = N\fB ⊆ A. Since f'B contains all but finitely many elements of fB, we see that A' remains infinite. Then A',B are as required. QED

LEMMA 2.5.12. Let f ∈ EVSD. There exist infinite A ⊆ B ⊆ N such that fB ⊆ B ∪. fA and A = B ∩ fB.

Proof: Let n be such that |x| ≥ n → f(x) > |x|. We can use Lemma 2.4.1 with N replaced by [n,∞). Let A,B ⊆ [n,∞), A ⊆ B, B ∪. fA = [n,∞), and A = B ∩ fB, where A is infinite. Since fB ⊆ [n,∞), the proof is complete. QED

LEMMA 2.5.13. Let f ∈ EVSD. There exist infinite A ⊆ N such that A ∩ f(A ∪ fA) = ∅.

Proof: Let n be such that |x| ≥ n → f(x) > |x|. Define $n_0 < n_1 < \ldots$ by induction as follows. Let $n_0 = n$. Suppose n_i has been defined, i ≥ 0. Let n_{i+1} be greater than all elements of f(A ∪ fA), thus far. Finally, let A = $\{n_0,n_1,\ldots\}$. QED

LEMMA 2.5.14. Let f ∈ EVSD and let X ⊆ N, where min(X) is sufficiently large. There exists a unique A such that A ⊆ X ⊆ A ∪. fA. If X is infinite then A is infinite.

Proof: Let f,X be as given. Then |x| ≥ min(X) → f(x) > |x|. We can use Lemma 2.4.3 with N replaced by [min(X),∞). Let A ⊆ X ∩ [min(X),∞) ⊆ A ∪. fA.

For uniqueness, suppose A ⊆ X ⊆ A ∪. fA, A' ⊆ X ⊆ A' ∪. fA', and let n = min(A Δ A'). Since f ∈ SD, clearly n ∈ fA ↔ n ∈ fA'. This is a contradiction. QED

As in section 2.4, we start with the 9 elementary inclusions in A,B,fA,fB,⊆.

EBRT in A,B,fA,fB,⊆ on (ELG,INF), (EVSD,INF).

A ∩ fA = ∅.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
A ⊆ fB.
B ∩ fB ⊆ A ∪ fA.
fA ⊆ B.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.

Our classification amounts to a determination of the subsets S of the above nine inclusions for which

(∀f ∈ ELG)(∃A ⊆ B from INF)(S)
(∀f ∈ EVSD)(∃A ⊆ B from INF)(S)

holds, where S is interpreted conjunctively.

EBRT in A,B,fA,fB,⊆ on (ELG,INF), (EGS ∩ SD,INF).*
5

A ∩ fA = ∅.
B ∪ fB = N.
fA ⊆ B.
A ⊆ fB.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 1.

A ∩ fA = ∅:
B ∪ fB = N.
fA ⊆ B.
A ⊆ fB.
B ⊆ A ∪ fB.

fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA. A ∩ fB = ∅.
B ∩ fA ⊆ A. B ∩ fA = ∅.
B ∩ fB ⊆ A ∪ fA.

LIST 1*.
6

A ∩ fA = ∅:
B ∩ fA = ∅.
A ∩ fB = ∅.
fA ⊆ B.
A ⊆ fB.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA.

LIST 1.1.

A ∩ fA = ∅: Redundant.
B ∩ fA = ∅:
A ∩ fB = ∅.
fA ⊆ B. No.
A ⊆ fB.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA. B ∩ fB ⊆ A.

LIST 1.1.*
4

B ∩ fA = ∅:
A ∩ fB = ∅.
A ⊆ fB.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A.

LIST 1.1.1.

B ∩ fA = ∅:
A ∩ fB = ∅:
A ⊆ fB. No.
B ∪ fB = N.
B ⊆ A ∪ fB.

fB ⊆ B ∪ fA.
B ∩ fB ⊆ A. B ∩ fB = ∅.

LIST 1.1.1.*
2

B ∩ fA = ∅:
A ∩ fB = ∅:
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB = ∅.

LIST 1.1.1.1.

B ∩ fA = ∅:
A ∩ fB = ∅:
B ∪ fB = N:
B ⊆ A ∪ fB. A ∪ fB = N.
fB ⊆ B ∪ fA. B ∪ fA = N. No. Lemma 2.5.8.
B ∩ fB = ∅. No. Lemma 2.5.10.

LIST 1.1.1.1.*
0

B ∩ fA = ∅:
A ∩ fB = ∅:
B ∪ fB = N:
A ∪ fB = N.

Entirely RCA_0 correct. Lemma 2.5.5.

LIST 1.1.1.2.

B ∩ fA = ∅:
A ∩ fB = ∅:
B ⊆ A ∪ fB:
fB ⊆ B ∪ fA.
B ∩ fB = ∅.

Entirely RCA_0 correct. Set A ∩ fA = ∅, B = A.

LIST 1.1.2.

B ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N.
B ⊆ A ∪ fB. B ⊆ fB. No.

fB ⊆ B ∪ fA.
B ∩ fB ⊆ A.

LIST 1.1.2.*
2

B ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A.

LIST 1.1.2.1.

B ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N:
fB ⊆ B ∪ fA. B ∪ fA = N.
B ∩ fB ⊆ A. No. Lemma 2.5.10.

LIST 1.1.2.1.*
0

B ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N:
B ∪ fA = N.

Entirely RCA_0 correct. Lemma 2.5.9.

LIST 1.1.2.2.

B ∩ fA = ∅:
A ⊆ fB:
fB ⊆ B ∪ fA:
B ∩ fB ⊆ A.

Entirely RCA_0 correct. Lemma 2.5.12.

LIST 1.1.3.

B ∩ fA = ∅:
B ∪ fB = N:
B ⊆ A ∪ fB. A ∪ fB = N.
fB ⊆ B ∪ fA. B ∪ fA = N.
B ∩ fB ⊆ A. No. Lemma 2.5.10.

LIST 1.1.3.*

0

B ∩ fA = ∅:
B ∪ fB = N:
A ∪ fB = N.
B ∪ fA = N.

Entirely RCA_0 correct. Lemma 2.5.4.

LIST 1.1.4.

B ∩ fA = ∅:
B ⊆ A ∪ fB:
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A.

Entirely RCA_0 correct. Set A ∩ fA = ∅, B = A.

LIST 1.2.

A ∩ fA = ∅: Redundant.
A ∩ fB = ∅:
fA ⊆ B.
A ⊆ fB. No.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA. B ∩ fB ⊆ fA.

LIST 1.2.*
3

A ∩ fB = ∅:
fA ⊆ B.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ fA.

LIST 1.2.1.

A ∩ fB = ∅:
fA ⊆ B:
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA. fB ⊆ B. No. Lemma 2.4.4.
B ∩ fB ⊆ fA.

LIST 1.2.1.*
2

A ∩ fB = ∅:
fA ⊆ B:
B ∪ fB = N.
B ⊆ A ∪ fB.
B ∩ fB ⊆ fA.

LIST 1.2.1.1.

A ∩ fB = ∅:
fA ⊆ B:
B ∪ fB = N:
B ⊆ A ∪ fB.
B ∩ fB ⊆ fA. No. Lemma 2.5.10.

LIST 1.2.1.1.*
0

A ∩ fB = ∅:
fA ⊆ B:
B ∪ fB = N:
B ⊆ A ∪ fB.

Entirely RCA_0 correct. See Lemma 2.5.11.

LIST 1.2.1.2.
0

A ∩ fB = ∅:
fA ⊆ B:
B ⊆ A ∪ fB:
B ∩ fB ⊆ fA.

Entirely RCA_0 correct. Le A be given by Lemma 2.5.13. Set B = A ∪ fA.

LIST 1.2.2.

A ∩ fB = ∅:
B ∪ fB = N:
B ⊆ A ∪ fB. A ∪ fB = N.
fB ⊆ B ∪ fA. No. Lemma 2.5.7.
B ∩ fB ⊆ fA. No. Lemma 2.5.10.

LIST 1.2.2.*
0

A ∩ fB = ∅:
B ∪ fB = N:
A ∪ fB = N.

Entirely RCA_0 correct. Lemma 2.5.5.

LIST 1.2.3.

A ∩ fB = ∅:
B ⊆ A ∪ fB:
fB ⊆ B ∪ fA.
B ∩ fB ⊆ fA.

Entirely RCA_0 correct. Set A ∩ fA = ∅, B = A.

LIST 1.3.

A ∩ fA = ∅:
fA ⊆ B:
A ⊆ fB.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA.

LIST 1.3.*
3

A ∩ fA = ∅:
fA ⊆ B:
A ⊆ fB.
B ∪ fB = N.
B ⊆ A ∪ fB.
fB ⊆ B.
B ∩ fB ⊆ A ∪ fA.

LIST 1.3.1.

A ∩ fA = ∅:
fA ⊆ B:
A ⊆ fB:
B ∪ fB = N.
B ⊆ A ∪ fB. B ⊆ fB. No. Lemma 2.4.5.
fB ⊆ B.
B ∩ fB ⊆ A ∪ fA.

LIST 1.3.1.*

2

A ∩ fA = ∅:
fA ⊆ B:
A ⊆ fB:
B ∪ fB = N.
fB ⊆ B.
B ∩ fB ⊆ A ∪ fA.

LIST 1.3.1.1.

A ∩ fA = ∅:
fA ⊆ B:
A ⊆ fB:
B ∪ fB = N:
fB ⊆ B.
B ∩ fB ⊆ A ∪ fA. No. Lemma 2.5.10.

LIST 1.3.1.1.*
0

A ∩ fA = ∅:
fA ⊆ B:
A ⊆ fB:
B ∪ fB = N:
fB ⊆ B.

Entirely RCA_0 correct. Let A be given by Lemma 2.4.3 with A ⊆ fN ⊆ A ∪. fA. Set B = N.

LIST 1.3.1.2.

A ∩ fA = ∅:
fA ⊆ B:
A ⊆ fB:
fB ⊆ B:
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Let B = [n,∞), n sufficiently large. By Lemma 2.5.14, let A ⊆ fB ⊆ A ∪. fA.

LIST 1.3.2.

A ∩ fA = ∅:
fA ⊆ B:
B ∪ fB = N:
B ⊆ A ∪ fB. A ∪ fB = N.
fB ⊆ B. B = N.

B ∩ fB ⊆ A ∪ fA. No. Lemma 2.5.10.

LIST 1.3.2.*
0

A ∩ fA = ∅:
fA ⊆ B:
B ∪ fB = N:
A ∪ fB = N.
B = N.

Entirely RCA_0 correct. Set A = N\fN, B = N.

LIST 1.3.3.

A ∩ fA = ∅:
fA ⊆ B:
B ⊆ A ∪ fB:
fB ⊆ B.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Let B = [n,∞) for n sufficiently large. Let A ⊆ B ⊆ A ∪. fA, by Lemma 2.5.14.

LIST 1.4.

A ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N.
B ⊆ A ∪ fB. B ⊆ fB. No. Lemma 2.4.5.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA.

LIST 1.4.*
2

A ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA.

LIST 1.4.1.

A ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N:
fB ⊆ B ∪ fA.

B ∩ fB ⊆ A ∪ fA. No. Lemma 2.5.10.

LIST 1.4.1.*
0

A ∩ fA = ∅:
A ⊆ fB:
B ∪ fB = N:
fB ⊆ B ∪ fA.

Entirely RCA_0 correct. Let A ⊆ fN ⊆ A ∪. fA be given by Lemma 2.4.3. Set B = N.

LIST 1.4.2.

A ∩ fA = ∅:
A ⊆ fB:
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Lemma 2.5.12.

LIST 1.5.

A ∩ fA = ∅:
B ∪ fB = N:
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA. No. Lemma 2.5.10.

LIST 1.5.*
0

A ∩ fA = ∅:
B ∪ fB = N:
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.

Entirely RCA_0 correct. Lemma 2.5.4.

LIST 1.6.

A ∩ fA = ∅:
B ⊆ A ∪ fB:
fB ⊆ B ∪ fA.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Let A ∩ fA = ∅, B = A.

LIST 2.

B ∪ fB = N:
fA ⊆ B.
A ⊆ fB.
B ⊆ A ∪ fB. A ∪ fB = N.
fB ⊆ B ∪ fA. B ∪ fA = N.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.*
3

B ∪ fB = N:
fA ⊆ B.
A ⊆ fB.
A ∪ fB = N.
B ∪ fA = N.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.1.

B ∪ fB = N:
fA ⊆ B:
A ⊆ fB.
A ∪ fB = N.
B ∪ fA = N. B = N.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A. fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.1.*
2

B ∪ fB = N:
fA ⊆ B:
A ⊆ fB.
A ∪ fB = N.
B = N.
A ∩ fB ⊆ fA.
fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.1.1.

B ∪ fB = N:
fA ⊆ B:
A ⊆ fB:
A ∪ fB = N. fB = N. No. Lemma 2.4.5.
B = N.
A ∩ fB ⊆ fA. A ⊆ fA. No. Lemma 2.4.5.
fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.1.1.*
0

B ∪ fB = N:
fA ⊆ B:
A ⊆ fB:
B = N.
fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = fN, B = N.

LIST 2.1.2.

B ∪ fB = N:
fA ⊆ B:
A ∪ fB = N.
B = N.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = B = N.

LIST 2.2.

B ∪ fB = N:
A ⊆ fB:
A ∪ fB = N. Yes.
B ∪ fA = N.
A ∩ fB ⊆ fA. A ⊆ fA. No. Lemma 2.4.5.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 2.2.*
0

B ∪ fB = N:

A ⊆ fB:
fB ⊆ B ∪ fA. B ∪ fA = N.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = fN, B = N.

LIST 2.3.

B ∪ fB = N:
A ∪ fB = N.
B ∪ fA = N.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = B = N.

LIST 3.

fA ⊆ B:
A ⊆ fB.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 3*.
2

fA ⊆ B:
A ⊆ fB.
B ⊆ A ∪ fB.
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 3.1.

fA ⊆ B:
A ⊆ fB:
B ⊆ A ∪ fB. B ⊆ fB. No. Lemma 2.4.5.
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA. A ⊆ fA. No. Lemma 2.4.5.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 3.1.*
0

fA ⊆ B:
A ⊆ fB:
fB ⊆ B ∪ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = fN, B = N.

LIST 3.2.

fA ⊆ B:
B ⊆ A ∪ fB:
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = B = fN.

LIST 4.

A ⊆ fB:
B ⊆ A ∪ fB. B ⊆ fB. No. Lemma 2.4.5.
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA. A ⊆ fA. No. Lemma 2.4.5.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

LIST 4.*
0

A ⊆ fB:
fB ⊆ B ∪ fA.
B ∩ fA ⊆ A.
B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = fN, B = N.

LIST 5.

B ⊆ A ∪ fB:
fB ⊆ B ∪ fA.
A ∩ fB ⊆ fA.
B ∩ fA ⊆ A.

B ∩ fB ⊆ A ∪ fA.

Entirely RCA_0 correct. Set A = B = N.

THEOREM 2.5.15. EBRT in A,B,fA,fB,⊆ on (ELG,INF), (EVSD,INF) have the same correct formats. EBRT in A,B,fA,fB,⊆ on (ELG,INF) and (EVSD,INF) are RCA_0 secure.

Proof: We have presented an RCA_0 classification of EBRT in A,B,fA,fB,⊆ on (ELG,INF), (EVSD,INF) in the sense of the tree methodology of section 2.1. All of the documentation works equally well on (ELG,INF) and (EVSD,INF). We have stayed within RCA_0. QED

THEOREM 2.5.16. There are at most 26 maximal α correct α formats, where α is EBRT in A,B,fA,fB,⊆ on (ELG,INF), (EVSD,INF).

Proof: Here is the list of numerical labels of terminal vertices in the RCA_0 classification of EBRT in A,B,fA,fB,⊆ on (ELG,INF), (EVSD,INF) given above:

1.1.1.1.*
1.1.1.2.
1.1.2.1.*
1.1.2.2.
1.1.3.*
1.1.3.
1.2.1.1.*
1.2.1.2.
1.2.2.*
1.2.3.
1.3.1.1.*
1.3.1.2.
1.3.2.*
1.3.3.
1.4.1.*
1.4.2.
1.5.*
1.6.
2.1.1.*
2.1.2.
2.2.*
2.3.
3.1.*
3.2.
4.*
5.

The count is 26. Apply Theorem 2.1.5. QED

2.6. EBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (MF,INF).

In this section, we use the tree methodology presented in section 2.1 to analyze EBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (MF,INF). This turns out to be very easy, and we obtain the same classification if we replace MF by any subset of MF satisfying some weak conditions. In particular, we show that EBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (MF,INF) is RCA_0 secure.

Note that in sections 2.4 and 2.5, we have stayed within EBRT in A,B,fA,fB,⊆. EBRT in A,B,fA,fB on (SD,INF),(ELG ∩ SD,INF), (ELG,INF),(EVSD,INF), is a major additional undertaking, and is beyond the scope of this book. The same can be said for various fragments of EBRT in A,B,C,fA,fB,fC,⊆ on (SD,INF),(ELG ∩ SD,INF),(ELG,INF),(EVSD,INF).

However, EBRT on (MF,INF) is considerably easier to analyze, due to the presence of constant functions and projection functions.

As usual, we start with the list of all $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ elementary inclusions.

EBRT in $A_1,...,A_k,fA_1,...,fA_k$ on (MF,INF).

$A_i = \emptyset$. No.
$fA_i = \emptyset$. No. Set $f(x) = 0$.
$A_i \cap fA_j = \emptyset$. No. Set $f(x) = x$.
$A_i = N$.
$fA_i = N$. No. Set $f(x) = 0$.
$A_i \cup fA_j = N$.
$A_i \subseteq A_j$, $j < i$.
$A_i \subseteq fA_j$. No. Set $f(x) = 0$.
$A_i \subseteq A_j \cup fA_p$, $j < i$.
$fA_i \subseteq A_j$.
$fA_i \subseteq fA_j$, $j < i$.
$fA_i \subseteq A_j \cup fA_p$, $p < i$.
$A_i \cap fA_j \subseteq A_p$, $p < i$.
$A_i \cap fA_j \subseteq fA_p$, $p < j$.
$A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < i$ and $q < j$.

EBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (MF,INF).*
0

$A_i = N$.
$A_i \cup fA_j = N$.
$A_i \subseteq A_j$, $j < i$.
$A_i \subseteq A_j \cup fA_k$, $j < i$.
$fA_i \subseteq A_j$.
$fA_i \subseteq fA_j$, $j < i$.
$fA_i \subseteq A_j \cup fA_p$, $p < i$.
$A_i \cap fA_j \subseteq A_p$, $p < i$.
$A_i \cap fA_j \subseteq fA_p$, $p < j$.
$A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < i$ and $q < j$.

Entirely RCA_0 correct. Set $A_1 = ... = A_k = N$.

THEOREM 2.6.1. The following is provable in RCA_0. Let $V \subseteq MF$ contain at least one constant function of some arity, and at least one projection function of some arity. For all $k \geq 1$, EBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (V,INF) and (MF,INF) have the same correct formats. For all $k \geq 1$, EBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (MF,INF) is RCA_0 secure.

Proof: We can use any constant function and any projection function in place of the unary functions $f(x) = 0$ and $f(x) = x$ that were used above. RCA_0 suffices due to the obvious explicitness of the classification. QED

THEOREM 2.6.2. There is an algorithm for determining the truth value of any statement in EBRT in any $A_1,...,A_k,fA_1,...,A_k,\subseteq$ on (MF,INF). In fact, an algorithm can be given that can be proved to work in RCA_0.

Proof: The result follows from the explicitness of the classification, the algorithm presented in section 2.1, and Theorem 2.1.4. QED

2.7. IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$.

In this section, we analyze IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (SD,INF), (ELG $\cap$ SD,INF), (ELG,INF), (EVSD,INF), and (MF,INF). We show that for all $k \geq 1$, IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on each of (SD,INF), (ELG $\cap$ SD,INF), (ELG,INF), (EVSD,INF) is RCA_0 secure. We show that IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (MF,INF) is ACA' secure (see Definition 1.4.1). We also show that the only correct format for IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (SD,INF), (ELG $\cap$ SD,INF), (ELG,INF), (EVSD,INF) is $\emptyset$. This is not true on (MF,INF).

We begin with (MF,INF), for some fixed $k \geq 1$. We need to analyze all statements of the form

$$\#)\ (\exists f \in MF)(\forall A_1,\ldots,A_k \in INF)(A_1 \subseteq \ldots \subseteq A_k \rightarrow \varphi).$$

where φ is an $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ format. Recall that the instances of #) are Boolean equivalent to the assertions of IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$, and the negations of the statements in IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$.

Recall the list of all $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ elementary inclusions that were used in section 2.6:

1. $A_i = \emptyset$.
2. $fA_i = \emptyset$.
3. $A_i \cap fA_j = \emptyset$.
4. $A_i = N$.
5. $fA_i = N$.
6. $A_i \cup fA_j = N$.
7. $A_i \subseteq A_j$, $j < i$.
8. $A_i \subseteq fA_j$.
9. $A_i \subseteq A_j \cup fA_p$, $j < i$.
10. $fA_i \subseteq A_j$.
11. $fA_i \subseteq fA_j$, $j < i$.
12. $fA_i \subseteq A_j \cup fA_p$, $p < i$.
13. $A_i \cap fA_j \subseteq A_p$, $p < i$.
14. $A_i \cap fA_j \subseteq fA_p$, $p < j$.
15. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < i$ and $q < j$.

For each of these elementary inclusions, ρ, we will provide a useful description of the witness set for ρ, in the following sense: The set of all $f \in MF$ such that

$$(\forall A_1,\ldots,A_k \in INF)(A_1 \subseteq \ldots \subseteq A_k \rightarrow \rho).$$

To analyze formats, we analyze the intersections of these witness sets, determining which intersections are nonempty. I.e., a format is correct if and only if the intersection of the set of witnesses of each element is nonempty (in IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (MF,INF)).

We also use this technique for the other four BRT settings. Thus a format is correct if and only if the intersection of the set of witnesses of each element meets V (in IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (V,INF), $V \subseteq MF$)).

Each numbered entry in the list represents several inclusions. In some numbered entries, all of the inclusions will have the same witness set. We call such an entry uniform. Unfortunately, some of the numbered entries are not uniform.

We shall see that entries 1-7,11 are uniform. We now determine their witnesses sets.

LEMMA 2.7.1. The inclusions in clauses 1-7 each have no witnesses. I.e., their witness sets are ∅.

Proof: Let f ∈ MF. We show that f is not a witness. For 1,2,3, let $A_1 = ... = A_k = N$. For 4,5,6 take $A_1 = ... = A_k = \emptyset$. For 7, take each $A_i = \{i\}$. QED

LEMMA 2.7.2. Let f ∈ MF and j < i. f witnesses $fA_i \subseteq fA_j$ if and only if (∀B ∈ INF)(fB = fN).

Proof: Let f,j,i be as given. Let f witness $fA_i \subseteq fA_j$. Let B ∈ INF. Set $A_1 = ... = A_j = B$, $A_{j+1} = ...= A_k = N$. Then fN = fB. For the converse, assume (∀B ∈ INF)(fB = fN). Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $fA_i = fN = fA_j$. QED

We now break the remaining numbered entries into uniform parts as follows.

8a. $A_i \subseteq fA_j$, $i \leq j$.
8b. $A_i \subseteq fA_j$, $j < i$.
9a. $A_i \subseteq A_j \cup fA_p$, $j,p < i$.
9b. $A_i \subseteq A_j \cup fA_p$, $j < i \leq p$.
10a. $fA_i \subseteq A_j$, $i \leq j$.
10b. $fA_i \subseteq A_j$, $j < i$.
12a. $fA_i \subseteq A_j \cup fA_p$, $p,j < i$.
12b. $fA_i \subseteq A_j \cup fA_p$, $p < i \leq j$.
13a. $A_i \cap fA_j \subseteq A_p$, $p < i,j$.
13b. $A_i \cap fA_j \subseteq A_p$, $j \leq p < i$.
14a. $A_i \cap fA_j \subseteq fA_p$, $p < i,j$.
14b. $A_i \cap fA_j \subseteq fA_p$, $i \leq p < j$.
15a. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < i \leq q < j$.
15b. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < i \leq j$.
15c. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \leq p < i \leq j$.
15d. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q = i < j$.
15e. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < j \leq i$.
15f. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \leq p < j \leq i$.
15g. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < j \leq p < i$.
15h. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < p = j < i$.

We need to show that this list includes all of 8-10,12-15 from the original list. This is evident by inspection for all but 15 = 15a-15h. Here we need Lemma 2.7.4 below.

LEMMA 2.7.3. Suppose $p < i$ and $q < j$. Then at least one of the following holds.
$p \leq i \leq q \leq j$.
$p \leq q \leq i \leq j$.
$q \leq p \leq i \leq j$.
$p \leq q \leq j \leq i$.
$q \leq p \leq j \leq i$.
$q \leq j \leq p \leq i$.

Proof: Let $p < i$ and $q < j$. Obviously, at least one of the $4! = 24$ four term inequalities with $\leq$ separating the four variables i,j,p,q, must hold. In any such true four term inequality with $\leq$, p must come before i and q must come before j. Of the $4! = 24$ permutations of the letters i,j,p,q, exactly 1/4 of them have p before i and q before j. Since the above lists 6 such, the above list must be complete. QED

LEMMA 2.7.4. Suppose $p < i$ and $q < j$. Then at least one of the following holds.
$p < i \leq q < j$
$p < q < i \leq j$
$q \leq p < i \leq j$
$p < q = i < j$
$p < q < j \leq i$
$q \leq p < j \leq i$
$q < j \leq p < i$
$q < p = j < i$.

Proof: We use Lemma 2.7.3, which provides six cases.

Suppose $p \leq i \leq q \leq j$. Then $p < i \leq q < j$.

Suppose $p \leq q \leq i \leq j$. If $p < q$ then $p < q < i \leq j \vee p < q = i < j$. If $p = q$ then $p = q < i \leq j$, and so $q \leq p < i \leq j$.

Suppose $q \leq p \leq i \leq j$. Then $q \leq p < i \leq j$.

Suppose $p \leq q \leq j \leq i$. If $p < q$ then $p < q < j \leq i$. If $p = q$ then $p = q < j \leq i$, and so $q \leq p < j \leq i$.

Suppose $q \leq p \leq j \leq i$. If $p < j$ then $q \leq p < j \leq i$. If $p = j$ then $q \leq p = j < i$, and hence $q < p = j < i$ (using $q < j$).

Suppose $q \le j \le p \le i$. Then $q < j \le p < i$. QED

We are now prepared to make the determination of witnesses for each of the entries 8a - 15h.

WITNESS SET ASSIGNMENT LIST

1-7. None. Lemma 2.7.1.
8a. $A_i \subseteq fA_j$, $i \le j$. $(\forall B \in INF)(B \subseteq fB)$. Lemma 2.7.5.
8b. $A_i \subseteq fA_j$, $j < i$. None. Lemma 2.7.6.
9a. $A_i \subseteq A_j \cup fA_p$, $j,p < i$. None. Lemma 2.7.7.
9b. $A_i \subseteq A_j \cup fA_p$, $j < i \le p$. $(\forall B \in INF)(B \subseteq fB)$. Lemma 2.7.8.
10a. $fA_i \subseteq A_j$, $i \le j$. $(\forall B \in INF)(fB \subseteq B)$. Lemma 2.7.9.
10b. $fA_i \subseteq A_j$, $j < i$. None. Lemma 2.7.10.
11. $fA_i \subseteq fA_j$, $j < i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.2.
12a. $fA_i \subseteq A_j \cup fA_p$, $p,j < i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.11.
12b. $fA_i \subseteq A_j \cup fA_p$, $p < i \le j$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.12.
13a. $A_i \cap fA_j \subseteq A_p$, $p < i,j$. None. Lemma 2.7.13.
13b. $A_i \cap fA_j \subseteq A_p$, $j \le p < i$. $(\forall B \in INF)(fB \subseteq B)$. Lemma 2.7.14.
14a. $A_i \cap fA_j \subseteq fA_p$, $p < i,j$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.15.
14b. $A_i \cap fA_j \subseteq fA_p$, $i \le p < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.16.
15a. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < i \le q < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.17.
15b. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < i \le j$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.18.
15c. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \le p < i \le j$. $(\forall B \in INF)(fN \subseteq B \cup fB)$. Lemma 2.7.19.
15d. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q = i < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.20.
15e. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < j \le i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.21.
15f. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \le p < j \le i$. $(\forall B \in INF)(fN \subseteq B \cup fB)$. Lemma 2.7.22.
15g. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < j \le p < i$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.23.
15h. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < p = j < i$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.24.

LEMMA 2.7.5. Let $f \in MF$ and $i \le j$. f witnesses $A_i \subseteq fA_j$ if and only if $(\forall B \in INF)(B \subseteq fB)$.

Proof: Let f,i,j be as given. Assume f witnesses $A_i \subseteq fA_j$. Let B ∈ INF. Set $A_1 = ... = A_k = B$. Then B ⊆ fB. For the converse, assume (∀B ∈ INF)(B ⊆ fB) and let $A_1 \subseteq ... A_k \subseteq$ N, where A_1 is infinite. Then $A_i \subseteq fA_i \subseteq fA_j$. QED

LEMMA 2.7.6. $A_i \subseteq fA_j$, j < i, has no witnesses.

Proof: Let f witness $A_i \subseteq fA_j$, j < i. By the Thin Set Theorem, let fB ≠ N. Set $A_1 = ... = A_j = B$, $A_{j+1} = ... = A_k =$ N. Then $A_i \subseteq fA_j$ is false. QED

LEMMA 2.7.7. $A_i \subseteq A_j \cup fA_p$, j,p < i, has no witnesses.

Proof: Let f witness $A_i \subseteq A_j \cup fA_p$, j,p < i. By the Thin Set Theorem (variant), let B ∈ INF where B ∪ fB ≠ N. Set $A_1 =$ ... $= A_{i-1} = B$, $A_i = ... = A_k =$ N. Then $A_i \subseteq A_j \cup fA_p$ is false. QED

LEMMA 2.7.8. Let f ∈ MF and j < i ≤ p. f witnesses $A_i \subseteq A_j \cup fA_p$ if and only if (∀B ∈ INF)(B ⊆ fB).

Proof: Let f,i,j,p be as given. Let f witness $A_i \subseteq A_j \cup fA_p$. Let B ∈ INF. Suppose B ⊆ fB fails, and let r ∈ B\fB. Set $A_1 = ... = A_j =$ B\{r}, $A_{j+1} = ... = A_k =$ B. Then B ⊆ B\{r} ∪ fB, which contradicts the choice of r. Hence B ⊆ fB. For the converse, assume (∀B ∈ INF)(B ⊆ fB). Let $A_1 \subseteq ... \subseteq A_k \subseteq$ N, where A_1 is infinite. Then $A_i \subseteq fA_i \subseteq fA_p \subseteq A_j \cup fA_p$. QED

LEMMA 2.7.9. Let f ∈ MF and i ≤ j. f witnesses $fA_i \subseteq A_j$ if and only if (∀B ∈ INF)(fB ⊆ B).

Proof: Let f,i,j be as given. Let f witness $fA_i \subseteq A_j$. Let B ∈ INF. Set $A_1 = ... = A_k = B$. Then fB ⊆ B. For the converse, assume (∀B ∈ INF)(fB ⊆ B). Let $A_1 \subseteq ... \subseteq A_k \subseteq$ N, where A_1 is infinite. Then $fA_i \subseteq A_i \subseteq A_j$. QED

LEMMA 2.7.10. $fA_i \subseteq A_j$, j < i, has no witnesses.

Proof: Let f witness $fA_i \subseteq A_j$, j < i. Let r ∈ fN. Set $A_1 =$ ... $= A_j =$ N\{r}, $A_{j+1} = ... A_k =$ N. Then $fA_i \subseteq A_j$ is false. QED

LEMMA 2.7.11. Let p,j < i. f witnesses $fA_i \subseteq A_j \cup fA_p$ if and only if (∀B ∈ INF)(fB = fN).

Proof: Let f,i,j,p be as given. Let f witness $fA_i \subseteq A_j \cup fA_p$. Let B ∈ INF. Suppose fB ⊆ fN fails. Let r ∈ fN\fB. Set

$A_1 = \ldots = A_{i-1} = B\backslash\{r\}$, $A_i = \ldots = A_k = N$. Then $fN \subseteq B\backslash\{r\} \cup f(B\backslash\{r\})$, which is a contradiction. For the converse, assume $(\forall B \in INF)(fB = fN)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $fA_i = fN \subseteq A_j \cup fN = A_j \cup fA_p$. QED

LEMMA 2.7.12. Let $f \in MF$ and $p < i \leq j$. f witnesses $fA_i \subseteq A_j \cup fA_p$ if and only if $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Proof: Let f,i,j,p be as given. Let f witness $fA_i \subseteq A_j \cup fA_p$. Let $B \subseteq C \subseteq N$, where B is infinite. Set $A_1 = \ldots = A_p = B$, $A_{p+1} = \ldots = A_k = C$. Then $fC \subseteq C \cup fB$. For the converse, assume $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $fA_i \subseteq A_i \cup fA_p \subseteq A_j \cup fA_p$. QED

LEMMA 2.7.13. $A_i \cap fA_j \subseteq A_p$, $p < i,j$, has no witnesses.

Proof: Let $p < i,j$. Let f witness $A_i \cap fA_j \subseteq A_p$. Let $r \in fN$. Let $A_1 = \ldots = A_p = N\backslash\{r\}$, $A_{p+1} = \ldots = A_k = N$. Then $A_i \cap fA_j \subseteq A_p$ is false. QED

LEMMA 2.7.14. Let $f \in MF$ and $j \leq p < i$. f witnesses $A_i \cap fA_j \subseteq A_p$ if and only if $(\forall B \in INF)(fB \subseteq B)$.

Proof: Let f,i,j,p be as given. Let f witness $A_i \cap fA_j \subseteq A_p$. Let $B \in INF$. Set $A_1 = \ldots = A_{i-1} = B$, $A_i = \ldots = A_k = N$. Then $fB \subseteq B$. For the converse, assume $(\forall B \in INF)(fB \subseteq B)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq A_i \cap A_j = A_j \subseteq A_p$. QED

LEMMA 2.7.15. Let $f \in MF$ and $p < i,j$. f witnesses $A_i \cap fA_j \subseteq fA_p$ if and only if $(\forall B \in INF)(fB = fN)$.

Proof: Let f,i,j,p be as given. Let f witness $A_i \cap fA_j \subseteq fA_p$. Let $B \in INF$. Set $A_1 = \ldots = A_p = B$, $A_{p+1} = \ldots = A_k = N$. Then $fN \subseteq fB$. For the converse, assume $(\forall B \in INF)(fB = fN)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fN = fA_p$. QED

LEMMA 2.7.16. Let $f \in MF$ and $i \leq p < j$. f witnesses $A_i \cap fA_j \subseteq fA_p$ if and only if f witnesses $A_i \cap fA_j \subseteq fA_p$ if and only if $(\forall B \in INF)(B \cap fN \subseteq fB)$.

Proof: Let f,i,j,p be as given. Let f witness $A_i \cap fA_j \subseteq fA_p$. Let $B \in INF$. Set $A_1 = \ldots = A_{j-1} = B$, $A_j = \ldots = A_k = N$. Then $B \cap fN \subseteq fB$. For the converse, assume $(\forall B \in INF)(B \cap fN \subseteq fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq A_i \cap fN \subseteq fA_i \subseteq fA_p$. QED

LEMMA 2.7.17. Let $f \in MF$ and $p < i \leq q < j$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(B \cap fN \subseteq fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \in INF$. Suppose $B \cap fN \subseteq fB$ is false. Let $r \in B,fN$, $r \notin fB$. Set $A_1 = \ldots = A_{i-1} = B\backslash\{r\}$, $A_i = \ldots = A_{j-1} = B$, $A_j = \ldots = A_k = N$. Then $B \cap fN \subseteq B\backslash\{r\} \cup fB$. This is a contradiction. For the converse, assume $(\forall B \in INF)(B \cap fN \subseteq fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq A_i \cap fN \subseteq fA_i \subseteq fA_q$. QED

LEMMA 2.7.18. Let $f \in MF$ and $p < q < i \leq j$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(fB = fN)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \in INF$. Suppose $fB \neq fN$. Let $r \in fN\backslash fB$. Set $A_1 = \ldots = A_{q-1} = B\backslash\{r\}$, $A_q = \ldots = A_{i-1} = B$, $A_i = \ldots = A_k = N$. Then $fN \subseteq B\backslash\{r\} \cup fB$. This is a contradiction. Conversely, assume $(\forall B \in INF)(fB = fN)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fN = fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.19. Let $f \in MF$ and $q \leq p < i \leq j$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(fN \subseteq B \cup fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Set $A_1 = \ldots = A_{i-1} = B$, $A_i = \ldots = A_k = N$. Then $fN \subseteq B \cup fB$. Conversely, assume $(\forall B \in INF)(fN \subseteq B \cup fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fN \subseteq A_q \cup fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.20. Let $f \in MF$ and $p < q = i < j$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(B \cap fN \subseteq fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \in INF$. Suppose $B \cap fN \subseteq fB$ is false. Let $r \in B,fN$, $r \notin fB$. Set $A_1 = \ldots = A_p = B\backslash\{r\}$, $A_{p+1} = \ldots = A_q = B$, $A_{q+1} = \ldots = A_k = N$. Then $B \cap fN \subseteq B\backslash\{r\} \cup fB$. This is a contradiction. For the converse, assume $(\forall B \in INF)(B \cap fN \subseteq fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq A_i \cap fN \subseteq fA_i = fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.21. Let $f \in MF$ and $p < q < j \leq i$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(fB = fN)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \in INF$. Suppose $fN \neq fB$. Let $r \in fN\backslash fB$. Set

$A_1 = ... = A_p = B\backslash\{r\}$, $A_{p+1} = ... = A_q = B$, $A_{q+1} = ... = A_k = N$. Then $fN \subseteq B\backslash\{r\} \cup fB$. This is a contradiction. For the converse, assume $(\forall B \in INF)(fN = fB)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fN = fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.22. Let $f \in MF$ and $q \leq p < j \leq i$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(fN \subseteq B \cup fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \in INF$. Set $A_1 = ... = A_{j-1} = B$, $A_j = ... = A_k = N$. Then $fN \subseteq B \cup fB$. For the converse, assume $(\forall B \in INF)(fN \subseteq B \cup fB)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fN \subseteq A_q \cup fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.23. Let $f \in MF$ and $q < j \leq p < i$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \subseteq C \subseteq N$, where B is infinite. Set $A_1 = ... = A_q = B$, $A_{q+1} = ... = A_p = C$, $A_{p+1} = ... = A_k = N$. Then $fC \subseteq C \cup fB$. For the converse, assume $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fA_j \subseteq A_j \cup fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.24. Let $f \in MF$ and $q < p = j < i$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \subseteq C \subseteq N$, where B is infinite. Set $A_1 = ... = A_q = B$, $A_{q+1} = ... = A_p = C$, $A_{p+1} = ... = A_k = N$. Then $fC \subseteq C \cup fB$. For the converse, assume $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq A_j \cup fA_q = A_p \cup fA_q$. QED

We now remove entries with no witnesses from the Witness Set Assignment List.

PRUNED WITNESS SET ASSIGNMENT LIST

8a. $A_i \subseteq fA_j$, $i \leq j$. $(\forall B \in INF)(B \subseteq fB)$. Lemma 2.7.5.
9b. $A_i \subseteq A_j \cup fA_p$, $j < i \leq p$. $(\forall B \in INF)(B \subseteq fB)$. Lemma 2.7.8.
10a. $fA_i \subseteq A_j$, $i \leq j$. $(\forall B \in INF)(fB \subseteq B)$. Lemma 2.7.9.
11. $fA_i \subseteq fA_j$, $j < i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.2.
12a. $fA_i \subseteq A_j \cup fA_p$, $p,j < i$. $(\forall B \in INF)(fB = fN)$.

Lemma 2.7.11.
12b. $fA_i \subseteq A_j \cup fA_p$, $p < i \leq j$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.12.
13b. $A_i \cap fA_j \subseteq A_p$, $j \leq p < i$. $(\forall B \in INF)(fB \subseteq B)$. Lemma 2.7.14.
14a. $A_i \cap fA_j \subseteq fA_p$, $p < i,j$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.15.
14b. $A_i \cap fA_j \subseteq fA_p$, $i \leq p < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.16.
15a. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < i \leq q < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.17.
15b. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < i \leq j$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.18.
15c. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \leq p < i \leq j$. $(\forall B \in INF)(fN \subseteq B \cup fB)$. Lemma 2.7.19.
15d. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q = i < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.20.
15e. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < j \leq i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.21.
15f. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \leq p < j \leq i$. $(\forall B \in INF)(fN \subseteq B \cup fB)$. Lemma 2.7.22.
15g. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < j \leq p < i$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.23.
15h. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < p = j < i$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.24.

Exactly six sets of witnesses appear in the Witness Set Assignment List.

WITNESS SET LIST (FOR MF).

$(\forall B \in INF)(fB = fN)$.
$(\forall B \in INF)(fN \subseteq B \cup fB)$.
$(\forall B \in INF)(B \subseteq fB)$.
$(\forall B \in INF)(fB \subseteq B)$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

We have only to determine which subsets of the above list have a common witness; i.e., which subsets have nonempty intersection. For this purpose, we use the "pure" application of the Tree Methodology mentioned at the very end of section 2.1.

WITNESS SET LIST*.
3

$(\forall B \in INF)(fB = fN)$.

$(\forall B \in INF)(fN \subseteq B \cup fB)$.
$(\forall B \in INF)(B \subseteq fB)$.
$(\forall B \in INF)(fB \subseteq B)$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

LIST 1.

$(\forall B \in INF)(fB = fN)$:
$(\forall B \in INF)(fN \subseteq B \cup fB)$.
$(\forall B \in INF)(B \subseteq fB)$. $fN = N$. No. By the Thin Set Theorem, let $fB \neq N$. Hence $fN \neq N$.
$(\forall B \in INF)(fB \subseteq B)$. No. Let $B = N\backslash\{r\}$, $r \in fN$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

LIST 1.*
0

$(\forall B \in INF)(fB = fN)$:
$(\forall B \in INF)(fN \subseteq B \cup fB)$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Nonempty intersection. Let $f(x) = 0$.

LIST 2.

$(\forall B \in INF)(fN \subseteq B \cup fB)$:
$(\forall B \in INF)(B \subseteq fB)$. $fN = N$. No. By the Thin Set Theorem (variant), let $B \cup fB \neq N$. Since $fN \subseteq B \cup fB$, we have $fN \neq N$.
$(\forall B \in INF)(fB \subseteq B)$. $(\forall B \in INF)(fN \subseteq B)$. No. Let $B = N\backslash\{r\}$, $r \in fN$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

LIST 2.*
0

$(\forall B \in INF)(fN \subseteq B \cup fB)$:
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Nonempty intersection. Let $f(x) = 0$.

LIST 3.

$(\forall B \in INF)(B \subseteq fB)$:
$(\forall B \in INF)(fB \subseteq B)$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Nonempty intersection. Let $f(x) = x$.

THEOREM 2.7.25. For all $k \geq 1$, IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (MF,INF) is ACA' secure.

Proof: Let S be a format in this BRT fragment α. Then S is a set of elementary inclusions in α, which are compiled in the first list of this section, 1-15. Correctness of S is equivalent to the existence of $f \in MF$ satisfying $(\forall A_1,\ldots,A_k \in INF)(A_1 \subseteq \ldots \subseteq A_k \rightarrow S)$. This can be rewritten in the following form:

the intersection of the witness sets
$\{f \in MF: (\forall A_1,\ldots,A_k \in INF)(A_1 \subseteq \ldots \subseteq A_k \rightarrow \varphi)\}$,
$\varphi \in S$, is nonempty.

A complete analysis of the non emptiness of these intersection has been presented. This analysis is explicit, except for the use of the Thin Set Theorem and Thin Set Theorem (variant). Recall from section 1.4 that the Thin Set Theorem and the Thin Set Theorem (variant) are provable in ACA'. QED

We now consider IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (SD,INF), (ELG ∩ SD,INF), (ELG,INF), and (EVSD,INF). We shall see that it suffices to consider only (EVSD,INF).

This amounts to determining which subsets of the Witness Set List have a common element from EVSD. For this purpose, we repeat the Tree Methodology on the witness list, this time with reference to EVSD only.

WITNESS SET LIST. (FOR EVSD).

$(\forall B \in INF)(fB = fN)$. No. By Theorem 2.2.1, let fN not be a subset of $B \cup fB$.
$(\forall B \in INF)(fN \subseteq B \cup fB)$. No. Theorem 2.2.1.
$(\forall B \in INF)(B \subseteq fB)$. No. By Theorem 2.2.1, let $B \cap fB = \emptyset$.
$(\forall B \in INF)(fB \subseteq B)$. No. By Theorem 2.2.1.
$(\forall B \in INF)(B \cap fN \subseteq fB)$. No. By Theorem 2.2.1, let $B \subseteq fN$, $B \cap fB = \emptyset$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. No. Lemma 2.7.26.

LEMMA 2.7.26. There is no f ∈ EVSD such that (∀B,C ∈ INF)(B ⊆ C → fC ⊆ C ∪ fB).

Proof: Let f ∈ EVSD. By Theorem 2.2.1, let C ∈ INF, where C ∩ fC = ∅. We now apply Theorem 2.2.1, with A = C and D = fC. Let B ⊆ C, B infinite, where fC ⊆ fB fails. Then fC ⊆ C ∪ fB also fails. QED

THEOREM 2.7.27. The following is provable in RCA_0. For all k ≥ 1, IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (SD,INF), (ELG ∩ SD,INF), (ELG,INF), (EVSD,INF), have no correct formats other than ∅. They are all RCA_0 secure.

Proof: First note that EVSD contains SD, ELG ∩ SD, and ELG.

The above analysis is explicit, except for the use of the Thin Set Theorem and Thin Set Theorem (variant). But we need only apply the Thin Set Theorem (variant) to functions from EVSD. By Theorem 2.2.1, there exists infinite B such that B ∩ fB = ∅, and so fB ≠ N. Now use the fact that Theorem 2.2.1 is provable in RCA_0. QED

It is clear that IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (MF,INF) has correct formats other than ∅. In particular,

$$(\exists f \in MF)(\forall A \in INF)(fA = A)$$

by setting f(x) = x.

CHAPTER 3
6561 CASES OF EQUATIONAL BOOLEAN RELATION THEORY

In this Chapter, we study $6561 = 3^8$ assertions of EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF) of a particularly simple form. We cannot come close to analyzing all assertions of EBRT in A,B,C,fA,fB,fC,gA,gB,gC on (ELG,INF), or even of EBRT in A,B,C,fA,fB,gB,gC,⊆ on (ELG,INF).

Recall the notation A ∪. B, introduced in Definition 1.3.1. Thus

$$A \cup. B \subseteq C \cup. D$$

means

$$A \cap B = \emptyset \wedge C \cap D = \emptyset \wedge A \cup B \subseteq C \cup D.$$

This is a very natural concept, and is illustrated by the following diagram.

```
 ______________________________
| C                            |
|                              |
|        ______________        |
|       | A      | B     |      |
|       |        |       |      |
|_______|________|_______|______|
| D     |        |       |      |
|       |        |       |      |
|       |________|_______|      |
|                              |
|                              |
|______________________________|
```

Our $6561 = 3^8$ cases take the following form.

TEMPLATE. For all f,g ∈ ELG there exist A,B,C ∈ INF such that

$$X \cup. fY \subseteq V \cup. gW$$
$$P \cup. fR \subseteq S \cup. gT.$$

Here X,Y,V,W,P,R,S,T are among the three letters A,B,C. We refer to the statements X ∪. fY ⊆ V ∪. gW, for X,Y,V,W ∈ {A,B,C}, as clauses.

In this Chapter, we determine the truth values of all of these 6561 statements. We prove a number of specific results about the Template. Here "Temp" is read "Template".

TEMP 1. Every assertion in the Template is either provable or refutable in $SMAH^+$. There exist 12 assertions in the Template, provably equivalent in RCA_0, such that the remaining 6549 assertions are each provable or refutable in RCA_0. Furthermore, these 12 are provably equivalent to the 1-consistency of SMAH over ACA' (Theorem 5.9.11).

We can be specific about the 12 exceptional cases.

DEFINITION 3.1.1. The Principal Exotic Case is Proposition A below. It is an instance of the Template.

PROPOSITION A. For all f,g ∈ ELG there exist A,B,C ∈ INF such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

In Chapter 4, we prove Proposition A in $SMAH^+$. In Chapter 5, we show that Proposition A is provably equivalent to 1-Con(SMAH) over ACA'.

DEFINITION 3.1.2. The Exotic Cases consist of the 12 variants of Proposition A where we (optionally) interchange the two clauses, and (optionally) permute the three letters A,B,C.

The Principal Exotic Case is among the Exotic Cases.

The Template is based on the BRT setting (ELG,INF). What if we use (ELG ∩ SD,INF), (SD,INF), (EVSD,INF)?

TEMP 2. Every one of the 6561 assertions in the Template, other than the 12 Exotic Cases, are provably equivalent to the result of replacing ELG by any of ELG ∩ SD, SD, EVSD. All 12 Exotic Cases are refutable in RCA_0 if ELG is replaced by SD or EVSD (Theorem 6.3.5).

TEMP 3. The Template behaves very differently for MF. For example, the Template is true (even provable in RCA_0) with A

$\cup$. fA $\subseteq$ B $\cup$. gB, A $\cup$. fA $\subseteq$ B $\cup$. gB, yet false (even refutable in RCA_0) with ELG replaced by MF.

DEFINITION 3.1.3. The "template attributes" are as follows. Below, α,β are clauses in the sense of the Template.

INF(α,β). For all f,g $\in$ ELG there exist A,B,C $\in$ INF such that α,β hold.

AL(α,β). For all f,g $\in$ ELG and n $\geq$ 0, there exist A,B,C $\subseteq$ N, each with at least n elements (possibly infinite), such that α,β holds. Here AL is read "arbitrarily large".

ALF(α,β). For all f,g $\in$ ELG and n $\geq$ 0, there exist finite A,B,C $\subseteq$ N, each with at least n elements, such that α,β holds. Here ALF is read "arbitrarily large finite".

FIN(α,β). For all f,g $\in$ ELG there exist nonempty finite A,B,C $\subseteq$ N such that α,β holds. Here FIN is read "nonempty finite".

NON(α,β). For all f,g $\in$ ELG there exist nonempty A,B,C $\subseteq$ N such that α,β hold. Here NON is read "nonempty".

Note that the Template is based on INF(α,β).

We write $\neg$INF(α,β), $\neg$AL(α,β), $\neg$ALF(α,β), $\neg$FIN(α,β), $\neg$NON(α,β) for the negations of the template attributes.

We analyze the following Extended Template based on the template attributes.

EXTENDED TEMPLATE. X(α,β), where X $\in$ {INF, AL, ALF, FIN, NON}, and α,β are among the X $\cup$. fY $\subseteq$ V $\cup$. gW, with X,Y,V,W $\in$ {A,B,C}.

Every assertion in the Template is an assertion in the Extended Template, using X = INF. The number of assertions in the Extended Template is obviously 5(81)(81) = 32,805.

We determine the truth value of every one of these 32,805 assertions in this Chapter.

Now 32,805 is a rather daunting number, and we take full advantage of an obvious symmetry and some general facts in order to carry out such a large tabular classification.

The obvious symmetry is that we can permute any two clauses, and also permute the three letters A,B,C. This results in an obvious equivalence relation on the ordered pairs of clauses, where the equivalence classes have at most 12 elements. In fact, the typical equivalence class has 12 elements, and we compute that there are exactly 574 equivalence classes under this equivalence relation. This equivalence relation is called the pair equivalence relation, and is introduced formally in Definition 3.1.1.

Thus, in this Chapter, we will be making a total of 5(574) = 2870 determinations up to pair equivalence.

Here is one of our main results of this Chapter. “ETEMP” is read “Extended Template”.

ETEMP. Every assertion in the Extended Template, other than the 12 Exotic Cases with INF, is provable or refutable in RCA_0.

The determination of the truth value of all assertions in the Extended Template is presented in section 3.14 as an annotated table.

The annotated table lists a representative from all 574 of the equivalence classes of the ordered pairs of clauses. To its right is the sequence of template attributes INF, ALF, ALF, FIN, NON, where none, some, or all appear with a negation sign in front. There are 5(574) = 2870 entries in the annotative table.

The 12 Exotic Cases then appear as entry 28 under ACBC, in the annotated table:

28. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.

This is the Principal Exotic Case. The justification of this single entry (with INF only) uses $SMAH^+$, and is given in Chapter 4.

In section 3.15, we make some observations about the classification in the annotated table of section 3.14. The most important is "BRT Transfer", which tells us that for the purposes of this Chapter, INF and ALF are equivalent.

We shall see that BRT Transfer is itself provably equivalent to the 1-consistency of SMAH over ACA'.

3.1. Preliminaries.

We begin with two background Theorems which show the equivalence of

ELG and ELG ∩ SD.
SD and EVSD.

for the Extended Template.

THEOREM 3.1.1. Suppose that for all f,g ∈ ELG ∩ SD there exist A,B,C ∈ INF such that X ∪. fY ⊆ V ∪. gW and P ∪. fR ⊆ S ∪. gT. Then for all f,g ∈ ELG there exist A,B,C ∈ INF such that X ∪. fY ⊆ V ∪. gW and P ∪. fR ⊆ S ∪. gT. The same is true if we replace "A,B,C ∈ INF" by "arbitrarily large A,B,C ⊆ N", "arbitrarily large finite A,B,C ⊆ N", "nonempty finite A,B,C ⊆ N", or "nonempty A,B,C ⊆ N".

Proof: Assume the hypothesis. Let f,g ∈ ELG, with arities p,q, respectively. Let f,g be strictly dominating on $[n,\infty)^p$ and $[n,\infty)^q$, respectively.

Let f',g' be defined by f'(x) = f(x+n)-n and g'(y) = g(y+n)-n. We claim that f',g' ∈ ELG ∩ SD. To see this, first note that f'(x) = f(x+n)-n > |x+n|-n = |x|, and g'(y) = g(y+n)-n > |y+n|-n = |y|. Hence f',g' ∈ SD. Now let 1 < c < d be such that

$$c|x| \le f(x) \le d|x|$$
$$c|y| \le g(y) \le d|y|$$

hold for all |x|,|y| > t. Then

$$c|x+n| \le f(x+n) = f'(x)+n \le d|x+n|$$
$$c|y+n| \le g(y+n) = g'(y)+n \le d|y+n|$$

hold for all |x|,|y| > t. Hence

$$c|x+n|-n \le f'(x) \le d|x+n|-n$$
$$c|y+n|-n \le g'(y) \le d|y+n|-n$$

hold for all |x|,|y| > t.

Hence

$$c|x| \le f'(x) \le d(|x|+n)-n = d|x|+(d-1)n \le (d+dn)|x|$$

$$c|y| \le g'(y) \le d(|y|+n)-n = d|y|+(d-1)n \le (d+dn)|y|$$

hold for all |x|,|y| > t. Hence f′,g′ ∈ ELG. So f′,g′ ∈ ELG ∩ SD.

Applying the hypothesis to f′,g′, let A,B,C ∈ INF, where X ∪. f'Y ⊆ V ∪. g'W and P ∪. fR ⊆ S ∪. gT. Let A′ = A+n, B′ = B+n, C′ = C+n. Obviously A′,B′,C′ ∈ INF, and X′,Y′,V′,W′,P′,R′,S′,T′ = X+n,Y+n,V+n,W+n,P+n,R+n,S+n,T+n, respectively, also lie in INF.

We claim that for all E ⊆ N, f(E+n) = (f′E)+n. To see this, note that r ∈ f(E+n) ↔ (∃x ∈ E)(r = f(x+n)) ↔ (∃x ∈ E)(r-n = f(x+n)-n) ↔ (∃x ∈ E)(r-n = f′(x)) ↔ r-n ∈ f′E ↔ r ∈ (f′E)+n. Analogously, g(E+n) = (g'E)+n.

We now have

X′ ∪ fY′ = X+n ∪ f(Y+n) = X+n ∪ (f′Y)+n = (X ∪ f′Y)+n ⊆ (V ∪ g′W)+n = V+n ∪ (g′W)+n = V+n ∪ g(W+n) = V′ ∪ gW′.

X′ ∩ fY′ = X+n ∩ f(Y+n) = X+n ∩ (f′Y)+n = (X ∩ f′Y)+n = ∅.
V′ ∩ gW′ = V+n ∩ g(W+n) = V+n ∩ (g′W)+n = (V ∩ g′W)+n = ∅.

The second clause

P′ ∪. fR′ ⊆ S′ ∪. gT′

is verified in the same way.

For the other four attributes, note that for all E ⊆ N, E and E+n have the same cardinality. QED

Theorem 3.1.1 does not mean that ELG and ELG ∩ SD behave the same way in other BRT contexts - e.g., in EBRT in A,fA. Nor does it mean that EVSD and SD behave the same way in other BRT contexts, either.

In fact, consider the equation A ∪. fA = U (the Complementation Theorem). This equation is correct in EBRT in A,fA on (SD,INF), but incorrect in EBRT in A,fA on (ELG,INF). The function f(x) = 2x serves as a counterexample.

THEOREM 3.1.2. Suppose that for all f,g ∈ SD there exist A,B,C ∈ INF such that X ∪. fY ⊆ V ∪. gW and P ∪. fR ⊆ S ∪. gT. Then for all f,g ∈ EVSD there exist A,B,C ∈ INF such that X ∪. fY ⊆ V ∪. gW and P ∪. fR ⊆ S ∪. gT. The same is true if we replace “A,B,C ∈ INF” by “arbitrarily large A,B,C ⊆ N”, “arbitrarily large finite A,B,C ⊆ N”, “nonempty finite A,B,C ⊆ N”, or “nonempty A,B,C ⊆ N”.

Proof: Follow the proof of Theorem 3.1.1. The only difference between the proofs is that here we need only verify that if f,g ∈ EVSD then f',g' ∈ SD. QED

We have observed that ELG, ELG ∩ SD, SD, EVSD behave the same with regard to the Template (i.e., with INF), except for the Exotic Cases (see Theorem 6.3.5). Thus in this Chapter, we will be using EVSD whenever we are proving INF.

We know that ELG (or equivalently, ELG ∩ SD) and SD (or equivalently EVSD) do behave differently on some of the five attributes, even with the non Exotic Cases. See Theorem 3.3.10 for an example with the attribute AL.

Note that there are exactly 81 clauses and $81^2 = 3^8 = 6561$ ordered pairs of clauses used in the Template. This is a large number of cases to analyze, and so we will take full advantage of whatever shortcuts we can find.

The main shortcut that we use very effectively is syntactic equivalence. We also need to make sure that we in fact determine all 6561 truth values, without leaving any cases out. This requires some effective organization of the work.

DEFINITION 3.1.4. We say that (α,β) and (γ,δ) are pair equivalent if and only if there is a permutation π of {A,B,C} such that

$$\text{i) } \pi\alpha = \gamma \wedge \pi\beta = \delta\text{; or}$$
$$\text{ii) } \pi\alpha = \delta \wedge \pi\beta = \gamma.$$

Obviously, if two ordered pairs of clauses are pair equivalent then the truth values of the corresponding Template statements are the same.

In this section, we generate a unique set of representatives for all the equivalence classes under the ordered pair equivalence relation. These representatives are organized into 11 groups that correspond to sections 3.3 - 3.13.

We find that there are a total of 574 equivalence classes under the pair equivalence relation. In sections 3.3 - 3.13, we determine the truth values of the 574 corresponding Template statement, within RCA_0, with the one exception of the Exotic Cases.

Section 3.14 annotates the set of representatives constructed in this section with these truth values. Section 3.15 is devoted to observed facts about the classification in section 3.14.

LEMMA 3.1.3. The following is provable in RCA_0. Let $(\alpha,\beta),(\gamma,\delta)$ be two pair equivalent ordered pairs of clauses, and let P be any one of our five attributes INF, AL, ALF, FIN, NON. Then $P(\alpha,\beta) \leftrightarrow P(\gamma,\delta)$. Moreover, if $\alpha = \beta$ then $P(\alpha) \leftrightarrow P(\beta) \leftrightarrow P(\alpha,\alpha) \leftrightarrow P(\beta,\beta)$.

Proof: Obvious. QED

Let the ordered pair of clauses

$$\alpha = X \cup. fY \subseteq V \cup. gW$$
$$\beta = P \cup. fR \subseteq S \cup. gT$$

be given.

DEFINITION 3.1.5. The inner (outer) trace of (α,β) is YVRS (XWPT).

We also consider traces independently of ordered pairs of clauses.

DEFINITION 3.1.6. A trace is a length 4 string from {A,B,C}. There are $3^4 = 81$ traces.

DEFINITION 3.1.7. Let XYVW be a trace. The reverse of XYVW is VWXY.

Any permutation π of {A,B,C} transforms any trace XYVW to the trace $\pi X\pi Y\pi V\pi W$.

DEFINITION 3.1.8. Two traces are equivalent if and only if there is a permutation that transforms the first into the second, or a permutation that transforms the first into the reverse of the second.

Equivalence of inner (outer) traces is easily seen to be an equivalence relation.

LEMMA 3.1.4. If two ordered pairs of clauses are pair equivalent, then their inner (outer) traces are equivalent.

Proof: Obvious. QED

LEMMA 3.1.5. Every trace is equivalent to exactly one of the following traces.
1. AAAA.
2. AAAB.
3. AABA.
4. AABB.
5. AABC.
6. ABAB.
7. ABAC.
8. ABBA.
9. ABBC.
10. ABCB.

Proof: We first show that every trace is equivalent to at least one of these 10. Let α be a trace. We go through a series of steps resulting in one of these 10.

First permute α so that the first term is A. Next, if the second term is C, interchange C with B so that the first two terms are AB. Note that the first two terms are AA or AB.

We now split into cases according to the first three terms.

case 1. AAA. Note that AAAA and AAAB are already on the list. AAAC is equivalent to AAAB.

case 2. AAB. Note that all three continuations are on the list.

case 3. AAC. Permute C and B, and apply case 2.

case 4. ABA. ABAB and ABAC are on the list. ABAA is the reversal of AAAB, and hence ABAA is equivalent to AAAB. AAAB is on the list.

case 5. ABB. ABBA and ABBC are on the list. ABBB is equivalent to BBAB and to AABA, which is on the list.

case 6. ABC. ABCA is equivalent to CAAB and to ABBC, which is on the list. ABCB is on the list. ABCC is equivalent to CCAB and to AABC, which is on the list.

Now we show that all 10 are inequivalent.

1. AAAA. This has the following property preserved under equivalence: just one letter is used. The remaining 9 do not have this property.
2. AAAB. This has the following property preserved under equivalence: there are exactly three equal letters and the first and third letters are the same. The remaining 9 do not have this property.
3. AABA. This has the following property preserved under equivalence: there are exactly three equal letters and the first and third letters are different. The remaining 9 do not have this property.
4. AABB. This has the following property preserved under equivalence: the first two letters equal, the last two letters are equal, and not all letters are equal. The remaining 9 do not have this property.
5. AABC. This has the following property preserved under equivalence: all three letters are used, and either the first two letters are the same, or the last two letters are the same. The remaining 9 do not have this property.
6. ABAB. This has the following property preserved under equivalence: the first and third letters are the same, the second and fourth letters are the same, and not all letters are equal. The remaining 9 do not have this property.
7. ABAC. This has the following property preserved under equivalence: all three letters are used, where the first and third letters are equal. The remaining 9 do not have this property.
8. ABBA. This has the following property preserved under equivalence: the first and last letters are equal, the middle two letters are equal, and not all letters are equal. The remaining 9 do not have this property.
9. ABBC. This has the following property preserved under equivalence: all three letters are used, where the two middle letters are equal, or the first and last letters are equal. The remaining 9 do not have this property.
10. ABCB. This has the following property preserved under equivalence: all three letters are used, where the second and fourth letters are equal. The remaining 9 do not have this property.

QED

LEMMA 3.1.6. Every ordered pair of clauses is pair equivalent to an ordered pair of clauses whose inner trace is among
1. AAAA.
2. AAAB.
3. AABA.

4. AABB.
5. AABC.
6. ABAB.
7. ABAC.
8. ABBA.
9. ABBC.
10. ACBC.

Proof: Immediate from Lemma 3.1.5. Note that we have changed item 10 from Lemma 1.3 by interchanging B and C. The reason for this change is that the inner trace of the ordered pair of clauses in Proposition A is ACBC, and we like the exact choice of letters in Proposition A. QED

In section 3.3 we handle all of the duplicates (α,α). We remove these duplicates from consideration in sections 3.4 and 3.9 where they arise. Obviously, they do not arise in the remaining sections.

We now wish to give the unique set of representatives of the pair equivalence classes of the ordered pairs of clauses that we use to tabulate our results in the annotated tables of section 3.14.

To support our choice of unique representatives, we establish a number of facts.

We have been working with pair equivalence, and inner (outer) traces, for ordered pairs of clauses. It is convenient to have these notions for a single clause:

DEFINITION 3.1.9. Two individual clauses are considered equivalent if and only if there is a permutation of {A,B,C} then sends one to the other. The inner (outer) trace of the single clause X ∪. fY ⊆ V ∪. gW. is defined to be YV, XW, respectively.

LEMMA 3.1.7. Every clause is equivalent to a clause where
i) the inner trace is AA; or
ii) the inner trace is AB.
No clause in one of these two categories is equivalent to any clause in the other of these two categories.

Proof: If the inner trace begins with B or C, then permute it with A, so that the inner trace now begins with A. If the inner trace is AC, then permute C and B, so that the inner trace is now AB.

Let π be a permutation of {A,B,C}. It is clear that π must map any clause with inner trace AA to a clause with trace XX. Hence no clause in category i) can be equivalent to a clause in category ii). Also, π must map any clause with inner trace AB to a clause with inner trace XY, X ≠ Y. Hence no clause in category ii) can be equivalent to a clause in category i). QED

Lemma 3.1.7 supports the unique set of representatives of individual clauses (or, equivalently, duplicates), presented in the following way.

We list all individual clauses according to Lemma 3.1.7, ordered first by the two categories i),ii), and then lexicographically (reading the four letters from left to right). These are consecutively numbered starting with 1. But if a clause is equivalent to some earlier clause, then we label it with an x, and also point to the earlier numbered clause to which it is equivalent.

SINGLE CLAUSES (14)

1. A ∪. fA ⊆ A ∪. gA.
2. A ∪. fA ⊆ A ∪. gB.
x. A ∪. fA ⊆ A ∪. gC. ≡ 2.

3. B ∪. fA ⊆ A ∪. gA.
4. B ∪. fA ⊆ A ∪. gB.
5. B ∪. fA ⊆ A ∪. gC.

x. C ∪. fA ⊆ A ∪. gA. ≡ 3.
x. C ∪. fA ⊆ A ∪. gB. ≡ 5.
x. C ∪. fA ⊆ A ∪. gC. ≡ 4.

6. A ∪. fA ⊆ B ∪. gA.
7. A ∪. fA ⊆ B ∪. gB.
8. A ∪. fA ⊆ B ∪. gC.

9. B ∪. fA ⊆ B ∪. gA.
10. B ∪. fA ⊆ B ∪. gB.
11. B ∪. fA ⊆ B ∪. gC.

12. C ∪. fA ⊆ B ∪. gA.
13. C ∪. fA ⊆ B ∪. gB.
14. C ∪. fA ⊆ B ∪. gC.

The numbered part of this table, annotated, appears in section 3.14.

DEFINITION 3.1.10. An AAAA ordered pair is an ordered pair of **distinct** clauses whose inner trace is AAAA. We also use this terminology for the other 9 traces in Lemma 3.1.6 (which are the titles of sections 3.5 - 3.13).

Thus we are using the ten inner traces of Lemma 3.1.6 to divide the (non duplicate) ordered pairs mod pair equivalence into ten more manageable categories. The ordered pairs within each category have different outer traces.

LEMMA 3.1.8. Every AAAA ordered pair is pair equivalent to an AAAA ordered pair whose outer trace
i) uses exactly A,B; or
ii) uses exactly B,C, with outer trace beginning with B; or
iii) uses exactly A,B,C, whose outer trace begins with AA,AB, or B.
No ordered pair of clauses in any one of these three categories is pair equivalent to any ordered pair of clauses in any other of these categories.

Proof: Let α be an AAAA ordered pair. The outer trace of α cannot use exactly one letter, since then the items in the ordered pair would be identical.

Suppose the outer trace of α uses exactly B or exactly C. Then the two components of β are the same, which is impossible.

Suppose the outer trace of α uses exactly A,C. By interchanging B,C, we obtain an AAAA ordered pair whose outer trace uses exactly A,B.

Suppose the outer trace of α uses exactly B,C, with outer trace beginning with C. By interchanging B,C, we obtain an AAAA ordered pair whose outer trace uses exactly B,C, and which begins with B.

Suppose the outer trace of α uses exactly A,B,C, and begins with C. By interchanging B,C, we obtain an AAAA ordered pair whose outer trace uses exactly A,B,C, and which begins with B.

Suppose the outer trace of α uses exactly A,B,C, and begins with AC. By interchanging B,C, we obtain an AAAA ordered pair whose outer trace uses exactly A,B,C, and which begins with AB.

Note that categories i)-iii) list all possibilities other than the ones in the previous five paragraphs. Hence i)-iii) is inclusive.

Now suppose $\alpha \neq \beta$ be pair equivalent AAAA ordered pairs. Let π transform α to β. Then $\pi A = A$. Clearly π cannot take us from an ordered pair in any category i)-iii) to any ordered pair in a different category i)-iii). This establishes the final claim. QED

Lemma 3.1.8 supports the unique set of representatives for AAAA ordered pairs, presented in the following way.

We list all ordered pairs of clauses according to Lemma 3.1.8, ordered first by the four categories i)-iii), and then lexicographically (reading the eight letters from left to right). These are consecutively numbered starting with 1. But if an ordered pair is pair equivalent to some earlier ordered pair, then we label it with an x, and also point to the earlier numbered ordered pair of clauses to which it is pair equivalent.

In fact, the previous paragraph describes exactly how we will present the ordered pairs according to later Lemmas.

AAAA (20)

1. A ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ A ∪. gB.
2. A ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gA.
3. A ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gB.

x. A ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ A ∪. gA. ≡ 1.
4. A ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gA.
5. A ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gB.

x. B ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ A ∪. gA. ≡ 2.
x. B ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ A ∪. gB. ≡ 4.
6. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gB.

x. B ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ A ∪. gA. ≡ 3.
x. B ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ A ∪. gB. ≡ 5.
x. B ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gA. ≡ 6.

7. B ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gC.
8. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gB.
9. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gC.

x. B ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ A ∪. gB. ≡ 7.
10. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ A ∪. gB.
x. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ A ∪. gC. ≡ 8.

11. A ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gC.
x. A ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gB. ≡ 11.

12. A ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ A ∪. gC.
13. A ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gC.
14. A ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gA.
15. A ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gB.
16. A ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gC.

x. B ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ A ∪. gC. ≡ 14.
17. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gC.
18. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gA.
19. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gB.
20. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gC.

x. B ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ A ∪. gC. ≡ 16.
x. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gA. ≡ 20.

x. B ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ A ∪. gA. ≡ 11.
x. B ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ A ∪. gB. ≡ 13.
x. B ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ A ∪. gC. ≡ 15.
x. B ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ A ∪. gA. ≡ 17.
x. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ A ∪. gA. ≡ 19.

The numbered part of this AAAA table, annotated, appears in section 3.14.

LEMAM 3.1.9. No AAAB ordered pair is pair equivalent to any other AAAB ordered pair. All 81 AAAB ordered pairs are pair inequivalent.

Proof: Let $\alpha \neq \beta$ be AAAB ordered pairs. First suppose π transforms α to β. Then πA = A and πB = B. Hence π is the identity, and $\alpha = \beta$.

Now suppose π transforms α to the reverse of β. Note that the reverse of β is an ABAA ordered pair. Then πA = A and πA = B, which is impossible. QED

Since all 81 AABA ordered pairs are pair inequivalent, there is no point in listing them here. The annotated AAAB table appears in section 3.14.

LEMMA 3.1.10. No AABA ordered pair is pair equivalent to any other AABA ordered pair. All 81 AABA ordered pairs are pair inequivalent.

Proof: Let $\alpha \neq \beta$ be AABA ordered pairs. First suppose π transforms α to β. Then $\pi A = A$ and $\pi B = B$. Hence π is the identity, and $\alpha = \beta$.

Now suppose π transforms α to the reverse of β. Note that the reverse of β is a BAAA ordered pair. Then $\pi A = B$ and $\pi A = A$, which is impossible. QED

The AABA table, annotated, appears in section 3.14.

LEMMA 3.1.11. Every AABB ordered pair is pair equivalent to an AABB ordered pair whose outer trace
i) uses exactly A; or
ii) uses exactly C; or
iii) uses exactly A,B; or
iv) uses exactly A,C; or
v) uses exactly A,B,C.
No ordered pair in any one of these 5 categories is pair equivalent to a ordered pair in any other category.

Proof: Let α be an AABB ordered pair. Suppose the outer trace of α uses exactly B. By interchanging A,B, we obtain a BBAA ordered pair β whose outer trace uses exactly A. Note that the reverse of β is an AABB ordered pair whose outer trace uses exactly A.

Suppose the outer trace of α uses exactly B,C. By interchanging A,B, we obtain a BBAA ordered pair β whose outer trace uses exactly A,C. Note that the reverse of β is an AABB ordered pair whose outer trace uses exactly A,C.

Note that categories i)-v) list all possibilities other than exactly B, exactly B,C, and so i)-v) is inclusive.

Now suppose $\alpha \neq \beta$ be pair equivalent AABB ordered pairs. Let π transform α to β. Then $\pi A = A$, $\pi B = B$, and so π is the identity Hence $\alpha = \beta$, which is impossible. Let π transform α to the reverse of β. Then π interchanges A,B. Clearly π cannot take us from an ordered pair in any category i)-v) to any ordered pair in a different category i)-v). This establishes the final claim. QED

We now list the AABB ordered pairs in our by now standard way.

AABB (45)

1. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gA.
2. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gC.

3. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gB.
4. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gA.
5. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gB.

6. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gA.
7. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gB.
8. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ B ∪. gA.
x. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ B ∪. gB. ≡ 4.

9. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gA.
10. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gB.
x. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gA. ≡ 7.
x. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gB. ≡ 3.

11. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gA.
x. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gB. ≡ 9.
x. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ B ∪. gA. ≡ 6.

12. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gC.
13. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gA.
14. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gC.

15. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gA.
16. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gC.
17. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gA.
18. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gC.

19. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gA.
20. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gC.
21. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gA.
22. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gC.

23. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gA.
24. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gC.
25. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gA.

26. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gC.
27. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gB.

28. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gC.
29. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ B ∪. gC.
30. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gA.

31. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gB.
32. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gC.

33. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gB.
x. A ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ B ∪. gA. ≡ 29.
x. A ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ B ∪. gB. ≡ 26.
34. A ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ B ∪. gC.
35. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gB.

36. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gC.
x. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gC. ≡ 33.
37. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gA.
38. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gB.
39. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gC.

40. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gC.
41. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gA.

x. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gA. ≡ 40.
x. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gB. ≡ 36.
42. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gC.
x. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ B ∪. gA. ≡ 28.
43. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gA.

x. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gB. ≡ 38.
x. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gA. ≡ 31.
x. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gB. ≡ 27.
x. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gC. ≡ 35.
44. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gB.

x. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gA. ≡ 41.
x. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gB. ≡ 37.
x. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gC. ≡ 43.
x. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ B ∪. gA. ≡ 30.
45. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gA.

x. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gB. ≡ 39.
x. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ B ∪. gA. ≡ 32.

The numbered part of this AABB table, annotated, appears in section 3.14.

LEMMA 3.1.12. No AABC ordered pair is pair equivalent to any other AABC ordered pair. All 81 AABC ordered pairs are pair inequivalent.

Proof: Let $\alpha \neq \beta$ be AABC ordered pairs. First suppose π transforms α to β. Then $\pi A = A$, $\pi B = B$, $\pi C = C$. Hence π is the identity, and $\alpha = \beta$.

Now suppose π transforms α to the reverse of β. Note that the reverse of β is a BCAA ordered pair. Then $\pi A = B$ and $\pi A = C$, which is impossible. QED

The AABC table, annotated, appears in section 3.14.

LEMMA 3.1.13. Two distinct ABAB ordered pairs α,β are pair equivalent if and only if the reverse of α is β.

Proof: Let $\alpha \neq \beta$ be pair equivalent ABAB ordered pairs. Let π transform α to β. Then $\pi A = A$, $\pi B = B$, and so π is the identity. Hence $\alpha = \beta$,

Now suppose π transforms α to the reverse of β. Then again π is the identity, and so α is the reverse of β. QED

ABAB (36)

1. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gB.
2. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gC.
3. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gA.
4. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gB.
5. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gC.
6. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gA.
7. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB.
8. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gC.

x. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gA. ≡ 1.
9. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gC.
10. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gA.
11. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gB.
12. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gC.
13. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gA.
14. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gB.
15. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gC.

x. A ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ B ∪. gA. ≡ 2.
x. A ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ B ∪. gB. ≡ 9.
16. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gA.
17. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gB.
18. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gC.
19. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gA.
20. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gB.
21. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gC.

x. B ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gA. ≡ 3.
x. B ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gB. ≡ 10.
x. B ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gC. ≡ 16.
22. B ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gB.
23. B ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gC.
24. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gA.
25. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB.
26. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gC.

x. B ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gA. ≡ 4.
x. B ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gB. ≡ 11.
x. B ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gC. ≡ 17.
x. B ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gA. ≡ 22.
27. B ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gC.
28. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gA.
29. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gB.
30. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gC.

x. B ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ B ∪. gA. ≡ 5.
x. B ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ B ∪. gB. ≡ 12.
x. B ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ B ∪. gC. ≡ 18.
x. B ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gA. ≡ 23.
x. B ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gB. ≡ 27.
31. B ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gA.
32. B ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gB.
33. B ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gC.

x. C ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gA. ≡ 6.
x. C ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gB. ≡ 13.
x. C ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gC. ≡ 19.
x. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gA. ≡ 24.
x. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gB. ≡ 28.
x. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gC. ≡ 31.
34. C ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB.
35. C ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gC.

x. C ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gA. ≡ 7.
x. C ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gB. ≡ 14.
x. C ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gC. ≡ 20.
x. C ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gA. ≡ 25.
x. C ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gB. ≡ 29.
x. C ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gC. ≡ 32.
x. C ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gA. ≡ 34.
36. C ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gC.

x. C ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ B ∪. gA. ≡ 8.
x. C ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ B ∪. gB. ≡ 15.

x. C ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ B ∪. gC. ≡ 21.
x. C ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gA. ≡ 26.
x. C ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gB. ≡ 30.
x. C ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gC. ≡ 33.
x. C ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gA. ≡ 35.
x. C ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gB. ≡ 36.

The numbered part of this ABAB table, annotated, appears in section 3.14.

LEMMA 3.1.14. Every ABAC ordered pair is pair equivalent to an ABAC ordered pair whose outer trace
i) uses exactly A; or
ii) uses exactly B; or
iii) uses exactly A,B; or
iv) uses exactly B,C; or
v) uses exactly A,B,C.
No ordered pair in any one of these 5 categories is pair equivalent to an ordered pair in any other category.

Proof: Let α be an ABAC ordered pair. Suppose the outer trace of α uses exactly C. By interchanging B,C, we obtain a pair equivalent ACAB ordered pair whose outer trace uses exactly B. Its reverse is a pair equivalent ABAC ordered pair whose outer trace uses exactly B.

Suppose the outer trace of α uses exactly A,C. By interchanging B,C, we obtain a pair equivalent ACAB ordered pair whose outer trace uses exactly A,B. Its reverse is a pair equivalent ABAC ordered pair whose outer trace uses exactly A,B.

Note that categories i)-v) list all possibilities other than exactly C, exactly A,C, and so i)-v) is inclusive.

Now suppose α ≠ β are pair equivalent ABAC ordered pairs. Let π transform α to β. Then πA = A, πB = B, πC = C, and so π is the identity. Hence α = β, which is impossible. Let π transform α to the reverse of β. Then π interchanges B,C. Clearly π cannot take us from an ordered pair in any category i)-v) to any ordered pair in a different category i)-v). This establishes the final claim. QED

ABAC (45)

1. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gA.
2. B ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gB.

3. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gB.
4. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gA.
5. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gB.

6. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gA.
7. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gB.
8. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gA.
9. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gB.

10. B ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gA.
11. B ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gB.
12. B ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gA.
13. B ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gB.

14. B ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gA.
15. B ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gB.
16. B ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gA.

17. B ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gC.
18. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gB.
19. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gC.

20. B ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gB.
21. B ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gC.
22. B ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ C ∪. gB.
x. B ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ C ∪. gC. ≡ 18.

23. C ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gB.
24. C ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gC.
x. C ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gB. ≡ 21.
x. C ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gC. ≡ 17.

25. C ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gB.
x. C ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gC. ≡ 23.
x. C ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ C ∪. gB. ≡ 20.

26. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gC.
27. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ C ∪. gB.

28. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gC.
29. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gC.
30. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gA.
31. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gB.
32. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gC.

33. A ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ C ∪. gB.
34. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gA.
35. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gB.

36. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gC.
37. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ C ∪. gB.

x. B ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gC. ≡ 30.
38. B ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gC.
39. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ C ∪. gA.
40. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ C ∪. gB.
41. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ C ∪. gC.

x. B ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gC. ≡ 32.
x. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gA. ≡ 41.

x. B ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ C ∪. gA. ≡ 27.
x. B ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ C ∪. gB. ≡ 37.
x. B ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ C ∪. gC. ≡ 31.
42. B ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gA.
x. B ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ C ∪. gA. ≡ 40.

x. C ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gB. ≡ 34.
43. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gA.
44. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gB.
45. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gC.
x. C ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ C ∪. gB. ≡ 42.

x. C ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gA. ≡ 26.
x. C ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gB. ≡ 36.
x. C ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gC. ≡ 29.
x. C ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gA. ≡ 45.
x. C ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gA. ≡ 38.

x. C ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ C ∪. gB. ≡ 35.
x. C ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gA. ≡ 44.

The numbered part of this ABAC table, annotated, appears in section 3.14.

LEMMA 3.1.15. Every ABBA ordered pair is pair equivalent to an ABBA ordered pair whose outer trace
i) uses exactly A; or
ii) uses exactly C; or
iii) uses exactly A,B; or
iv) uses exactly A,C; or
v) uses exactly A,B,C.
No ordered pair in any one of these 5 categories is pair equivalent to an ordered pair in any other category. Two distinct ABBA ordered pairs are pair equivalent if and only if the result of interchanging A,B in α is the reverse of β.

Proof: Let α be an ABBA ordered pair. Suppose the outer trace of α uses exactly B. By interchanging A,B, we obtain a pair equivalent BAAB ordered pair whose outer trace uses exactly A. Its reverse is a pair equivalent ABBA ordered pair whose outer trace uses exactly A.

Suppose the outer trace of α uses exactly B,C. By interchanging A,B, we obtain a pair equivalent BAAB ordered pair whose outer trace uses exactly A,C. Its reverse is a pair equivalent ABBA ordered pair whose outer trace uses exactly A,C.

Note that categories i)-v) list all possibilities other than exactly B, exactly B,C, and so i)-v) is inclusive.

Let $\alpha \neq \beta$ be pair equivalent ABBA ordered pairs. Let π be a permutation of {A,B,C} that transforms α to β. Then πA = A, πB = B, and so π is the identity. Hence $\alpha = \beta$, which is impossible. Suppose π transforms α to the reverse of β. Then β is a BAAB ordered pair, and so πA = B, πB = A. Clearly π cannot take us from an ordered pair in any category i)-v) to any ordered pair in a different category i)-v). This establishes the final claim. QED

ABBA (45)

1. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gA.
2. C ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gC.

3. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gB.
4. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gA.
5. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gB.

6. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gA.
7. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gB.
8. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ A ∪. gA.
x. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ A ∪. gB. ≡ 4.

9. B ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gA.
10. B ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gB.
x. B ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gA. ≡ 7.
x. B ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gB. ≡ 3.

11. B ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gA.
x. B ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gB. ≡ 9.
x. B ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ A ∪. gA. ≡ 6.

12. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gC.

13. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gA.
14. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gC.

15. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gA.
16. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gC.
17. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gA.
18. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gC.

19. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gA.
20. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gC.
21. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gA.
22. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gC.

23. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gA.
24. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gC.
25. C ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gA.

26. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gC.
27. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gB.

28. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gC.
29. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ A ∪. gC.
30. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gA.
31. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gB.
32. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gC.

33. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gB.
x. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ A ∪. gA. ≡ 29.
x. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ A ∪. gB. ≡ 26.
34. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ A ∪. gC.
35. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gB.

36. B ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gC.
x. B ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gC. ≡ 33.
37. B ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gA.
38. B ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gB.
39. B ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gC.

40. B ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gC.
41. B ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gA.

x. B ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gA. ≡ 40.
x. B ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gB. ≡ 36.
42. B ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gC.
x. B ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ A ∪. gA. ≡ 28.
43. B ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gA.

x. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gB. ≡ 38.

x. C ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gA. ≡ 31.
x. C ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gB. ≡ 27.
x. C ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gC. ≡ 35.
44. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gB.

x. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gA. ≡ 41.
x. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gB. ≡ 37.
x. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gC. ≡ 43.
x. C ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ A ∪. gA. ≡ 30.
45. C ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gA.

x. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gB. ≡ 39.
x. C ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ A ∪. gA. ≡ 32.

The numbered part of this ABBA list, annotated, appears in section 3.14.

LEMMA 3.1.16. No ABBC ordered pair is pair equivalent to any other ABBC ordered pair. All 81 ABBC ordered pairs are pair inequivalent.

Proof: Let $\alpha \neq \beta$ be ABBC ordered pairs. First suppose π transforms α to β. Then $\pi A = A$, $\pi B = B$, $\pi C = C$. Hence π is the identity, and $\alpha = \beta$.

Now suppose π transforms α to the reverse of β. Note that the reverse of β is a BCAB ordered pair. Then $\pi B = C$, $\pi B = A$, which is a contradiction. QED

The ABBC table, annotated, appears in section 3.14.

LEMMA 3.1.17. Every ACBC ordered pair is pair equivalent to an ACBC ordered pair whose outer trace
i) uses exactly A; or
ii) uses exactly C; or
iii) uses exactly A,C; or
iv) uses exactly A,B; or
v) uses exactly A,B,C.
No ordered pair in any one of these 5 categories is pair equivalent to an ordered pair in any other category.

Proof: Let α be an ACBC ordered pair. Suppose the outer trace of α uses exactly B. By interchanging A,B, we obtain a pair equivalent BCAC ordered pair whose outer trace uses exactly A. Its reverse is a pair equivalent ACBC ordered pair whose outer trace uses exactly A.

Suppose the outer trace of α uses exactly B,C. By interchanging A,B, we obtain a pair equivalent BCAC ordered pair whose outer trace uses exactly A,C. Its reverse is a pair equivalent ACBC ordered pair whose outer trace uses exactly A,C.

Note that categories i)-v) list all possibilities other than exactly B, exactly B,C, and so i)-v) is inclusive.

Let α ≠ β be pair equivalent ACBC ordered pairs. Let π be a permutation of {A,B,C} that transforms α to β. Then πA = A, πC = C, and so π is the identity. Hence α = β, which is impossible. Suppose π transforms α to the reverse of β. Then β is a BCAC ordered pair, and so πA = B, πB = A. Clearly β cannot transform any ordered pair in any category 1)-v) to any ordered pair in any different category i)-v). This establishes the final claim. QED

ACBC (45)

1. A ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gA.
2. C ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gC.

3. A ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gC.
4. A ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gA.
5. A ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gC.

6. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gA.
7. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gC.
8. A ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gA.
9. A ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gC.

10. C ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gA.
11. C ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gC.
12. C ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gA.
13. C ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gC.

14. C ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gA.
15. C ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gC.
16. C ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gA.

17. A ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gB.
18. A ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gA.
19. A ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gB.

20. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gA.
21. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gB.
22. A ∪. fA ⊆ C ∪. gB, B ∪. fB ⊆ C ∪. gA.

x. A ∪. fA ⊆ C ∪. gB, B ∪. fB ⊆ C ∪. gB. ≡ 18.

23. B ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gA.
24. B ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gB.
x. B ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gA. ≡ 21.
x. B ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gB. ≡ 17.

25. B ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gA.
x. B ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gB. ≡ 23.
x. B ∪. fA ⊆ C ∪. gB, B ∪. fB ⊆ C ∪. gA. ≡ 20.

26. A ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gC.
27. A ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gB.

28. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gC.
29. A ∪. fA ⊆ C ∪. gB, B ∪. fB ⊆ C ∪. gC.
30. A ∪. fA ⊆ C ∪. gB, C ∪. fB ⊆ C ∪. gA.
31. A ∪. fA ⊆ C ∪. gB, C ∪. fB ⊆ C ∪. gB.
32. A ∪. fA ⊆ C ∪. gB, C ∪. fB ⊆ C ∪. gC.

33. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gB.
x. A ∪. fA ⊆ C ∪. gC, B ∪. fB ⊆ C ∪. gA. ≡ 29.
x. A ∪. fA ⊆ C ∪. gC, B ∪. fB ⊆ C ∪. gB. ≡ 26.
34. A ∪. fA ⊆ C ∪. gC, B ∪. fB ⊆ C ∪. gC.
35. A ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gB.

36. B ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gC.
x. B ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gC. ≡ 33.
37. B ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gA.
38. B ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gB.
39. B ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gC.

40. B ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gC.
41. B ∪. fA ⊆ C ∪. gB, C ∪. fB ⊆ C ∪. gA.

x. B ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gA. ≡ 40.
x. B ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gB. ≡ 36.
42. B ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gC.
x. B ∪. fA ⊆ C ∪. gC, B ∪. fB ⊆ C ∪. gA. ≡ 28.
43. B ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gA.

x. C ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gB. ≡ 38.
x. C ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gA. ≡ 31.
x. C ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gB. ≡ 27.
x. C ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gC. ≡ 35.
44. C ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gB.

x. C ∪. fB ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gA. ≡ 41.

x. C ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gB. ≡ 37.
x. C ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gC. ≡ 43.
x. C ∪. fA ⊆ C ∪. gB, B ∪. fB ⊆ C ∪. gA. ≡ 30.
45. C ∪. fA ⊆ C ∪. gB, C ∪. fB ⊆ C ∪. gA.

C ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gB. ≡ 39.
C ∪. fA ⊆ C ∪. gC, B ∪. fB ⊆ C ∪. gA. ≡ 32.

The numbered part of this ACBC table, annotated, appears in section 3.14.

THEOREM 3.1.18. There are exactly 574 ordered pairs of clauses up to pair equivalence.

Proof: From the above tables and lemmas, we have the following counts.

SINGLE CLAUSES (DUPLICATES). 14.
AAAA. 20.
AAAB. 81.
AABA. 81.
AABB. 45.
AABC. 81.
ABAB. 36.
ABAC. 45.
ABBA. 45.
ABBC. 81.
ACBC. 45.

This adds up to a total of 574 ordered pairs up to equivalence (including the 14 duplicates). As expected, this number is a bit larger than 6561/12 = 546.75, since the overwhelmingly majority of equivalence classes have 12 elements, with a few exceptions. QED

3.2. Some Useful Lemmas.

DEFINITION 3.2.1. The standard pairing function on N is the function $P:N^2 \rightarrow N$ due (essentially) to Cantor:

$$P(n,m) = (n^2+m^2+2nm+n+3m)/2 \geq n,m.$$

It is well known that P is a bijection, and also that for all n ≥ 0, $[0,n(n+1)/2) \subseteq P[[0,n)^2]$. In addition, P is strictly increasing in each argument.

Let $T:N^2 \to N$ be such that $T(2n,2m) = P(n,m)$, $T(2n,2m+1) = T(2n+1,2m) = T(2n+1,2m+1) = 2n+2m+2$. Then for all $n \geq 0$, $[0,n(n+1)/2) \subseteq T[([0,2n) \cap 2N)^2]$. Hence for all $n \geq 8$, every element of $[0,n^2/8)$ is realized as a value of T at even pairs from $[0,n)$.

It is clear that $T(2n,2m) \geq (n^2+2n)/2,(m^2+2m)/2 \geq 2n,2m$. Hence for $n,m \geq 2$, $T(n,m) \geq n,m$.

LEMMA 3.2.1. There exists 3-ary $f \in ELG \cap SD$ such that the following holds. Let $A \subseteq N$ be nonempty, where $fA \cap 2N \subseteq A$. Then fA is cofinite. We can also require that for all $n \geq 0$, $f(n,n,n) \in 2N$.

Proof: We define $f \in ELG \cap SD$ as follows. Let $p,q \in [2^n,2^{n+1})$, $n \geq 0$. Define $f(2^n,p,q) = \min(2^{n+1}+T(p-2^n,q-2^n),2^{n+2})$. Note that for $n \geq 8$, as p,q vary over the even elements of $[2^n,2^{n+1})$, every value in $[2^{n+1},2^{n+2})$ is realized. Also note that for all $n \geq 0$, $f(2^n,2^n,2^n) = 2^{n+1}$.

For all $n > 0$, define $f(n,n,n)$ to be the least $2^k \geq 2n$; $f(0,0,0) = 2$.

For all $n < m < r$, define $f(r,n,n) = 2r+1$, $f(r,n,m) = 2r+2$, $f(r,n,r) = 2r+3$, $f(r,m,n) = 2r+4$, $f(r,r,n) = 2r+5$. For all triples a,b,c, if f(a,b,c) has not yet been defined, define $f(a,b,c) = 2|a,b,c|+1$.

It is obvious that $f \in SD$. To see that $f \in ELG$, we need only examine the definition of $f(2^n,p,q)$, $p,q \in [2^n,2^{n+1})$, where n is sufficiently large. If $p,q \in [2^n,2^n+2^{n-1})$, then obviously $f(2^n,p,q) \geq 2^{n+1} \geq 4|2^n,p,q|/3$. If $p,q \notin [2^n,2^n+2^{n-1})$, then $f(2^n,p,q) \geq 2^{n+1}+T(p-2^n,q-2^n) \geq 2^{n+1} + 2^{n-1} \geq 5p/4,5q/4$. Also, $f(2^n,p,q) \leq 2^{n+2} \leq 2p,2q$. Therefore $f \in ELG$.

Let $A \subseteq N$ be nonempty, where $fA \cap 2N \subseteq A$. Let $f(\min(A),\min(A),\min(A)) = 2^k \geq 2$. Then $2^k \in fA \cap 2N$. Therefore $2^k \in A$.

Suppose $j \geq k$ and $2^j \in A$. Then $f(2^j,2^j,2^j) = 2^{j+1} \in fA$. We have thus established by induction that for all $j \geq k$, $2^j \in A$.

We now fix t such that $t > 8,\min(A)$, and $2^t \in A$. Then $\min(A) < 2^t < 2^{t+1}$ are all in A. Hence $\{2^{t+2},2^{t+2}+5] \subseteq fA$.

We inductively define $\alpha(0) = 6$, $\alpha(i+1) = \min((\alpha(i)^2-1)/8, 2^{t+i+3})$. Note that for all sufficiently large i, $\alpha(i) = 2^{t+i+2}$.

We now prove by induction on i that for all $i \geq 0$,

1) $[2^{t+i+2}, 2^{t+i+2} + \alpha(i)) \subseteq fA$.

We have already established that this is true for i = 0. Suppose this is true for a particular $i \geq 0$. We claim that

2) $[2^{t+i+2}, 2^{i+t+2} + \alpha(i)) \subseteq fA$.
3) $[2^{t+i+2}, 2^{i+t+2} + \alpha(i)) \cap 2N \subseteq A$.
4) $[2^{t+i+3}, 2^{t+i+3} + \alpha(i+1)) \subseteq f(([2^{t+i+2}, 2^{t+i+2} + \alpha(i)) \cap 2N)^2) \subseteq fA$.

2) is the induction hypothesis. 3) follows from 2) and $fA \cap 2N \subseteq A$.

For 4), let $x \in [2^{t+i+3}, 2^{t+i+3} + \alpha(i+1)) \subseteq [2^{t+i+3}, 2^{t+i+4})$. Then $0 \leq x-2^{t+i+3} < \alpha(i+1) \leq (\alpha(i)^2-1)/8$. By the choice of T, let $a,b < \alpha(i)$, $T(a,b) = x-2^{t+i+3}$, where a,b are even. Let $p = 2^{t+i+2} + a$, $q = 2^{t+i+2} + b$. Then $p,q \in [2^{t+i+2}, 2^{t+i+2} + \alpha(i))$, p,q are even, and $f(2^{t+2i+2},p,q) = x$.

This establishes that $[2^{t+i+3}, 2^{t+i+3} + \alpha(i+1)) \subseteq f[([2^{t+i+2}, 2^{t+i+1} + \alpha(i)) \cap 2N)^2]$. $f[([2^{t+i+2}, 2^{t+i+1} + \alpha(i)) \cap 2N)^2] \subseteq fA$ is immediate from $[2^{t+i+2}, 2^{i+t+2} + \alpha(i)) \cap 2N \subseteq A$.

This concludes the inductive argument for 1). Since for sufficiently large i, $\alpha(i) = 2^{t+i+2}$, we see that fA is cofinite. QED

We will need the following technical refinement of Lemma 3.2.1.

LEMMA 3.2.2. There exists 4-ary $g \in ELG \cap SD$ such that the following holds. Let $A \subseteq N$ have at least two elements, where $(\forall n \in gA \cap 2N)(4n+3 \in gA \rightarrow n \in A)$. Then gA is cofinite. We can also require that for all $n \in N$, $g(n,n,n,n) \in 2N$.

Proof: Let $f:N^3 \rightarrow N$ be as given by Lemma 3.2.1. We define $g:N^4 \rightarrow N$ as follows. Let $x \in N^3$. If $n = |x|$ then define $g(n,x) = f(x)$. If $n < |x|$ then define $g(n,x) = 4f(x)+3$. If $n > |x|$ then define $g(n,x) = 2n+1$. Note that $g(n,n,n,n) = f(n,n,n) \in 2N$. Also, if $n < |m,r,s|$ then $g(n,m,r,s) \geq$

$f(m,r,s) > m,r,s$, and if $n > m,r,s$, then $g(n,m,r,s) > n,m,r,s$. Hence $g \in ELG \cap SD$.

Let A be as given. Let $A' = A\backslash\{\min(A)\}$. Then A' is nonempty. Let $n \in fA' \cap 2N$. Let $n = f(x)$, $x \in A'^3$. Hence $4n+3 \in gA$ using min(A) as the first argument for g. Therefore $n \in A$, and so $n \in A'$.

We have thus shown that $fA' \cap 2N \subseteq A'$. By Lemma 3.2.1, fA' is cofinite. Hence gA is cofinite. QED

We will need a refinement of Lemma 3.2.1 in a different direction (Lemma 3.2.4).

LEMMA 3.2.3. Let $f \in ELG \cap SD$ have arity p. There exists $g,h_1,h_2 \in ELG \cap SD$, with arities 2p,1,1 respectively, such that $f(x_1,\ldots,x_p) = g(h_1(x_1),\ldots,h_1(x_p),h_2(x_1),\ldots,h_2(x_p))$ holds, with finitely many exceptional p-tuples. We can also require that $rng(h_1),rng(h_2) \subseteq 2N$, and each $g(n,\ldots,n)$ is even.

Proof: Let f,p be as given. Let $c,d > 1$ be rational constants such that

$$c|x| \le f(x) \le d|x|$$

holds with finitely many exceptions. Let t be sufficiently large relative to c,d. We can assume that $1 < c < 2 < d$.

We first define $h_1,h_2:[t,\infty) \to N$ by

$$h_1(x) = \text{the first integer} > c^{1/3}x \text{ that is divisible by } 4.$$
$$h_2(x) = h_1(x) + 4(x \bmod 8) + 4.$$

To see that $h(x) = (h_1(x),h_2(x))$ is one-one on $[t,\infty)$, suppose $h_1(x) = h_1(y)$ and $h_2(x) = h_2(y)$ and $x < y$. By subtraction, $4(x \bmod 8) + 4 = 4(y \bmod 8) + 4$, $x \equiv y \bmod 8$, and so $y \ge x+8$. Hence the first integer $> c^{1/3}y$ is at least the first integer $> c^{1/3}x$, plus 8. Hence $h_1(x) \ne h_1(y)$.

Extend h_1,h_2 on $[0,t)$ by

$$h_1(x) = h_2(x) = 2x+2.$$

Note that

$$c^{1/3}x \le h_1(x),h_2(x) \le 2x+2.$$

Hence $h_1,h_2 \in ELG \cap SD$, $rng(h_1) \cup rng(h_2) \subseteq 2N$, and h is one-one. Also $h_1(x) \leq h_1(x+1)$, and $h_1(x) < h_2(x) \leq h_1(x) + 36$.

We define $g:N^{2p} \rightarrow N$ as follows.

case 1. $(y_1,z_1),\ldots,(y_p,z_p) \in rng(h)$, and $|y_1,\ldots,y_p,z_1,\ldots,z_p| > ct$. Set $g(y_1,\ldots,y_p,z_1,\ldots,z_p) = f(h^{-1}(y_1,z_1),\ldots,h^{-1}(y_p,z_p))$.

case 2. Otherwise. Set $g(y_1,\ldots,y_p,z_1,\ldots,z_p) = 2|y_1,\ldots,y_p,z_1,\ldots,z_p|+2$.

We claim that $g \in ELG \cap SD$. To see this, note that g restricted to case 2 lies in $ELG \cap SD$. So it remains to consider case 1.

Let $h(x_1) = (y_1,z_1),\ldots,h(x_p) = (y_p,z_p)$. Then for all i,

$$h_1(x_i) = y_i,\ h_2(x_i) = z_i.$$
$$y_i,z_i \geq x_i.$$

Also let j be such that x_j is largest. Then $x_j = |y_1,\ldots,y_j| \geq t$, and so $x_j \geq |y_1,\ldots,y_p,z_1,\ldots,z_p| - 36$. Hence

$$x_j \geq c^{-1/3}|y_j,z_j| \geq c^{-1/2}|y_1,\ldots,y_p,z_1,\ldots,z_p|.$$

$$g(y_1,\ldots,y_p,z_1,\ldots,z_p) = f(x_1,\ldots,x_p) \leq d|x_1,\ldots,x_p| \leq d|y_1,\ldots,y_p,z_1,\ldots,z_p|.$$

$$g(y_1,\ldots,y_p,z_1,\ldots,z_p) = f(x_1,\ldots,x_p) \geq c|x_1,\ldots,x_p| = cx_j \geq cc^{-1/2}|y_1,\ldots,y_p,z_1,\ldots,z_p| \geq c^{1/2}|y_1,\ldots,y_p,z_1,\ldots,z_p|.$$

Hence $g \in ELG \cap SD$. Note that the case $g(n,\ldots,n)$ must lie in case 2. Hence $g(n,\ldots,n) \in 2N$.

Finally,

$$f(x_1,\ldots,x_p) = g(h_1(x_1),\ldots,h_1(x_p),h_2(x_1),\ldots,h_2(x_p))$$

holds according to case 1. The only exceptions are if $|h_1(x_1),\ldots,h_1(x_p),h_2(x_1),\ldots,h_2(x_p)| \leq ct$. But that is at most finitely many exceptions. QED

LEMMA 3.2.4. There exists a 8-ary $F \in ELG \cap SD$ such that the following holds. Let $A \subseteq N$ be nonempty, where $F(FA \cap 2N) \cap 2N \subseteq A$. Then FA is cofinite.

Proof: Let $f:N^3 \to N$ be as given by Lemma 3.2.1. By Lemma 3.2.3, let $g,h_1,h_2 \in ELG \cap SD$, with arities 6,1,1 respectively, such that

$$f(x,y,z) = g(h_1(x),h_1(y),h_1(z),h_2(x),h_2(y),h_2(z))$$

with finitely many exceptions, where $rng(h_1),rng(h_2) \subseteq 2N$, and each $g(n,...,n) \in 2N$.

We now define $F:N^8 \to N$ by cases.

case 1. $x_1 = x_2 = |x_3,...,x_8|$. Set $F(x_1,...,x_8) = g(x_3,...,x_8)$.

case 2. $x_1 = x_2 < x_3 = ... = x_8$. Set $F(x_1,...,x_8) = h_1(x_3)$.

case 3. $x_1 < x_2 < x_3 = ... = x_8$. Set $F(x_1,...,x_8) = h_2(x_3)$.

case 4. $x_2 < x_1 < |x_3,x_4,x_5| = |x_1,...,x_8|$. Set $F(x_1,...,x_8) = f(x_3,x_4,x_5)$.

case 5. Otherwise. Set $F(x_1,...,x_8) = 2|x_1,...,x_8|+1$.

It is obvious that $F \in ELG \cap SD$.

Assume $F(FA \cap 2N) \cap 2N \subseteq A$, where A is nonempty. Let $n \in A$. Then $F(n,...,n) \in 2N$, and we can keep applying F to diagonals, thereby obtaining an infinite subset of $A \cap 2N$.

Let A′ be the tail of A whose least element is greater than exactly two elements of A.

We claim that $fA' \subseteq F(FA' \cap 2N)$. To see this, let $n < m$ be the first two elements of A. Then by cases 2 and 3 above, for all $r \in A'$, $h_1(r),h_2(r) \in FA \cap 2N$. Let $x,y,z \in A'$. Now $f(x,y,z) = g(h_1(x),h_1(y),h_1(z),h_2(x),h_2(y),h_2(z)) = F(p,p,h_1(x),h_1(y),h_1(z),h_2(x),h_2(y),h_2(z)) \in F(FA \cap 2N)$, where $p = |h_1(x),h_1(y),h_1(z),h_2(x),h_2(y),h_2(z)|$.

In particular, $fA' \cap 2N \subseteq F(FA \cap 2N) \cap 2N \subseteq A$. Since f is strictly dominating, $fA' \cap 2N \subseteq A'$. By Lemma 3.2.1, fA′ is cofinite.

Clearly $fA' \subseteq FA$ by case 4. Hence FA is cofinite. QED

Let $f_1,...,f_k$ be indeterminate functions from EVSD. We consider the class of $f_1,...,f_k$,A-terms defined as follows.

i. A is an $f_1,...,f_k$,A-term.
ii. If s,t are $f_1,...,f_k$,A-terms, then s ∪ t is an $f_1,...,f_k$,A-term.
iii. If s is an $f_1,...,f_k$,A-term, then each f_is is an $f_1,...,f_k$,A-term.

LEMMA 3.2.5. Let k ≥ 1, $f_1,...,f_k$ ∈ EVSD, and $t_1,...,t_r$ be $f_1,...,f_k$,A-terms. There exists A ∈ INF such that each A ∩ t_i = ∅. We can require that min(A) be any given sufficiently large integer.

Proof: Let $f_1,...,f_k$ ∈ EVSD. Write each $t_i = t_i(f_1,...,f_k,A)$. Let n be sufficiently large. We define integers $n_0 < n_1 < ...$ as follows. Let $n_0 = n$. Suppose n_j has been defined, j ≥ 0. Let n_{j+1} to be such that

n_{j+1} is greater than n_j and all elements of each $t_i(f_1,...,f_k,\{n_0,...,n_j\})$.

Take A = $\{n_j: j \geq 0\}$. QED

3.3. Single Clauses (duplicates).

In this section we handle the relatively easy case of ordered pairs α,β of clauses, where α = β. We these duplicate ordered pairs as single clauses, α.

As we shall see, several single clauses have ¬NON, and so any ordered pair of clauses, at least one of which is such a clause, also has ¬NON, and does not have to be further considered. This will allow us to cut down significantly on the number of pairs of clauses that have to be considered in sections 3.4 - 3.13.

By Lemma 3.1.5, we see that every clause is equivalent to a clause whose inner signature is AA or AB.

Here are what we call the AA and AB tables, together with the outcomes of our five attributes, INF, AL, ALF, FIN, NON, introduced in section 3.1. These entries are justified by the Lemmas that follow.

AA

1. A ∪. fA ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2. A ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3. A ∪. fA ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

4. B ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5. B ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
6. B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
7. C ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
8. C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
9. C ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

AB

1. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
2. A ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
4. B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
7. C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
8. C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
9. C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

According to the procedure specified at the beginning of this Chapter, in order to validate TEMP 3, we use EVSD for the positive entries with attribute INF (other than the Exotic Case). Otherwise, we will always use ELG.

The following pertains to AA 1-3. Note that in the statement of Lemma 3.3.1, we use X as an unknown representing A,B, or C. We will make use of this convention throughout this Chapter.

LEMMA 3.3.1. A ∪. fA ⊆ A ∪. gX has ¬NON.

Proof: Define f,g ∈ ELG as follows. Let f(n) = 2n, g(n) = 2n+1. Let A ∪. fA ⊆ A ∪. gX, where A,X are nonempty. Let n ∈ A. Then 2n ∈ fA, 2n ∈ A. This contradicts A ∩ fA = ∅. QED

The following pertains to AA 4-9.

LEMMA 3.3.2. X ∪. fA ⊆ A ∪. gY has ¬INF, ¬FIN.

Proof: Let f be as given by Lemma 3.2.1. Let g ∈ ELG be defined by g(n) = 2n+1. Suppose X ∪. fA ⊆ A ∪. gY, where X,A,Y are nonempty. Then fA ∩ 2N ⊆ A. Hence fA is cofinite. Since X ∩ fA = ∅, we have that A is infinite and X is finite. This establishes that ¬INF, ¬FIN. QED

LEMMA 3.3.3. Let $g \in$ EVSD. Let n be sufficiently large. For all $S \subseteq [n,\infty)$, there exists a unique $A \subseteq S \subseteq A \cup. gA$. Furthermore, if S is infinite then A is infinite.

Proof: This is a variant of the Complementation Theorem from Section 1.3. Since n is sufficiently large, g is strictly dominating at all tuples x with $|x| \geq n$.

We define $A \subseteq S$ by induction on $k \in S$. Suppose membership in A for all $i \in S \cap [n,k)$ has been determined, where $k \in S$. We put k in A if and only if k is not yet a value of g at arguments from A. Note that if k is not yet a value of g at arguments from A, then k will never become a value of g at arguments from A. Hence $S \subseteq A \cup. gA$. It is clear from this inclusion that if S is infinite, then A is infinite.

For uniqueness, let $A \subseteq S \subseteq A \cup. gA$ and $B \subseteq S \subseteq B \cup. gB$. Let k be least such that $k \in A \leftrightarrow k \notin B$. Obviously, $k \in S$ and

$$k \in A \leftrightarrow k \notin gA.$$
$$k \in B \leftrightarrow k \notin gB.$$

Since g is strictly dominating on $[n,\infty)$, $A,B \subseteq [n,\infty)$, and $k \geq n$, we see that

$$k \in gA \leftrightarrow k \in g(A \cap [0,k)).$$
$$k \in gB \leftrightarrow k \in g(B \cap [0,k)).$$

Hence

$$k \in A \leftrightarrow k \notin g(A \cap [0,k)).$$
$$k \in B \leftrightarrow k \notin g(B \cap [0,k)).$$

Since $A \cap [0,k) = B \cap [0,k)$, we have

$$k \in A \leftrightarrow k \in B$$

contradicting the choice of k. QED

The following pertains to AA 4.

LEMMA 3.3.4. $B \cup. fA \subseteq A \cup. gA$ has AL.

Proof: Let $f,g \in$ ELG and $p > 0$. Let n be sufficiently large. Then $[n,n+p] \notin f[[n,\infty)] \cup g[[n,\infty)]$. By Lemma 3.3.3, let $A \subseteq [n,\infty) \subseteq A \cup. gA$. Then $[n,n+p] \subseteq A$. Let $B = [n,n+p]$. QED

The following pertains to AA 5.

LEMMA 3.3.5. B ∪. fA ⊆ A ∪. gB has AL.

Proof: Let f,g ∈ ELG and p > 0. Let B = [n,n+p], where n is sufficiently large. Let A = [n,∞)\gB. Since B ∪ fA ⊆ [n,∞), we have B ∪ fA ⊆ A ∪ gB. Also B ∩ f([n,∞)) = ∅. QED

The following pertains to AA 4 - 9.

LEMMA 3.3.6. X ∪. fA ⊆ A ∪. gY has AL, provided X ∈ {B,C}.

Proof: Let f,g ∈ ELG and p > 0. By Lemma 3.3.4, let A,B have at least p elements, where B ∪. fA ⊆ A ∪. gA. By setting C = B, we see that AA 7 has AL.

By Lemma 3.3.5, let A,B have at least p elements, where B ∪. fA ⊆ A ∪. gB. By setting C = B, we see that AA 6,8,9 have AL. QED

The following pertains to AB 4 - 6.

LEMMA 3.3.7. B ∪. fA ⊆ B ∪. gX has ¬NON.

Proof: Define f,g ∈ ELG by f(n) = 2n, g(n) = 2n+1. Let B ∪. fA ⊆ B ∪. gX, where A,B,X are nonempty. Let n ∈ A. Then 2n ∈ fA, 2n ∈ B. This contradicts B ∩ fA = ∅. QED

The following pertains to AB 1,3,7,9.

LEMMA 3.3.8. X ∪. fA ⊆ B ∪. gY has INF, ALF, provided X,Y ∈ {A,C}, even for EVSD.

Proof: Let f,g ∈ EVSD. By Theorem 3.2.5, let A be infinite, where A ∩ fA = A ∩ gA = ∅. Let C = A and B = (A ∪ fA)\gA. Then A ⊆ B, and so A,B,C are infinite. This establishes INF.

For ALF, let p > 0. Let A be the first p elements of the above A, where A ∩ fA = A ∩ gA = ∅. Let C = A and B = (A ∪ fA)\gA. Then A ⊆ B, and so |B| ≥ p and A,B,C are finite. QED

The following pertains to AB 2,8.

LEMMA 3.3.9. X ∪. fA ⊆ B ∪. gB has INF, ALF, provided X ∈ {A,C}, even for EVSD.

Proof: Let f,g ∈ EVSD and n be sufficiently large. By Theorem 3.2.5, let A ⊆ [n,∞) be infinite, where A ∩ fA = A ∩ gA = ∅. By Lemma 3.3.3, let B be unique such that B ⊆ A ∪ fA ⊆ B ∪. gB. Let C = A. Since A ∪ fA is infinite, B is infinite. This establishes INF.

Now let p > 0 be given. Let A be the first p elements of the above A. Then A ∩ fA = A ∩ gA = ∅. Let B be the unique B ⊆ A ∪ fA such that A ∪ fA ⊆ B ∪. gB. Let C = A. Since A ∩ gB = ∅, we have A ⊆ B. This establishes ALF. QED

The information contained in these Lemmas is sufficient to justify all determinations made on the AA and AB tables, using the obvious implications

ALF → AL → NON.
ALF → FIN → NON.
INF → AL → NON.

and contrapositives.

Lemma 3.3.7 is particularly useful. It allows us to remove a large number of pairs of clauses in sections 3.4 - 3.13 (e.g., see the reduced AA table at the beginning of section 3.4). Also, it allows us to automatically annotate a very large number of entries in the annotated tables of section 3.14.

We now illustrate a difference between ELG and SD with respect to AL. We have the following, in contrast to Lemma 3.3.4.

THEOREM 3.3.10. There exist f,g ∈ SD such that the following holds. Let B ∪. fA ⊆ A ∪. gA. If A is nonempty then B has at most one element. In particular, this clause for SD has attribute ¬AL, and this clause for ELG has attribute AL (Lemma 3.3.4).

Proof: For n < m, let f(n,n) = n+1, f(n,m) = m+1, f(m,n) = m+2. Let g(n) = 2n+3. Let B ∪. fA ⊆ A ∪. gA, where A is nonempty. Let n = min(A). Then n+1 ∈ A ∪ gA, n+1 ∉ gA, n+1 ∈ A.

We claim that [n+1,∞) ⊆ fA. Since n ∈ A, clearly n+1 ∈ fA. Hence n+1 ∈ A ∪ gA. Now n+1 ∈ gA is impossible since n = min(A). Hence n+1 ∈ A, n+2 ∈ fA.

Now let [n+1,m] ⊆ fA, m ≥ n+2. To establish the claim, it suffices to prove that m+1 ∈ fA. Now m ∈ fA, m ∈ A ∪ gA. If m ∈ A then m+1 ∈ fA. So it suffices to assume that m ∈ gA. Hence m is odd. Also m-1 ∈ fA, m-1 ∈ A ∪ gA. Since m-1 is even, m-1 ∈ A. Let r < m-1, r ∈ A. Then f(m-1,r) = m+1 ∈ fA.

We have thus established that [n+1,∞) ⊆ fA.

Now let r ∈ B. By the above claim, r ≤ n, r ∈ A ∪ gA, r ∈ A, r = n. Hence B has exactly one element. QED

3.4. AAAA.

Recall the AA table from section 3.3.

AA

1. A ∪. fA ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2. A ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3. A ∪. fA ⊆ A ∪. gC ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4. B ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5. B ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
6. B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
7. C ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
8. C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
9. C ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

It is clear that there is no reason to further consider clauses 1-3 from the AA table, as all of our five proposition attributes already come out false. So we instead work with the following reduced AA table. Note that we have renumbered the clauses.

REDUCED AA

1. B ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
2. B ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
3. B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
4. C ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5. C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
6. C ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

We need only consider ordered pairs of these clauses i,j, where i < j.

1,2. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gB.

1,3. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gC.
1,4. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gA.
1,5. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gB.
1,6. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gC.
2,3. B ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gC.
2,4. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gA. Equivalent to 1,6.
2,5. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gB.
2,6. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gC.
3,4. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ A ∪. gA. Equivalent to 1,5.
3,5. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ A ∪. gB.
3,6. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ A ∪. gC. Equivalent to 2,5.
4,5. C ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gB. Equivalent to 1,3.
4,6. C ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gC. Equivalent to 1,2.
5,6. C ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gC. Equivalent to 2,3.

Thus we need only examine

REDUCED AAAA

1,2. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,3. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
1,4. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
1,5. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,6. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,3. B ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
2,5. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
2,6. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
3,5. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.

Note that we have used an entirely different method for compiling the ordered pairs to be analyzed than the purely syntactic method used in section 3.1 to compile the master list for AAAA that is used in the Annotated Table, section

3.14. Here we take full advantage of the fact that ¬NON implies ¬INF, ¬AL, ¬ALF, ¬FIN. The result is that on the master list for AAAA, there are 20 entries, whereas on the above Reduced AAAA list, there are only 9 entries.

The same considerations apply in sections 3.5 - 3.13, where the number of ordered pairs actually requiring analysis is considerably smaller than the number of ordered pairs in the relevant part of the Annotated Table.

By the reduced AA table, we see that all of these pairs must have ¬INF, ¬ALF, ¬FIN. It remains to determine the status of AL and NON.

In the next Lemma, we use this method of substitution: Suppose α,β are pairs of clauses, where β is the result of substituting one letter by another letter in α. Then any of our five attributes that holds of β also holds of α. As a consequence, if the negation of any of our five attributes holds of α then that negation also holds of β.

LEMMA 3.4.1. 1,3, 1,4 have AL.

Proof: From the reduced AA table, B ∪. fA ⊆ A ∪. gA has AL. In the cited ordered pairs, replace C by A, and C by B, respectively. QED

The following pertains to 1,2, 1,5, 1,6.

LEMMA 3.4.2. fX ⊆ A ∪. gA, fA ⊆ A ∪. gY, Y ∩ fA = ∅ has ¬NON.

Proof: Let f be as given by Lemma 3.2.1. Let g ∈ ELG be defined by g(n) = 2n+1. Let fX ⊆ A ∪. gA, fA ⊆ A ∪. gY, Y ∩ fA = ∅, where A,B,C are nonempty.

Let n ∈ fA ∩ 2N. Then n ∈ A. Hence fA ∩ 2N ⊆ A. By Lemma 3.2.1, fA is cofinite. Since Y ∩ fA = ∅, Y is finite. Hence A is cofinite. This contradicts A ∩ gA = ∅. QED

The following pertains to 2,3, 2,5, 2,6.

LEMMA 3.4.3. B ∪. fA ⊆ A ∪. gB, X ∪. fA ⊆ A ∪. gY has AL, provided X,Y ∈ {B,C}.

Proof: From the reduced AA table, B ∪. fA ⊆ A ∪. gB has AL. In the cited ordered pairs, replace C by B. QED

The following pertains to 3,5.

LEMMA 3.4.4. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ A ∪. gX has AL, provided X ∈ {B,C}.

Proof: From the reduced AA table, B ∪. fA ⊆ A ∪. gB has AL. In the cited ordered pair, replace C by B. QED

3.5. AAAB.

Recall the reduced AA table from section 3.4.

REDUCED AA

1. B ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
2. B ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
3. B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
4. C ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5. C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
6. C ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

Recall the AB table from section 3.3.

AB

1. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
2. A ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
4. B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
7. C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
8. C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
9. C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

Here is the reduced AB table, renumbered with ′ to distinguish it from the reduced AA table above.

REDUCED AB

1′. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
2′. A ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
3′. A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
4′. C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
5′. C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
6′. C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

We consider all 36 ordered pairs, arranged in cases according to the first clause of the ordered pair.

As before, we need only obtain the status of AL and NON for the ordered pairs, because of the reduced AA table.

part 1. B ∪. fA ⊆ A ∪. gA.

1,1′. B ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,2′. B ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,3′. B ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,4′. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,5′. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,6′. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

The following pertains to 1,1′ - 1,6′.

LEMMA 3.5.1. fA ⊆ A ∪. gX, fA ⊆ B ∪. gY, Z ∩ fA = ∅ has ¬NON, where X,Y ∈ {A,B,C} and Z ∈ {A,B}.

Proof: Let f be as given by Lemma 3.2.1. Let g ∈ ELG be defined by g(n) = 2n+1. Let fA ⊆ A ∪. gX, fA ⊆ B ∪. gY, Z ∩ fA = ∅, where A,B,C are nonempty. Let n ∈ fA ∩ 2N. Then n ∈ A. Hence fA ∩ 2N ⊆ A. So fA is cofinite. Hence A is infinite. Also fA ∩ 2N ⊆ B, and so B is infinite. Hence Z is infinite. This contradicts Z ∩ fA = ∅. QED

part 2. B ∪. fA ⊆ A ∪. gB.

2,1′. B ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,2′. B ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,3′. B ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,4′. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,5′. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,6′. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

LEMMA 3.5.2. 2,1′ - 2,6′ have ¬NON.

Proof: By Lemma 3.5.1. QED

part 3. B ∪. fA ⊆ A ∪. gC.

3,1′. B ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,2′. B ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,3′. B ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,4′. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,5′. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,6′. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

LEMMA 3.5.3. 3,1′ - 3,6′ have ¬NON.

Proof: By Lemma 3.5.1. QED

part 4. C ∪. fA ⊆ A ∪. gA.

4,1′. C ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,2′. C ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,3′. C ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,4′. C ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
4,5′. C ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
4,6′. C ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

LEMMA 3.5.4. 4,1′ - 4.3′ have ¬NON.

Proof: By Lemma 3.5.1. QED

LEMMA 3.5.5. 4,4′, 4,5′ have AL.

Proof: From the reduced AA table, C ∪. fA ⊆ A ∪. gA has AL. In the cited ordered pairs, replace B by A. QED

The following pertains to 4,6′.

LEMMA 3.5.6. C ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gC has AL.

Proof: Let f,g ∈ ELG and p > 0. Let C = [n,n+p], where n is sufficiently large. By Lemma 3.3.3, let A be unique such that A ⊆ [n,∞) ⊆ A ∪. gA. Let B = (C ∪ fA)\gC.

Note that fA ⊆ [n,∞), and so C ∪ fA ⊆ A ∪ gA. Also C ∩ fA = C ∩ gA = C ∩ gC = ∅. Hence C ⊆ A,B, and so A,B,C have at least p elements. QED

part 5. C ∪. fA ⊆ A ∪. gB.

5,1′. C ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,2′. C ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,3′. C ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,4′. C ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5,5′. C ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
5,6′. C ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

LEMMA 3.5.7. 5,1′ - 5,3′ have ¬NON.

Proof: By Lemma 3.5.1. QED

LEMMA 3.5.8. 5,4′, 5,5′ have AL.

Proof: From the reduced AA table, C ∪. fA ⊆ A ∪. gA has AL. In the cited ordered pairs, replace B by A. QED

The following pertains to 5,6′.

LEMMA 3.5.9. C ∪. fA ⊆ A ∪. gX, C ∪. fA ⊆ B ∪. gY has AL, provided X ∈ {B,C} and Y ∈ {A,C}.

Proof: Let f,g ∈ ELG and p > 0. Let C = [n,n+p], where n is sufficiently large. Let A = [n,∞)\gX. Let B = [n,∞)\gY. These are ordinary explicit definitions provided X ≠ A and Y ≠ B.

Clearly C ∩ fA = C ∩ gA = C ∩ gB = C ∩ gC = ∅. Hence C ⊆ A,B, and so |A|,|B| ≥ p. Since C ∪ fA ⊆ [n,∞), we have C ∪ fA ⊆ A ∪. gX, C ∪ fA ⊆ B ∪ gY. QED part 6. C ∪. fA ⊆ A ∪. gC.

6,1′. C ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,2′. C ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,3′. C ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,4′. C ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gA. ¬INF, AL, ¬ALF, ¬FIN. NON.
6,5′. C ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gB. ¬INF, AL, ¬ALF, ¬FIN. NON.
6,6′. C ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gC. ¬INF, AL, ¬ALF, ¬FIN. NON.

LEMMA 3.5.10. 6,1′ - 6,3′ have ¬NON.

Proof: By Lemma 3.5.1. QED

The following pertains to 6,6′.

LEMMA 3.5.11. C ∪ fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gC has AL.

Proof: From the reduced AA table, C ∪. fA ⊆ A ∪. gC has AL. In the cited ordered pair, replace B by A. QED

The following pertains to 6,4′.

LEMMA 3.5.12. C ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gA has AL.

Proof: By Lemma 3.5.9. QED

The following pertains to 6,5′.

LEMMA 3.5.13. C ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gB has AL.

Proof: Let f,g ∈ ELG and p > 0. Let C = [n,n+p], where n is sufficiently large. Let A = [n,∞)\gC. By Lemma 3.3.3, let B be unique such that B ⊆ C ∪ fA ⊆ B ∪. gB.

Clearly C ∩ fA = C ∩ gB = C ∩ gC = ∅ and C ⊆ A,B. Hence |A|,|B| ≥ p. Also C ∪ fA ⊆ B ∪ gB, and C ∪ fA ⊆ [n,∞) ⊆ A ∪ gC. QED

3.6. AABA.

Recall the reduced AA table from section 3.4.

REDUCED AA

1. B ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
2. B ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
3. B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
4. C ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5. C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
6. C ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

Recall the reduced AB table from section 3.5.

REDUCED AB

1. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
2. A ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
4. C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
5. C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
6. C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

The reduced BA table is obtained from the reduced AB table by switching A,B. We use 1′-6′ to avoid any confusion.

REDUCED BA

1′. B ∪. fB ⊆ A ∪. gB. INF. AL. ALF. FIN. NON.
2′. B ∪. fB ⊆ A ∪. gA. INF. AL. ALF. FIN. NON.
3′. B ∪. fB ⊆ A ∪. gC. INF. AL. ALF. FIN. NON.
4′. C ∪. fB ⊆ A ∪. gB. INF. AL. ALF. FIN. NON.
5′. C ∪. fB ⊆ A ∪. gA. INF. AL. ALF. FIN. NON.
6′. C ∪. fB ⊆ A ∪. gC. INF. AL. ALF. FIN. NON.

We consider all 36 pairs, arranged in cases according to the first clause of the ordered pair.

The status of all of our proposition attributes are determined by the reduced AA table except AL and NON. Thus, we need only obtain the status of AL and NON.

part 1. B ∪. fA ⊆ A ∪. gA.

1,1′. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.
1,2′. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.

1,3′. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
1,4′. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.
1,5′. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
1,6′. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.

LEMMA 3.6.1. There exists g ∈ ELG ∩ SD such that the following holds. Suppose A ∪ gB is cofinite and A ∩ gA = ∅. Then A ⊆ B. We can require that rng(g) ⊆ 2N+1. Furthermore, we can require that for all X and n, 4n+3 ∈ gX ↔ n ∈ X.

Proof: Define g ∈ ELG ∩ SD as follows. For all m > n, define

$$g(n,4m^2+4n+1) = 16m^2+4n+1.$$

For all other pairs p,q, define

$$g(p,q) = 4|p,q|+3.$$

Let A ∪ gB be cofinite and A ∩ gB = ∅. Let n ∈ A\B. We derive a contradiction.

Note that the last two requirements on g hold.

We first claim that

$$m > n \rightarrow 4m^2+4n+1 \notin gB.$$

To see this, let m > n, $4m^2+4n+1$ ∈ gB. Note that $4m^2+4n+1 \equiv 1 \bmod 4$. Hence for some n′,m′ ∈ B, m′ > n′, we have

$$4m^2+4n+1 = g(n',m') = 16m'^2+4n'+1.$$

Since n ∉ B and n′ ∈ B, we have n ≠ n′. Also

$$16m'^2 - 4m^2 = 4n - 4n'.$$
$$4m'^2 - m^2 = n - n'.$$
$$(2m' - m)(2m' + m) = n - n'.$$
$$2m' - m \neq 0.$$
$$2m' + m > 2n' + n.$$
$$2n' + n < |(2m' - m)(2m' + m)| = |n - n'| \leq n + n'.$$
$$n' < 0.$$

Now fix $m > n$, where $4m^2+4n+1$, $16m^2+4n+1 \in A \cup gB$. By the first claim applied to m and to 2m, we have

$$4m^2+4n+1,\ 16m^2+4n+1 \notin gB.$$
$$4m^2+4n+1,\ 16m^2+4n+1 \in A.$$
$$n \in A.$$
$$g(n,4m^2+4n+1) = 16m^2+4n+1 \in gA.$$

This contradicts $A \cap gA = \emptyset$. QED

LEMMA 3.6.2. $B \cup. fA \subseteq X \cup. gX$, $fB \subseteq X \cup. gB$ has ¬AL.

Proof: Let f be given by Lemma 3.2.2. Let g be as given by Lemma 3.6.1. Let $B \cup. fA \subseteq X \cup. gX$, $fB \subseteq X \cup. gB$, where A,B,C have at least two elements. We now use Lemma 3.2.2 to show that fB is cofinite.

Let $n \in fB \cap 2N$, $4n+3 \in fB$. Then $n \in X$, $4n+3 \in gX$, $4n+3 \notin X$. Since $4n+3 \in fB$, we have $4n+3 \in gB$. Hence $n \in B$. We have thus established that $(\forall n \in fB \cap 2N)(4n+3 \in fB \rightarrow n \in B)$. By Lemma 3.2.2, fB is cofinite.

We have thus established that $X \cup gB$ is cofinite and $X \cap gX = \emptyset$. By Lemma 3.6.1, $X \subseteq B$. By Lemma 3.2.2, fA has an even element 2r. Hence $2r \in X$, $2r \in B$. This contradicts $B \cap fA = \emptyset$. QED

LEMMA 3.6.3. 1,1', 1,4' have ¬AL.

Proof: By Lemma 3.6.2, setting X = A. QED

The following pertains to 1,6'.

LEMMA 3.6.4. $B \cup. fA \subseteq A \cup. gA$, $C \cup. fB \subseteq A \cup. gC$ has ¬AL.

Proof: Define $f,g \in ELG$ as follows. For all $n < m$, let $f(n,n) = 2n+2$, $f(n,m) = f(m,n) = 4m+5$, $g(n) = 2n+1$. Let $B \cup. fA \subseteq A \cup. gA$, $C \cup. fB \subseteq A \cup. gC$, where A,B,C have at least two elements. Let $n < m$ be from B.

Clearly $2m+2, 4m+5 \in fB$, $2m+2 \notin C$, $4m+5 \notin gC$, $4m+5 \in A$, $4m+5 \notin gA$, $2m+2 \notin A$, $2m+2 \in gC$. This is impossible since g is odd valued. QED

The following pertains to 1,2', 1,5'.

LEMMA 3.6.5. $X \cup. fA \subseteq A \cup. gA$, $Y \cup. fB \subseteq A \cup. gA$ has AL, provided $X,Y \in \{B,C\}$.

Proof: Let $f,g \in ELG$ and $p > 0$. Let $B = C = [n,n+p]$, where n is sufficiently large. By Lemma 3.3.3, let A be unique such that $A \subseteq [n,\infty) \subseteq A \cup. gA$.

Obviously $X \cap fA = X \cap gA = A \cap gA = Y \cap fB = \emptyset$. Hence $B,C \subseteq A$. Also $fA,fB \subseteq [n,\infty) \subseteq A \cup gA$. QED

The following pertains to 1,3'.

LEMMA 3.6.6. $B \cup. fA \subseteq A \cup. gA$, $B \cup. fB \subseteq A \cup. gC$ has AL.

Proof: By Lemma 3.6.5, $B \cup. fA \subseteq A \cup. gA$, $B \cup. fB \subseteq A \cup. gA$ has AL. Replace C by A in the cited pair. QED

LEMMA 3.6.7. $X \cup. fA \subseteq A \cup. gA$, $Y \cup. fZ \subseteq A \cup. gW$ has NON, provided $X,Y,Z,W \in \{B,C\}$.

Proof: Let $f,g \in ELG$. Let n be sufficiently large.

case 1. $f(n,...,n) = g(n,...,n)$. Let $A = B = C = \{n\}$.

case 2. $f(n,...,n) \neq g(n,...,n)$. Let $B = C = \{n\}$. By Lemma 3.3.3, let A be unique such that $A \subseteq [f(n,...,n),\infty) \cup \{n\} \subseteq A \cup. gA$.

In case 1, both inclusions have the same left and right sides, and are easily verified.

We assume case 2 holds. Obviously $B \cap fA = B \cap fB = A \cap gA = \emptyset$. Also $n \in A$, and hence $X \subseteq A$ and $Y \subseteq A$. Since $g(n,...,n) \in gA$, we have $g(n,...,n) \notin A$. Hence $A \cap gB = A \cap gC = \emptyset$.

We have thus shown that $X \cap fA = A \cap gA = Y \cap fZ = A \cap gW = \emptyset$.

Note that $f(n,...,n) \notin gA$. To see this, let $f(n,...,n) = g(b_1,...,b_r)$, $b_1,...,b_r \in A$. Clearly not every b_i is n. Hence some b_i is at least $f(n,...,n)$. This is a contradiction.

Since $f(n,...,n) \notin gA$, we see that $f(n,...,n) \in A$. Hence $fZ \subseteq A$. Also $fA \subseteq [f(n,...,n),\infty) \subseteq A \cup gA$. QED

LEMMA 3.6.8. 1,1', 1,4', 1,6' have NON.

Proof: Immediate from Lemma 3.6.7. QED

part 2. B ∪. fA ⊆ A ∪. gB.

2,1′. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
2,2′. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,3′. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
2,4′. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
2,5′. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,6′. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

The following pertains to 2,1′, 2,3′, 2,4′, 2,6′.

LEMMA 3.6.9. X ∪. fA ⊆ A ∪. gY, Z ∪. fB ⊆ A ∪. gW has AL, provided X,Y,Z,W ∈ {B,C}.

Proof: Let f,g ∈ ELG and p > 0. Let B = C = [n,n+p], where n is sufficiently large. Let A = [n,∞)\gB. Then A is infinite.

Clearly B ∩ fA = C ∩ fA = B ∩ fB = C ∩ fB = A ∩ gB = A ∩ gC = B ∩ gB = C ∩ gB = ∅. Hence B,C ⊆ A. Also fA,fB ⊆ [n,∞) ⊆ A ∪ gB = A ∪ gC. QED

LEMMA 3.6.10. fA ⊆ A ∪. gB, B ∩ fA = A ∩ gA = ∅ has ¬NON.

Proof: Let f be given by Lemma 3.2.1. Define g ∈ ELG by g(n) = 2n+1. Let fA ⊆ A ∪. gB, B ∩ fA = A ∩ gA = ∅, where A,B,C are nonempty.

Obviously fA ∩ 2N ⊆ A. By Lemma 3.2.1, fA is cofinite. Since A ∩ gA = ∅, we see that A is not cofinite. Since fA ⊆ A ∪ gB and fA is cofinite, we see that gB is infinite. Hence B is infinite. This contradicts B ∩ fA = ∅. QED

LEMMA 3.6.11. 2,2′, 2,5′ have ¬NON.

Proof: Immediate from Lemma 3.6.10. QED

part 3. B ∪. fA ⊆ A ∪. gC.

3.1′. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.

3,2′. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
3,3′. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
3,4′. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
3,5′. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,6′. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

LEMMA 3.6.12. 3,1′, 3,3′, 3,4′, 3,6′ have AL.

Proof: By Lemma 3.6.9. QED

The following pertains to 3,2′.

LEMMA 3.6.13. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gA has AL.

Proof: By Lemma 3.6.5, B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gA has AL. Replace C by A in the cited ordered pair. QED

The following pertains to 3,5′.

LEMMA 3.6.14. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gA has ¬NON.

Proof: For n < m, define f(n,n,n) = 2n+2, f(n,m,m) = 4m+5, f(n,n,m) = 2m+1, f(m,n,n) = 8m+9. Define f(a,b,c) = 2|a,b,c|+1 for all other triples a,b,c. Define g(n) = 4n+5. Obviously f,g ∈ ELG.

Let B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gA, where A,B,C ⊆ N are nonempty. Let n ∈ B. Then n ∈ A ∪ gC.

case 1. n ∈ A. Then 2n+2 ∈ fA, 2n+2 ∈ A, 8n+13 ∈ fA,gA, 8n+13 ∉ A, 8n+13 ∈ gC, 2n+2 ∈ C, 2n+2 ∈ fB. This contradicts C ∩ fB = ∅.

case 2. n ∈ gC. Let n = 4m+5, m ∈ C. Then m ∈ A ∪ gA.

case 2a. m ∈ A. Then 2m+2 ∈ fA, 2m+2 ∈ A, 4m+5 ∈ fA, 4m+5 = n ∈ B. This contradicts B ∩ fA = ∅.

case 2b. m ∈ gA. Let m = 4r+5, r ∈ A. Then 2r+2 ∈ fA, 2r+2 ∈ A. Since n = 4m+5 and m = 4r+5, we have n = 16r+25. Hence n = f(2r+2,r,r) ∈ fA, n ∈ B. This contradicts B ∩ fA = ∅. QED part 4. C ∪. fA ⊆ A ∪. gA.

4,1′. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.
4,2′. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
4,3′. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.
4,4′. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
4,5′. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
4,6′. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.

The following pertains to 4,1′.

LEMMA 3.6.15. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gB has ¬AL.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n, f(n,m) = f(m,n) = 4m+1, g(n) = 2n+1. Let fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gB, where A,B,C have at least two elements. Let n < m be from B.

Note that 2m ∈ fB, 2m ∈ A, 2m ∉ B, 4m+1 ∉ gB, 4m+1 ∈ fB, 4m+1 ∈ A, 4m+1 ∈ gA. This contradicts A ∩ gA = ∅. QED

LEMMA 3.6.16. 4,2′, 4,5′ have AL.

Proof: By Lemma 3.6.5. QED

The following pertains to 4,3′.

LEMMA 3.6.17. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gC has ¬AL.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n, f(n,m) = 4m, f(m,n) = 8m+1, g(n) = 2n+1. Let C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gC, where A,B,C have at least two elements. Let n < m be from B.

Clearly 2m ∈ fB, 2m ∈ A, 2m ∉ B, 4m ∈ fB, 4m ∈ A, 4m ∉ B, 8m+1 ∈ gA, 8m+1 ∉ A, 8m+1 ∈ fB, 8m+1 ∈ gC, 4m ∈ C, 4m ∈ fA. This contradicts C ∩ fA = ∅. QED

The following pertains to 4,4′.

LEMMA 3.6.18. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gB has AL.

Proof: From the reduced AA table, C ∪. fA ⊆ A ∪. gA has AL. Replace B by A in the cited ordered pair. QED

The following pertains to 4,6'.

LEMMA 3.6.19. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gC has ¬AL.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n, f(n,m) = f(m,n) = 4m+1, g(n) = 2n+1. Let C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gC, where A,B,C have at least two elements. Let n < m be from B.

Clearly 2m ∈ fB, 2m ∈ A, 4m+1 ∈ gA, 4m+1 ∉ A, 4m+1 ∈ fB, 4m+1 ∈ gC, 2m ∈ C. This contradicts C ∩ fB = ∅. QED

LEMMA 3.6.20. 4,1', 4,3', 4,6' have NON.

Proof: By Lemma 3.6.7, X ∪. fA ⊆ A ∪. gA, Y ∪. fZ ⊆ A ∪. gW has NON, provided X,Y,Z,W ∈ {B,C}. QED

part 5. C ∪. fA ⊆ A ∪. gB.

5,1'. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
5,2'. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,3'. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
5,4'. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
5,5'. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5,6'. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

LEMMA 3.6.21. 5,1', 5,3', 5,4', 5,6' have AL.

Proof: By Lemma 3.6.9, X ∪. fA ⊆ A ∪. gY, Z ∪. fB ⊆ A ∪. gW has AL, provided X,Y,Z,W ∈ {B,C}. QED

The following pertains to 5,5'.

LEMMA 3.6.22. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gA has AL.

Proof: From the reduced table for AA, we see that C ∪. fA ⊆ A ∪. gA has AL. In the cited ordered pair, replace B by A. QED

The following pertains to 5,2'.

LEMMA 3.6.23. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gA has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(m,n) = f(n,m) = 2m+1, g(n) = 2n+1. Let fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gA, where A,B are nonempty.

Let n ∈ A. Then 2n+2 ∈ fA, 2n+2 ∈ A, 4n+5 ∈ gA, 4n+5 ∉ A. Since n < 2n+2 are from A, we have 4n+5 ∈ fA, 4n+5 ∈ gB, 2n+2 ∈ B, 4n+6 ∈ fB, 4n+6 ∈ A. Since n < 4n+6 are from A, we have 8n+13 ∈ fA, 8n+13 ∈ gA, 8n+13 ∉ A, 8n+13 ∈ gB, 4n+6 ∈ B. This contradicts B ∩ fB = ∅. QED

part 6. C ∪. fA ⊆ A ∪. gC.

6,1'. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
6,2'. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,3'. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
6,4'. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
6,5'. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,6'. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

LEMMA 3.6.24. 6,1', 6,3', 6,4', 6,6' have AL.

Proof: By Lemma 3.6.9, X ∪. fA ⊆ A ∪. gY, Z ∪. fB ⊆ A ∪. gW has AL, provided X,Y,Z,W ∈ {B,C}. QED

The following pertains to 6,2' and 6,5'.

LEMMA 3.6.25. C ∪. fA ⊆ A ∪. gC, A ∩ gA = ∅ has ¬NON.

Proof: Let f be as given by Lemma 3.2.1. Define g ∈ ELG by g(n) = 2n+1. Let C ∪. fA ⊆ A ∪. gC, A ∩ gA = ∅, where A,B,C are nonempty.

We claim that fA ∩ 2N ⊆ A. To see this, let n ∈ fA ∩ 2N. Then n ∉ gC, and so n ∈ A.

By Lemma 3.2.1, fA is cofinite. Hence C is finite. Therefore gC is finite. Hence A is cofinite. Therefore gA is infinite. This contradicts A ∩ gA = ∅. QED

3.7. AABB.

Recall the reduced AA table from section 3.4.

REDUCED AA

1. B ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
2. B ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
3. B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
4. C ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5. C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
6. C ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

The reduced BB table is obtained from the reduced AA table by interchanging A,B. We use 1'-6' to avoid any confusion. We use 1’-6’ to avoid any confusion.

REDUCED BB

1’. A ∪. fB ⊆ B ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
2’. A ∪. fB ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
3’. A ∪. fB ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
4’. C ∪. fB ⊆ B ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
5’. C ∪. fB ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
6’. C ∪. fB ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

LEMMA 3.7.1. X ∪. fA ⊆ A ∪. gY, Z ∪. fB ⊆ B ∪. gW has ¬NON, provided X = B or Z = A.

Proof: Let f be as given by Lemma 3.2.1. Define g ∈ ELG by g(n) = 2n+1. Let X ∪. fA ⊆ A ∪. gY, Z ∪. fB ⊆ B ∪. W, where A,B,C are nonempty. Assume X = B or Z = A.

Clearly fA ∩ 2N ⊆ A and fB ∩ 2N ⊆ B. By Lemma 3.2.1, fA and fB are cofinite. Hence A,B are infinite. Since X ∩ fA = ∅, we see that X is finite. Since Z ∩ fB = ∅, we see that Z is finite. Hence A is finite or B is finite. This is a contradiction. QED

By Lemma 3.7.1, we can eliminate B ∪. fA ⊆ A ∪. gX from consideration. For the same reason, we can eliminate A ∪.

fB ⊆ B ∪. gX from consideration. Thus we need only handle the two tables

4. C ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5. C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
6. C ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

and

4′. C ∪. fB ⊆ B ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
5′. C ∪. fB ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
6′. C ∪. fB ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

It is clear by switching A,B, that i,j′ and i′,j are equivalent, where 4 ≤ i,j ≤ 6. Hence we need only consider i,j′, where i ≤ j′.

4,4′. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
4,5′. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
4,6′. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
5,5′. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5,6′. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
6,6′. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

As before, all proposition attributes are determined from the above tables, except for AL and NON. So we merely have to determine the status of AL and NON.

LEMMA 3.7.2. 4,4′, 4,5′, 5,5′ have AL.

Proof: From the reduced AA table, C ∪. fA ⊆ A ∪. gA has AL. In the cited pairs, replace B by A. QED

The following pertains to 4,6′.

LEMMA 3.7.3. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gC has AL.

Proof: Let f,g ∈ ELG be given and p > 0. Let C = [n,n+p], where n is sufficiently large. By Lemma 3.3.3, let A be unique such that A ⊆ [n,∞) ⊆ A ∪. gA. Let B = [n,∞)\gC.

Clearly C ∩ fA = C ∩ fB = C ∩ gA = C ∩ gC = ∅. Hence C ⊆ A,B. Also A ∩ gA = B ∩ gC = ∅.

Clearly C ∪ fB ⊆ [n,∞) = B ∪ gC. Also C ∪ fA ⊆ [n,∞) = A ∪ gA. QED

The following pertains to 5,6'.

LEMMA 3.7.4. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gC has AL.

Proof: Let f,g ∈ ELG(N) and p > 0. Let C = [n,n+p], where n is sufficiently large. Let B = [n,∞)\gC and A = [n,∞)\gB.

Obviously C ∩ fA = C ∩ fB = C ∩ gC = C ∩ gB = A ∩ gB = B ∩ gC = ∅. Hence C ⊆ A,B. Furthermore, fA ⊆ [n,∞) ⊆ A ∪ gB, and fB ⊆ [n,∞) ⊆ B ∪ gC. QED

The following pertains to 6,6'.

LEMMA 3.7.5. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gC has AL.

Proof: From the reduced AA table, C ∪. fA ⊆ A ∪. gC has AL. Replace B by A in the cited ordered pair. QED

3.8. AABC.

Recall the reduced AA table from section 3.4.

REDUCED AA

1. B ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
2. B ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
3. B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
4. C ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5. C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
6. C ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

Recall the reduced AB table from section 3.5.

REDUCED AB

1. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
2. A ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
4. C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
5. C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
6. C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

The reduced BC table is obtained from the reduced AB table via the permutation sending A to B, B to C, C to A. We use 1'-6' to avoid any confusion.

REDUCED BC

1′. B ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
2′. B ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
3′. B ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
4′. A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
5′. A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
6′. A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.

All attributes are determined from the reduced AA table, except for AL and NON. So we merely have to determine the status of AL and NON.

part 1. B ∪. fA ⊆ A ∪. gA.

1,1′. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
1,2′. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
1,3′. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
1,4′. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,5′. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,6′. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

The following pertains to 1,1′, 1,3′.

LEMMA 3.8.1. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gX has AL, provided X ∈ {A,B}.

Proof: Let f,g ∈ ELG(N) and p > 0. Let B = [n,n+p], where n is sufficiently large. By Lemma 3.3.3, let A be unique such that A ⊆ [n,∞) ⊆ A ∪. gA. Let C = [n,∞)\gX.

Note that B ∩ fA = B ∩ fB = B ∩ gA = A ∩ gA = B ∩ gB = C ∩ gX = ∅. Hence B ⊆ A,C. Also B ∪ fA ⊆ [n,∞) = A ∪ gA, and B ∪ fB ⊆ [n,∞) ⊆ C ∪ gX. QED

The following pertains to 1,2′.

LEMMA 3.8.2. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gC has AL.

Proof: Let f,g ∈ ELG and p > 0. Let B = [n,n+p], where n is sufficiently large. By Lemma 3.3.3, let A be unique such that A ⊆ [n,∞) ⊆ A ∪. gA. By Lemma 3.3.3, let C be unique such that C ⊆ B ∪ fB ⊆ C ∪. gC.

Note that B ∩ fA = B ∩ fB = B ∩ gC = B ∩ gA = A ∩ gA = C ∩ gC = ∅. Hence B ⊆ A,C. Also B ∪ fA ⊆ [n,∞) = A ∪ gA. QED

The following pertains to 1,4′, 1,5′, 1,6′.

LEMMA 3.8.3. B ∪. fA ⊆ A ∪. gA, A ∩ fB = ∅ has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = f(m,n) = 2m+1, g(n) = 4n+5. Let B ∪. fA ⊆ A ∪. gA, A ∩ fB = ∅, where A,B,C are nonempty.

We claim that gA ⊆ fA. I.e., n ∈ A → 4n+5 ∈ fA. To see this, let n ∈ A. Then 2n+2 ∈ fA, 2n+2 ∈ A. Since n < 2n+2 are from A, we have 4n+5 ∈ fA.

We claim that B ⊆ A. To see this, let n ∈ B\A. Then n ∈ A ∪ gA, n ∈ gA, n ∈ fA. This contradicts B ∩ fA = ∅.

Now let n ∈ B. Then n ∈ A, 2n+2 ∈ fA, 2n+2 ∈ A, 2n+2 ∈ fB. This contradicts A ∩ fB = ∅. QED

part 2. B ∪. fA ⊆ A ∪. gB.

2,1′. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
2,2′. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
2,3′. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
2,4′. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,5′. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,6′. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

The following pertains to 2,1′, 2,3′.

LEMMA 3.8.4. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gX has AL, provided X ∈ {A,B}.

Proof: Let f,g ∈ ELG and p > 0. Let B = [n,n+p], where n is sufficiently large. Let A = [n,∞)\gB. Let C = [n,∞)\gX.

Note that B ∩ fA = B ∩ fB = B ∩ gB = B ∩ gA = A ∩ gB = C ∩ gX = ∅. Hence B ⊆ A,C. Also B ∪ fA ⊆ [n,∞) = A ∪ gB, and B ∪ fB ⊆ [n,∞) = C ∪ gX. QED

The following pertains to 2,2’.

LEMMA 3.8.5. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gC has AL.

Proof: Let f,g ∈ ELG and p > 0. Let B = [n,n+p], where n is sufficiently large. Let A = [n,∞)\gB. Let C ⊆ [n,∞) ⊆ C ∪. gC.

Note that B ∩ fA = B ∩ fB = B ∩ gC = B ∩ gB = A ∩ gB = C ∩ gC = ∅. Hence B ⊆ A,C. Also B ∪ fA ⊆ [n,∞) = A ∪ gB, and B ∪ fB ⊆ [n,∞) = C ∪ gC. QED

The following pertains to 2,4’ - 2,6’.

LEMMA 3.8.6. B ∪. fA ⊆ A ∪. gB, A ∩ fB = ∅ has ¬NON.

Proof: Let f,g ∈ ELG be defined as follows. For all n, f(n) = 2n, g(n) = 2n+1. Let B ∪. fA ⊆ A ∪. gB, A ∩ fB = ∅, where A,B are nonempty.

Let n = min(B). Then n ∈ B, n ∉ gB, n ∈ A, 2n ∈ fA, 2n ∈ A, 2n ∈ fB. This contradicts A ∩ fB = ∅. QED

part 3. B ∪. fA ⊆ A ∪. gC.

3,1’. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
3,2’. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
3,3’. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
3,4’. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
3,5’. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
3,6’. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.

The following pertains to 3,1’.

LEMMA 3.8.7. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gB has AL.

Proof: Let f,g ∈ ELG and $p > 0$. Let B = [n,n+p], where n is sufficiently large. Let C = [n,∞)\gB, A = [n,∞)\gC.

Note that B ∩ fA = B ∩ fB = A ∩ gC = C ∩ gB = B ∩ gB = B ∩ gC = ∅. Hence B ⊆ A,C. Also B ∪ fA ⊆ [n,∞) = A ∪ gC and B ∪ fB ⊆ [n,∞) ⊆ C ∪ gB. QED

The following pertains to 3,2'.

LEMMA 3.8.8. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gC has AL.

Proof: Let f,g ∈ ELG and $p > 0$. Let B = [n,n+p], where n is sufficiently large. By Lemma 3.3.3, let C be unique such that C ⊆ B ∪ fB ⊆ C ∪. gC. Let A = [n,∞)\gC.

Note that B ∩ fA = B ∩ fB = A ∩ gC = C ∩ gC = B ∩ gB = B ∩ gC = ∅. Hence B ⊆ A,C. Also B ∪ fA ⊆ [n,∞) = A ∪ gC and B ∪ fB ⊆ C ∪ gC. QED

The following pertains to 3,3'.

LEMMA 3.8.9. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gA has AL.

Proof: Let f,g ∈ ELG and $p > 0$. Let B = [n,n+p], where n is sufficiently large. We define A,C inductively. Suppose membership in A,C have been defined for all elements of [n,k), where $k \geq n$. We define membership of k in A,C as follows.

If k is already in B ∪ fA but not yet in gC, put k in A. if k is already in B ∪ fB but not yet in gA, put k in C. Obviously A,C ⊆ [n,∞).

Clearly B ∩ fA = B ∩ gA = B ∩ fB = B ∩ gC = A ∩ gC = C ∩ gA = ∅. Hence we have put every element of B in A, and every element of B in C. Also fA ⊆ A ∪ gC, fB ⊆ C ∪ gA. QED

LEMMA 3.8.10. Let g ∈ ELG and $p > 0$. There exist finite D such that D,gD,ggD are pairwise disjoint and each have at least p elements.

Proof: Let g,p be as given, and n be sufficiently large. Let $n = b_1 < \ldots < b_p$, where for all $1 \leq i \leq p$, $b_{i+1} > b_i^n$. Let $D = \{b_1,\ldots,b_p\}$. QED

The following pertains to 3,4'.

LEMMA 3.8.11. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gB has AL.

Proof: Let f,g ∈ ELG and p > 0. Let D be as given by Lemma 3.8.10. Let B = gD.

Let n be sufficiently large. By an obvious generalization of Lemma 3.3.3, let A be unique such that A ⊆ [n,∞) ⊆ A ∪. g(A ∪ D ∪ (fB\gB)). Let C = A ∪ D ∪ (fB\gB). Then [n,∞) ⊆ A ∪. gC.

Obviously B,D are finite and A,C are infinite. Since n is sufficiently large, we have B ∩ fA = A ∩ fB = A ∩ gB = D ∩ gB = ∅. Hence C ∩ gB = ∅.

Since B = gD ⊆ gC and fA ⊆ [n,∞) ⊆ A ∪ gC, we have B ∪ fA ⊆ A ∪ gC.

Since A ⊆ C and fB\gB ⊆ C, we have A ∪ fB ⊆ C ∪ gB. QED

The following pertains to 3,6'.

LEMMA 3.8.12. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gA has AL.

Proof: Let f,g ∈ ELG and p > 0. Let D be as given by Lemma 3.8.10. Let B = gD.

Let n be sufficiently large. Let A ⊆ [n,∞) ⊆ A ∪. g(A ∪ D ∪ fB). Let C = A ∪ D ∪ fB. Then [n,∞) ⊆ A ∪. gC.

Obviously D,B are finite and A,C are infinite. Since n is sufficiently large, we have B ∩ fA = A ∩ fB = fB ∩ gA = ∅. Also A ∩ gA ⊆ A ∩ gC = ∅, and D ∩ gA = ∅. Hence C ∩ gA = ∅.

Since B = gD ⊆ gC and fA ⊆ [n,∞) ⊆ A ∪ gC, we have B ∪ fA ⊆ A ∪ gC. Also A ∪ fB ⊆ C. QED

The following pertains to 3,5'.

LEMMA 3.8.13. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gC has AL.

Proof: Let f,g ∈ ELG and p > 0. Let n be sufficiently large. Let C ⊆ [n,∞) ⊆ C ∪. gC.

Clearly C is infinite. Let B ⊆ gC have cardinality p. Let m be sufficiently large relative to p,n,max(B). Let A = C ∩ [m,∞). Then A,C are infinite.

Clearly B ∩ fA = A ∩ gC = A ∩ fB = C ∩ gC = ∅.

We claim that fA ⊆ A ∪ gC. To see this, let r ∈ fA. Then r > m > n, and so r ∈ C ∪ gC. If r ∈ gC then we are done. If r ∈ C, then r ∈ A.

Finally, A ∪ fB ⊆ A ∪ fgC ⊆ [n,∞) ⊆ C ∪. gC. QED

part 4. C ∪. fA ⊆ A ∪. gA.

4,1'. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,2'. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,3'. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,4'. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,5'. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,6'. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

The following pertains to 4,1'.

LEMMA 3.8.14. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gB has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = 2m+1, f(m,n) = 4m+6, g(n) = 4n+5. Let C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gB, where A,B,C are nonempty.

Let m ∈ B. Then 2m+2 ∈ fB, 2m+2 ∈ C, 2m+2 ∈ A, 4m+6 ∈ fA, 2m+2 ∉ fA, m ∉ A, m ∈ C ∪ gB.

case 1. m ∈ C. Then m ∈ A ∪ gA, m ∈ gA. Let m = 4n+5, n ∈ A. Then 2n+2 ∈ fA, 2n+2 ∈ A. Since n < 2n+2 are from A, we have 4n+5 ∈ fA. This contradicts C ∩ fA = ∅.

case 2. m ∈ gB. Let m = 4n+5, n ∈ B. Since n < m are from B, we have 4m+6 ∈ fB, 4m+6 ∈ C. Since 4m+6 ∈ fA, this contradicts C ∩ fA = ∅. QED

The following pertains to 4,2'.

LEMMA 3.8.15. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gC has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = 2m+1, f(m,n) = 2m, g(n) = 4n+5. Let C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gC, where A,B,C are nonempty.

Let m ∈ B. Then 2m+2 ∈ fB, 2m+2 ∈ C, 2m+2 ∉ fA, m ∉ A, m ∈ C ∪ gC.

case 1. m ∈ C. Then m ∈ A ∪ gA, m ∈ gA. Let m = 4n+5, n ∈ A. Hence 2n+2 ∈ fA, 2n+2 ∈ A. Since n < 2n+2 are from A, we have 4n+5 = m ∈ fA. This contradicts C ∩ fA = ∅.

case 2. m ∈ gC. Let m = 4n+5, n ∈ C. Hence n ∈ A ∪ gA.

case 2a. n ∈ A. Then 2n+2 ∈ fA, 2n+2 ∈ A, 4n+6 ∈ fA, 4n+6 ∈ A, 8n+12 ∈ fA. Since m ∈ B, we have 2m+2 = 8n+12 ∈ fB, 8n+12 ∈ C. This contradicts C ∩ fA = ∅.

case 2b. n ∈ gA. Let n = 4r+5, r ∈ A. Then 2r+2 ∈ fA, 2r+2 ∈ A, 4r+6 ∈ fA, 4r+6 ∈ A, 8r+12 ∈ fA, 8r+12 ∈ A, 16r+26 ∈ fA, 16r+26 ∈ A, 32r+52 ∈ fA.

Since m ∈ B, we have 2m+2 = 8n+12 = 32r+52 ∈ fB, and so 32r+52 ∈ C. This contradicts C ∩ fA = ∅. QED

The following pertains to 4,3’.

LEMMA 3.8.16. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gA has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = 2m+1, f(m,n) = 2m, g(n) = 4n+5. Let C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gA, where A,B,C are nonempty.

Let m ∈ B. Then 2m+2 ∈ fB, 2m+2 ∈ C, 2m+2 ∉ fA, m ∉ A, m ∈ C ∪ gA.

case 1. m ∈ C. Then m ∈ A ∪ gA, m ∈ gA. Let m = 4n+5, n ∈ A. Hence 2n+2 ∈ fA, 2n+2 ∈ A. Since n < 2n+2 are from A, we have m = 4n+5 ∈ fA. This contradicts C ∩ fA = ∅.

case 2. m ∈ gA. Let m = 4n+5, n ∈ A. Hence 2n+2 ∈ fA, 2n+2 ∈ A, 4n+6 ∈ fA, 4n+6 ∈ A, 8n+12 = 2m+2 ∈ fA. Since 2m+2 ∈ C, this contradicts C ∩ fA = ∅. QED

The following pertains to 4,4’, 4,5’, 4,6’.

LEMMA 3.8.17. C ∪. fA ⊆ A ∪. gX, A ∪. fB ⊆ C ∪. gY has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = f(m,n) = 2m+2, g(n) = 2n+1. Let C ∪. fA ⊆ A ∪. gX, B ∪. fB ⊆ C ∪. gY, where A,B,C are nonempty.

Let m ∈ A. Then 2m+2 ∈ fA, 2m+2 ∈ A, 2m+2 ∈ C. This contradicts C ∩ fA = ∅. QED

part 5. C ∪. fA ⊆ A ∪. gB.

5,1′. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,2′. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,3′. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,4′. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,5′. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,6′. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

The following pertains to 5,1′.

LEMMA 3.8.18. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gB has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = f(m,n) = 4m+6, g(n) = 2n+1. Let C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gB, where A,B,C are nonempty.

Let m ∈ B. Then 2m+2 ∈ fB, 2m+2 ∈ C, 2m+2 ∈ A, 4m+6 ∈ fA, 2m+2 ∉ fA, m ∉ A, m ∈ C ∪ gB.

case 1. m ∈ C. Then m ∈ A ∪ gB, m ∈ gB. This contradicts C ∩ gB = ∅.

case 2. m ∈ gB. Let m = 2n+1, n ∈ B. Since n < m are from B, we have 4m+6 ∈ fB, 4m+6 ∈ C. Since 4m+6 ∈ fA, this contradicts C ∩ fA = ∅.

QED

The following pertains to 5,2’.

LEMMA 3.8.19. $C \cup. fA \subseteq A \cup. gB$, $B \cup. fB \subseteq C \cup. gC$ has $\neg$NON.

Proof: Define $f,g \in ELG$ as follows. For all $n < m$, let $f(n,n) = 2n+2$, $f(n,m) = 2m+8$, $f(m,n) = 2m+4$, $g(n) = 2n+3$. Let $C \cup. fA \subseteq A \cup. gB$, $B \cup. fB \subseteq C \cup. gC$, where A,B,C are nonempty.

Let $m \in B$. Then $2m+2 \in fB$, $2m+2 \in C$, $2m+2 \notin fA$, $m \notin A$, $m \in C \cup gC$.

case 1. $m \in C$. Then $m \in A \cup gB$. Hence $m \in gB$. This contradicts $B \cap gB = \emptyset$.

case 2. $m \in gC$. Let $m = 2n+3$, $n \in C$. Hence $n \in A \cup gB$.

case 2a. $n \in A$. Then $2n+2 \in fA$, $2n+2 \in A$. Since $n < 2n+2$ are from A, we have $4n+8 = 2m+2 \in fA$. But $2m+2 \notin fA$.

case 2b. $n \in gB$. Let $n = 2r+3$, $r \in B$. Now $m = 2n+3 = 4r+9 \in B$. So $2m+2 = 8r+20 \in fB$, $2m+2 = 8r+20 \in C$. Note that $2r+2 \in fB$, $2r+2 \in C$, $2r+2 \in A$, $4r+6 \in fA$, $4r+6 \in A$. Since $2r+2 < 4r+6$ are from A, we have $8r+20 \in fA$. This contradicts $C \cap fA = \emptyset$. QED

The following pertains to 5,3’.

LEMMA 3.8.20. $C \cup. fA \subseteq A \cup. gB$, $B \cup. fB \subseteq C \cup. gA$ has $\neg$NON.

Proof: Define $f,g \in ELG$ as follows. For all $n < m$, let $f(n,n) = 2n+2$, $f(n,m) = 4m+6$, $f(m,n) = 2m$, $g(n) = 4n+5$. Let $C \cup. fA \subseteq A \cup. gB$, $B \cup. fB \subseteq C \cup. gA$, where A,B,C are nonempty.

Let $m \in B$. Then $2m+2 \in fB$, $2m+2 \in C$, $2m+2 \in A$, $4m+6 \in fA$, $2m+2 \notin fA$, $m \notin A$, $m \in C \cup gA$.

case 1. $m \in C$. Then $m \in A \cup gB$, $m \in gB$. Let $m = 4n+5$, $n \in B$. Since $n < m$ are from B, we have $4m+6 \in fB$, $4m+6 \in C$. This contradicts $C \cap fA = \emptyset$.

case 2. $m \in gA$. Let $m = 4n+5$, $n \in A$. Then $2n+2 \in fA$, $2n+2 \in A$, $4n+6 \in fA$, $4n+6 \in A$. Since $2n+2 < 4n+6$ are from A, we have 8n+12 = 2m+2 ∈ fA. Since 2m+2 ∈ C, this contradicts C ∩ fA = ∅.

QED

LEMMA 3.8.21. X ∪. fA ⊆ A ∪. gY, A ∪. fZ ⊆ X ∪. gW has ¬NON.

Proof: Let f be as given by Lemma 3.2.1. Let g ∈ ELG be defined by g(n) = 2n+1. Let X ∪. fA ⊆ A ∪. gY, A ∪. fZ ⊆ X ∪. gW, where X,A,Y,Z,W are nonempty.

Let n ∈ fA ∩ 2N. Then n ∈ A. Hence fA ∩ 2N ⊆ A. By Lemma 3.2.1, fA is cofinite. Hence A contains almost all of 2N. Therefore X contains almost all of 2N. This contradicts X ∩ fA = ∅. QED

LEMMA 3.8.22. 5,4', 5,5', 5,6' have ¬NON.

Proof: By Lemma 3.8.21. QED

part 6. C ∪. fA ⊆ A ∪. gC.

6,1'. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,2'. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,3'. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,4'. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,5'. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,6'. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

The following pertains to 6,1'.

LEMMA 3.8.23. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gB has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = f(m,n) = 2m, g(n) = 2n+1. Let C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gB, where A,B,C are nonempty.

We claim that for all t ∈ A and p ≥ 0, $2g^p(t)+2$ ∈ A ∩ fA. To see this, fix t ∈ A and argue by induction on p ≥ 0. Obviously $2g^0(t)+2$ = 2t+2 ∈ fA, and so $2g^0(t)+2$ = 2t+2 ∈ A ∩

fA. Suppose $2g^p(t)+2 \in A \cap fA$. Note that $2g^{p+1}(t)+2 = 2(2g^p(t)+1)+2 = 2(2g^p(t)+2) \in fA$, since $t < 2g^p(t)+2$ are from A. Hence $2g^{p+1}(t)+2 \in A \cap fA$.

Let m = min(B). Then $2m+2 \in fB$, $2m+2 \in C$, $2m+2 \notin fA$, $m \notin A$, $m \in C \cup gB$, $m \notin gB$, $m \in C$, $m \in A \cup gC$, $m \in gC$, $g^{-1}(m) \in C$.

Let p be greatest such that

$g^{-1}(m),\ldots,g^{-p}(m) \in C$.

Then $p \geq 1$ and $g^{-p}(m) \in C\backslash gC$. Hence $g^{-p}(m) \in A$.

By the claim, $2g^p(g^{-p}(m))+2 \in A \cap fA$. Hence $2m+2 \in A \cap fA$. Since $2m+2 \in C$, this contradicts $C \cap fA = \emptyset$. QED

The following pertains to 6,2'.

LEMMA 3.8.24. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gC has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = f(m,n) = 2m, g(n) = 2n+1. Let C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gC, where A,B,C are nonempty.

Let $m \in B$. Then $m \in C \cup gC$.

case 1. $m \in C$. Then $m \in A \cup gC$, $m \notin gC$, $m \in A$, $2m+2 \in fA$, $2m+2 \in A$, $2m+2 \in fB$, $2m+2 \in C$. This contradicts $C \cap fA = \emptyset$.

case 2. $m \in gC$. Let $m = 2n+1$, $n \in C$. Then $n \notin gC$, $n \in A$, $2n+2 \in fA$, $2n+2 \in A$. Since $n < 2n+2$ are from A, we have $4n+4 = 2m+2 \in fA$, $2m+2 \in fB$, $2m+2 \in C$. This contradicts $C \cap fA = \emptyset$. QED

The following pertains to 6,3'.

LEMMA 3.8.25. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gA has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = f(m,n) = 2m, g(n) = 2n+1. Let C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gA, where A,B,C are nonempty.

As in the proof of Lemma 3.8.23, for all $t \in A$ and $p \geq 0$, $2g^p(t)+2 \in A \cap fA$.

Let $m \in B$. Then $2m+2 \in fB$, $2m+2 \in C$, $2m+2 \notin fA$, $m \notin A$, $m \in C \cup gA$.

case 1. $m \in C$. Then $m \in A \cup gC$, $m \in gC$, $g^{-1}(m) \in C$.

Let p be greatest such that $g^{-1}(m),\ldots,g^{-p}(m) \in C$.

Then $p \geq 1$ and $g^{-p}(m) \in C\backslash gC$. Hence $g^{-p}(m) \in A$.

By the claim, $2g^p(g^{-p}(m))+2 \in A \cap fA$. Hence $2m+2 \in A \cap fA$. Since $2m+2 \in C$, this contradicts $C \cap fA = \emptyset$.

case 2. $m \in gA$. Let $m = 2n+1$, $n \in A$. Then $2n+2 \in fA$, $2n+2 \in A$. Since $n < 2n+2$ are from A, we have $4n+4 = 2m+2 \in fA$. Since $2m+2 \in C$, this contradicts $C \cap fA = \emptyset$.

QED

LEMMA 3.8.26. 6,4', 6,5', 6,6' have ¬NON.

Proof: By Lemma 3.8.21. QED

3.9. ABAB.

Recall the following reduced table for AB from section 3.5.

REDUCED AB

1. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
2. A ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
4. C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
5. C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
6. C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

The duplicate pairs were treated in section 3.3. We now treat the 15 ordered pairs from this table, where the first clause is earlier in the list than the second clause. We determine the status of INF, AL, ALF, FIN, NON for each such ordered pair.

1,2. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
1,3. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
1,4. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.

1,5. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
1,6. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
2,3. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
2,4. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. FIN, NON.
2,5. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
2,6. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
3,4. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
3,5. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
3,6. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
4,5. C ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. AL. ¬ALF. FIN. NON.
4,6. C ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
5,6. C ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. FIN, NON.

LEMMA 3.9.1. (1,3), (1,4), (1,6), (2,3), (2,5), (3,4), (3,6), (4,6) have INF, ALF, even for EVSD.

Proof: Note that A ∪. fA ⊆ B ∪. gA has INF, ALF, and A ∪. fA ⊆ B ∪. gB has INF, ALF, even for EVSD, by the AB table in section 3.3. Now set C = A in all of the above ordered pairs except (2,3). For (2,3), set C = B. QED

The following pertains to (1,2).

LEMMA 3.9.2. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gB has FIN.

Proof: Let f,g ∈ ELG. Let A = {n}, where n is sufficiently large.

case 1. f(n,...,n) = g(n,...,n). Set A = B = {n}.

case 2. f(n,...,n) ≠ g(n,...,n). Set A = {n}, B = {n,f(n,...,n)}. Note that A ⊆ B.

In case 1, fA = gA = gB, A ∩ fA = B ∩ gA = B ∩ gB = ∅.

In case 2, note that A ⊆ B, A ∩ fA = B ∩ gA = ∅, fA ⊆ B.

We claim that $B \cap gB = \emptyset$. To see this, first note that $n \notin gB$ since n is sufficiently large. Also note that $f(n,...,n) \notin gB$, since $f(n,...,n) \neq g(n,...,n)$, and $f(n,...,n) \neq g(...,f(n,...,n)...)$. QED

LEMMA 3.9.3. (1,5), (2,4), (2,6), (3,5), (4,5), (5,6) have FIN.

Proof: From Lemma 3.9.2, by setting C = A in the cited ordered pairs. QED

LEMMA 3.9.4. $fA \subseteq B \cup. gA$, $A \cap fA = B \cap gB = \emptyset$ has ¬AL.

Proof: Define $f,g \in ELG$ as follows. For all $n < m$, let $f(n,n) = 2n$, $f(n,m) = 4m$, $f(m,n) = 8m$, $g(n) = 2n$. Let $fA \subseteq B \cup. gA$, $A \cap fA = B \cap gB = \emptyset$, where A,B have at least two elements. Let $n < m$ be from A.

Clearly $2m,4m,8m \in fA$. Hence $2m,4m,8m \notin A$. So $4m,8m \notin gA$. Hence $4m,8m \in B$, $8m \in fB$. This contradicts $B \cap fB = \emptyset$. QED

LEMMA 3.9.5. (1,2), (1,5) have ¬AL.

Proof: By Lemma 3.9.4. QED

The following pertains to (2,4).

LEMMA 3.9.6. $A \cup. fA \subseteq B \cup. gB$, $C \cup. fA \subseteq B \cup. gA$ has ¬AL.

Proof: Define $f,g \in ELG$ as follows. For all $n < m$, let $f(n,n) = 2n$, $f(n,m) = f(m,n) = 4m+1$, $g(n) = 2n+1$. Let $A \cup. fA \subseteq B \cup. gB$, $C \cup. fA \subseteq B \cup. gA$, where A,B have at least two elements. Let $n < m$ be from A.

Clearly $2m \in fA$, $2m \in B$, $2m \notin A$, $4m+1 \notin gA$, $4m+1 \in fA$, $4m+1 \in B$, $4m+1 \in gB$. This contradicts $B \cap gB = \emptyset$. QED

LEMMA 3.9.7. $fA \subseteq B \cup. gB$, $fA \subseteq B \cup. gC$, $C \cap fA = \emptyset$ has ¬AL.

Proof: Define $f,g \in ELG$ as follows. For all $n < m$, let $f(n,n) = 2n$, $f(n,m) = f(m,n) = 4m+1$, $g(n) = 2n+1$. Let $fA \subseteq B \cup. gB$, $fA \subseteq B \cup. gC$, $C \cap fA = \emptyset$, where A,B,C have at least two elements. Let $n < m$ be from A.

Clearly $2m \in fA$, $2m \in B$, $2m \notin C$, $4m+1 \notin gC$, $4m+1 \in fA$, $4m+1 \in B$, $4m+1 \in gB$. This contradicts $B \cap gB = \emptyset$. QED

LEMMA 3.9.8. (2,6), (3,5), (5,6) have ¬AL.

Proof: By Lemma 3.9.7. QED

The following pertains to (4,5).

LEMMA 3.9.9. C ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB has AL.

Proof: Note that C ∪. fA ⊆ A ∪. gA has AL by the AA table of section 3.3. Replace B by A in the cited pair. QED

The following pertains to (4,5).

LEMMA 3.9.10. C ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB has ¬INF, ¬ALF.

Proof: Let f be as given by Lemma 3.2.1. Let f′ ∈ ELG be given by f′(a,b,c,d) = f(a,b,c) if c = d; 2f(a,b,c)+1 if c > d; 2|a,b,c,d|+2 if c < d. Let g ∈ ELG be given by g(n) = 2n+1. Let C ∪. f′A ⊆ B ∪. gA, C ∪. f′A ⊆ B ∪. gB, where A,B,C have at least two elements. Let A′ = A\{min(A)}.

Note that fA′ ⊆ fA ⊆ f′A. To see this, let a,b,c ∈ A. Then f(a,b,c) = f′(a,b,c,c).

Let n ∈ fA′ ∩ 2N. Write n = f(a,b,c), a,b,c ∈ A'. Then 2n+1 = f'(a,b,c,min(A)), 2n+1 ∈ f'A. Also n ∈ f'A. Hence n ∈ B, 2n+1 ∈ gB, 2n+1 ∉ B, 2n+1 ∈ gA, n ∈ A, n > min(A), n ∈ A'. Thus we have shown that fA′ ∩ 2N ⊆ A′. Hence by Lemma 3.2.1, fA′ is cofinite.

It is now clear that A′ is infinite, and therefore A is infinite. This establishes ¬ALF.

We also see that C is finite, since f′A is cofinite and C ∩ f′A = ∅. This establishes ¬INF. QED

3.10. ABAC.

Recall the reduced AB table from section 3.5.

REDUCED AB

1. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
2. A ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

4. C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
5. C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
6. C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

The reduced AC table is obtained from the reduced AB table by interchanging B and C. We use 1'-6' to avoid confusion.

REDUCED AC

1′. A ∪. fA ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
2′. A ∪. fA ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
3′. A ∪. fA ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
4′. B ∪. fA ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
5′. B ∪. fA ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
6′. B ∪. fA ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.

We will use the reduced AB table and the reduced AC table.

Note that each i,j′ is equivalent to j,i′, because each i,j′ is sent to i′,j by interchanging B and C.

Hence we need only consider i,j′ where i ≤ j′.

We need to determine the status of INF, AL, ALF, FIN, NON for each pair.

1,1′. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
1,2′. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gC. INF. AL. ALF. FIN, NON.
1,3′. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
1,4′. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,5′. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,6′. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,2′. A ∪. fA ⊆ B ∪. gB. A ∪. fA ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
2,3′. A ∪. fA ⊆ B ∪. gB. A ∪. fA ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
2,4′. A ∪. fA ⊆ B ∪. gB. B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,5′. A ∪. fA ⊆ B ∪. gB. B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,6′. A ∪. fA ⊆ B ∪. gB. B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

3,3′. A ∪. fA ⊆ B ∪. gC. A ∪. fA ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
3,4′. A ∪. fA ⊆ B ∪. gC. B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,5′. A ∪. fA ⊆ B ∪. gC. B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,6′. A ∪. fA ⊆ B ∪. gC. B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,4′. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,5′. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,6′. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,5′. C ∪. fA ⊆ B ∪. gB. B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,6′. C ∪. fA ⊆ B ∪. gB. B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FiN. ¬NON.
6,6′. C ∪. fA ⊆ B ∪. gC. B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

LEMMA 3.10.1. fA ⊆ B ∪. gY, B ∩ fA = ∅ has ¬NON.

Proof: Define f,g ∈ ELG as follows. f(n) = 2n+2, g(n) = 2n+1. Let X ∪. fA ⊆ B ∪. gY, B ∪. fA ⊆ Z ∪. gW, where A,B,C are nonempty.

Clearly fA ⊆ B. This contradicts B ∩ fA = ∅. QED

LEMMA 3.10.2. 1,4′ - 1,6′, 2,4′ - 2,6′, 3,4′ - 6,6′ have ¬NON.

Proof: By Lemma 3.10.1. QED

LEMMA 3.10.3. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gX has INF, ALF, provided X ∈ {A,B}, even for EVSD.

Proof: Let f,g ∈ EVSD. By Lemma 3.2.5, let A ⊆ N be infinite, where A is disjoint from fA ∪ g(A ∪ fA), and min(A) is sufficiently large.

Let B = (A ∪ fA)\gA. Let C = (A ∪ fA)\gX.

Clearly A ∩ fA = B ∩ gA = A ∩ gA = A ∩ gB = C ∩ gX = ∅. Hence A ⊆ B, A ⊆ C. Also A ∪ fA ⊆ B ∪ gA, A ∪ fA ⊆ C ∪ gX. This establishes INF.

We can repeat the argument using A of any given finite cardinality. This establishes ALF. QED

LEMMA 3.10.4. 1,1′ and 1,3′ have INF, ALF, even for EVSD.

Proof: Immediate from Lemma 3.10.3. QED

The following pertains to 1,2′.

LEMMA 3.10.5. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gC has INF, ALF, even for EVSD.

Proof: Let f,g ∈ EVSD. By Lemma 3.2.5, let A ⊆ N be infinite, where A is disjoint from fA ∪ g(A ∪ fA), and min(A) is sufficiently large.

Let B = (A ∪ fA)\gA. By Lemma 3.3.3, let C be unique such that C ⊆ A ∪ fA ⊆ C ∪. gC. Then C is infinite.

Clearly A ∩ fA = B ∩ gA = C ∩ gC = A ∩ gA = ∅. Also A ∩ gC ⊆ A ∩ g(A ∪ fA) = ∅. Hence A ⊆ B, A ⊆ C. Also A ∪ fA ⊆ B ∪ gA, A ∪ fA ⊆ C ∪ gC. This establishes INF.

We can repeat the argument using A of any given finite cardinality. This establishes ALF. QED

The following pertains to 2,3′.

LEMMA 3.10.6. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gB has INF, ALF, even for EVSD.

Proof: Let f,g ∈ EVSD. By Lemma 3.2.5, let A ⊆ N be infinite, where A is disjoint from fA ∪ g(A ∪ fA), and min(A) is sufficiently large.

By Lemma 3.3.3, let B be unique such that B ⊆ A ∪ fA ⊆ B ∪. gB. Define C = (A ∪ fA)\gB.

Clearly A ∩ fA = B ∩ gB = C ∩ gB = ∅. Also A ∩ gB ⊆ A ∩ g(A ∪ fA) = ∅. Hence A ⊆ B, A ⊆ C. Also A ∪ fA ⊆ B ∪ gB, A ∪ fA ⊆ C ∪ gB. This establishes INF.

We can repeat the argument using A of any given finite cardinality. This establishes ALF. QED

The following pertains to 2,2′.

LEMMA 3.10.7. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gC has INF, ALF, even for EVSD.

Proof: From the AB table, A ∪. fA ⊆ B ∪. gB has INF, ALF. Replace C by B in the cited pair. QED

The following pertains to 3,3'.

LEMMA 3.10.8. A ∪. fA ⊆ B ∪. gC. A ∪. fA ⊆ C ∪. gB has INF, ALF, even for EVSD.

Proof: A ∪. fA ⊆ B ∪. gB has INF, ALF, by the AB table. Replace C by B in the cited pair. QED

3.11. ABBA.

Recall the reduced AB table from section 3.5.

REDUCED AB

1. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
2. A ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
4. C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
5. C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
6. C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

Recall the reduced BA table from section 3.6.

REDUCED BA

1'. B ∪. fB ⊆ A ∪. gB. INF. AL. ALF. FIN. NON.
2'. B ∪. fB ⊆ A ∪. gA. INF. AL. ALF. FIN. NON.
3'. B ∪. fB ⊆ A ∪. gC. INF. AL. ALF. FIN. NON.
4'. C ∪. fB ⊆ A ∪. gB. INF. AL. ALF. FIN. NON.
5'. C ∪. fB ⊆ A ∪. gA. INF. AL. ALF. FIN. NON.
6'. C ∪. fB ⊆ A ∪. gC. INF. AL. ALF. FIN. NON.

This results in 36 ordered pairs.

We can take advantage of symmetry through interchanging A with B as follows. Clearly (i,j') and (j,i') are equivalent, since interchanging A and B takes us from p to p' and back. So we can require that i ≤ j. Thus we have the following 21 ordered pairs to consider.

We need to determine the status of all attributes INF, Al, ALF, FIN, NON, for each pair.

1,1′. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,2′. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,3′. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,4′. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,5′. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,6′. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,2′. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,3′. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,4′. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,5′. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2,6′. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,3′. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,4′. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,5′. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3,6′. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,4′. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
4,5′. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
4,6′. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
5,5′. C ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
5,6′. C ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
6,6′. C ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

LEMMA 3.11.1. 1,1′ - 6,6′ have ¬INF, ¬FIN.

Proof: Let f be as given by Lemma 3.2.4. Let g ∈ ELG be defined by g(n) = 2n+1. Let

X ∪. fA ⊆ B ∪. gY
S ∪. fB ⊆ A ∪. gT

where X,A,B,Y,S,T are nonempty subsets of N. Then fA ∩ 2N ⊆ B and fB ∩ 2N ⊆ A. Hence f(fA ∩ 2N) ∩ 2N ⊆ fB ∩ 2N ⊆ A. By Lemma 3.2.4, fA is cofinite. Thus A is infinite. This establishes ¬FIN. Also X is finite, since X ∩ fA = ∅. This establishes ¬INF. QED

Lemma 3.11.1 establishes that we have ¬INF, ¬ALF, ¬FIN for all of the pairs of clauses considered in this section. It remains to determine the status of AL and NON.

LEMMA 3.11.2. fA ⊆ B ∪. gY, fB ⊆ A ∪. gZ, A ∩ fA = ∅ has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = 2m, f(m,n) = 4m, g(n) = 2n+1. Let fA ⊆ B ∪. gY, fB ⊆ A ∪. gZ, A ∩ fA = ∅, where A,B,Y,Z are nonempty subsets of N.

Let n ∈ B. Then 2n+2 ∈ fB, 2n+2 ∈ A, 4n+6 ∈ fA, 4n+6 ∈ B. Since n < 4n+6 are from B, we have 8n+12 ∈ fB, 8n+12 ∈ A. Since 2n+2 < 8n+12 are from A, we have 16n+24 ∈ fA. Also since n < 4n+6 are from B, we have 16n+24 ∈ fB, 16n+24 ∈ A. This contradicts A ∩ fA = ∅. QED

LEMMA 3.11.3. 1,1′ - 3,6′ have ¬NON.

Proof: By Lemma 3.11.2. QED

LEMMA 3.11.4. C ∪. fA ⊆ B ∪. gX, C ∪. fB ⊆ A ∪. gY has AL.

Proof: Let f,g ∈ ELG and p ≥ 0. Let C = [n,n+p], where n is sufficiently large. Throw all elements of [n,n+p] into A,B. A,B will have no elements < n.

We determine membership of all k > n+p in A,B by induction as follows. Suppose membership in A,B has been determined for all integers < k, where k > n+p is fixed. If k is not already in gX then put k in B. If k is not already in gY then put k in A.

Note that C ⊆ A,B ⊆ [n,∞), C ∩ fA = C ∩ fB = B ∩ gX = A ∩ gY = ∅. Also we have fA ⊆ [n,∞) ⊆ B ∪ gX, fB ⊆ [n,∞) ⊆ A ∪ gY. QED

LEMMA 3.11.5. 4,4′ - 6,6′ have AL.

Proof: By Lemma 3.11.4. QED

3.12. ABBC.

Recall the following reduced table for AB from section 3.5.

REDUCED AB

1. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
2. A ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
4. C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
5. C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
6. C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

The reduced table for BC is obtained from the reduced table for AB via the permutation that sends A to B, B to C, and C to A. We use 1'-6' to avoid confusion.

REDUCED BC

1′. B ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
2′. B ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
3′. B ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
4′. A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
5′. A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
6′. A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.

This results in 36 ordered pairs, which we divide into six cases. We begin with two Lemmas.

We will determine the status of all attributes INF, AL, ALF, FIN, NON, for all ordered pairs.

LEMMA 3.12.1. C ∪. fX ⊆ B ∪. gY, Z ∪. fB ⊆ C ∪. gW has ¬INF, ¬FIN.

Proof: Let f be as given by Lemma 3.2.1. Let g ∈ ELG be given by g(n) = 2n+1. Let C ∪. fX ⊆ B ∪. gY, Z ∪. fB ⊆ C ∪. gW, where A,B,C are nonempty.

Clearly fB ∩ 2N ⊆ C. By C ⊆ B ∪ gY, we have fB ∩ 2N ⊆ B. Hence by Lemma 3.2.1, fB is cofinite. Hence B is infinite. This establishes that ¬FIN. Also Z is finite. This establishes that ¬INF. QED

LEMMA 3.12.2. C ∪. fX ⊆ B ∪. gY, Z ∪. fB ⊆ C ∪. gW, B ∩ fB = ∅ has ¬NON.

Proof: We can continue the proof of Lemma 3.12.1. Using fB is cofinite and B is finite, we obtain an immediate contradiction from B ∩ fB = ∅. QED

We use Lemmas 3.12.1 and 3.12.2 in cases 5,6 below.

part 1. A ∪. fA ⊆ B ∪. gA.

1,1′. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,2′. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,3′. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
1,4′. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
1,5′. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
1,6′. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.

The following pertains to 1,4′, 1,6′.

LEMMA 3.12.3. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gX has INF, ALF provided X ∈ {A,B}, even for EVSD.

Proof: Let f,g ∈ EVSD. Let n be sufficiently large. By Lemma 3.2.5, let A ⊆ [n,∞) be infinite, where A is disjoint from f(A ∪ fA) ∪ g(A ∪ fA). Let B = (A ∪ fA)\gA, and C = (A ∪ fB)\gX.

Clearly A ∩ fA = B ∩ gA = A ∩ fB = C ∩ gX = A ∩ gA = A ∩ gB = ∅. Hence A ⊆ B and A ⊆ C. Also fA ⊆ B ∪ gA and fB ⊆ C ∪ gX. This establishes INF.

We can repeat the argument where A is chosen to be of any finite cardinality. This establishes ALF. QED

The following pertains to 1,5′.

LEMMA 3.12.4. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gC has INF, ALF, even for EVSD.

Proof: Let f,g ∈ EVSD. Let n be sufficiently large. By Lemma 3.2.5, let A ⊆ [n,∞) be infinite, where A is disjoint from f(A ∪ fA) ∪ g(A ∪ fA) ∪ g(A ∪ f(A ∪ fA)). Let B = (A ∪ fA)\gA. By Lemma 3.3.3, let C be unique such that C ⊆ A ∪ fB ⊆ C ∪. gC.

Clearly A ∩ fA = B ∩ gA = A ∩ fB = C ∩ gC = A ∩ gA = A ∩ gC = ∅. Hence A ⊆ B and A ⊆ C. Also fA ⊆ B ∪ gA and fB ⊆ C ∪ gC. This establishes INF.

We can repeat the proof where A is chosen to be of any finite cardinality. This establishes ALF. QED

The following pertains to 1,1′, 1,2′, 1,3′.

LEMMA 3.12.5. A ∪. fA ⊆ B ∪. gA, B ∩ fB = ∅ has ¬NON.

Proof: Define f,g ∈ ELG as follows. Let f(n) = 2n+2 and g(n) = 2n+1. Let A ∪. fA ⊆ B ∪. gA, B ∩ fB = ∅, where A,B are nonempty.

Let n = min(A). Then n ∉ gA, n ∈ B, 2n+2 ∈ fB, 2n+2 ∈ fA, 2n+2 ∈ B. This contradicts B ∩ fB = ∅. QED

part 2. A ∪. fA ⊆ B ∪. gB.

2,1′. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
2,2′. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
2,3′. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. FIN. NON.
2,4′. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
2,5′. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
2,6′. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.

The following pertains to 2,4′, 2,6′.

LEMMA 3.12.6. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gX has INF, ALF, provided X ∈ {A,B}, even for EVSD.

Proof: Let f,g ∈ EVSD. Let n be sufficiently large. By Lemma 3.2.5, let A ⊆ [n,∞) be infinite, where A is disjoint from f(A ∪ fA) ∪ g(A ∪ fA). By Lemma 3.3.3, let B be unique such that B ⊆ A ∪ fA ⊆ B ∪. gB. Let C = (A ∪ fB)\gX.

Clearly A ∩ fA = B ∩ gB = A ∩ fB = C ∩ gX = A ∩ gB = A ∩ gA = ∅. Hence A ⊆ B and A ⊆ C. Also fA ⊆ B ∪ gB and fB ⊆ C ∪ gX. This establishes INF.

We can repeat the argument where A is chosen to be of any finite cardinality. This establishes ALF. QED

The following pertains to 2,5'.

LEMMA 3.12.7. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gC has INF, ALF, even for EVSD.

Proof: Let f,g ∈ EVSD. Let n be sufficiently large. By Lemma 3.2.5, let A ⊆ [n,∞) be infinite, where A is disjoint from f(A ∪ fA) ∪ g(A ∪ fA) ∪ g(A ∪ f(A ∪ fA)). By Lemma 3.3.3, let B be unique such that B ⊆ A ∪ fA ⊆ B ∪. gB. By Lemma 3.3.3, let C be unique such that C ⊆ A ∪ fB ⊆ C ∪. gC.

Clearly A ∩ fA = B ∩ gB = A ∩ fB = C ∩ gC = A ∩ gB = A ∩ gC = ∅. Hence A ⊆ B and A ⊆ C. Also fA ⊆ B ∪ gB and fB ⊆ C ∪ gC. This establishes INF.

We can repeat the argument where A is chosen to be of any finite cardinality. This establishes ALF. QED

The following pertains to 2,1', 2,3'.

LEMMA 3.12.8. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gX has FIN, provided X ∈ {A,B}.

Proof: Let f,g ∈ ELG. We claim that there exists arbitrarily large n such that f(n,...,n) ≠ f(g(n,...,n),...,g(n,...,n)). Suppose this is false. I.e., let r be such that for all n ≥ r, f(n,...,n) = f(g(n,...,n),...,g(n,...,n)). We can assume that r is chosen so that f,g is strictly dominating on [r,∞).

Define $t_0 = r$, $t_{i+1} = g(t_i,...,t_i)$. An obvious induction shows that $r \leq t_0 < t_1 < ...$.

We now prove by induction that for all i ≥ 0,

$$f(r,...,r) = f(t_i,...,t_i).$$

Obviously this is true for i = 0. Suppose this is true for a given i ≥ 0. Then

$$f(r,...,r) = f(t_i,...,t_i).$$
$$t_i \geq r.$$
$$f(t_i,...,t_i) = f(g(t_i,...,t_i),...,g(t_i,...,t_i)).$$
$$f(r,...,r) = f(t_{i+1},...,t_{i+1}).$$

However some t_i is greater than f(r,...,r), since the t's are strictly increasing. This is a contradiction. The claim is now established.

Now let n be sufficiently large with the property that f(n,...,n) ≠ f(g(n,...,n),...,g(n,...,n)). Let A = {g(n,...,n)}. Let B = {n,f(g(n,...,n),...,g(n,...,n))}. Let C = (B ∪ fB)\gX.

Clearly A ∩ fA = B ∩ gB = B ∩ fB = C ∩ gX = ∅. Also A ⊆ gB, fA ⊆ B, B ∪ fB ⊆ C ∪ gX. In addition, n ∉ gX, n ∈ B, and so n ∈ C. Hence A,B,C are nonempty finite sets. QED

The following pertains to 2,2'.

LEMMA 3.12.9. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gC has FIN.

Proof: Let f,g ∈ ELG. We define n,A,B exactly as in the proof of Lemma 3.12.8. By Lemma 3.3.3, let C be unique such that C ⊆ B ∪ fB ⊆ C ∪. gC.

Clearly A ∩ fA = B ∩ gB = B ∩ fB = C ∩ gC = ∅. Also A ⊆ gB, fA ⊆ B, B ∪ fB ⊆ C ∪ gC. In addition, n ∉ gC, and so n ∈ C. Hence A,B,C are nonempty finite sets. QED

The following pertains to 2,1', 2,2', 2,3'.

LEMMA 3.12.10. fA ⊆ B ∪. gX, B ∩ fB = ∅ has ¬AL.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(m,n) = f(n,m) = 4m+6, g(n) = 2n+1. Let fA ⊆ B ∪. gX, B ∩ fB = ∅, where A,B,C have at least two elements. Let n < m be from A. Then 2m+2,4m+6 ∈ fA, 2m+2,4m+6 ∈ B, 4m+6 ∈ fB. This contradicts B ∩ fB = ∅. QED

part 3. A ∪. fA ⊆ B ∪. gC.

3,1′. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
3,2′. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
3,3′. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. FIN. NON.
3,4′. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
3,5′. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
3,6′. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.

LEMMA 3.12.11. 3,1′ - 3,3′ have ¬AL.

Proof: By Lemma 3.12.10. QED

The following pertains to 3,1′, 3,3′.

LEMMA 3.12.12. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gX has FIN, where X ∈ {A,B}.

Proof: Let f,g ∈ ELG. Let n be sufficiently large. Define A = {g(n,...,n)}, B = {f(g(n,...,n),...,g(n,...,n))}, C = (B ∪ fB ∪ {n})\gX.

Obviously A ∩ fA = B ∩ fB = C ∩ gX = ∅. Also n ∉ gX, n ∈ C. Hence A ⊆ gC and fA ⊆ B. Therefore A ∪ fA ⊆ B ∪ gC. Obviously B ∪ fB ⊆ C ∪ gX.

It remains to verify that B ∩ gC = ∅. Every element of C is either n or f(g(n,...,n),...,g(n,...,n)) or the value of a term of depth ≤ 3 in f,g,n with f(g(n,...,n),...,g(n,...,n)) as a subterm. Hence every element of gC is either g(n,...,n) or the value of a term in f,g,n of depth ≤ 4 with f(g(n,...,n),...,g(n,...,n)) as a proper subterm. Since n is sufficiently large, f(g(n,...,n),...,g(n,...,n)) does not lie in gC. QED

The following pertains to 3,2′.

LEMMA 3.12.13. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gC has FIN.

Proof: Let f,g ∈ ELG. Let n be sufficiently large. Define A = {g(n,...,n)}, B = {f(g(n,...,n),...,g(n,...,n))}. By Lemma 3.3.3, let C be unique such that C ⊆ B ∪ fB ∪ {n} ⊆ C ∪. gC.

Obviously A ∩ fA = B ∩ fB = C ∩ gC = ∅. Also n ∉ gC, n ∈ C. A ⊆ gC, and fA ⊆ B. Therefore A ∪ fA ⊆ B ∪ gC. In addition, B ∪ fB ⊆ C ∪ gC.

It remains to verify that B ∩ gC = ∅. Argue exactly as in the proof of Lemma 3.12.12. QED

The following pertains to 3,4′, 3,5′, 3,6′.

LEMMA 3.12.14. A ∪. fA ⊆ B ∪. gC. A ∪. fB ⊆ C ∪. gX has INF, ALF, even for EVSD.

Proof: Let f,g ∈ EVSD. Let n be sufficiently large. By Lemma 3.2.5, let A ⊆ [n,∞) be infinite, where A is disjoint from f(A ∪ fA) ∪ g(A ∪ f(A ∪ fA)). We inductively determine membership in B,C for all elements of [n,∞). B,C will have no elements < n.

Suppose membership in B,C has been determined for all elements of [n,k), k ≥ n. We now determine membership in B,C for k. If k is already in A ∪ fA and k is not yet in gC, put k ∈ B. If k is already in A ∪ fB and k is not yet in gX, put k in C.

Clearly B ⊆ A ∪ fA and C ⊆ A ∪ fB ⊆ A ∪ f(A ∪ fA). Hence A ∩ fA = A ∩ fB = C ∩ gX = ∅. Also A ∪ fA ⊆ B ∪ gC and A ∪ fB ⊆ C ∪ gX. In addition, A ∩ gC ⊆ A ∩ g(A ∪ fB) ⊆ A ∩ g(A ∪ f(A ∪ fA)) = ∅, and so A ∩ gX = ∅. Hence A ⊆ B, A ⊆ C. This establishes INF.

We can instead use A of any finite cardinality. We obtain finite B,C with A ⊆ B,C. This establishes ALF. QED

part 4. C ∪. fA ⊆ B ∪. gA.

4,1′. C ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,2′. C ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,3′. C ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,4′. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,5′. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4,6′. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

The following pertains to 4,1′, 4,2′, 4,3′.

LEMMA 3.12.15. C ∪. fA ⊆ B ∪. gA. B ∪. fB ⊆ C ∪. gX has ¬NON.

Proof: Let f be as given by Lemma 3.2.1. Define g ∈ ELG by g(n) = 2n+1. Let C ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gX, where A,B,C are nonempty.

Let n ∈ fB ∩ 2N. Then n ∈ C, n ∈ B. Hence fB ∩ 2N ⊆ B. By Lemma 3.2.1, fB is cofinite. Hence B is infinite. This contradicts B ∩ fB = ∅. QED

The following pertains to 4,4′.

LEMMA 3.12.16. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gB has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(2n,2n,2n) = f(2n+1,2n+1,2n+1) = 4n, f(n,m,m) = 2m, f(n,m,n) = 4m, f(m,n,n) = 8m, g(2n) = g(2n+1) = 4n+1. For all other triples a,b,c, let f(a,b,c) = 2|a,b,c|.

We claim that

f(f(m,m,m),f(m,m,m),f(m,m,m)) = f(g(m),g(m),g(m)).

To see this, let m = 2r ∨ m = 2r+1. Then

f(f(m,m,m),f(m,m,m),f(m,m,m)) = f(4r,4r,4r) = 8r

and

f(g(m),g(m),g(m)) = f(4r+1,4r+1,4r+1) = 8r.

Now let C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gB, where A,B,C are nonempty. Let n ∈ A. Then n ∈ C ∪. gB.

case 1. n ∈ C. Then n ∈ B ∪ gA. First suppose n ∈ B. Then f(n,n,n) ∈ C ∪ gB. Hence f(n,n,n) ∈ C. This contradicts C ∩ fA = ∅.

Now suppose n ∈ gA. Let n = g(m), m ∈ A, m < n. Then 2n-2,4n-4,8n-8 ∈ fA, and so 2n-2,4n-4,8n-8 ∈ B, 8n-8 ∈ fB, 8n-8 ∈ C. This contradicts C ∩ fA = ∅.

case 2. $n \in gB$. Let $n = g(m)$, $m \in B$. Then $f(m,m,m) \in fB$, $f(m,m,m) \in C$. Hence $f(m,m,m) \in B$. Therefore $f(f(m,m,m),f(m,m,m),f(m,m,m)) \in fB$, $f(f(m,m,m),f(m,m,m),f(m,m,m)) \in C$. Note that $f(f(m,m,m),f(m,m,m),f(m,m,m)) = f(g(m),g(m),g(m)) = f(n,n,n) \in fA$. This contradicts $C \cap fA = \emptyset$.

QED

The following pertains to 4,6'.

LEMMA 3.12.17. $C \cup. fA \subseteq B \cup. gA$, $A \cup. fB \subseteq C \cup. gA$ has ¬NON.

Proof: Define f,g as in the proof of Lemma 3.12.16. Now let $C \cup. fA \subseteq B \cup. gA$, $A \cup. fB \subseteq C \cup. gA$, where A,B,C are nonempty. Let $n \in A$. Then $n \in C \cup. gA$.

case 1. $n \in gA$. Let $n = g(m)$, $m \in A$, $m < n$. Then $2n-2,4n-4,8n-8 \in fA$, $2n-2,4n-4,8n-8 \in B$, $8n-8 \in fB$, $8n-8 \in C$. This contradicts $C \cap fA = \emptyset$.

case 2. $n \in C$. Then $n \notin gA$, $n \in B$, $f(n,n,n) \in fB$, $f(n,n,n) \in C$. Since $f(n,n,n) \in fA$, this contradicts $C \cap fA = \emptyset$.

QED

The following pertains to 4,5'.

LEMMA 3.12.18. $C \cup. fA \subseteq B \cup. gA$, $A \cup. fB \subseteq C \cup. gC$ has ¬NON.

Proof: Define f,g as in the proof of Lemma 3.12.16. Now let $C \cup. fA \subseteq B \cup. gA$, $A \cup. fB \subseteq C \cup. gC$, where A,B,C are nonempty. Let $n = \min(A)$. Then $n \in C \cup. gC$.

case 1. $n \in C$. By the choice of n, $n \notin gA$, $n \in B$. Hence $f(n,n,n) \in fB$, $f(n,n,n) \in C$. Since $f(n,n,n) \in fA$, this contradicts $C \cap fA = \emptyset$.

case 2. $n \in gC$. Let $n = g(m)$, $m \in C$, $m < n$. Then $m \in B \cup gA$. By the choice of n, $m \notin gA$, $m \in B$. Hence $f(m,m,m) \in fB$, $f(m,m,m) \in C$, $f(m,m,m) \in B \cup gA$.

We claim that $f(m,m,m) \notin gA$. To see this, note that by quantitative considerations, $f(m,m,m) \in gA$ implies that there is an element of A that is $\leq m < n$, which contradicts the choice of n.

Hence f(m,m,m) ∈ B. Therefore

$$f(f(m,m,m),f(m,m,m),f(m,m,m)) \in fB.$$
$$f(f(m,m,m),f(m,m,m),f(m,m,m)) \in C.$$

As in the proof of Lemma 3.12.16,

$$f(f(m,m,m),f(m,m,m),f(m,m,m)) =$$
$$f(g(m),g(m),g(m)) = f(n,n,n) \in fA.$$

This contradicts C ∩ fA = ∅.

QED

part 5. C ∪. fA ⊆ B ∪. gB.

5,1'. C ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,2'. C ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,3'. C ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,4'. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,5'. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5,6'. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

LEMMA 3.12.19. 5,1', 5,2', 5,3' have ¬NON.

Proof: By Lemma 3.12.2. QED

The following pertains to 5,4'.

LEMMA 3.12.20. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gB has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = f(m,n) = 2m+1, g(n) = 4n+5. Let C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gB, where A,B,C are nonempty.

Let n ∈ A. Then n ∈ C ∪ gB.

case 1. n ∈ C\gB. Then n ∈ B, 2n+2 ∈ fB, 2n+2 ∈ C, 2n+2 ∈ fA. This contradicts C ∩ fA = ∅.

case 2. n ∈ gB. Let n = 4m+5, m ∈ B. Then 2m+2 ∈ fB, 2m+2 ∈ C, 2m+2 ∈ B. Since m < 2m+2 are from B, we have 4m+5 ∈ fB. Since 4m+5 = n ∈ A, this contradicts A ∩ fB = ∅. QED

The following pertains to 5,6'.

LEMMA 3.12.21. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gA has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = f(m,n) = 2m+1, g(n) = 4n+5. Let C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gA, where A,B,C are nonempty.

Let n = min(A). Then n ∈ C ∪ gA. Clearly n ∉ gA, n ∈ C, n ∈ B ∪ gB.

case 1. n ∈ B. Then 2n+2 ∈ fB, 2n+2 ∈ C, 2n+2 ∈ fA. This contradicts C ∩ fA = ∅.

case 2. n ∈ gB. Let n = 4m+5, m ∈ B. Then 2m+2 ∈ fB, 2m+2 ∈ C, 2m+2 ∈ B. Since m < 2m+2 are from B, we have 4m+5 ∈ fB. Since 4m+5 ∈ A, this contradicts A ∩ fB = ∅. QED

The following pertains to 5,5'.

LEMMA 3.12.22. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gC has ¬NON.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = 2m, f(m,n) = 4m, g(n) = 2n+1. Let C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gC, where A,B,C are nonempty.

Let n ∈ A. Then 2n+2 ∈ fA, n ∈ C ∪ gC.

case 1. n ∈ C. Then n ∈ B ∪ gB.

Suppose n ∈ B. Then 2n+2 ∈ fB, 2n+2 ∈ C. Since 2n+2 ∈ fA, this contradicts C ∩ fA = ∅.

Suppose n ∈ gB. Let n = 2m+1, m ∈ B. Then 2m+2 ∈ fB, 2m+2 ∈ C, 2m+2 ∈ B. Since m < 2m+2 are from B, we have 4m+4 = 2n+2 ∈ fB, 2n+2 ∈ C. Since 2n+2 ∈ fA, this contradicts C ∩ fA = ∅.

case 2. n ∈ gC. Let n = 2m+1, m ∈ C, m ∈ B ∪ gB.

Suppose m ∈ B. Then 2m+2 ∈ fB, 2m+2 ∈ C, 2m+2 ∈ B. Since m < 2m+2 are from B, we have 4m+4 = 2n+2 ∈ fB, 2n+2 ∈ C. Since 2n+2 ∈ fA, this contradicts C ∩ fA = ∅.

Suppose m ∈ gB. Let m = 2r+1, r ∈ B. Then 2r+2 ∈ fB, 2r+2 ∈ C, 2r+2 ∈ B. Since r < 2r+2 are from B, we have 8r+8 = 4m+4 = 2n+2 ∈ fB, 2n+2 ∈ C. Since 2n+2 ∈ fA, this contradicts C ∩ fA = ∅.

QED

part 6. C ∪. fA ⊆ B ∪. gC.

6,1′. C ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,2′. C ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,3′. C ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,4′. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,5′. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6,6′. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

LEMMA 3.12.23. 6,1′ - 6,3′ have ¬NON.

Proof: By Lemma 3.12.2. QED

The following pertains to 6,5′.

LEMMA 3.12.24. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gC has ¬NON.

Proof: Let f,g ∈ ELG be defined as follows. For all n < m, let f(n,n) = 2n+2, f(n,m) = f(m,n)= 2m+1, g(n) = 4n+5. Let C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gC, where A,B,C are nonempty.

Let n ∈ A. Then n ∈ C ∪ gC, 2n+2 ∈ fA.

case 1. n ∈ C. Then n ∈ B ∪ gC, n ∉ gC, n ∈ B, 2n+2 ∈ fB, 2n+2 ∈ C. This contradicts C ∩ fA = ∅.

case 2. n ∈ gC. Let n = 4r+5, r ∈ C. Then r ∈ B ∪ gC, r ∈ B, 2r+2 ∈ fB, 2r+2 ∈ C, 2r+2 ∈ B ∪ gC, 2r+2 ∈ B. Since r <

2r+2 are from B, we have 4r+5 = n ∈ fB. Since n ∈ A, this contradicts A ∩ fB = ∅.

QED

The following pertains to 6,4'.

LEMMA 3.12.25. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gB has ¬NON.

Proof: Let f,g ∈ ELG be defined as in the proof of Lemma 3.12.16, whose definitions we repeat here. For all n < m, let f(2n,2n,2n) = f(2n+1,2n+1,2n+1) = 4n, f(n,m,m) = 2m, f(n,m,n) = 4m, f(m,n,n) = 8m, g(2n) = g(2n+1) = 4n+1. For all other triples a,b,c, let f(a,b,c) = 2max(a,b,c). Let C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gB, where A,B,C are nonempty.

Let n = min(A). Then n ∈ C ∪ gB.

case 1. n ∈ C. Then n ∈ B ∪ gC.

case 1a. n ∈ C, n ∈ B. Clearly f(n,n,n) ∈ fB, f(n,n,n) ∈ C. Since f(n,n,n) ∈ fA, this contradicts C ∩ fA = ∅.

case 1b. n ∈ C, n ∈ gC. Let n' = min(C ∩ gC). Let n' = g(m), m ∈ C. Then m ∈ B ∪ gC. If m ∈ B then n' ∈ gB, which contradicts C ∩ gB = ∅. Hence m ∈ gC. So m ∈ C ∩ gC and m < n', which is a contradiction.

case 2. n ∈ gB. Let n = g(m), m ∈ B. Then f(m,m,m) ∈ fB, f(m,m,m) ∈ C, f(m,m,m) ∈ B. So f(f(m,m,m),f(m,m,m),f(m,m,m)) ∈ fB, f(f(m,m,m),f(m,m,m),f(m,m,m)) ∈ C.

By the proof of Lemma 3.12.16,

f(f(m,m,m),f(m,m,m),f(m,m,m)) = f(g(m),g(m),g(m)) = f(n,n,n) ∈ fA.

This contradicts C ∩ fA = ∅. QED

The following pertains to 6,6'.

LEMMA 3.12.26. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gA has ¬NON.

Proof: Let f,g ∈ ELG be defined as follows. For all n < m, let f(n,n,n) = 2n, f(n,n,m) = 2n+2, f(n,m,n) = 4m+2, f(n,m,m) = 4m-3, g(n) = 4n+1. At all other triples define f(a,b,c) = |a,b,c|+2. Let C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gA, where A,B,C are nonempty.

Let n = min(A). We claim that n ∉ B. To see this, let n ∈ B. Then 2n ∈ fB, 2n ∉ gA, 2n ∈ C, 2n ∈ fA. This contradicts C ∩ fA = ∅.

Since n ∈ C ∪ gA, we have n ∈ C, n ∈ B ∪ gC, n ∈ gC.

Let n = 4m+1, m ∈ C. Suppose m ∉ gC. Then m ∈ B, 2m ∈ fB, 2m ∈ C, 2m ∈ B. Since m,2m ∈ B, we have 4m+1 ∈ fB, 4m+1 ∈ A, contradicting A ∩ fB = ∅. Hence m ∈ gC.

Let p be greatest such that the sequence $n,g^{-1}(n),...,g^{-p}(n)$ is defined and remains in C. Then p ≥ 2.

Note that $g^{-p}(n)$ ∈ C\gC, $g^{-p}(n)$ ∈ B ∪ gC, $g^{-p}(n)$ ∈ B. We have gone down by g^{-1}. We can go back up from $g^{-p}(n)$ ∈ B as follows.

First we apply the function 2n followed by the function 2n+2 (available through f(n,n,n) and f(n,n,m)). After applying the function 2n, we obtain an even element of fB, which must lie in C,B. After applying the function 2n+2, we arrive at $g^{-p+1}(n)+1$, which is also even and lies in C,B. Then we apply the function 4n+2 successively until arriving at $g^{-1}(n)+1$, which lies in C,B. Finally apply the function 4n-3, which arrives at n, and lies in fB. Since n ∈ A, we have contradicted A ∩ fB = ∅. QED

3.13. ACBC.

Recall the reduced table for AC from section 3.10.

REDUCED AC

1. A ∪. fA ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
2. A ∪. fA ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
4. B ∪. fA ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
5. B ∪. fA ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
6. B ∪. fA ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.

Recall the reduced table for BC from section 3.8.

REDUCED BC

1′. B ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
2′. B ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
3′. B ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
4′. A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
5′. A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
6′. A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.

We can take advantage of symmetry through interchanging A with B as follows. Clearly (i,j′) and (j,i′) are equivalent, by interchanging A and B. So we can require that i ≤ j. Thus we have the following 21 ordered pairs to consider.

We must determine the status of all attributes INF, AL, ALF, FIN, NON, for each pair.

1,1′. A ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
1,2′. A ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
1,3′. A ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
1,4′. A ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
1,5′. A ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
1,6′. A ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
2,2′. A ∪. fA ⊆ C ∪. gC, B ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
2,3′. A ∪. fA ⊆ C ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. FIN. NON.
2,4′. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gB. ¬INF. AL. ¬ALF. FIN. NON.
2,5′. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
2,6′. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. FIN. NON.
3,3′. A ∪. fA ⊆ C ∪. gB, B ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
3,4′. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
3,5′. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gC. ***<u>INF</u>***. AL. ALF. FIN. NON.

3,6′. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
4,4′. B ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
4,5′. B ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
4,6′. B ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
5,5′. B ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
5,6′. B ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. FIN. NON.
6,6′. B ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.

It is among the 36 ordered pairs treated here that we finally find an ordered pair that cannot be handled within RCA_0. This is pair 3,5′. In fact, here only the attribute INF requires more than RCA_0. Note that we have notated this above in large underlined bold italics. The pair 3,5′ with INF is called the Principal Exotic Case, and is treated as Proposition A in Chapters 4 and 5. The equivalence class of the Principal Exotic Case has 12 elements, and consists of the Exotic Cases.

The following pertains to 1,1′ - 6,6′.

LEMMA 3.13.1. X ∪. fY ⊆ C ∪. gZ, W ∪. fU ⊆ C ∪. gV has FIN, provided X,Y,W,U ∈ {A,B}.

Proof: Let f,g ∈ EVSD. Let A = B = {n}, where n is sufficiently large.

case 1. f(n,...,n) = g(n,...,n). Let C = {n}.

case 2. f(n,...,n) ≠ g(n,...,n). Let C = {n,f(n,...,n)}.

In case 1, A = B = C, fA = gA, and A ∩ fA = ∅. The two inclusions are identities.

In case 2, X = Y = W = U = A = B. So it suffices to verify that A ∪. fA ⊆ C ∪. gZ and A ∪. fA ⊆ C ∪. gV. Note that A ∩ fA = C ∩ gA = C ∩ gB = C ∩ gC = ∅. Also A ∪ fA ⊆ C. QED

LEMMA 3.13.2. 1,1′, 1,3′, 1,4′, 1,6′, 3,3′, 3,4′, 3,6′, 4,4′, 4,6′, 6,6′ have INF, ALF, even for EVSD.

Proof: By the AC table, A ∪. fA ⊆ C ∪. gA has INF, ALF. Replace B by A in the cited ordered pairs. QED

LEMMA 3.13.3. 2,2′, 2,5′, 5,5′ have INF, ALF.

Proof: By the AC table, A ∪. fA ⊆ C ∪. gC has INF, ALF. Replace B by A in the cited ordered pairs. QED

The following pertains to 1,2′, 1,5′.

LEMMA 3.13.4. A ∪. fA ⊆ C ∪. gA, C ∩ gC = ∅ has ¬AL.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n, f(m,n) = 4m, f(n,m) = 4m+1, g(n) = 2n+1. Let A ∪. fA ⊆ C ∪. gA. C ∩ gC = ∅, where A,B,C have at least 2 elements. Let n < m be from A.

Clearly 2m ∈ fA, 4m+1 ∈ fA, 2m ∈ C, 2m ∉ A, 4m+1 ∉ gA, 4m+1 ∈ C, 4m+1 ∈ gC. This contradicts C ∩ gC = ∅. QED

The following pertains to 2,3′, 2,6′.

LEMMA 3.13.5. A ∪. fA ⊆ C ∪. gC, fB ⊆ C ∪. gA has ¬AL.

Proof: Define f,g ∈ ELG as follows. For all n < m < r, let f(n,n,n) = 2n, f(n,n,m) = 4m, f(n,m,n) = 4m+1, f(m,n,n) = 8m+1, g(n) = 2n+1. Let A ∪. fA ⊆ C ∪. gC, fB ⊆ C ∪. gA, where A,B,C have at least two elements. Let n < m be from B.

Note that 2m ∈ fB, 2m ∈ C, 4m+1 ∈ gC, 4m+1 ∉ C, 4m+1 ∈ fB, 4m+1 ∈ gA, 2m ∈ A, 4m ∈ fB, 4m ∈ C, 8m+1 ∈ gC, 8m+1 ∉ C, 8m+1 ∈ fB, 8m+1 ∈ gA, 4m ∈ A, 4m ∈ fA. This contradicts A ∩ fA = ∅. QED

The following pertains to 2,4′.

LEMMA 3.13.6. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gB has ¬INF, ¬ALF.

Proof: Let f be as given by Lemma 3.2.1. Let f′ ∈ ELG be given by f′(a,b,c,d) = f(a,b,c) if c = d; 2f(a,b,c)+1 if c > d; 2|a,b,c,d|+2 if c < d. Let g ∈ ELG be given by g(n) = 2n+1. Let A ∪. f′A ⊆ C ∪. gC. A ∪. f′B ⊆ C ∪. gB, where A,B,C have at least two elements. Let B′ = B\{min(B)}. Note that fB ⊆ f'B.

Let n ∈ fB′ ∩ 2N. Then n ∈ f′B ∩ 2N, n ∈ C, 2n+1 ∈ gC, 2n+1 ∉ C.

We claim that 2n+1 ∈ f′B. To see this, write n = f(a,b,c), a,b,c ∈ B'. Then 2n+1 = f'(a,b,c,min(B)) ∈ f'B.

Hence 2n+1 ∈ gB, n ∈ B, n ∈ B′. Thus we have shown that fB′ ∩ 2N ⊆ B′. Hence by Lemma 3.2.1, fB′ is cofinite. Since fB ⊆ f′B, f'B is also cofinite. Therefore B is infinite and A is finite. The former establishes ¬ALF, and the latter establishes ¬INF. QED

The following pertains to 2,4′.

LEMMA 3.13.7. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gB has AL.

Proof: Let f,g ∈ ELG and p > 0. Let A = [n,n+p], where n is sufficiently large. By Lemma 3.3.3, let C be unique such that C ⊆ [n,∞) ⊆ C ∪. gC. Let B = C.

Clearly A ∩ fA = C ∩ gC = A ∩ fB = C ∩ gB = ∅.

Since A ∪ fA ∪ fB ⊆ [n,∞), we have A ∪ fA ⊆ C ∪ gC, A ∪ fB ⊆ C ∪ gB = C ∪ gC. Obviously C = B is infinite. QED

The following pertains to 4,5′.

LEMMA 3.13.8. B ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gC has ¬AL.

Proof: Let f be as given by Lemma 3.2.1. Let f′ ∈ ELG be defined by f′(a,b,c,d) = f(a,b,c) if c = d; 4f(a,b,c)+3 if c > d; 2|a,b,c,d|+2 if c < d. Let g be as given by Lemma 3.6.1. Let B ∪. f′A ⊆ C ∪. gA, A ∪. f′B ⊆ C ∪. gC, where A,B,C have at least two elements. Let A′ = A\{min(A)}.

Let n ∈ fA′ ∩ 2N. Then n ∈ f′A ∩ 2N, n ∈ C, 4n+3 ∈ gC, 4n+3 ∉ C, 4n+3 ∈ f′A, 4n+3 ∈ gA, n ∈ A, n ∈ A'. By Lemma 3.2.1, fA' is cofinite. Since fA ⊆ f'A, we see that f'A is cofinite.

We have established that C ∪ gA is cofinite and C ∩ gC = ∅. Hence by Lemma 3.6.1, C ⊆ A. Since fB contains an even element 2r, we have 2r ∈ C,A,f′B. This contradicts A ∩ f′B = ∅. QED

The following pertains to 5,6′.

LEMMA 3.13.9. B ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gA has ¬AL.

Proof: Define f,g ∈ ELG as follows. For all n < m, let f(n,n) = 2n, f(n,m) = f(m,n) = 4m+1, g(n) = 2n+1. Let B ∪. fA ⊆ C ∪. gC. A ∪. fB ⊆ C ∪. gA, where A,B,C have at least two elements. Let n < m be from B.

Clearly 2m ∈ fB, 2m ∈ C, 4m+1 ∈ gC, 4m+1 ∉ C, 4m+1 ∈ fB, 4m+1 ∈ gA, 2m ∈ A. This contradicts A ∩ fB = ∅. QED

The following pertains to 3,5'.

LEMMA 3.13.10. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gC has ALF.

Proof: Let f,g ∈ ELG and p > 0. Let A = [n,n+p], where n is sufficiently large. By Lemma 3.3.3, let S be unique such that S ⊆ [n,∞) ⊆ S ∪. gS. Let B = S ∩ [n,max(fA)]. Let C = S ∩ [n,max(fB)].

Clearly A ∩ fA = A ∩ fB = A ∩ fS = A ∩ gS = ∅. Hence A ⊆ S. Therefore A ⊆ B, A ⊆ C, B ⊆ C. Hence A,B,C are finite and have at least p elements.

Since B,C ⊆ S, we have S ∩ gS = ∅, C ∩ gC ⊆ S ∩ gS = ∅, and C ∩ gB ⊆ S ∩ gS = ∅.

We claim fA ⊆ C ∪ gB. To see this, let m ∈ fA. Then m ∈ S ∪ gS.

case 1. m ∈ S. Then m ∈ B, m ∈ C.

case 2. m ∈ gS. Write m = g(s_1,...,s_q), s_1,...,s_q ∈ S ⊆ [n,∞). Then s_1,...,s_q < m ≤ max(fA). Hence s_1,...,s_q ∈ B. So m ∈ gB.

We claim fB ⊆ C ∪ gC. To see this, let m ∈ fB. Then m ∈ S ∪ gS.

case 3. m ∈ S. Then m ∈ C.

case 4. m ∈ gS. Write m = g(t_1,...,t_q), t_1,...,t_q ∈ S ⊆ [n,∞). Then t_1,...,t_q < m ≤ max(fB). Hence t_1,...,t_q ∈ C. So m ∈ gC. QED

The Proposition asserting that 3,5' has INF is the subject of the next two Chapters of this book. This is the

Principal Exotic Case. It is not provable in ZFC (assuming ZFC is consistent). See Definitions 3.1.1 and 3.1.2.

3.14. Annotated Table of Representatives.

SINGLE CLAUSES

1. A ∪. fA ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2. A ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3. B ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
4. B ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
5. B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
6. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
7. A ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
8. A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
9. B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
10. B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
11. B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
12. C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
13. C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
14. C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.

AAAA

1. A ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2. A ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3. A ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4. A ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. A ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
7. B ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
8. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
9. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
10. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
11. A ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

12. A ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
13. A ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
14. A ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
15. A ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
16. A ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
17. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
18. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
19. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
20. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

AAAB

1. A ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2. A ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3. A ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4. A ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. A ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. A ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
7. A ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
8. A ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
9. A ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
10. A ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
11. A ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
12. A ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
13. A ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

14. A ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
15. A ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
16. A ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
17. A ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
18. A ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
19. A ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
20. A ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
21. A ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
22. A ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
23. A ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
24. A ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
25. A ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
26. A ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
27. A ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
28. B ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
29. B ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
30. B ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
31. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
32. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
33. B ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
34. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
35. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
36. B ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
37. B ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

38. B ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
39. B ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
40. B ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
41. B ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
42. B ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
43. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
44. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
45. B ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
46. B ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
47. B ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
48. B ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
49. B ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
50. B ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
51. B ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
52. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
53. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
54. B ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
55. C ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
56. C ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
57. C ∪. fA ⊆ A ∪. gA, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
58. C ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
59. C ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
60. C ∪. fA ⊆ A ∪. gA, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
61. C ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.

62. C ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
63. C ∪. fA ⊆ A ∪. gA, C ∪. fA ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
64. C ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
65. C ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
66. C ∪. fA ⊆ A ∪. gB, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
67. C ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
68. C ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
69. C ∪. fA ⊆ A ∪. gB, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
70. C ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
71. C ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
72. C ∪. fA ⊆ A ∪. gB, C ∪. fA ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
73. C ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
74. C ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
75. C ∪. fA ⊆ A ∪. gC, A ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
76. C ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
77. C ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
78. C ∪. fA ⊆ A ∪. gC, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
79. C ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gA. ¬INF, AL, ¬ALF, ¬FIN. NON.
80. C ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gB. ¬INF, AL, ¬ALF, ¬FIN. NON.
81. C ∪. fA ⊆ A ∪. gC, C ∪. fA ⊆ B ∪. gC. ¬INF, AL, ¬ALF, ¬FIN. NON.

AABA

1. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

3. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
7. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
8. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
9. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
10. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
11. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
12. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
13. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
14. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
15. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
16. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
17. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
18. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
19. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
20. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
21. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
22. A ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
23. A ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
24. A ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
25. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
26. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

27. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
28. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
29. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
30. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
31. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
32. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.
33. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
34. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
35. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.
36. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.
37. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
38. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
39. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
40. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
41. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
42. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
43. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
44. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
45. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
46. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
47. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
48. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
49. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
50. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.

51. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
52. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
53. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
54. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
55. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
56. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
57. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
58. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
59. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.
60. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.
61. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
62. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
63. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.
64. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
65. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
66. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
67. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
68. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
69. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
70. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
71. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
72. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
73. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
74. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

75. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
76. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
77. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
78. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
79. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
80. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
81. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.

AABB

1. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
3. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
7. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
8. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
9. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
10. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
11. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
12. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
13. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
14. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
15. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

16. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
17. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
18. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
19. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
20. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
21. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
22. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
23. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
24. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
25. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
26. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
27. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
28. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
29. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
30. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
31. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
32. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
33. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
34. A ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
35. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
36. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
37. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
38. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
39. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

40. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
41. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
42. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
43. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
44. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ B ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
45. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ B ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.

AABC

1. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3. A ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. A ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
7. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
8. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
9. A ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
10. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
11. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
12. A ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
13. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
14. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
15. A ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
16. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

17. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
18. A ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
19. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
20. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
21. A ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
22. A ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
23. A ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
24. A ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
25. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
26. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
27. A ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
28. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
29. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
30. B ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
31. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
32. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
33. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
34. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
35. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
36. B ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
37. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
38. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
39. B ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
40. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.

41. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
42. B ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
43. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
44. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
45. B ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
46. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
47. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
48. B ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
49. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
50. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
51. B ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
52. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
53. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
54. B ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
55. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
56. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
57. C ∪. fA ⊆ A ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
58. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
59. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
60. C ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
61. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
62. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
63. C ∪. fA ⊆ A ∪. gA, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
64. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

65. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
66. C ∪. fA ⊆ A ∪. gB, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
67. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
68. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
69. C ∪. fA ⊆ A ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
70. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
71. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
72. C ∪. fA ⊆ A ∪. gB, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
73. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
74. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
75. C ∪. fA ⊆ A ∪. gC, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
76. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
77. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
78. C ∪. fA ⊆ A ∪. gC, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
79. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
80. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
81. C ∪. fA ⊆ A ∪. gC, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

ABAB

1. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
2. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

6. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
7. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
8. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
9. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
10. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
11. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
12. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
13. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. FIN, NON.
14. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gB. INF. AL. ALF. FIN. NON.
15. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
16. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
17. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
18. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
19. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.
20. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
21. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
22. B ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
23. B ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
24. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
25. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
26. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
27. B ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
28. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
29. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

30. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
31. B ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
32. B ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
33. B ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
34. C ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. AL. ¬ALF. FIN. NON.
35. C ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gC. INF. AL. ALF. FIN. NON.
36. C ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ B ∪. gC. ¬INF. ¬AL. ¬ALF. FIN, NON.

ABAC

1. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gA. INF, AL, ALF, FIN, NON.
2. B ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gB. INF, AL, ALF, FIN, NON.
4. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gA. INF, AL, ALF, FIN, NON.
7. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
8. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
9. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
10. B ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
11. B ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
12. B ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
13. B ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
14. B ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
15. B ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

16. B ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
17. B ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
18. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
19. B ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
20. B ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
21. B ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
22. B ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
23. C ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
24. C ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FiN. ¬NON.
25. C ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FiN. ¬NON.
26. A ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
27. A ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
28. A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
29. A ∪. fA ⊆ B ∪. gB, B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
30. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
31. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
32. A ∪. fA ⊆ B ∪. gB, C ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
33. A ∪. fA ⊆ B ∪. gC, A ∪. fA ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
34. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
35. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
36. A ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
37. A ∪. fA ⊆ B ∪. gC, C ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
38. B ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
39. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

40. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
41. B ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
42. B ∪. fA ⊆ B ∪. gC, B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
43. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FiN. ¬NON.
44. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FiN. ¬NON.
45. C ∪. fA ⊆ B ∪. gA, B ∪. fA ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FiN. ¬NON.

ABBA

1. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
2. C ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
3. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
4. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
7. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
8. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
9. B ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
10. B ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
11. B ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
12. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
13. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
14. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
15. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
16. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

17. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
18. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
19. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
20. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
21. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
22. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gC. ¬INF. AL. ¬ALF. ¬FIN. NON.
23. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
24. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
25. C ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
26. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
27. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
28. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
29. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
30. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
31. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
32. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
33. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
34. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
35. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
36. B ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
37. B ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
38. B ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
39. B ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
40. B ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

41. B ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
42. B ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ A ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
43. B ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
44. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ A ∪. gB. ¬INF. AL. ¬ALF. ¬FIN. NON.
45. C ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.

ABBC

1. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
2. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
3. A ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
4. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. A ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
7. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
8. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
9. A ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
10. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
11. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
12. A ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
13. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. FIN. NON.
14. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
15. A ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
16. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
17. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

18. A ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
19. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
20. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
21. A ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
22. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. FIN. NON.
23. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
24. A ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
25. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
26. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
27. A ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
28. B ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
29. B ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
30. B ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
31. B ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
32. B ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
33. B ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
34. B ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
35. B ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
36. B ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
37. B ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
38. B ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
39. B ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
40. B ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
41. B ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

42. B ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
43. B ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
44. B ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
45. B ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
46. B ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
47. B ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
48. B ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
49. B ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
50. B ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
51. B ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
52. B ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
53. B ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
54. B ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
55. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
56. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
57. C ∪. fA ⊆ B ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
58. C ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
59. C ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
60. C ∪. fA ⊆ B ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
61. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
62. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
63. C ∪. fA ⊆ B ∪. gA, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
64. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
65. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

66. C ∪. fA ⊆ B ∪. gB, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
67. C ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
68. C ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
69. C ∪. fA ⊆ B ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
70. C ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
71. C ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
72. C ∪. fA ⊆ B ∪. gB, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
73. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
74. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
75. C ∪. fA ⊆ B ∪. gC, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
76. C ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
77. C ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
78. C ∪. fA ⊆ B ∪. gC, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
79. C ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
80. C ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
81. C ∪. fA ⊆ B ∪. gC, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

ACBC

1. A ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
2. C ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3. A ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
4. A ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
5. A ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
6. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. FIN. NON.

7. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
8. A ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
9. A ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
10. C ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
11. C ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
12. C ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
13. C ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
14. C ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
15. C ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
16. C ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
17. A ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
18. A ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
19. A ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
20. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
21. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
22. A ∪. fA ⊆ C ∪. gB, B ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
23. B ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
24. B ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gB. INF. AL. ALF. FIN. NON.
25. B ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gA. INF. AL. ALF. FIN. NON.
26. A ∪. fA ⊆ C ∪. gA, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
27. A ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
28. A ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gC. ***INF***. AL. ALF. FIN. NON.
29. A ∪. fA ⊆ C ∪. gB, B ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.

30. A ∪. fA ⊆ C ∪. gB, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
31. A ∪. fA ⊆ C ∪. gB, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
32. A ∪. fA ⊆ C ∪. gB, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
33. A ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gB. ¬INF. AL. ¬ALF. FIN. NON.
34. A ∪. fA ⊆ C ∪. gC, B ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
35. A ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
36. B ∪. fA ⊆ C ∪. gA, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
37. B ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
38. B ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
39. B ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
40. B ∪. fA ⊆ C ∪. gB, A ∪. fB ⊆ C ∪. gC. ¬INF. ¬AL. ¬ALF. FIN. NON.
41. B ∪. fA ⊆ C ∪. gB, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
42. B ∪. fA ⊆ C ∪. gC, A ∪. fB ⊆ C ∪. gC. INF. AL. ALF. FIN. NON.
43. B ∪. fA ⊆ C ∪. gC, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
44. C ∪. fA ⊆ C ∪. gA, C ∪. fB ⊆ C ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
45. C ∪. fA ⊆ C ∪. gB, C ∪. fB ⊆ C ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

3.15. Some Observations.

Recall the Template and Extended Template introduced at the beginning of this Chapter before section 3.1. We now justify the claims TEMP 1,2, and ETEMP, which were also presented there.

TEMP 1. Every one of the 6561 assertions in the Template is either provable or refutable in SMAH+. There exist 12 assertions in the Template, provably equivalent in RCA_0, such that the remaining 6549 assertions are each provable or refutable in RCA_0. Furthermore, these 12 are provably equivalent to the 1-consistency of SMAH over ACA’ (Theorem 5.9.11).

To see how the Annotated Table of section 3.14 justifies Temp 1, recall how it was constructed. The ordered pairs of clauses in the Annotated Table comprise a list of representatives from each equivalence class of the ordered pairs of clauses under the equivalence relation used in section 3.1.

The entries that correspond to the assertions in the Template are the entries in the Annotated Table with INF or ¬INF. The 12 Exotic Cases (see Definition 3.1.2) correspond to the single entry in 28 under ACBC, INF. Every entry in the Annotated Table, with the sole exception of this single entry for INF, was justified in sections 3.3 - 3.13. All of the arguments in sections 3.3 - 3.13 were conducted within RCA_0.

This single entry for INF, corresponding to the 12 Exotic Cases, is equivalent to

PROPOSITION A. For all f,g ∈ ELG there exist A,B,C ∈ INF such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

Proposition A is the Principal Exotic Case - a particular one of the 12 Exotic Cases that we have chosen on aesthetic grounds. According to Theorem 5.9.11, Proposition A, and hence all 12 Exotic Cases, are provably equivalent to 1-Con(SMAH) over ACA'.

TEMP 2. Every one of the 6561 assertions in the Template, other than the 12 Exotic Cases, are provably equivalent, in RCA_0, to the result of replacing ELG by any of ELG ∩ SD, SD, EVSD. All 12 Exotic Cases are refutable in RCA_0 if ELG is replaced by SD or EVSD (Theorem 6.3.5).

The first claim of TEMP 2 is justified by the way we derived each entry in the Annotated Table other than 28 under ACBC, INF. Namely, when deriving INF, we always assumed f,g ∈ EVSD rather than f,g ∈ ELG. Note that ELG, ELG ∩ SD, SD ⊆ EVSD. Also see Theorem 3.1.1.

TEMP 3. The Template behaves very differently for MF. For example, the Template is true (even provable in RCA_0) with A ∪. fA ⊆ B ∪. gB, A ∪. fA ⊆ B ∪. gB, yet false (even refutable in RCA_0) with ELG replaced by MF.

To see this, use a constant function $f:N \to N$, and the identity function $g:N \to N$. Then the left side is infinite, whereas the right side is empty.

ETEMP. Every assertion in the Extended Template, other than the 12 Exotic Cases with INF, is provable or refutable in RCA_0.

Clearly ETEMP follows from the observation that all of the derivations in this Chapter are conducted in RCA_0. Consideration of the Exotic Cases with INF is postponed to Chapters 4-6.

BRT TRANSFER. Let X,Y,V,W,P,R,S,T be among the letters A,B,C. The following are equivalent.
i. for all $f,g \in ELG$ and $n \geq 1$, there exist finite $A,B,C \subseteq N$, each with at least n elements, such that $X \cup. fY \subseteq V \cup. gW$, $P \cup. fR \subseteq S \cup. gT$.
ii. for all $f,g \in ELG$, there exist infinite $A,B,C \subseteq N$, such that $X \cup. fY \subseteq V \cup. gW$, $P \cup. fR \subseteq S \cup. gT$.

THEOREM 3.15.1. BRT transfer is provably equivalent to 1-Con(SMAH) over ACA'. Furthermore, BRT forward transfer (i $\to$ ii) is provably equivalent to 1-Con(SMAH) over ACA'. BRT backward transfer (ii $\to$ i) is provable in RCA_0. Furthermore, BRT forward transfer for the Exotic Cases is provably equivalent to 1-Con(SMAH) over ACA', and BRT forward transfer for ordered pairs other than the Exotic Cases, is provable in RCA_0.

Proof: As entered in the Annotated Table, $A \cup. fA \subseteq C \cup. gB$, $A \cup. fB \subseteq C \cup. gC$ has ALF, provably in RCA_0. Hence BRT forward transfer, for the Exotic Cases, is provably equivalent, in RCA_0, to $A \cup. fC \subseteq C \cup. gB$, $A \cup. fB \subseteq C \cup. gC$ has INF. I.e., BRT forward transfer, for the Exotic Cases, is provably equivalent, in RCA_0, to Proposition A. Hence BRT Forward transfer, for the Exotic Cases, is provably equivalent, in ACA', to 1-Con(SMAH).

BRT forward transfer, for other than the Exotic Cases, and BRT backward transfer, are seen, by inspection of the Annotated Table, to be true. Since the Annotated Table was constructed within RCA0, the remainder of Theorem 3.15.1 has been established. QED

There are some other notable facts concerning the Annotated Table. Recall the obvious implications between our five attributes:

ALF → AL → NON.
ALF → FIN → NON.
INF → AL → NON.

We have also discussed the observed Transfer Property:

INF → ALF → INF.

Are there any other observations to be made from the annotated tables?

Here is the compilation of all attribute lists that are compatible with the above implications:

INF. AL. ALF. FIN. NON.
¬INF. AL. ¬ALF. FIN. NON.
¬INF. AL. ¬ALF. ¬FIN. NON.
¬INF. ¬AL. ¬ALF. FIN. NON.
¬INF. ¬AL. ¬ALF. ¬FIN. NON.
¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.

All of these are realized from the annotated table:

SINGLE CLAUSES

1. A ∪. fA ⊆ A ∪. gA. ¬INF. ¬AL. ¬ALF. ¬FIN. ¬NON.
3. B ∪. fA ⊆ A ∪. gA. ¬INF. AL. ¬ALF. ¬FIN. NON.
6. A ∪. fA ⊆ B ∪. gA. INF. AL. ALF. FIN. NON.

ABAB

1. A ∪. fA ⊆ B ∪. gA, A ∪. fA ⊆ B ∪. gB. ¬INF. ¬AL. ¬ALF. FIN. NON.
34. C ∪. fA ⊆ B ∪. gA, C ∪. fA ⊆ B ∪. gB. ¬INF. AL. ¬ALF. FIN. NON.

AABA

32. B ∪. fA ⊆ A ∪. gA, B ∪. fB ⊆ A ∪. gB. ¬INF. ¬AL. ¬ALF. ¬FIN. NON.

So there are no more implications between the attributes, in the context of this Chapter.

CHAPTER 4.

PROOF OF PRINCIPAL EXOTIC CASE

4.1. Strongly Mahlo Cardinals of Finite Order.

The large cardinal properties used in this book are the strongly Mahlo cardinals of order n, where $n \in \omega$. These are defined inductively as follows.

DEFINITION 4.1.1. The strongly 0-Mahlo cardinals are the strongly inaccessible cardinals (uncountable regular strong limit cardinals).
The strongly n+1-Mahlo cardinals are the infinite cardinals all of whose closed unbounded subsets contain a strongly n-Mahlo cardinal.

It is easy to prove by induction on n that for all $n < m < \omega$, every strongly m-Mahlo cardinal is a strongly n-Mahlo cardinal.

There is a closely related notion: n-Mahlo cardinal.

DEFINITION 4.1.2. The 0-Mahlo cardinals are the weakly inaccessible cardinals (uncountable regular limit cardinals). The n+1-Mahlo cardinals are the infinite cardinals all of whose closed unbounded subsets contain an n-Mahlo cardinal.

Again, for all $n < m < \omega$, every m-Mahlo cardinal is an n-Mahlo cardinal.

NOTE: Sometimes (strongly) n-Mahlo cardinals are called (strongly) Mahlo cardinals of order $\leq$ n. Also, sometimes what we call n-Mahlo cardinals are called weakly n-Mahlo cardinals.

The well known relationship between n-Mahlo cardinals and strongly n-Mahlo cardinals is given as follows.

THEOREM 4.1.1. The following is provable in ZFC. Let $n < \omega$. A cardinal is strongly n-Mahlo if and only if it is n-Mahlo and strongly inaccessible. Under the GCH, a cardinal is strongly n-Mahlo if and only if it is n-Mahlo.

Proof: For the first claim, note that it is obvious for n = 0. Assume that every strongly inaccessible n-Mahlo cardinal is strongly n-Mahlo. Let κ be a strongly inaccessible n+1-Mahlo cardinal. Let $A \subseteq \kappa$ be closed and unbounded. Since κ is strongly inaccessible, the set $B \subseteq \kappa$ consisting of the strong limit cardinals in A is closed and unbounded. Let $\lambda \in B$ be an n-Mahlo cardinal. As previously remarked, λ is an inaccessible cardinal. Since λ is a strong limit cardinal, λ is a strongly inaccessible cardinal. By the induction hypothesis, λ is a strongly n-Mahlo cardinal.

We have thus shown that every closed unbounded $A \subseteq \kappa$ contains a strongly n-Mahlo element. Hence κ is strongly n+1-Mahlo.

For the final claim, assume the GCH. By an obvious induction, every strongly n-Mahlo cardinal is an n-Mahlo cardinal. For the converse, let κ be an n-Mahlo cardinal. As previously remarked, κ is a weakly inaccessible cardinal. Hence κ is a strongly inaccessible cardinal (by GCH). By the first claim, κ is a strongly n-Mahlo cardinal. QED

We now develop the essential combinatorics of strongly Mahlo cardinals of finite order used in this Chapter.

DEFINITION 4.1.3. Let $[A]^n$ be the set of all n element subsets of A. Sometimes we write $x \in [A]^n$ in the form $\{x_1,...,x_n\}_<$ to indicate that the xi are strictly increasing. Let A be a set of ordinals. We say that $f:[A]^n \rightarrow On$ is regressive if and only if for all $x \in [A\backslash\{0\}]^n$, $f(x) < \min(x)$.

DEFINITION 4.1.4. We say that E is min homogenous for $f:[A]^n \rightarrow On$ if and only if $E \subseteq A$ and for all $x,y \in [E]^n$, $\min(x) = \min(y) \rightarrow f(x) = f(y)$.

LEMMA 4.1.2. Let $n \geq 0$, κ a strongly n-Mahlo cardinal, $A \subseteq \kappa$ unbounded, and $f:[A]^{n+2} \rightarrow \kappa$ be regressive. For all $\alpha < \kappa$, there exists $E \subseteq A$ of order type α which is min homogenous for f.

Proof: This result originally appeared in [Sc74], in somewhat sharper form, using different notation. We present the proof in [HKS87], p. 147, using Erdös-Rado trees.

DEFINITION 4.1.5. Let A be a set of ordinals with at least two elements. An A-tree is an irreflexive transitive relation T with field A such that

i. α T $\beta \rightarrow \alpha < \beta$.
ii. $\{\beta: \beta$ T $\alpha\}$ is linearly (and hence well) ordered by T.

DEFINITION 4.1.6. Let $m \geq 2$, A be a nonempty set of ordinals, and $f:[A]^m \rightarrow$ On be regressive. The Erdos-Rado tree ERT(f) is the unique A-tree T with field A such that for all $\alpha,\beta \in A$, α T β if and only if

i. $\alpha < \beta$.
ii. For all $\gamma_1,\ldots,\gamma_{m-1}$ T α with $\gamma_1 < \ldots < \gamma_{m-1}$, $f(\{\gamma_1,\ldots,\gamma_{m-1},\alpha\}) = f(\{\gamma_1,\ldots,\gamma_{m-1},\beta\})$.

To see that there is such a unique T, build ERT(f,α), $\alpha \in$ A, by transfinite recursion on $\alpha \in A$. Here ERT(f,α) is ERT(f) restricted to $A \cap \alpha$. The details are left to the reader.

DEFINITION 4.1.7. For $\alpha \in A$, the height of α in ERT(f) is the order type of $\{\beta: \beta$ ERT(f) $\alpha\}$. We say that $\alpha,\beta \in A$ are siblings in ERT(f) if and only if they are distinct, and have the same strict predecessors in ERT(f). For ordinals γ, let ERT(f)[$<\gamma$] be the restriction of ERT(f) to the elements of A (vertices) of height $< \gamma$.

We now assume that $f:[A]^{n+2} \rightarrow$ On is regressive and sup(A) is a strongly inaccessible cardinal κ. Observe that for all $\alpha \in A$, the number of siblings of α in ERT(f) is at most the number of functions from α^{n+1} into α, which is at most $2^{|\alpha|}+\omega$. Next observe that by transfinite induction on $\alpha < \kappa$, ERT(f)[$<\alpha$] has $< \kappa$ vertices. Hence for all $\alpha < \kappa$, ERT(f) has a vertex of height α. By the construction of ERT(f), every vertex has height $< \kappa$.

Now observe that if n = 0 then the set of strict predecessors of every element of ERT(f) is min homogeneous for f. This establishes the Lemma for the basis case n = 0.

Suppose that the Lemma holds for a fixed $n \geq 0$. Let κ be a strongly n+1-Mahlo cardinal, $A \subseteq \kappa$ be unbounded, $\alpha < \kappa$, and

$f:[A]^{n+3} \to \kappa$ be regressive. We use the Erdös-Rado tree ERT(f).

Since κ is strongly inaccessible, $C = \{\lambda < \kappa$: λ is a limit ordinal $> \alpha$ and ERT(f)[$<\lambda$] is an $A \cap \lambda$-tree and $A \cap \lambda$ is unbounded in $\lambda\}$ is a closed and unbounded subset of κ. Since κ is a strongly n+1-Mahlo cardinal, fix $\lambda < \kappa$ to be a strongly n-Mahlo cardinal $> \alpha$ such that ERT(f)[$<\lambda$] is an $A \cap \lambda$-tree and $A \cap \lambda$ is unbounded in λ.

Let v be a vertex of ERT(f) of height λ. Let B = {w: w ERT(f) v}. Then B is an unbounded subset of λ.

B naturally gives rise to a regressive function $f^*:[B]^{n+2} \to \lambda$ by taking $f^*(x) = f(x \cup \{\gamma\})$, where $\gamma \in B$, $\gamma > \max(x)$. Note that this definition is independent of the choice of γ.

By the induction hypothesis, let $E \subseteq B$ be min homogenous for f*, E of order type α. Then $E \subseteq B \subseteq A$ is min homogenous for f. QED

DEFINITION 4.1.8. For all ordinals α, let α^+ be the least infinite cardinal $> \alpha$. Let $f:[A]^n \to \kappa$. We say that f is next regressive if and only if every $f(x_1,\ldots,x_n) < \min(x_1,\ldots,x_n)^+$.

LEMMA 4.1.3. Let $n \geq 0$, κ a strongly n-Mahlo cardinal, and $A \subseteq \kappa$ be unbounded. For all $i \in \omega$, let $f_i:[A]^{n+2} \to \kappa$ be next regressive. For all $\alpha < \kappa$, there exists $E \subseteq A$ of order type α such that for all $i \in \omega$, E is min homogenous for f_i.

Proof: This is by a straightforward modification of the proof of Lemma 4.1.2. Modify the definition of the Erdös-Rado tree ERT(f) accordingly, and derive a similar upper bound on the number of siblings of a vertex in ERT(f). QED

Let $n \geq 1$ and $f:[A]^n \to \kappa$. We wish to define n+1 kinds of infinite sets $E \subseteq A$ for f.

DEFINITION 4.1.9. We say that E is of kind 0 for f if and only if f is constant on $[E]^n$, where the constant value is less than the strict sup of E.

DEFINITION 4.1.10. We say that E is of kind $1 \leq j \leq n$ for f if and only if the following holds. For all $\{x_1,\ldots,x_n\}_<$, $\{x_1,\ldots,x_j,y_{j+1},\ldots,y_n\}_< \subseteq E$, $f(x_1,\ldots,x_n) = f(x_1,\ldots,x_j,y_{j+1},\ldots,y_n)$ is greater than every element of $E < x_j$ and smaller than every element of $E > x_j$.

For $E \subseteq On$ and $\delta < ot(E)$, we write $E[\delta]$ for the δ-th element of E.

We fix $H:On^{<\omega} \to On\backslash\{0\}$, where H is one-one and for all $x \in On^{<\omega}$, $H(x) < \max(x)^+$.

LEMMA 4.1.4. Let $n \geq 1$, κ a strongly n-Mahlo cardinal, and $A \subseteq \kappa$ unbounded. For all $i \in \omega$, let $f_i:[A]^{n+1} \to \kappa$. For all $\alpha < \kappa$, there exists $E \subseteq A$ of order type α such that the following holds. For all $i \in \omega$, there exists $0 \leq j \leq n+1$ such that E is of kind j for f_i.

Proof: Let n,κ,A,f_i,α be as given. We can assume that $\alpha > \omega$, $A \subseteq \kappa\backslash\omega$, and there is an infinite cardinal strictly between any two elements of A. We can also assume that for all $\alpha_1,\ldots,\alpha_{n+1} < \beta$ from A, $f_i(\alpha_1,\ldots,\alpha_{n+1}) < \beta$.

For all $i \in \omega$, define $g_{i,0}\{u,x_1,\ldots,x_{n+1}\}_< = 1+f_i\{x_1,\ldots,x_{n+1}\}$ if $f_i\{x_1,\ldots,x_{n+1}\} \leq u$; 0 otherwise.

For $1 \leq j \leq n+1$, define $g_{i,j}\{u,x_{j+1},\ldots,x_{n+2}\}_<$ as follows. Let $z_1 < \ldots < z_j \leq u$ be such that $f_i\{z_1,\ldots,z_j,x_{j+1}\ldots,x_{n+1}\} \neq f_i\{z_1,\ldots,z_j,x_{j+2},\ldots,x_{n+2}\}$ and $f_i\{z_1,\ldots,z_j,x_{j+1}\ldots,x_{n+1}\} \leq u$. Set $g_{i,j}\{u,x_{j+1},\ldots,x_{n+2}\} = H(z_1,\ldots,z_j,f_i\{z_1,\ldots,z_j,x_{j+1},\ldots,x_{n+1}\})$. If such z's do not exist, then set $g_{i,j}\{u,x_{j+1},\ldots,x_{n+2}\} = 0$.

Note that each $g_{i,j}$ is next regressive. By Lemma 4.1.3, let $E' \subseteq A\backslash\omega$ be min homogeneous for all $g_{i,j}$, where E' has cardinality $\geq \mathfrak{I}_\omega(\alpha+\omega)$ = the first strong limit cardinal $> \alpha+\omega$.

We can partition the tuples from E' of length $\leq 2n+2$ in a strategic way, with 2^ω pieces, and apply the Erdös-Rado theorem to obtain $E \subseteq E'$ with order type α, with the following three properties. Write E[1],E[2],... for the first ω elements of E. Let $i \in \omega$.

1) For all $\{x_1,\ldots,x_{n+1}\}_< \in [E]^{n+1}$, $f_i\{x_1,\ldots,x_{n+1}\} \in E \to f_i\{x_1,\ldots,x_{n+1}\} \in \{x_1,\ldots,x_{n+1}\}$.

2) Suppose $f_i\{E[2],\ldots,E[n+2]\} = f_i\{E[n+3],\ldots,E[2n+3]\}$. Then f_i is constant on $[E]^{n+1}$.

3) Suppose $1 \leq j \leq n+1$, and $f_i\{E[2],E[4],\ldots,E[2n+2]\} = f_i\{E[2],E[4],\ldots,E[2j],E[2j+4],E[2j+6],\ldots,E[2n+4]\} \in (E[2j-1],E[2j+1])$. Then E is of kind j for f_i.

For the remainder of the proof, we fix $i \in \omega$. The first case that applies is the operative case.

case 1. $f_i\{E[2],E[4],...,E[2n+2]\} \leq E[1]$. Then $g_{i,0}\{E[1],E[2],E[4],...,E[2n+2]\} = 1+f_i\{E[2],E[4],...,E[2n+2]\} > 0$. Since E is min homogenous for $g_{i,0}$ we see that for all $x,y \in [E]^{n+1}$ such that $\min(x),\min(y) \geq E[2]$, we have $g_{i,0}(\{E[1]\} \cup x) = g_{i,0}(\{E[1]\} \cup y) = 1+f_i(x) = 1+f_i(y)$. In particular, $f_i\{E[2],...,E[n+2]\} = f_i\{E[n+3],...,E[2n+3]\}$. By 2), f_i is constant on $[E]^{n+1}$. Hence E is of kind 0 for f_i.

case 2. Let j be the greatest element of [1,n+1] such that $f_i\{E[2],E[4],...,E[2n+2]\} \in (E[2j-1],E[2j+1])$. Note that $g_{i,j}\{E[2j+1],E[2j+2],E[2j+4],...,E[2n+4]\} = g_{i,j}\{E[2j+1],E[2j+4],E[2j+6],...,E[2n+6]\}$.

Suppose the main clause in the definition of $g_{i,j}\{E[2j+1],E[2j+2],E[2j+4],...,E[2n+4]\}$ holds, with $z_1 < ... < z_j \leq E[2j+1]$. Since H is nonzero, the main clause in the definition of $g_{i,j}\{E[2j+1],E[2j+4],E[2j+6],...,E[2n+6]\}$ holds with, say, $w_1 < ... < w_j \leq E[2j+1]$. Hence $H(z_1,...,z_j,f_i\{z_1,...,z_j,E[2j+2],E[2j+4],...,E[2n+2]\}) = H(w_1,...,w_j,f_i\{w_1,...,w_j,E[2j+4],E[2j+6],...,E[2n+4]\})$. Therefore $z_1,...,z_j = w_1,...,w_j$, respectively, and $f_i\{z_1,...,z_j,E[2j+2],E[2j+4],...,E[2n+2]\} = f_i\{w_1,...,w_j,E[2j+4],E[2j+6],...,E[2n+4]\}$. This contradicts the choice of $z_1,...,z_j$.

Hence the main clause in the definition of $g_{i,j}\{E[2j+1],E[2j+2],E[2j+4],...,E[2n+4]\}$ fails. In particular, it fails with $z_1,...,z_j = E[2],E[4],...,E[2j]$, respectively. Then $f_i\{E[2],E[4],...,E[2n+2]\} = f_i\{E[2],E[4],...,E[2j],E[2j+4],E[2j+6],...,E[2n+4]\}$. By 3), E is of kind j for f_i.

case 3. Otherwise. Then $f_i\{E[2],E[4],...,E[2n+2]\} \in \{E[1],E[3],...,E[2n+1]\}$, or $f_i\{E[2],E[4],...,E[2n+2]\} \geq E[2n+3]$. The first disjunct is impossible by 1), and the second disjunct is impossible by the assumption on A.

We have thus shown that for some $j \in [0,n+1]$, E is of kind j for f_i. Since i is arbitrarily chosen from ω, we are done.

QED

DEFINITION 4.1.11. Let $f:[A]^n \to \kappa$ and $E \subseteq A$. We define fE to be the range of f on $[E]^n$.

LEMMA 4.1.5. Let $n,m \geq 1$, κ a strongly n-Mahlo cardinal, and $A \subseteq \kappa$ unbounded. For all $i \in \omega$, let $f_i:[A]^{n+1} \to \kappa$, and let $g_i:[A]^m \to \omega$. There exists $E \subseteq \kappa$ of order type ω such that
i) for all $i \in \omega$, f_i is either constant on $[E]^{n+1}$, with constant value < sup(E), or f_iE is of order type ω with the same sup as E;
ii) for all $i \in \omega$, g_i is constant on $[E]^m$.

Proof: Let n,m,κ,A,f_i,g_i be as given. Apply Lemma 4.1.4 to obtain $E' \subseteq \kappa$ of order type $\Im_\omega(\omega)$ such that the following holds. For all $i \in \omega$ there exists $0 \leq j \leq n+1$ such that E is of kind j for f_i. By the Erdös-Rado theorem, let $E \subseteq E'$ be of order type ω, where for all $i \in \omega$, g_i is constant on $[E]^m$. Write $E = \{E[1],E[2],...\}_<$.

Let $i \in \omega$ and E be of kind j for f_i. If $j = 0$ then f_i is constant on $[E]^{n+1}$, where the constant value is less than sup(E).

Now suppose $1 \leq j \leq n+1$. For all $\{x_1,...,x_{n+1}\}_<$, $\{x_1,...,x_j,y_{j+1},...,y_{n+1}\}_< \subseteq E$, $f_i\{x_1,...,x_{n+1}\} = f\{x_1,...,x_j,y_{j+1},...,y_{n+1}\}$ is greater than every element of E $< x_j$ and smaller than every element of E $> x_j$. Since we can set x_j to vary among E[j],E[j+1],..., we see that f_iE has the same sup as E. In particular, f_iE is infinite.

Also, for any particular E[p], the values $f_i\{x_1,...,x_{n+1}\} < E[p]$, $x_1 < ... < x_{n+1} \in A$, can arise only if $x_j \leq E[p+1]$. Since the arguments $x_{j+1},...,x_{n+1}$ don't matter (kind j for f_i), there are at most finitely many such values.

We have shown that f_iE has at most finitely many elements not exceeding any given element of E. Therefore f_iE has order type $\leq \omega$. Since f_iE is infinite, the order type of f_iE is ω. QED

We now switch over to ordered tuples. Let $f:A^n \to \kappa$ and $E \subseteq A$. Here we also define fE to be the range of f on E^n.

LEMMA 4.1.6. Let $n,m \geq 1$, κ a strongly n-Mahlo cardinal, and $A \subseteq \kappa$ unbounded. For all $i \in \omega$, let $f_i:A^{n+1} \to \kappa$, and let $g_i:A^m \to \omega$. There exists $E \subseteq \kappa$ of order type ω such that
i) for all $i \geq 1$, f_iE is either a finite subset of sup(E), or of order type ω with the same sup as E;
ii) for all $i \in \omega$, g_iE is finite.

Proof: Let n,m,κ,A,f_i,g_i be as given. Each f_i gives rise to finitely many corresponding $f_{i,\sigma}$, where σ ranges over the order types of n+1 tuples. Also each g_i gives rise to finitely many corresponding $g_{i,\sigma}$, where σ ranges over the order types of m tuples. Any f_iE is the union of the $f_{i,\sigma}E$, and any g_iE is the union of the $g_{i,\sigma}E$. Choose E according to Lemma 4.1.5. Then E will be as required. QED

DEFINITION 4.1.12. Let $SMAH^+$ be ZFC + $(\forall n < \omega)(\exists\kappa)$($\kappa$ is a strongly n-Mahlo cardinal). Let SMAH be ZFC + $\{(\exists\kappa)$(κ is a strongly n-Mahlo cardinal)$\}_{n<\omega}$.

DEFINITION 4.1.13. Let MAH^+ be ZFC + $(\forall n < \omega)(\exists\kappa)$($\kappa$ is an n-Mahlo cardinal). Let MAH be ZFC + $\{(\exists\kappa)$(κ is an n-Mahlo cardinal)$\}_{n < \omega}$.

We will use the following (known) relationship between $SMAH^+$, MAH^+, SMAH, and MAH.

DEFINITION 4.1.14. The system EFA = exponential function arithmetic is defined to be the system $I\Sigma_0(exp)$; see [HP93].

THEOREM 4.1.7. $SMAH^+$ and MAH^+ prove the same Π^1_2 sentences. SMAH and MAH prove the same Π^1_2 sentences. SMAH is 1-consistent if and only if MAH is 1-consistent. SMAH is consistent if and only if MAH is consistent. These results are provable in EFA.

Proof: We first prove the following well known theorem in ZFC.

1) Let $n \geq 0$. Every n-Mahlo cardinal is an n-Mahlo cardinal in the sense of L.

The basis case asserts that every weakly inaccessible cardinal is a weakly inaccessible cardinal in L. This is particularly well known and easy to check.

Fix $n \geq 0$ and assume that every n-Mahlo cardinal is an n-Mahlo cardinal in L. Let κ be an n+1-Mahlo cardinal. Let $A \subseteq \kappa$, $A \in L$, where A is closed and unbounded in κ (in the sense of L). Let $\lambda \in A$ be an n-Mahlo cardinal. Then $\lambda \in A$ is an n-Mahlo cardinal in L. Hence κ is an n+1-Mahlo cardinal in L.

If T is a sentence or set of sentences in the language of set theory, then we write $T^{(L)}$ for the relativization of T to Godel's constructible universe L.

For the first claim, let $SMAH^+$ prove φ, where φ is Π^1_2. By Lemma 4.1.1, MAH^+ + GCH proves φ. Hence ZFC + $MAH^{+(L)}$ + $GCH^{(L)}$ proves $\varphi^{(L)}$ by, e.g., [Je78], section 12. Therefore ZFC + $MAH^{+(L)}$ proves $\varphi^{(L)}$ by, e.g., [Je78], section 13. By the Shoenfield absoluteness theorem (see, e.g., [Je78], p. 530), ZFC + $MAH^{+(L)}$ proves φ. By 1), MAH^+ proves φ.

For the second claim, we repeat the proof of the first claim for any specific level of strong Mahloness.

For the third claim, assume 1-Con(MAH). Let φ be a Σ^0_1 sentence provable in SMAH. By the second claim, φ is provable in MAH. Hence φ is true.

For the final claim, assume Con(MAH). Then MAH does not prove 1 = 0. By the second claim, SMAH does not prove 1 = 0. Hence Con(SMAH). QED

Theorem 4.1.7 tells us that for the purposes of this book, $SMAH^+$ and SMAH are equivalent to MAH^+ and MAH. We will always use $SMAH^+$ and SMAH.

4.2. Proof using Strongly Mahlo Cardinals.

Recall Proposition A from the beginning of section 3.1. This is the Principal Exotic Case.

PROPOSITION A. For all f,g $\in$ ELG there exist A,B,C $\in$ INF such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

Recall the definitions of N, ELG, INF, $\cup.$, fA, in Definitions 1.1.1, 1.1.2, 1.1.10, 1.3.1, and 2.1.

In this section, we prove Proposition A in $SMAH^+$. It is convenient to prove a stronger statement.

PROPOSITION B. Let f,g $\in$ ELG and $n \geq 1$. There exist infinite sets $A_1 \subseteq \ldots \subseteq A_n \subseteq N$ such that
i) for all $1 \leq i < n$, $fA_i \subseteq A_{i+1} \cup. gA_{i+1}$;
ii) $A_1 \cap fA_n = \emptyset$.

LEMMA 4.2.1. The following is provable in RCA_0. Proposition B implies Proposition A. In fact, Proposition B for n = 3 implies Proposition A.

Proof: Let $f,g \in ELG$. By Proposition B for n = 3, let $A \subseteq B \subseteq C \subseteq N$ be infinite sets, where $fA \subseteq B \cup. gB$, $fB \subseteq C \cup. gC$, and $A \cap fC = \emptyset$.

Note that C,gC are disjoint. Hence C,gB are disjoint. In addition, A,fA are disjoint, and A,fB are disjoint. We now verify the inclusion relations.

Let $x \in A \cup fA$. If $x \in fA$ then $x \in B \cup gB \subseteq C \cup gB$. If $x \in A$ then $x \in C \subseteq C \cup gB$.

Let $x \in A \cup fB$. If $x \in fB$ then $x \in C \cup gC$. If $x \in A$ then $x \in C \subseteq C \cup gC$. QED

Recall the definition of $f \in ELG$ from section 2.1: there are rational constants $c,d > 1$ such that for all but finitely many $x \in dom(f)$, $c|x| \leq f(x) \leq d|x|$.

We wish to put this in more explicit form. Assume f,c,d are as above. Let t be a positive integer so large that $1 + 1/t < c,d < t$, and for all $x \in dom(f)$, $|x| > t \rightarrow c|x| \leq f(x) \leq d|x|$. Let b be an integer greater than t and $\max\{f(x): |x| \leq t\}$. Then for all $x \in dom(f)$,

$$|x| > t \rightarrow f(x) \leq b|x|.$$
$$|x| \leq t \rightarrow f(x) \leq b.$$
$$|x| \leq b \rightarrow f(x) \leq b^2.$$

Hence $f \in ELG$ if and only if there exists a positive integer b such that for all $x \in dom(f)$,

$$|x| > b \rightarrow (1 + 1/b)|x| \leq f(x) \leq b|x|.$$
$$|x| \leq b \rightarrow f(x) \leq b^2.$$

We now fix $f,g \in ELG$, where f is p-ary and g is q-ary. According to the above, we also fix a positive integer b such that for all $x \in N^p$ and $y \in N^q$,

i. if $|x|,|y| > b$ then

$$(1 + 1/b)|x| \leq f(x) \leq b|x|$$
$$(1 + 1/b)|y| \leq g(y) \leq b|y|.$$

ii. if $|x|,|y| \leq b$ then $f(x),g(y) \leq b^2$.

We also fix $n \geq 1$ and a strongly p^{n-1}-Mahlo cardinal κ.

We begin with the discrete linearly ordered semigroup with extra structure, M = (N,<,0,1,+,f,g).

The plan will be to first construct a structure of the form M* = (N*,<*,0*,1*,+*,f*,g*,c_0*,...), where the c*'s are indexed by N. This structure is non well founded and generated by the constants 0*,1*, and the c*'s. The indiscernibility of the c*'s will be with regard to atomic formulas only. The first nonstandard point in M* will be c_0*.

While it is obvious that we cannot embed M* back into M, we use the fact that we can embed any partial substructure of M* that is "boundedly generated" back into M.

Of course, M* is not well founded, but we prove the well foundedness of the crucial irreflexive transitive relation

$$sx <^* y$$

on N*, where s > 1 is any fixed rational number.

Using the atomic indiscernibility of the c*'s, we canonically extend M* to a structure M** = (N**,<**,0**,1**,+**,f**,g**,c_0**,...,c_α**,...), $\alpha < \kappa$. Many properties of M* are preserved when passing to M**. The appropriate embedding property asserts that any partial substructure of M** boundedly generated by 0**,1**, and a set of c**'s of order type ω is embeddable back into M* and M.

Recall that the proof of the Complementation Theorem (Theorem 1.3.1) requires that the function is strictly dominating with respect to a well founded relation <. Here we verify that g** is strictly dominating on the nonstandard part of M** with respect to the above crucial irreflexive transitive relation. This enables us to apply the Complementation Theorem 1.3.1) to g** on the nonstandard part of M** in order to obtain a unique set $W \subseteq$ nst(M**) such that for all $x \in$ nst(M**), $x \in W \leftrightarrow x \notin$ g**W.

We then build a Skolem hull construction of length ω consisting entirely of elements of W. The construction starts with the set of all c**'s. Witnesses are thrown in from W that verify that values of f** at elements thrown in at previous stages do not lie in W (provided they in fact do not lie in W). Only the first n stages of the construction will be used.

Every element of the n-th stage of the Skolem hull construction has a suitable name involving e = e(p,q) of the c**'s.

At this crucial point, we then apply Lemma 4.1.6 to the large cardinal κ, with arity n = e, in order to obtain a suitably indiscernible set S of the c**'s of order type ω, with respect to this naming system.

We can redo the length n Skolem hull construction starting with S. This is just a restriction of the original Skolem hull construction that started with all of the c**'s.

Because of the indiscernibility, we generate a subset of N** whose elements are given by terms of bounded length in c**'s of order type ω. This forms a suitable partial substructure of M**, so that it is embeddable back into M. The image of this embedding on the n stages of the Skolem hull construction will comprise the $A_1 \subseteq \ldots \subseteq A_n$ satisfying the conclusion of Proposition B. This completes the description of the plan for the proof.

We now begin the detailed proof of Proposition B. We begin with the structure M = (N,<,0,1,+,f,g) in the language L consisting of the binary relation <, constants 0,1, the binary function +, the p-ary function f, the q-ary function g, and equality.

DEFINITION 4.2.1. Let $V(L) = \{v_i: i \geq 0\}$ be the set of variables of L. Let TM(L) be the set of terms of L, and AF(L) be the set of atomic formulas of L. For $t \in TM(L)$, we define lth(t) as the total number of occurrences of functions, constants, and variables, in t. For $\varphi \in AF(L)$, we also define lth(φ) as the total number of occurrences of functions, constants, and variables, in φ.

DEFINITION 4.2.2. An M-assignment is a partial function $h:V(L) \rightarrow N$. We write Val(M,t,h) for the value of the term t in M at the assignment h. This is defined if and only if h is adequate for t; i.e., h is defined at all variables in t.

DEFINITION 4.2.3. We write Sat(M,φ,h) for atomic formulas φ. This is true if and only if h is adequate for φ and M satisfies φ at the assignment h. Here h is adequate for φ if and only if h is defined at (at least) all variables in φ.

DEFINITION 4.2.4. We say that a partial function $h:V(L) \to N$ is increasing if and only if for all $i < j$, if $v_i,v_j \in dom(h)$ then $h(v_i) < h(v_j)$.

LEMMA 4.2.2. There exist infinite sets $N \supseteq E_0 \supseteq E_1 \supseteq \ldots$ indexed by N, such that for all $i \geq 0$, $\varphi \in AF(L)$, $lth(\varphi) \leq i$, and increasing partial functions $h_1,h_2:V(L) \to N$ adequate for φ with $rng(h_1),rng(h_2) \subseteq E_i$, we have $Sat(M,\varphi,h_1) \leftrightarrow Sat(M,\varphi,h_2)$.

Proof: A straightforward application of the usual infinite Ramsey theorem, repeated infinitely many times. Each E_{i+1} is obtained by Ramsey's theorem applied to a coloring of i-tuples from E_i. QED

DEFINITION 4.2.5. We fix the E's in Lemma 4.2.2. In an abuse of notation, we write $Sat(M,\varphi,E)$ if and only if $\varphi \in AF(L)$ and for all increasing h adequate for φ with range included in E_i, we have $Sat(M,\varphi,h)$, where $lth(\varphi) = i$.

Note that by Lemma 4.2.2, this is equivalent to: $\varphi \in AF(L)$ and for some increasing h adequate for φ with range included in E_i, we have $Sat(M,\varphi,h)$, where $lth(\varphi) = i$. We can also use any i with $i \geq lth(\varphi)$ and get an equivalent definition of $Sat(M,\varphi,E)$.

DEFINITION 4.2.6. We now introduce constants c_i, $i \in N$. Let C be the set of all such constants. Let L* be L expanded by these constants. Structures for L* will be written $M^* = (N^*,<^*,0^*,1^*,+^*,f^*,g^*,c_0^*,\ldots)$. Here each c_i is interpreted by c_i^*.

DEFINITION 4.2.7. We let CT(L*) be the set of closed terms of L*, and AS(L*) be the set of atomic sentences of L*. We define lth(t), $lth(\varphi)$ for $t \in AS(L^*)$, $\varphi \in AS(L^*)$.

DEFINITION 4.2.8. For $\varphi \in AS(L^*)$, $t \in CT(L^*)$, we write $Sat(M^*,\varphi)$ and $Val(M^*,t)$ for the usual model theoretic notions.

For each $t \in CT(L^*)$, let $X(t) \in TM(L)$ be the result of replacing all occurrences of 'c' by 'v'. For each $\varphi \in AS(L^*)$, let $X(\varphi) \in AF(L)$ be the result of replacing all occurrences of 'c' by 'v'.

DEFINITION 4.2.9. Let T = {$\varphi \in$ AS(L*): Sat(M,X(φ),E)}.

LEMMA 4.2.3. T is consistent. For all s,t $\in$ CT(L*), exactly one of s = t, s < t, t < s belongs to T. For all n $\in$ N, $c_n < c_{n+1} \in$ T.

Proof: It suffices to show that every finite subset of T is consistent. Let $\varphi_1,\ldots,\varphi_k \in$ T. Then each Sat(M,X(φ_i),E) holds. Let j = max(lth(φ_1),...,lth(φ_k)) and h:V(L) $\to E_j$ be the increasing bijection. Then each Sat(M,X(φ_i),h) holds. Let M' be the expansion of M that interprets each constant c_n as h(v_n). Then each Sat(M',φ_i) holds.

For the second claim, let s,t $\in$ CT(L*). Let i = lth(s = t) and h:V(L) $\to E_i$ be the increasing bijection. Then Sat(M,X(s = t),h) or Sat(M,X(s < t),h) or Sat(M,X(t < s),h). Therefore at least one of s = t, s < t, t < s lies in T. Since at most one of Sat(M,X(s = t),E), Sat(M,X(s < t),E), Sat(M,X(t < s),E) can hold, clearly at most one of s = t, s < t, t < s lies in T.

For the third claim, let n $\in$ N, and let h:V(L) $\to E_2$ be the increasing bijection. Obviously Sat(M,$v_n < v_{n+1}$,h). Hence $c_n < c_{n+1} \in$ T. QED

We now fix M* = (N*,0*,1*,<*,+*,f*,g*,c_0*,...) to be any model of T which is generated from its constants. Such an M* exists by Lemma 4.2.3 and the fact that T consists entirely of atomic sentences. Clearly M* is unique up to isomorphism.

DEFINITION 4.2.10. For d $\in$ N and t $\in$ CT(L*) or t $\in$ TM(L). Define dt to be the term

$$t + t + \ldots + t$$

associated to the left, where there are d t's. If d = 0, then take dt to be 0. Obviously dt $\in$ CT(L*) or dt $\in$ TM(L), respectively.

LEMMA 4.2.4. Let $\varphi \in$ AS(L*). Sat(M*,φ) if and only if $\varphi \in$ T. <* is a linear ordering on N*. For all n,d $\in$ N, $dc_n < c_{n+1}$ $\in$ T.

Proof: Since M* satisfies T, the reverse direction of the first claim is immediate.

Suppose $\varphi \notin T$. First assume φ is of the form $s < t$. By Lemma 4.2.3, $t < s \in T$ or $s = t \in T$. Then Sat(M*,t < s) or Sat(M*,s = t). Therefore Sat(M*,φ) is false. Now assume φ is of the form $s = t$. By Lemma 4.2.3, $s < t \in T$ or $t < s \in T$. Hence Sat(M*,s < t) or Sat(M*,t < s). Therefore Sat(M*,φ) is false.

The second claim follows immediately from the first claim and the second claim of Lemma 4.2.3.

For the third claim, let $i = lth(dc_n < c_{n+1})$. The unique increasing bijection $h:V(L) \to E_i$ has $dh(v_n) < h(v_{n+1})$. Hence Sat(M,$dv_n < v_{n+1}$,h), Sat(M,$dv_n < v_{n+1}$,E), and $X(dc_n < c_{n+1}) = dv_n < v_{n+1}$. Hence $dc_n < c_{n+1} \in T$. QED

DEFINITION 4.2.11. For $r \geq 1$, we write M*[r] for the set of all values in M* of the terms $t \in CT(L^*)$ of length $\leq r$.

DEFINITION 4.2.12. We say that H is an r-embedding from M* into M if and only if

i) H:M*[r(p+q+1)] $\to$ N;
ii) H(0*) = 0, H(1*) = 1;
iii) for all x,y $\in$ M*[r(p+q+1)], x <* y $\leftrightarrow$ H(x) < H(y);
iv) for all x,y $\in$ M*[r], H(x+*y) = H(x)+H(y).
v) for all $x_1,...,x_p \in$ M*[r], $H(f^*(x_1,...,x_p)) = f(H(x_1),...,H(x_p))$;
vi) for all $x_1,...,x_q, \in$ M*[r], $H(g^*(x_1,...,x_q)) = g(H(x_1),...,H(x_q))$.

Note that by the second claim of Lemma 4.2.4, iii) implies that H is one-one.

LEMMA 4.2.5. For all $r \geq 1$, there exists an r-embedding H from M* into M.

Proof: Let $r \geq 1$ and $h:V(L) \to E_{2r(p+q+1)}$ be the unique increasing bijection.

We define H:M*[r(p+q+1)] $\to$ N as follows. Let x = Val(M*,t), where $t \in CT(L^*)$, $lth(t) \leq r(p+q+1)$. Define H(x) = Val(M,X(t),h).

To see that H is well defined, let x = Val(M*,t'), where $t' \in CT(L^*)$, $lth(t') \leq r(p+q+1)$. We must verify that Val(M,X(t),h) = Val(M,X(t'),h). Since $lth(t = t') \leq 2r(p+q+1)$,

$$\mathrm{Val}(M,X(t),h) = \mathrm{Val}(M,X(t'),h) \leftrightarrow$$
$$\mathrm{Sat}(M,X(t = t'),E) \leftrightarrow$$
$$t = t' \in T \leftrightarrow$$
$$\mathrm{Sat}(M^*,t = t') \leftrightarrow$$
$$\mathrm{Val}(M^*,t) = \mathrm{Val}(M^*,t') \leftrightarrow$$
$$x = x.$$

For ii), $H(0^*) = \mathrm{Val}(M,X(0),h) = 0$. $H(1^*) = \mathrm{Val}(M,X(1),h) = 1$. Also, $c_i^* = \mathrm{Val}(M^*,c_i)$, $H(c_i^*) = \mathrm{Val}(M,X(c_i),h) = \mathrm{Val}(M,v_i,h) = h(v_i) \in E_{r(p+q+1)}$.

For iii), we must verify that for $\mathrm{lth}(t),\mathrm{lth}(t') \leq r(p+q+1)$, $\mathrm{Val}(M^*,t) <^* \mathrm{Val}(M^*,t') \leftrightarrow \mathrm{Val}(M,X(t),h) < \mathrm{Val}(M,X(t'),h)$. Using Lemma 4.2.4, the left side is equivalent to $\mathrm{Sat}(M^*,t < t')$, and to $t < t' \in T$. The right side is equivalent to $\mathrm{Sat}(M,X(t < t'),h)$, to $\mathrm{Sat}(M,X(t < t'),E)$, and to $t < t' \in T$, using $\mathrm{lth}(t < t') \leq 2r(p+q+1)$.

For iv), we must verify that for $\mathrm{lth}(t),\mathrm{lth}(t') \leq r$, $H(\mathrm{Val}(M^*,t)+^*\mathrm{Val}(M^*,t')) = H(\mathrm{Val}(M^*,t))+H(\mathrm{Val}(M^*,t'))$. Since $\mathrm{lth}(t+t') \leq 2r \leq r(p+q+1)$, the left side is $H(\mathrm{Val}(M^*,t+t')) = \mathrm{Val}(M,X(t+t'),h)$. The right side is $\mathrm{Val}(M,X(t),h)+\mathrm{Val}(M,X(t'),h)$. Equality is immediate.

For v), we must verify that for $\mathrm{lth}(t_1),\ldots,\mathrm{lth}(t_p) \leq r$, $H(f^*(\mathrm{Val}(M^*,t_1),\ldots,\mathrm{Val}(M^*,t_p)) = f(H(\mathrm{Val}(M^*,t_1)),\ldots,H(\mathrm{Val}(M^*,t_p)))$. Since $\mathrm{lth}(f(t_1,\ldots,t_p)) \leq r(p+q+1)$, the left side is $H(\mathrm{Val}(M^*,f(t_1,\ldots,t_p))) = \mathrm{Val}(M,X(f(t_1,\ldots,t_p)),h)$. The right side is $f(\mathrm{Val}(M,t_1,h),\ldots,\mathrm{Val}(M,t_p,h))$. Equality is immediate.

For vi), see v). QED

DEFINITION 4.2.13. For quantifier free formulas φ in L^*, we define $\mathrm{lth}'(\varphi)$ as the total number of occurrences of functions, constants, and variables. We do not count the occurrences of connectives for lth'.

LEMMA 4.2.6. For all $r \geq 1$, there is an r-embedding from M^* into M with the following properties.
i. each $H(c_i^*) \in E_{2r(p+q+1)}$.
ii if $t \in CT(L^*)$, $\mathrm{lth}(t) \leq r(p+q+1)$, then $H(\mathrm{Val}(M^*,t)) = \mathrm{Val}(M,X(t),h)$.
iii. if $\varphi \in AS(L^*)$, $\mathrm{lth}(\varphi) \leq r(p+q+1)$, then $\mathrm{Sat}(M^*,\varphi) \leftrightarrow \mathrm{Sat}(M,X(\varphi),E)$.
iv. if φ is a quantifier free sentence in L^*, $\mathrm{lth}'(\varphi) \leq r(p+q+1)$, then $\mathrm{Sat}(M^*,\varphi) \leftrightarrow \mathrm{Sat}(M,X(\varphi),E)$.

Proof: Let $H:M^*[r(p+q+1)] \to N$ be an r-embedding of M^* into M, constructed in the proof of Lemma 4.2.5, using the strictly increasing bijection $h:V(L) \to E_{2r(p+q+1)}$. Then each $H(c_i^*) \in E_{2r(p+q+1)}$. Let $t \in CT(L^*)$, $lth(t) \leq r(p+q+1)$. Then $H(Val(M^*,t)) = Val(M,X(t),h)$ by definition. Let $\varphi \in AS(L^*)$, $lth(\varphi) \leq r(p+q+1)$. Then $Sat(M^*,s = t) \leftrightarrow Val(M^*,s) = Val(M^*,t) \leftrightarrow Val(M,X(s),h) = Val(M,X(t),h) \leftrightarrow Sat(M,X(s = t),E)$. We can use < in place of =. Finally, iv follows from iii. QED

LEMMA 4.2.7. Every universal sentence of L that holds in M holds in M*. For any quantifier free sentence of L*, if we replace equal c*'s by equal c*'s in a manner that is order preserving on indices, then the truth value in M* is preserved. The c*'s are strictly increasing and unbounded in N*.

Proof: For the first claim, let $(\forall v_1)\ldots(\forall v_m)(\varphi)$ be a universal sentence of L that holds in M. Suppose it fails in M*. Let $v_1,\ldots,v_m \in N^*$, where $\varphi(v_1,\ldots,v_m)$ fails in M*. Let $t_1,\ldots,t_m \in CT(L^*)$ be such that each $v_i = Val(M^*,t_i)$. Let $lth(\varphi(t_1,\ldots,t_m)) \leq r$.

By Lemmas 4.2.5 and 4.2.6, let $H:M^*[r] \to N$ be an r-embedding of M* into M. By the final claim of Lemma 4.2.6, since not $Sat(M^*,\varphi(t_1,\ldots,t_m))$, we have not $Sat(M,X(\varphi(t_1,\ldots,t_m)),E)$. This contradicts $Sat(M,(\forall v_1)\ldots(\forall v_m)(\varphi))$.

For the second claim, let $\varphi \in AS(L^*)$. Let ψ be obtained from φ by replacing equal c*'s by equal c*'s in an order preserving way. Let $lth(\varphi) \leq r$. By Lemmas 4.2.5 and 4.2.6, let $H:M^*[r] \to N$ be an r-embedding of M* into M. By Lemma 4.2.6,

$$Sat(M^*,\varphi) \leftrightarrow Sat(M,X(\varphi),E).$$
$$Sat(M^*,\psi) \leftrightarrow Sat(M,X(\psi),E).$$

Since $X(\psi)$ is obtained from $X(\varphi)$ by replacing equal v_i's by equal v_i's in an order preserving way, the right sides of the above two equivalences are equivalent. Hence the left sides are also equivalent.

For the third claim, let $i < j$. Let $h:\{i,j\} \to E_2$ be increasing. Since $Sat(M,X(c_i < c_j),h)$, we have $Sat(M,X(c_i < c_j),E)$, and so $c_i < c_j \in T$ and $Sat(M^*,c_i < c_j)$. Hence $c_i^* <^* c_j^*$.

To see that the c^*'s are unbounded in N^*, let $x \in N^*$, and let $t \in CT(L^*)$ be such that $x = Val(M^*,t)$. Let c_i be the largest element of C appearing in t. We claim that $t < c_{i+1}$ lies in T. To see this, let $r = lth(t < c_{i+1})$ and $h:V(L) \to E_r$ be strictly increasing, where $h(v_{i+1}) >^* Val(M,t,h)$. Then $Sat(M,X(t < c_{i+1}),h)$, and so $Sat(M,X(t < c_{i+1}),E)$, and hence $t < c_{i+1} \in T$. Therefore $Val(M^*,t) <^* c_{i+1}^*$. QED

DEFINITION 4.2.14. Let $C' = \{c_\alpha: \alpha < \kappa\}$. C' is the set of transfinite constants. Note that $C \subseteq C'$.

DEFINITION 4.2.15. Let L** be the language L extended by constants c_α, $\alpha < \kappa$. Note that the c_i in L* are already present in L**. The new constants are the c_α, $\omega \leq \alpha < \kappa$.

DEFINITION 4.2.16. Let CT(L**) be the set of all closed terms of L**. Let AS(L**) be the set of all atomic sentences of L**.

DEFINITION 4.2.17. A reduction is a partial function $J:C' \to C$, where for all $\alpha < \beta$ and $i,j < \omega$, if $J(c_\alpha) = c_i$ and $J(c_\beta) = c_j$, then $i < j$. Any reduction J extends to a partial map from CT(L**) into CT(L*), and to a partial map AS(L**) into AS(L*) in the obvious way. Here J is defined at a closed term or atomic sentence of L** if and only if J is defined at every constant appearing in that closed term or atomic sentence.

DEFINITION 4.2.18. For $s,t \in CT(L^{**})$, we define $s \equiv t$ if and only if for all reductions J defined at s,t, $Sat(M^*,J(s = t))$.

LEMMA 4.2.8. Let $s,t \in CT(L^{**})$ and J,J' be reductions defined at $s,t \in CT(L^{**})$. Then $Sat(M^*,J(s = t)) \leftrightarrow Sat(M^*,J'(s = t))$, and $Sat(M^*,J(s < t)) \leftrightarrow Sat(M^*,J'(s < t))$. $\equiv$ is an equivalence relation on CT(L**).

Proof: Let s,t,J,J' be as given. Then $J(s = t)$ and $J'(s = t)$ are the same up to an increasing change in the c's appearing in s, as in the second claim of Lemma 4.2.7. Hence by the second claim of Lemma 4.2.7, $Sat(M^*,J(s = t)) \leftrightarrow Sat(M^*,J'(s = t))$, and $Sat(M^*,J(s < t)) \leftrightarrow Sat(M^*,J'(s < t))$.

For the second claim, obviously $\equiv$ is reflexive and symmetric. Now suppose $s \equiv t$ and $t \equiv r$. Let J be any increasing reduction defined at s,t,r. Then $Sat(M^*,J(s =$

t)) and Sat(M*,J(t = r)). Hence Sat(M*,J(s = r)). Therefore s ≡ r. QED

DEFINITION 4.2.19. We now define the structure M** = (N**,<**,0**,1**,+**,f**,g**,c_0**,...,c_α**,...), $\alpha < \kappa$. Here the interpretation of < is <**, of 0 is 0**, of 1 is 1**, of f is f**, of g is g**, and of each c_α is c_α**.

DEFINITION 4.2.20. We will define M** as a stretching of M*. We define N** to be the set of all equivalence classes of terms in CT(L**) under the ≡ of Lemma 4.2.8. We define 0** = [0]. We define 1** = [1]. We define c_α** = [c_α].

We define [s] <** [t] if and only if Sat(M*,J(s < t)), where J is any (some) reduction defined at s,t.

We define [s] +** [t] = [s + t].

We define f**([t_1],...,[t_p]) = [f(t_1,...,t_p)].

We define g**([t_1],...,[t_q]) = [g(t_1,...,t_q)].

DEFINITION 4.2.21. For t ∈ CT(L**) and d ∈ N, we write dt for t + ... + t, where there are d t's, associated to the left. If d = 0, then use 0.

DEFINITION 4.2.22. For x ∈ N** and d ∈ N, we write dx for x +** ... +** x, where there are d x's associated to the left. If d = 0, then use 0.

LEMMA 4.2.9. These definitions of <**, +**, f**, g** are well defined. For all $\alpha < \beta < \kappa$ and d ∈ N, dc_α** <** c_β**.

Proof: Suppose s ≡ s', t ≡ t'. We freely use Lemma 4.2.8.

Suppose Sat(M*,J(s < t)) holds for all reductions J defined at s,t. Let s ≡ s' and t ≡ t'. Let J' be any reduction defined at s,s',t,t'. Then Sat(M*,J'(s < t)), Sat(M*,J'(s = s')), and Sat(M*,J'(t = t')). Hence Sat(M*,J'(s' < t')). By Lemma 4.2.8, for all reductions J'' defined at s',t', Sat(M*,J''(s < t)).

Suppose s ≡ s', t ≡ t'. We want to show s + t ≡ s' + t'. Obviously for all reductions J defined at s,t,s',t', Sat(M*,J(s + t = s' + t')).

Suppose s_1 ≡ t_1, ..., s_p ≡ t_p. We want to show f(s_1,...,s_p) ≡ f(t_1,...,t_p). Obviously for all reductions J defined at

$s_1,\ldots,s_p,t_1,\ldots,t_p$, $\mathrm{Val}(M^*,J(f(s_1,\ldots,s_p))) = \mathrm{Val}(M^*,J(f(t_1,\ldots,t_p)))$. Hence $f(s_1,\ldots,s_p) \equiv f(t_1,\ldots,t_p)$.

The remaining case with g is handled analogously.

For the second claim, let $\alpha < \beta < \kappa$, $d \in N$, and J be any reduction defined at $dc_\alpha < c_\beta$, where $J(c_\alpha) = c_n$ and $J(c_\beta) = c_m$, $n < m$. Then $dc_\alpha^{**} <^{**} c_\beta^{**} \leftrightarrow [dc_\alpha] <^{**} [c_\beta] \leftrightarrow \mathrm{Sat}(M^*,J(dc_\alpha < c_\beta)) \leftrightarrow \mathrm{Sat}(M^*,dc_n < c_m)$, which holds by Lemma 4.2.4. QED

We write $M^{**} = (N^{**},<^{**},0^{**},1^{**},+^{**},f^{**},g^{**},c_0^{**},\ldots,c_\alpha^{**},\ldots)$, $\alpha < \kappa$.

The terms $t \in CT(L^{**})$ play a dual role. We used them to define N^{**} as the set of all $[t]$, $t \in CT(L^{**})$, under the equivalence relation $\equiv$.

However, now that we have defined the structure M^{**}, we can use the terms $t \in CT(L^{**})$ in the expression $\mathrm{Val}(M^{**},t)$.

LEMMA 4.2.10. For all $t \in CT(L^{**})$, $\mathrm{Val}(M^{**},t) = [t]$. In particular, every element of N^{**} is generated in M^{**} from the set of all constants of M^{**}, which is $C' \cup \{0,1\}$.

Proof: By induction on lth(t). QED

DEFINITION 4.2.23. Let $S \subseteq \kappa$. The S-constants are the c_α, $\alpha \in S$. The S-terms are the $t \in CT(L^{**})$, where all transfinite constants in t are S-constants.

LEMMA 4.2.11. Let $S \subseteq \kappa$. $\{[t]$: t is an S-term$\}$ contains 0^{**}, 1^{**}, the c_α^{**}, $\alpha \in S$, and is closed under $+^{**}$, f^{**}, g^{**}.

Proof: Let $S \subseteq \kappa$. Since $0,1,c_\alpha$, $\alpha \in S$, are S-terms, we can obviously form $[0],[1],[c_\alpha]$, $\alpha \in S$, which are, respectively, $0^{**},1^{**},c_\alpha^{**}$, $\alpha \in S$. Now let s,t be S-terms. Then $[s] +^{**} [t] = [s + t]$, and $s + t$ is an S-term. The f^{**},g^{**} cases are treated in the same way. QED

By Lemma 4.2.11, we let $M^{**}<S>$ be the substructure of M^{**} whose domain is $\{[t]$: t is an S-term$\}$, where only the interpretations of S-constants are retained. By Lemma 4.2.11, $M^{**}<S>$ is a structure.

DEFINITION 4.2.24. Let $N^{**}<S> = \mathrm{dom}(M^{**}<S>) = \{[t]$: t is an S-term$\}$.

LEMMA 4.2.12. Let $S \subseteq \kappa$ have order type ω. Then there is a unique isomorphism from M**<S> onto M* which maps the c_α**, $\alpha \in S$, onto the c_n*, $n \in N$.

Proof: Let J be the unique reduction from the S-constants onto C. Define h:N**<S> → N* as follows. Let t be an S-term. Set h([t]) = Val(M*,J(t)).

To see that h is well defined, let [t] = [t'], where t,t' are S-terms. Since J is a reduction defined at t,t', we have Val(M*,J(t = t')), and so Val(M*,J(t)) = Val(M*,J(t')).

For $\alpha \in S$, h(c_α**) = h([c_α]) = Val(M*,J(c_α)) = J(c_α)*. This establishes that h maps the c_α**, $\alpha \in S$, onto the c_n*, $n \in N$.

We now verify that h is an isomorphism from M**<S> onto M*.

Suppose h([s]) = h([t]), where s,t are S-terms. Then Val(M*,J(s)) = Val(M*,J(t)). Hence Sat(M*,J(s = t)), and so s ≡ t, [s] = [t], using Lemma 4.2.8. Hence h is one-one.

Let x ∈ N*, and write x = Val(M*,t), t ∈ CT(L*). By the construction of J, let t' be the unique S-term such that J(t') = t. Then h([t']) = Val(M*,J(t')) = Val(M*,t) = x. Hence h is onto N*.

Let s,t be S-terms. Then [s] <** [t] ↔ Val(M*,J(s)) <* Val(M*,J(t)) ↔ h([s]) <* h([t]).

h([s] +** [t]) = h([s + t]) = Val(M*,J(s + t)) =
Val(M*,J(s) + J(t)) = Val(M*,J(s)) +* Val(M*,J(t))
= h([s]) +* h([t]).

h(f**([t_1],...,[t_p])) = h([f(t_1,...,t_p)]) =
Val(M*,J(f(t_1,...,t_p))) = Val(M*,f(J(t_1),...,J(t_p))) =
f*(Val(M*,J(t_1)),...,Val(M*,J(t_p))) =
f*(h([t_1]),...,h([t_p])).

The g** case is handled analogously.

Finally,

h(0**) = h[0] = Val(M*,J(0)) = 0.
h(1**) = h[1] = Val(M*,J(1)) = 1.

The uniqueness of h follows from the fact that the 0**, 1** and c_α**, $\alpha \in S$, generate N**<S> in M**<S>, and the 0*, 1* and c_n*, n ∈ N, generate N* in M*. QED

DEFINITION 4.2.25. For $S \subseteq \kappa$ and $r \geq 1$, we write M**[S,r] = {Val(M**,t): t is an S-term of length ≤ r}.

DEFINITION 4.2.26. We say that H is an S,r-embedding from M** into M if and only if

i) H:M**[S,r(p+q+1)] → N;
ii) H(0**) = 0, H(1**) = 1;
iii) for all x,y ∈ M**[S,r(p+q+1)], x <** y ↔ H(x) < H(y);
iv) for all x,y ∈ M**[S,r], H(x+*y) = H(x)+H(y).
v) for all $x_1,...,x_p$ ∈ M**[S,r], H(f**($x_1,...,x_p$)) = f(H(x_1),...,H(x_p));
vi) for all $x_1,...,x_q$, ∈ M**[S,r], H(g**($x_1,...,x_q$)) = g(H(x_1),...,H(x_q)).

LEMMA 4.2.13. Let $S \subseteq \kappa$ be of order type ω and $r \geq 1$. There is an S,r-embedding from M** into M. Every universal sentence of L that holds in M holds in M**. For any atomic sentence of L**, if we replace equal transfinite constants by equal transfinite constants in a manner that is order preserving on indices, then the truth value in M** is preserved. The c_α**, $\alpha \in S$, are unbounded in M**[S,r].

Proof: By Lemma 4.2.12, let h be the unique isomorphism h from M**<S> onto M* which maps the c_α**, $\alpha \in S$, onto the c_n*, n ∈ N. By Lemma 4.2.5, there is an r-embedding from M* into M. By composing these two mappings, we obtain the desired S,r-embedding from M** into M. The remaining claims follow from Lemma 4.2.7 by the isomorphism h. QED

We refer to the second claim of Lemma 4.2.13 as universal sentence preservation (from M to M**). We refer to the third claim of Lemma 4.2.13 as atomic indiscernibility.

DEFINITION 4.2.27. For m ∈ N, we write m^ for the term 1+...+1 with m 1's, where 0^ is 0. We say that x ∈ N** is standard if and only if it is the value in M** of some m^, m ≥ 0. We say that x ∈ N** is nonstandard if and only if x is not standard. We write st(M**) for the standard elements of N**, and nst(M**) for the nonstandard elements of N**.

LEMMA 4.2.14. Let x ∈ nst(M**) and m ∈ N. Then x >** m^. c_0** ∈ nst(M**).

Proof: Let $m < \omega$. Then $(\forall x)(x \leq m \rightarrow (x = 0\hat{} \vee \ldots \vee x = m\hat{}))$ holds in M. By universal sentence preservation, it holds in M**. Let x be nonstandard in M**. Then $x \leq^{**} m\hat{}$ is impossible by the above, and hence $x >^{**} m\hat{}$.

Suppose c_0^{**} is standard, and let $c_0^{**} = m\hat{}$. By atomic indiscernibility in M**, for all $n \in N$, $c_n^{**} = m\hat{}$. This is impossible, since $\alpha < \beta \rightarrow c_\alpha^{**} < c_\beta^{**}$. QED

Obviously, (n/m)x generally makes no sense in M**, where $n,m \in N$, $m \neq 0$. We have no division operation in M**, and certainly there is no 1/2 (there is no 1/2 in M). However, we can make perfectly good sense, in M**, of equations and inequalities

$$(n/m)x = (n'/m')x$$
$$(n/m)x <^{**} (n'/m')x$$
$$(n/m)x \leq^{**} (n'/m')x$$

by interpreting them as

$$nm'x = n'mx$$
$$nm'x <^{**} n'mx$$
$$nm'x \leq^{**} n'mx.$$

Universal sentence preservation can be used to support natural reasoning in M** involving such equations and inequalities.

We have been using | | for the sup norm, or max, for elements of N^t, $t \geq 1$.

DEFINITION 4.2.28. We now use | | for elements of N** = dom(M**).

LEMMA 4.2.15. Let $x_1,\ldots,x_p,y_1,\ldots,y_q \in N^{**}$, where $|x_1,\ldots,x_p|,|y_1,\ldots,y_q| >^{**} b\hat{}$. Then

$$(1 + 1/b)|x_1,\ldots,x_p| \leq^{**} f^{**}(x_1,\ldots,x_p) \leq^{**} b|x_1,\ldots,x_p|.$$
$$(1 + 1/b)|y_1,\ldots,y_q| \leq^{**} g^{**}(y_1,\ldots,y_q) \leq^{**} b|y_1,\ldots,y_q|.$$

If $|x_1,\ldots,x_p|,|y_1,\ldots,y_q| \leq^{**} b\hat{}$, then

$$f(x_1,\ldots,x_p),g(y_1,\ldots,y_q) \leq b^2\hat{}.$$

Proof: Recall the choice of $b \in N\backslash\{0,1\}$ made at the beginning of this section. These inequalities are purely universal, and hold in M. Hence they hold in M** by universal sentence preservation. QED

DEFINITION 4.2.29. Let t ∈ CT(L**). We write #(t) for the transfinite constant of greatest index that appears in t. If none appears, then we take #(t) to be -1.

LEMMA 4.2.16. Let t ∈ CT(L**). #(t) = -1 ↔ Val(M**,t) is standard. There exists a positive integer d such that the following holds. Suppose #(t) = c_α. Then c_α** ≤** Val(M**,t) <** dc_α** <** $c_{\alpha+1}$**.

Proof: We first claim the following. Suppose #(t) = c_α. Then c_α** ≤** Val(M**,t). This follows easily using Lemmas 4.2.14, 4.2.15, and the monotonicity of +.

Now suppose #(t) = -1. Since no transfinite constants appear in t, compute Val(M,t) = m ∈ N. Hence t = m^ holds in M. By universal sentence preservation, t = m^ holds in M**, and so Val(M**,t) = m^. Now suppose #(t) ≠ -1, and let #(t) = c_α. By the first claim in the previous paragraph, c_α** ≤ Val(M**,t), and so Val(M**,t) is nonstandard.

We now prove by induction on t ∈ CT(L**) that there exists d ∈ N\{0} such that for all $\alpha < \kappa$, if #(t) = c_α then Val(M**,t) <** dc_α**.

This is clearly true if t is a constant of L**. Let #(s + t) = c_α. Then #(s),#(t) ≤ c_α. By the induction hypothesis, let d ∈ N\{0} be such that #(s) = c_α → Val(M**,s) <** dc_α**, and #(t) = c_α → Val(M**,t) <** dc_α**. Then #(s + t) = c_α → Val(M**,s + t) <** $2dc_\alpha$**.

Let #(f(t_1,...,t_p)) = c_α. Then #(t_1),...,#(t_p) ≤ c_α. By the induction hypothesis, let d ∈ N\{0} be such that for all 1 ≤ i ≤ p, #(t_i) = c_α → Val(M**,t_i) <** dc_α**. Let #(f(t1,...,tp)) = c_α. By Lemma 4.2.15, Val(M**,f(t_1,...,t_p)) <** bdc_α**. The case of g(t_1,...,t_q) is argued in the same way. This completes the argument by induction.

We also need to establish that for all d ∈ N and $\alpha < \kappa$, dc_α** <** $c_{\alpha+1}$**. This is from Lemma 4.2.9. QED

LEMMA 4.2.17. c_0** is the least element of nst(M**).

Proof: By Lemma 4.2.14, c_0** ∈ nst(M**). Suppose x <** c_0**. Write x = Val(M**,t), t ∈ CT(L**). By Lemma 4.2.16, #(t) = -1. By Lemma 4.2.16, x is standard. QED

LEMMA 4.2.18. Let $x_1,\ldots,x_p \in N^{**}$ and $\alpha < \kappa$. Then $f^{**}(x_1,\ldots,x_p) <^{**} c_\alpha^{**} \leftrightarrow x_1,\ldots,x_p <^{**} c_\alpha^{**}$. Let $x_1,\ldots,x_q \in N^{**}$ and $\alpha < \kappa$. Then $g^{**}(x_1,\ldots,x_q) <^{**} c_\alpha^{**} \leftrightarrow x_1,\ldots,x_q <^{**} c_\alpha^{**}$. Let $x,y \in N^{**}$ and $\alpha < \kappa$. Then $x + y <^{**} c_\alpha^{**} \leftrightarrow x,y < c_\alpha^{**}$.

Proof: Let $x_1,\ldots,x_p \in N^{**}$ and $\alpha < \kappa$. Let $t_1,\ldots,t_p \in CT(L^{**})$, where each $x_i = Val(M^{**},t_i)$.

First suppose that $f^{**}(x_1,\ldots,x_p) < c_\alpha^{**}$. By Lemma 4.2.16, $\#(f(t_1,\ldots,t_p)) < c_\alpha$ or $\#(f(t_1,\ldots,t_p)) = -1$. Hence for all i, $\#(t_i) < c_\alpha$ or $\#(t_i) = -1$. Fix i. Then $\#(t_i) = -1$ or for some $\beta < \alpha$, $\#(t_i) = c_\beta$. In the former case, by Lemma 4.2.16, $Val(M^{**},t_i)$ is standard, and so is $< c_\alpha^{**}$, by Lemma 4.2.17. In the latter case, $Val(M^{**},t_i) <^{**} c_{\beta+1} \leq^{**} c_\alpha^{**}$, by Lemma 4.2.16.

For the converse, assume $x_1,\ldots,x_p <^{**} c_\alpha^{**}$. Then $Val(M^*,t_1),\ldots,Val(M^*,t_p) <^{**} c_\alpha^{**}$. If $\alpha = 0$ then by Lemmas 4.2.16 and 4.2.17, $\#(f(t_1,\ldots,t_p)) = -1$, and so $Val(M^{**},f(t_1,\ldots,t_p))$ is standard. So we can assume that $\alpha > 0$. By Lemma 4.2.16, none of $\#(t_1),\ldots,\#(t_p)$ is $\geq c_\alpha$. Hence $\#(t_1),\ldots,\#(t_p) < c_\alpha$. Let $\beta < \alpha$, where $\#(t_1),\ldots,\#(t_p) \leq c_\beta$. By Lemma 4.2.16, $Val(M^*,f(t_1,\ldots,t_p)) <^{**} c_{\beta+1}^{**} \leq c_\alpha^{**}$.

The remaining two claims are established analogously. QED

DEFINITION 4.2.30. Let s be a rational number. We write $<_s^{**}$ for the relation on N^{**} given by $x <_s^{**} y \leftrightarrow sx <^{**} y$.

LEMMA 4.2.19. Let s be a rational number > 1. There exists $k \geq 1$ such that for all $x_1 <_s^{**} x_2 <_s^{**} \ldots <_s^{**} x_k$, we have $2x_1 <^{**} x_k$.

Proof: Fix s as given, and let $k \geq 1$. Using universal sentence preservation, we see that for all $x_1,\ldots,x_k \in N^{**}$, if $x_1 <_s^{**} x_2 <_s^{**} \ldots <_s^{**} x_k$ then $x_1 <_{s'}^{**} x_k$, where s' is s^{k-1}. Choose k large enough so that $s^{k-1} \geq 2$. QED

LEMMA 4.2.20. Let s be a rational number > 1. The relation $<_s^{**}$ on N^{**} is transitive, irreflexive, and well founded.

Proof: Transitivity and irreflexivity follow from universal sentence preservation. By well foundedness, we mean that every nonempty subset of N^{**} has a $<_s^{**}$ minimal element. This is equivalent to: there is no infinite $x_1 >_s^{**} >_s^{**} x_2 >_s^{**} x_3 \ldots$.

By Lemma 4.2.19, if $<_2$** is well founded then $<_s$** is well founded. We now show that $<_2$** is well founded.

Let Y be a nonempty subset of N**. Choose t ∈ CT(L**) such that #(t) is least with Val(M**,t) ∈ Y. If #(t) = -1 then Y has a standard element. Let x be the least standard element of Y. Then x is a $<_2$** minimal element of S. Therefore, we can assume without loss of generality that Y has no standard elements, and #(t) ≥ 0.

Let #(t) = c_α and assume Y has no $<_2$** minimal element. By Lemma 4.2.16, fix d ∈ N\{0} such that Val(M**,t) <** dc_α**. Let t = $t_1,...,t_{d+1}$ ∈ CT(L**) be such that Val(M**,t_1) $>_2$** ... $>_2$** Val(M**,t_{d+1}), where Val(M**,t_1),...,Val(M**,t_{d+1}) ∈ Y. Then dVal(M**,t_{d+1}) <** Val(M**,t) <** dc_α**, and so Val(M**,t_{d+1}) <** c_α**. Since Y has no standard elements, α > 0. By Lemma 4.2.16, #(t_{d+1}) < c_α, which contradicts the choice of t, α. QED

DEFINITION 4.2.31. It is convenient to set s = 1 + 1/2b for using Lemma 4.2.20.

We now apply the well foundedness of $<_s$** in an essential way.

LEMMA 4.2.21. There is a unique set W such that W = {x ∈ nst(M**): x ∉ g**W}. For all $\alpha < \kappa$, c_α** ∉ rng(f**),rng(g**). In particular, each c_α** ∈ W.

Proof: By Lemma 4.2.15,

$$g^{**}(x_1,...,x_q) \geq_{1+(1/b)}^{**} |x_1,...,x_q|$$
$$g^{**}(x_1,...,x_q) >_s^{**} |x_1,...,x_q|$$

holds for all $x_1,...,x_q$ ∈ nst(M**). Hence g** is strictly dominating on nst(M**). By Lemma 4.2.20, $<_s$** is well founded on nst(M**). Hence we can apply the Complementation Theorem (for well founded relations), Theorem 1.3.1. Let W be the unique set such that W = {x ∈ nst(M**): x ∉ g**W}.

For the second claim, write c_α** = f**($x_1,...,x_p$). By Lemma 4.2.15, each x_i <** c_α**. By Lemma 4.2.18, f**($x_1,...,x_p$) <** c_α**. This is a contradiction. The same argument applies to g**.

The third claim follows immediately from the second claim. QED

We fix the unique W from Lemma 4.2.21. We will use q choice functions $F_1,\ldots,F_q$:N** → W such that for all x ∈ g**W,

$$x = g^{**}(F_1(x),\ldots,F_q(x))$$

and for all x ∉ g**W,

$$F_1(x) = \ldots = F_q(x) = c_0^{**}.$$

We now come to the Skolem hull construction.

DEFINITION 4.2.32. Let E ⊆ κ. Define E[1] = $\{c_\alpha^{**}: \alpha \in E\}$. Suppose E[1] ⊆ ... ⊆ E[k] ⊆ κ have been defined, k ≥ 1. Define E[k+1] = E[k] ∪ (W ∩ f**E[k]) ∪ F_1f**E[k] ∪ ... ∪ F_qf**E[k].

LEMMA 4.2.22. Let E ⊆ κ and i ≥ 1. E[i] ⊆ E[i+1] ⊆ W. f**E[i] ⊆ E[i+1] ∪. g**E[i+1]. E[1] ∩ f**E[i] = ∅.

Proof: Let E ⊆ κ and i ≥ 1. E[i] ⊆ E[i+1] ⊆ W is obvious by construction and the third claim of Lemma 4.2.21. Let x ∈ f**E[i]. Since E[i] ⊆ nst(M**), by Lemma 4.2.15, we have x ∈ nst(M**).

case 1. x ∈ W. Then x ∈ E[i+1].

case 2. x ∉ W. Since x ∈ nst(M**), we have x ∈ g**W. Hence x = g**(F_1(x),...,F_q(x)). Now each F_i(x) ∈ E[i+1] since x ∈ f**E[i]. Hence x ∈ g**E[i+1].

We have thus established that f**E[i] ⊆ E[i+1] ∪ g**E[i+1].

E[i+1] ∩ g**E[i+1] = ∅ follows from W ∩ g**W = ∅.

E[1] ∩ f**E[i] = ∅ follows from the second claim of Lemma 4.2.21. QED

Note that Proposition B is essentially the same as Lemma 4.2.22, for 1 ≤ i < n. However Proposition B lives in N and Lemma 4.2.22 lives way up in M**. The remainder of the proof of Proposition B surrounds the choice of a suitable E such that E[n] can be suitably embedded back into M.

Recall the positive integer e = p^{n-1} fixed at the beginning of this section, where κ is strongly e-Mahlo. Recall that we have also fixed n ≥ 1.

LEMMA 4.2.23. There is an integer m depending only on p,n, such that the following holds. There exist finitely many functions $G_1,G_2,...,G_m:\kappa^e \to W$, such that for all $E \subseteq \kappa$, $E[n] = G_1E \cup ... \cup G_mE$.

Proof: We show by induction on $1 \leq i \leq n$ that there exist finitely many functions $G_1,G_2,...,G_m$, where each G_i is a multivariate function from κ into W of various arities $\leq p^{i-1}$, with the desired property.

For i = 1, take $G_1:\kappa \to W$, where $G_1(\alpha) = c_\alpha{**}$.

Suppose $G_1,...,G_m$ works for fixed $1 \leq i < n$, with arities $\leq p^{i-1}$. For i+1, we start with $G_1,...,G_m$ in order to generate E[i] from E. In order to generate W ∩ f**E[i], we need finitely many functions, each built from f** composed with p of the $G_1,...,G_m$. The element $c_0{**} \in W$ is used to make sure that only values in W are generated. Each of these finitely many functions have arity at most $p(p^{i-1}) = p^i$. Each of $F_jf{**}[E_i]$, $1 \leq j \leq q$, are generated similarly.

So arities $\leq p^{n-1}$ are sufficient for the case i = n. We can obviously arrange for all of these functions to have arity $e = p^{n-1}$ by adding dummy variables. QED

We fix the functions $G_1,...,G_m$ given by Lemma 4.2.23.

We now define "term decomposition" functions $H_i:W \to \kappa$, indexed by the natural numbers. Let $x \in W$.

DEFINITION 4.2.33. To define the $H_i(x)$, first choose $t \in CT(L{**})$ such that Val(M**,t) = x. Let $c_{\alpha\_1},c_{\alpha\_2},...,c_{\alpha\_s}$ be a listing of all transfinite constants appearing in t from left to right, with repetitions allowed.

DEFINITION 4.2.34. For $x \in W$, set $H_0(x) = lth(t)$. For $1 \leq i \leq s$, set $H_i(x) = \alpha_i$. For i > s, set $H_i(x) = 0$.

DEFINITION 4.2.35. Finally, define functions $J_{i,j}:\kappa^e \to \kappa$, $i \geq 0$, $1 \leq j \leq m$, by $J_{i,j}(\alpha_1,...,\alpha_e) = H_i(G_j(\alpha_1,...,\alpha_e))$.

LEMMA 4.2.24. Let $E \subseteq \kappa$. Every element of E[n] is of the form Val(M**,t), where the length of $t \in CT(L{**})$ lies in $\cup\{J_{0,j}E: 1 \leq j \leq m\}$ and the transfinite constants of t have subscripts lying in $\cup\{J_{i,j}E: 1 \leq i \leq lth(t) \wedge 1 \leq j \leq m\}$.

Proof: Let $E \subseteq \kappa$ and $x \in E[n]$. By Lemma 4.2.23, let $x \in G_jE$, $1 \leq j \leq m$. Let $t \in CT(L{**})$ be the term used to write x

= Val(M**,t) in the definition of the $H_i(x)$. Write x = $G_j(\alpha_1,\ldots,\alpha_e)$, $\alpha_1,\ldots,\alpha_e \in E$. Then $J_{0,j}(\alpha_1,\ldots,\alpha_e) = H_0(x)$ = lth(t), and $J_{1,j}(\alpha_1,\ldots,\alpha_e), J_{2,,j}(\alpha_1,\ldots,\alpha_e), \ldots$, $J_{lth(t),j}(\alpha_1,\ldots,\alpha_e)$ enumerates at least the subscripts of transfinite constants of t. QED

LEMMA 4.2.25. There exists $E \subseteq S \subseteq \kappa$, E,S of order type ω, and a positive integer r, such that $E[n] \subseteq M^{**}[S,r]$.

Proof: We apply Lemma 4.1.6 to the following two sequences of functions. The first is the $J_{i,j}:\kappa^e \to \kappa$, where $i \geq 1$ and $1 \leq j \leq m$ (here m is as given by Lemma 4.2.23, and depends only on p,k). The first can be construed as an infinite sequence of functions from κ^e into κ, and the second can also be construed as an infinite sequence of functions from κ into ω by infinite repetition.

By Lemma 4.1.6, let $E \subseteq \kappa$ be of order type ω such that for all $i \geq 1$ and $1 \leq j \leq m$, $J_{i,j}E$ is either a finite subset of sup(E), or has order type ω with the same sup as E, and $J_{0,j}E$ is finite.

Let $r = \max(J_{0,1}E \cup \ldots \cup J_{0,m}E)$. By Lemma 4.2.24, every element of E[n] is the value in M** of a closed term t of length at most r, whose transfinite constants have subscripts lying in $S = \cup\{J_{ij}E\colon 1 \leq i \leq lth(t) \wedge 1 \leq j \leq m\}$. I.e., $E[n] \subseteq M^{**}[S,r]$. Note that S is a finite union of sets of ordinals, each of which is either a finite subset of sup(E), or is of order type ω with the same sup as E. Since $E \subseteq S$, we see that S is of order type ω. QED

DEFINITION 4.2.36. We fix E,S,r as given by Lemma 4.2.25.

THEOREM 4.2.26. Proposition B is provable in $SMAH^+$. In fact, it is provable in MAH^+.

Proof: By Lemma 4.2.22, for all $1 \leq i < n$, $f^{**}E[i] \subseteq E[i+1] \cup. g^{**}E[i+1]$, and $E[1] \cap f^{**}E[n] = \emptyset$. By Lemma 4.2.13, there is an S,r-embedding T from M** into M. Note that $f^{**}[E[n]] \cup g^{**}[E[n]] \subseteq M^{**}[S,r(p+q)] = dom(T)$.

For $1 \leq i \leq n$, let $A_i = TE[i]$. Since $E[1] \subseteq \ldots \subseteq E[n]$, we have $A_1 \subseteq \ldots \subseteq A_n \subseteq N$. By Lemma 4.2.25, $E[n] \subseteq M^{**}[S,r]$.

We first claim that for all $1 \leq i < n$, $fA_i \subseteq A_{i+1} \cup gA_{i+1}$.

Let $1 \leq i < n$, and $x \in fA_i$. Write $x = f(Ty_1,\ldots,Ty_p)$, $y_1,\ldots,y_p \in E[i]$. Hence $Tf^{**}(y_1,\ldots,y_p) = f(Ty_1,\ldots,Ty_p) = x$.

By Lemma 4.2.22, $f^{**}(y_1,\ldots,y_p) \in E[i+1] \cup g^{**}E[i+1]$. First suppose $f^{**}(y_1,\ldots,y_p) \in E[i+1]$. Then $Tf^{**}(y_1,\ldots,y_p) = x \in A_{i+1}$.

Secondly suppose $f^{**}(y_1,\ldots,y_p) \in g^{**}E[i+1]$, and write $f^{**}(y_1,\ldots,y_p) = g^{**}(z_1,\ldots,z_q)$, where $z_1,\ldots,z_q \in E[i+1]$. Then $Tf^{**}(y_1,\ldots,y_p) = Tg^{**}(z_1,\ldots,z_q) = g(Tz_1,\ldots,Tz_q) = f(Ty_1,\ldots,Ty_p) = x$. Hence $x \in gA_{i+1}$.

We next claim that for all $1 \leq i < n$, $A_{i+1} \cap gA_{i+1} = \emptyset$. We must verify that $TE[i+1] \cap gTE[i+1] = \emptyset$. Let $x,y_1,\ldots,y_q \in E[i+1]$, $T(x) = g(Ty_1,\ldots,Ty_q)$. Clearly $T(x) = Tg^{**}(y_1,\ldots,y_q)$, and so $x = g^{**}(y_1,\ldots,y_q)$. This contradicts $E[i+1] \cap g^{**}E[i+1] = \emptyset$.

We finally claim that $A_1 \cap fA_n = \emptyset$. Let $x \in A_1$, $y_1,\ldots,y_p \in A_n$, $x = f(y_1,\ldots,y_p)$. Let $x' \in E[1]$, $y_1',\ldots,y_p' \in E[n]$, where $x = T(x')$, and $y_1,\ldots,y_p = T(y_1'),\ldots,T(y_p')$ respectively. Note that $Tf^{**}(y_1',\ldots,y_p') = f(T(y_1'),\ldots,T(y_p')) = f(y_1,\ldots,y_p) = x = T(x')$. Therefore $x' = f^{**}(y_1',\ldots,y_p')$, contradicting the last claim of Lemma 4.2.22.

The second claim in the Lemma follows from the first by Theorem 4.1.7. This is because Proposition B is obviously in Π^1_2 form. QED

Obviously the proof of Theorem 4.2.26 gives an upper bound on the order of strongly Mahlo cardinal sufficient to prove Proposition B that depends exponentially on the arity of f and the length of the tower. Without attempting to optimize the level, we have shown the following.

COROLLARY 4.2.27. The following is provable in ZFC. Let $p,n \geq 1$. If there exists a strongly p^{n-1}-Mahlo cardinal then Proposition B holds for p-ary f, multivariate g, and n. If there exists a strongly p^2-Mahlo cardinal, then Proposition A holds for p-ary f and multivariate g. Furthermore, we can drop "strongly" from both results.

Corollary 4.2.27 is far from optimal. For instance, if n = 2 then Proposition B is provable in RCA_0, as we shall see now.

THEOREM 4.2.28. The following is provable in RCA_0. For all $f,g \in ELG$ there exist infinite $A \subseteq B \subseteq N$ such that

$$fA \subseteq B \cup. \ gB$$
$$A \cap fB = \emptyset.$$

Proof: Let $f,g \in$ EVSD. Let n be sufficiently large. By Theorem 3.2.5, let $A \subseteq [n,\infty)$ be infinite where $A \cap g(A \cup fA) = \emptyset$. By Lemma 3.3.3, let B be unique such that $B \subseteq A \cup fA \subseteq B \cup. \ gB$. Then $A \cap gB \subseteq A \cap g(A \cup fA) = \emptyset$, and hence $A \subseteq B$. Also $A \cap fB \subseteq A \cap f(A \cup fA) = \emptyset$, and $fA \subseteq B \cup. \ gB$. QED

4.3. Some Existential Sentences.

In this section, we prove a crucial Lemma needed for section 4.4. We consider existential sentences of the following special form.

DEFINITION 4.3.1. Define $\lambda(k,n,m,R_1,\ldots,R_{n-1})$ =

$$(\exists \text{ infinite } B_1,\ldots,B_n \subseteq N^k)$$
$$(\forall i \in \{1,\ldots,n-1\})(\forall x_1,\ldots,x_m \in B_i)$$
$$(\exists y_1,\ldots,y_m \in B_{i+1})(R_i(x_1,\ldots,x_m,y_1,\ldots,y_m))$$

where $k,n,m \geq 1$, and $R_1,\ldots,R_{n-1} \subseteq N^{2km}$ are order invariant relations. Recall that order invariant sets of tuples are sets of tuples where membership depends only on the order type of a tuple.

Note the stratified structure of $\lambda(k,n,m,R_1,\ldots,R_{n-1})$. It asserts that there are n infinite sets such that for all elements of the first there are elements of the second with a property, and for all elements of the second there are elements of the third with a property, etcetera.

It is evident that even RCA_0 suffices to define truth for the sentences of the form $\lambda(k,n,m,R_1,\ldots,R_{n-1})$. For in RCA_0, we can

i. Appropriately code finite sequences of subsets of N^k as subsets of N.
ii. Appropriately code finite sequences of elements of N as elements of N.
iii. Appropriately treat order invariant sets of tuples from N.

This does not mean that we can form the set of all true sentences of the form $\lambda(k,n,m,R_1,\ldots,R_{n-1})$ in RCA_0 or even

ACA'. However, we will show that this is in fact the case for ACA'. See Definition 1.4.1.

Specifically, we will present a primitive recursive criterion for the truth of sentences $\lambda(k,n,m,R_1,\ldots,R_{n-1})$, and prove that the criterion is correct, within the system ACA'.

We first put the sentences $\lambda(k,n,m,R_1,\ldots,R_{n-1})$ in substantially simpler form.

DEFINITION 4.3.2. Define $\lambda'(k,n,R_1,\ldots,R_{n-1})$ =

$$(\exists \text{ infinite } B_1,\ldots,B_n \subseteq N^k)$$
$$(\forall i \in \{1,\ldots,n-1\})$$
$$(\forall x,y,z \in B_i)(\exists w \in B_{i+1})(R_i(x,y,z,w))$$

where $k,n \geq 1$, and $R_1,\ldots,R_{n-1} \subseteq N^{4k}$ are order invariant relations.

LEMMA 4.3.1. There is a primitive recursive procedure for converting any sentence $\lambda(k,n,m,R_1,\ldots,R_{n-1})$ to a sentence $\lambda'(k',n',S_1,\ldots,S_{n'-1})$ with the same truth value. In fact, ACA' proves that any $\lambda(k,n,m,R_1,\ldots,R_{n-1})$ has the same truth value as its conversion $\lambda'(k',n',S_1,\ldots,S_{n'-1})$.

Proof: Start with

*) $(\exists \text{ infinite } B_1,\ldots,B_n \subseteq N^k)(\forall i \in \{1,\ldots,n-1\})$ $(\forall x_1,\ldots,x_m \in B_i)(\exists y_1,\ldots,y_m \in B_{i+1})(R_i(x_1,\ldots,x_m,y_1,\ldots,y_m))$.

Let $C,D \subseteq N^{km}$. We think of C,D as sets of m-tuples from N^k. We write $C\# \subseteq N^k$ for the set of all k-tuple components of elements of C.

We write $C \leq D$ if and only if $C,D \subseteq N^{km}$, and for all $(x_1,\ldots,x_m),(y_1,\ldots,y_m),(z_1,\ldots,z_m) \in C$,

i. If $(x_1,\ldots,x_m) = (y_1,\ldots,y_m) = (z_1,\ldots,z_m)$ then $(x_1,\ldots,x_m) \in D$.
ii. If $(x_1,\ldots,x_m),(y_1,\ldots,y_m),(z_1,\ldots,z_m)$ are distinct then $(x_2,\ldots,x_m,x_1) \in D$.
iii. If $(x_1,\ldots,x_m) \neq (y_1,\ldots,y_m) = (z_1,\ldots,z_m)$ then $(x_1,y_1,\ldots,y_{m-1}) \in D$.
iv. If $(x_1,\ldots,x_m) = (y_1,\ldots,y_m) \neq (z_1,\ldots,z_m)$ then $(x_1,y_1,\ldots,y_{m-1}) \in D$.

We claim that if C_1 has at least three elements and $C_1 \leq \ldots \leq C_{2m}$, then $C_1\#^m \subseteq C_{2m} \subseteq N^{km}$. To see this, let $C_1,\ldots,C_{2m}$ be as given. By i), $C_1 \subseteq \ldots \subseteq C_{2m}$. By ii), $(x_1,\ldots,x_m) \in C_1 \rightarrow (x_2,\ldots,x_m,x_1) \in C_2$. We can continue for m steps, obtaining that for all $(x_1,\ldots,x_m) \in C_1$, all m rotations of $(x_1,\ldots,x_m)$ lie in C_m.

It follows that every $\alpha \in C_1\#^m$ is the sequence of first terms of some $\beta_1,\ldots,\beta_m \in C_m$. (Here α is an m tuple from $C_1\#$ and $\beta_1,\ldots,\beta_m$ are m tuples from C_m). By iii,iv, we can replace the first term of β_m by the first term of β_{m-1}, and shift the remaining terms of β_m to the right, removing the last term of β_m, with the resulting m tuple β' starting with the first term of β_{m-1} followed by the first term of β_m. Thus $\beta' \in C_{m+1}$. At the second stage, we can use β_{m-2} and β' to form $\beta'' \in C_{m+2}$. We continue this process until we finally use β_1, to arrive at $\alpha \in C_{2m}$.

We now claim that *) is equivalent to

**) $(\exists$ infinite $C_1,\ldots,C_{2nm} \subseteq N^{km})(C_1 \leq \ldots \leq C_{2m} \wedge C_{2m+1} \leq \ldots \leq C_{4m} \wedge \ldots \wedge C_{2nm-2m+1} \leq \ldots \leq C_{2nm} \wedge (\forall i \in \{1,\ldots,n-1\}) (\forall x \in C_{2im})(\exists y \in C_{2im+1})(R_i(x,y)))$.

To see this, let $B_1,\ldots,B_n$ witness *). Set

$$C_1 = \ldots = C_{2m} = B_1{}^m$$
$$\ldots$$
$$C_{2nm-2m+1} = \ldots = C_{2nm} = B_n{}^m.$$

Clearly

$$C_1 \leq \ldots \leq C_{2m}$$
$$\ldots$$
$$C_{2nm-2m+1} \leq \ldots \leq C_{2nm}.$$

Conversely, let $C_1,\ldots,C_{2nm}$ witness **). Since $C_1,\ldots,C_{2nm}$ are infinite, we see that $C_1\#^m \subseteq C_{2m} \wedge \ldots \wedge C_{2nm-2m+1}\#^m \subseteq C_{2nm}$. For all $1 \leq i \leq n$, set $B_i = C_{2(i-1)m+1}\#$. Then these B's witness *).

It is easy to see that **) is a sentence of the form $\lambda'(k',n',S_1,\ldots,S_{n'-1})$. The relations in **) between successive $C_1,\ldots,C_{2m}$, and between successive $C_{2m+1},\ldots,C_{4m}$, etcetera, are of the form $\forall\forall\forall\exists$ according to the definition of $\leq$. The relations in **) between C_{2m},C_{2m+1}, and between C_{4m},C_{4m+1}, etcetera, are of the form $\forall\exists$. QED

We now define sets $Y_1,\ldots,Y_n$ by

i. $Y_1 = N$.
ii. For $1 \le i < n$, $Y_{i+1} = Y_i \times Y_i \times Y_i \times Y_i$.

LEMMA 4.3.2. A sentence $\lambda'(k,n,R_1,\ldots,R_{n-1})$ holds if and only if there exist functions $f_i:Y_i \to N^k$, $1 \le i \le n$, such that the following holds.
i. f_1 is one-one.
ii. For all $1 \le i \le n$ and $x,y,z \in Y_i$, $f_i(x,y,z,w)$ as a function of $w \in Y_i$, is one-one.
iii. For all $1 \le i < n$ and $x,y,z \in Y_i$, $R_i(f_i(x),f_i(y),f_i(z),f_{i+1}(x,y,z,z))$.

Proof: Let $\lambda'(k,n,R_1,\ldots,R_{n-1})$ be given. Suppose $\lambda'(k,n,R_1,\ldots,R_{n-1})$ is true. Let $B_1,\ldots,B_n \subseteq N^k$ be infinite, where for all $1 \le i < n$, $(\forall x,y,z \in B_i)(\exists w \in B_{i+1})(R_i(x,y,z))$.

We now define $f_1,\ldots,f_n$ inductively as follows. Let $f_1:N \to B_1$ be a bijection. Suppose surjective $f_i:Y_i \to B_i$ has been defined, $1 \le i < n$. To define $f_{i+1}:Y_{i+1} \to B_{i+1}$, let $x,y,z \in Y_i$. Since $f_i(x),f_i(y),f_i(z) \in B_i$, set $f_{i+1}(x,y,z,z) \in B_{i+1}$ to be such that $R_i(f_i(x),f_i(y),f_i(z),f_{i+1}(x,y,z,z))$. Define $f_{i+1}(x,y,z,w)$, $w \in Y_i$, $w \neq z$, so that $f_{i+1}(x,y,z,w)$ is a bijection from Y_{i+1} onto B_{i+1} as a function of w.

Conversely, let $f_i:Y_i \to N^k$, $1 \le i \le n$, be such that i)-iii) above hold. For all $1 \le i \le n$, let $B_i = \text{rng}(f_i)$. Then each B_i is infinite. Let $1 \le i < n$ and $u,v,w \in B_i$. Let $u = f_i(x)$, $v = f_i(y)$, $w = f_i(z)$, where $x,y,z \in Y_i$. Then $R_i(u,v,w,f_{i+1}(x,y,z,z))$. Since $f_{i+1}(x,y,z,z) \in B_{i+1}$, we are done. QED

We can use Lemma 4.3.2 to convert $\lambda'(k,n,R_1,\ldots,R_{n-1})$ into a sentence of a rather simple form.

DEFINITION 4.3.3. Define $\mu(p,q,\varphi)$ =

$$(\exists f:N^p \to N)(\forall x_1,\ldots,x_q \in N)(\varphi)$$

where φ is a propositional combination of atomic formulas of the forms $x_i < x_j$, $f(y_1,\ldots,y_p) < f(z_1,\ldots,z_p)$, where $x_i,x_j,y_1,\ldots,y_p,z_1,\ldots,z_p$ are among the (distinct) variables $x_1,\ldots,x_q$.

LEMMA 4.3.3. There is a primitive recursive procedure for converting any sentence $\lambda'(k,n,S_1,\ldots,S_{n-1})$ to a sentence $\mu(p,q,\varphi)$, with the same truth value. In fact, ACA′ proves that any $\lambda'(k,n,S_1,...,S_{n-1})$ has the same truth value as its conversion $\mu(p,q,\varphi)$.

Proof: We use Lemma 4.3.2. We can obviously identify each Y_i with $N^{4\hat{}(i-1)}$. Then the condition in Lemma 4.3.2 takes the following form: there exists a definite finite number of functions from various Cartesian powers of N into N^k such that a universally quantified statement (quantifiers in N) holds whose matrix is a propositional combination of numerical comparisons, either between integer variables, or designated coordinates of values (which lie in N^k) of the functions at tuples of variables. This is clear by examining clauses i) - iii) in Lemma 4.3.2, and noting that the S_i are order invariant.

The use of N^k as a range here can be eliminated in favor of using more functions from various Cartesian powers of N into N. Thus we obtain an equivalent of the following form: there exists a definite finite number of functions from various Cartesian powers of N into N such that a universally quantified statement holds whose matrix is a propositional combination of numerical comparisons, either between integer variables, or values of the functions at tuples of variables.

By adding dummy variables, we can assume that all of the functions have the same arity. Thus we have

$$*)\ (\exists f_1,...,f_r:N^p \rightarrow N)(\forall x_1,...,x_q \in N)(\varphi)$$

where φ is a propositional combination of atomic formulas of the forms $x_i < x_j$, $f_a(y_1,...,y_p) < f_b(z_1,...,z_p)$, where $x_i,x_j,y_1,...,y_p,z_1,...,z_p$ are among the (distinct) variables $x_1,...,x_q$. It remains to reduce this to quantification over a single function.

The idea is to introduce a single function variable $f:N^{p+r} \rightarrow N$ which does the work of $f_1,...,f_r$ in a sufficiently explicit way. We say that f is special if and only if for all distinct $c,d \in N$, $f(y_1,...,y_p,c,...,c,d,...,d)$ depends only on $y_1,...,y_p$ and the number of c's displayed (which is from 1 to r), and not what integers c,d are (as long as $c \neq d$).

It is now clear that *) is equivalent to

$$**)\ (\exists f:N^{p+r} \rightarrow N)(\forall u,v \in N)(\forall x_1,...,x_p \in N)$$
$$(f \text{ is special} \wedge (u \neq v \rightarrow \varphi'))$$

where φ' is obtained from φ by replacing each $f_i(y_1,\ldots,y_p)$ in *) by $f(y_1,\ldots,y_p,u,\ldots,u,v,\ldots,v)$, where the number of u's displayed is i. QED

We now prove a combinatorial lemma.

DEFINITION 4.3.4. Let $f:N^p \to N$ and $A \subseteq N$. We say that A is an SOI for f if and only if the truth value of any statement

$$f(x_1,\ldots,x_p) < f(y_1,\ldots,y_p)$$

where $x_1,\ldots,x_p,y_1,\ldots,y_p \in A$, depends only on the order type of the 2p-tuple $(x_1,\ldots,x_p,y_1,\ldots,y_p)$.

DEFINITION 4.3.5. We say that A is a strong SOI for f if and only if A is an SOI for f such that the following holds. Let $x_1,\ldots,x_p,y_1,\ldots,y_p \in A$. Suppose $(x_1,\ldots,x_p)$ and $(y_1,\ldots,y_p)$ have the same order type. Suppose also that for all $1 \leq i \leq p$, $x_i = y_i \vee y_i > \max(x_1,\ldots,x_p)$. Then $f(x_1,\ldots,x_p) \leq f(y_1,\ldots,y_p)$;

DEFINITION 4.3.6. We say that A is a special SOI for f if and only if A is a strong SOI for f such that the following holds. Let $x1,\ldots,xp,y1,\ldots,yp \in A$. Suppose $(x_1,\ldots,x_p)$ and $(y_1,\ldots,y_p)$ have the same order type. Suppose also that for all $1 \leq i \leq p$, $x_i = y_i \vee y_i > \max(x_1,\ldots,x_p)$. If $f(x_1,\ldots,x_p) < f(y_1,\ldots,y_p)$ then $f(y_1,\ldots,y_p)$ is greater than all $f(z_1,\ldots,z_p)$, with $|z_1,\ldots,z_p| \leq |x_1,\ldots,x_p|$.

The above definitions makes perfectly good sense for functions $f:A^p \to N$ where A is finite. In this finite context, we will be particularly interested in the case $A = [0,q]$.

LEMMA 4.3.4. The following is provable in ACA'. For all $p \geq 1$, every $f:N^p \to N$ has an infinite special SOI $A \subseteq N$. In fact, every infinite SOI for $f:N^p \to N$ is a special SOI for f.

Proof: Let $f:N^p \to N$. By the infinite Ramsey theorem for 2p-tuples, let $A \subseteq N$ be an infinite SOI for f. We now show that A is a special SOI for f.

Let $x_1,\ldots,x_p,y_1,\ldots,y_p \in A$. Suppose $x = (x_1,\ldots,x_p)$ and $y = (y_1,\ldots,y_p)$ have the same order type, and for all $1 \leq i \leq p$, $x_i = y_i \vee y_i > \max(x_1,\ldots,x_p)$.

Suppose $x \neq y$. We claim that x,y are the first two terms of an infinite sequence of elements of N^p, written $x,y,w_1,w_2,\ldots$, such that the order types of (x,y), (y,w_1), (w_1,w_2), ..., are the same. To see this, let $x_1' < \ldots < x_i'$ and $y_1' < \ldots < y_j'$ be the strictly increasing enumeration of the terms of $(x_1,\ldots,x_p)$ and $(y_1,\ldots,y_p)$, respectively. Since $(x_1,\ldots,x_p)$ and $(y_1,\ldots,y_p)$ have the same order type, i = j. It is also clear that for the least k such that $x_k' \neq y_k'$, we have $y_k' > x_i'$. Now choose w_1 of the same order type as x,y so that its strictly increasing enumeration starts with the same $x_1' < \ldots < x_{k-1}'$ and continues higher than y_i'. Then obviously (x,y) and (y,w_1) have the same order type. Continue in this way indefinitely.

Now suppose $f(x) > f(y)$. Then $x \neq y$ and we can use the $x,y,w_1,w_2,\ldots$ constructed in the previous paragraph. Since A is an SOI for f, if $f(x) > f(y)$ then $f(x) > f(y) > f(w_1) > f(w_2) \ldots$, which is impossible. Hence $f(x) \leq f(y)$.

Finally, suppose $f(x) < f(y)$, and let $z \in [0,\max(x)]^p$. Since $x \neq y$, we can use the $x,y,w_1,w_2,\ldots$ constructed previously. Note that the pairs $(y,z),(w_1,z),(w_2,z)$, ... all have the same order type. Suppose $f(y) \leq f(z)$. Since A is an SOI for f, we see that each $f(w_i) \leq f(z)$. Also since A is an SOI for f and $f(x) < f(y)$, we have that each $f(w_i) < f(w_{i+1})$, and therefore the $f(w_i)$ are unbounded. This is a contradiction. QED

LEMMA 4.3.5. The following is provable in ACA'. Let $q \geq 3p \geq 1$, and $f:[0,q]^p \to N$. Assume $[0,q]$ is a special SOI for f. There exists $g:N^p \to N$ such that N is a special SOI for g, where for all $x,y \in [0,q]^p$, $f(x) \leq f(y) \leftrightarrow g(x) \leq g(y)$.

Proof: Let p,q,f be as given. We now put a relation $\leq^*$ on N^p as follows. Let $x,y \in N^p$. Then $x \leq^* y$ if and only if there exists $\alpha,\beta \in [0,q]^p$ such that

i. (x,y) and (α,β) have the same order type.
ii. $f(\alpha) \leq f(\beta)$.

Since $[0,q]$ is an SOI for f, we have that $x \leq y^*$ if and only if

for all $\alpha,\beta \in [0,q]^p$, if (x,y) and (α,β) have the same order type then $f(\alpha) \leq f(\beta)$.

Since $q \geq 2p$, every element of N^{2p} is of the same order type as an element of $[0,q]^{2p}$. Hence $\leq^*$ is reflexive and connected.

To see that $\leq^*$ is transitive, let $x \leq^* y \wedge y \leq^* z$. Let $a_1 < \ldots < a_r$ be an enumeration of the combined coordinates of x,y,z. Clearly $1 \leq r \leq 3p \leq q$. Let (x,y,z) have the same order type as $(\alpha,\beta,\gamma) \in [0,q]^{3p}$. Then $f(\alpha) \leq f(\beta)$ and $f(\beta) \leq f(\gamma)$. Hence $f(\alpha) \leq f(\gamma)$ and $(x,z),(\alpha,\gamma)$ have the same order type. Therefore $x \leq^* z$.

It is standard to define the equivalence relation of $\leq^*$ by $x =^* y \leftrightarrow (x \leq^* y \wedge y \leq^* x)$. This is obviously equivalent to the existence of $\alpha,\beta \in [0,q]^p$ such that $(x,y),(\alpha,\beta)$ have the same order type and $f(\alpha) = f(\beta)$. This is also equivalent to: for all $\alpha,\beta \in [0,q]^p$, if (x,y) and (α,β) have the same order type then $f(\alpha) = f(\beta)$.

We now show that the order type of $\leq^*$, modulo its equivalence relation $=^*$, is finite or ω.

We first verify that $\leq^*$ is well founded. Suppose $x_1 >^* x_2 >^* \ldots$. Apply Ramsey's theorem to the comparison of the b-th coordinate of x_i with the b-th coordinate of x_j, $b = 1,\ldots,p$. Then we obtain an infinite subsequence $y_1 >^* y_2 >^* \ldots$ such that for all $1 \leq b \leq p$, either the b-th coordinates of the y's are constant, or strictly increasing. We can then pass to an infinite subsequence $z_1 >^* z_2 >^* \ldots$ such that for all $i < j$, the p-tuples z_i,z_j satisfy the hypotheses in the definition of strong SOI. Let (z_1,z_2) and (α,β) have the same order type, where $\alpha,\beta \in [0,q]^p$. Then α,β satisfy the hypotheses in the definition of strong SOI. Therefore $f(\alpha) \leq^* f(\beta)$, and hence $z_1 \leq^* z_2$. This is a contradiction.

We now verify that $\leq^*$ has no limit points. Suppose $y_1 <^* y_2 \ldots <^* x$. As before, pass to an infinite subsequence $z_1 <^* z_2 \ldots <^* x$, such that for all $i < j$ the p-tuples z_i,z_j satisfy the hypotheses in the definition of strong SOI. Choose $z_i <^* z_{i+1}$ such that $\max(z_i) > \max(x)$. Let $\alpha,\beta,\gamma \in [0,q]^p$, where (α,β,γ) and (x,z_i,z_{i+1}) have the same order type. Then β,γ satisfy the hypotheses in the definition of special SOI. Also $f(\beta) < f(\gamma)$ and $|\alpha| < |\beta|$. Since $[0,q]$ is a special SOI for f, $f(\gamma) > f(\alpha)$. Hence $z_{i+1} >^* x$. This is a contradiction.

So we have now shown that the order type of ≤* is finite or ω. Note that ≤* is order invariant. Hence =*, <* are also order invariant.

We define $g:N^p \to N$ by: g(x) is the position of x in the ordering ≤*, counting from 0. Obviously N is an SOI for g, since <* is order invariant. Hence by Lemma 4.3.4, N is a special SOI for g.

For the final claim of Lemma 4.3.5, let $x,y \in [0,q]^p$. Suppose f(x) ≤ f(y). Then x ≤* y, and hence g(x) ≤ g(y). Suppose g(x) ≤ g(y). Then x ≤* y. Let (x,y) and (α,β) have the same order type, $\alpha,\beta \in [0,q]^p$, where f(α) ≤ f(β). Then f(x) ≤ f(y). QED

LEMMA 4.3.6. The following is provable in ACA'. Let q ≥ 3p ≥ 1, and $f:[0,q]^p \to N$. Assume [0,q] is a special SOI for f. Let $g:N^p \to N$ be such that N is a special SOI for g, where for all $x,y \in [0,q]^p$, f(x) ≤ f(y) ↔ g(x) ≤ g(y). Then μ(p,q,φ) holds with f, where the universal quantifiers are restricted to [0,q], if and only if μ(p,q,φ) holds with g.

Proof: Let p,q,f,g, and μ(p,q,φ) be as given. Assume μ(p,q,φ) holds with f, where the universal quantifiers are restricted to [0,q].

Suppose μ(p,q,φ) fails with g. Let $x_1,\ldots,x_q \in N$ be a counterexample to μ(p,q,φ) with g.

We claim that we can push this counterexample down to lie within [0,q], by merely choosing $x_1',\ldots,x_q' \in [0,q]$ such that $(x_1',\ldots,x_q')$ and $(x_1,\ldots,x_q)$ have the same order type. The reason is that φ is a propositional combination of formulas of the forms

$$y < z$$
$$f(y_1,\ldots,y_q) < f(z_1,\ldots,z_q)$$

where $y,z,y_1,\ldots,y_q,z_1,\ldots,z_q$ are among the variables $x_1,\ldots,x_q$. Using the fact that N is a special SOI for g, the above inequalities have the same truth values as the inequalities

$$y' < z'$$
$$f(y_1',\ldots,y_q') < f(z_1',\ldots,z_q').$$

By hypothesis, we can now replace f by g in φ with $x_1',\ldots,x_q' \in [0,q]$, obtaining ¬μ(p,q,φ) with g.

Conversely, suppose $\mu(p,q,\varphi)$ fails with f. Let $x_1,...,x_q \in [0,q]$ be a counterexample to $\mu(p,q,\varphi)$ with f. Then by the same argument, $x_1,...,x_q$ is a counterexample to $\mu(p,q,\varphi)$ with g.

It is worth noting that this argument would fail if we allowed inequalities of the form $u < f(v_1,...,v_q)$ in φ. Thus the restriction on φ is important. QED

LEMMA 4.3.7. The following is provable in ACA'. A sentence $\mu(p,q,\varphi)$, $q \geq 3p$, holds if and only if there exists $f:[0,q]^p \to [0,(q+1)^p]$ such that $[0,q]$ is a special SOI for f, and φ holds for f (with universal quantifiers ranging over $[0,q]$).

Proof: Let $\mu(p,q,\varphi)$ be given, $q \geq 3p$. Let $f:[0,q]^p \to [0,(q+1)^p]$, where $[0,q]$ is a special SOI for f, and $\mu(p,q,\varphi)$ holds with f, with universal quantifiers restricted to $[0,q]$. Let g be as given by Lemma 4.3.5. By Lemma 4.3.6, $\mu(p,q,\varphi)$ holds with g. In particular, $\mu(p,q,\varphi)$ holds.

Conversely, let $\mu(p,q,\varphi)$ hold with $g:N^p \to N$. By Lemma 4.3.4, let $A \subseteq N$ be a special SOI for g of cardinality q+1. Then $\mu(p,q,\varphi)$ holds for g with universal quantifiers restricted to A. Note that $g|A^p$ is isomorphic to a unique $f:[0,q]^p \to N$ by the unique increasing bijection h from A onto $[0,q]$. (Here the isomorphism h acts only on the domains, and so only provides the transfer of statements of the form $f(x_1,...,x_p)\ \tau\ f(y_1,...,y_p)$ to $g(h(x_1),...,h(x_p))\ \tau\ g(h(y_1),...,h(y_p))$, where $\tau \in \{\leq,<,=\}$). Hence $\mu(p,q,\varphi)$ holds with f.

Now A is a special SOI for $g|A^p$. We now show that $[0,q]$ is a special SOI for f. By the isomorphism h from $g|A^p$ onto f, clearly $[0,q]$ is a strong SOI for f. Now let $(x_1,...,x_p)$ and $(y_1,...,y_p)$ from $[0,q]^p$ have the same order type. Suppose also that for all $1 \leq i \leq p$, $x_i = y_i \lor y_i > \max(x_1,...,x_p)$. Suppose

$$1)\ f(x_1,...,x_p) < f(y_1,...,y_p)$$
$$|z_1,...,z_p| \leq |x_1,...,x_p|.$$

We must show that $f(y_1,...,y_p) > f(z_1,...,z_p)$. Since $|z_1,...,z_p| \leq q$, we can take h^{-1} throughout 1), and then apply that A is a special SOI for $g|A^p$.

Note that we can obviously arrange that rng(f) ⊆ $[0,(q+1)^p]$ by counting. QED

THEOREM 4.3.8. There is a presentation of a primitive recursive function h such that the following holds. ACA′ proves that $\lambda(k,n,m,R_1,\ldots,R_{n-1})$ is true if and only if $h(k,n,m,R_1,\ldots,R_{n-1}) = 1$.

Proof: Start with $\lambda(k,n,m,R_1,\ldots,R_{n-1})$. Pass to $\lambda'(k',n',S_1,\ldots,S_{n'-1})$ by Lemma 4.3.1. Pass to $\mu(p,q,\varphi)$, $q \geq 3p$, by Lemma 4.3.3. Now apply Lemma 4.3.7. QED

4.4. Proof using 1-consistency.

In this section we show that Propositions A,B can be proved in ACA′ + 1-Con(SMAH). Here 1-Con(T) is the 1-consistency of T, which asserts that “every Σ^0_1 sentence provable in T is true”. 1-Con(T) is also equivalent to “every Π^0_2 sentence provable in T is true”.

By Lemma 4.2.1, Proposition B implies Proposition A in RCA_0. Hence it suffices to show that Proposition B can be proved in ACA′ + 1-Con(SMAH).

DEFINITION 4.4.1. We write ELG(p,b) for the set of all f ∈ ELG of arity p satisfying the following conditions. For all $x \in N^p$,

i. if $|x| > b$ then $(1 + 1/b)|x| \leq f(x) \leq b|x|$.
ii. if $|x| \leq b$ then $f(x) \leq b^2$.

Note that from Definition 2.1, f ∈ ELG if and only if there exist positive integers p,b such that f ∈ ELG(p,b). Also note that each ELG(p,b) forms a compact subspace of the Baire space of functions from N^k into N.

DEFINITION 4.4.2. Let $p,q,b \geq 1$. A p,q,b-structure is a system of the form

$$M^* = (N^*,0^*,1^*,<^*,+^*,f^*,g^*,c_0^*,\ldots)$$

such that

1. N* is countable. For specificity, we can assume that N* is N.
2. (N*,0*,1*,<*,+*) is a discretely ordered commutative semigroup (see definition below).

3. $+^*:N^{*2} \to N^*$, $f^*:N^{*p} \to N^*$, $g^*:N^{*q} \to N^*$.
4. f^* obeys the above two inequalities for membership in ELG(p,b), internally in M^*.
5. g^* obeys the above two inequalities for membership in ELG(q,b), internally in M^*.
6. Let $i \geq 0$. The sum of any finite number of copies of c_i^* is $< c_{i+1}^*$.
7. The c^*'s form a strictly increasing set of indiscernibles for the atomic sentences of M^*.

Note that the conditions under clauses 4-7 are all universal sentences.

Note that we do not require every element of N^* to be the value of a closed term.

DEFINITION 4.4.3. A discretely ordered commutative semigroup is a system $(G,0,1,<,+)$ such that

i. $<$ is a linear ordering of G.
ii. 0,1 are the first two elements of G.
iii. $x+0 = x$.
iv. $x+y = y+x$.
v. $(x+y)+z = x+(y+z)$.
vi. $x < y \to x+z < y+z$.
vii. $x+1$ is the immediate successor of x.

Note that the cancellation law

$$x+z = y+z \to x = y$$

holds in any discretely ordered commutative semigroup (in this sense), since assuming $x+z = y+z$, the cases $x < y$ and $y < x$ are impossible.

In any p,q,b-structure, the c_n^* have an important inaccessibility condition: any closed term whose value is c_n^* is a sum consisting of c_n^* and zero or more 0^*'s. To see this, write $c_n^* = t$, and write t as a sum, $t = s_1 + ... + s_k$, $k \geq 1$, where each s_i is either a constant or starts with f or g. By 7, c_n^* is infinite, and so all s_i that begin with f or g must have immediate subterms $< c_n^*$ (using 4,5). Hence all s_i that begin with f or g must be $< c_n^*$ (using 4,5,6). Hence all s_i are either $< c_n^*$ or are a constant. If no s_i is c_i^* then all s_i are $< c_n^*$, violating 6. Hence some s_i is c_n^*. By 2, the remaining s_i must be 0.

We can follow the development of section 4.2 starting right after the proof of Lemma 4.2.7. In this rerun, we do not fix f ∈ ELG(p,b), and g ∈ ELG(q,b).

Instead we fix p,q,b,n ≥ 1, a strongly p^{n-1}-Mahlo cardinal κ, and a p,q,b-structure M*, where every element of N* is the value of a closed term in M*. Note that we must have b ≥ 2.

As in the development of section 4.2 after the proof of Lemma 4.2.7, we extend M* to the structure

$$M^{**} = (N^{**},<^{**},0^{**},1^{**},+^{**},f^{**},g^{**},c_0^{**},\ldots,c_\alpha^{**},\ldots), \alpha < \kappa.$$

We follow this prior development through the first line of the proof of Theorem 4.2.26.

Thus we have r ≥ 1, E ⊆ S ⊆ κ of order type ω, and sets E[1] ⊆ ... ⊆ E[n] ⊆ M**[S,r] such that

i. E[1] = {c_α**: α ∈ E}.
ii. For all 1 ≤ i < n, f**E[i] ⊆ E[i+1] ∪. g**E[i+1].

This construction of E ⊆ S ⊆ κ of order type ω uses that κ is strongly p^{n-1}-Mahlo.

In the proof of Theorem 4.2.26, we continued by transferring this situation back into N via an S,r(p+q)-embedding T from M** into M, thus establishing Proposition B with the sets TE[1] ⊆ ... ⊆ TE[n].

Here we want to merely transfer this situation back into M* via an S,r(p+q)-embedding from M** into M*, and then establish uniformities. By Lemma 4.2.12, we use the unique isomorphism from M**<S> onto M* which maps {c_α**: α ∈ S} onto {c_j*: j ≥ 0}.

As in section 4.2, for r ≥ 1, we write M*[r] for the set of all values of closed terms of length ≤ r in M*.

Thus we obtain r ≥ 1 and infinite sets D[1] ⊆ ... ⊆ D[n] ⊆ M*[r] such that

iii. D[1] ⊆ {c_j*: j ≥ 0}.
iv. For all 1 ≤ i < n, f*D[i] ⊆ D[i+1] ∪. g*D[i+1].

We summarize this modified development as follows.

LEMMA 4.4.1. Let p,q,b,n ≥ 1. The following is provable in SMAH. Let M* = (N*,0*,1*,<*,+*,f*,g*,c_0*,...) be a p,q,b-structure. There exist r ≥ 1 and infinite sets D[1] ⊆ ... ⊆ D[n] ⊆ M*[r] such that D[1] ⊆ {c_j*: j ≥ 0}, and for all 1 ≤ i < n, f*D[i] ⊆ D[i+1] ∪. g*D[i+1]. Furthermore, this entire Lemma, starting with "Let p...", is provable in RCA_0.

Proof: Let p,q,b,n,M* be as given. Proceed as discussed above. One of the important points is that we only need M* = (N*,0*,1*,<*,+*) to obey the axioms for a discretely ordered commutative group. QED

By using Lemma 4.4.1, we will no longer need to refer back to section 4.2.

We can obviously view clauses 3-7 in the definition of p,q,b-structure as universal axioms. Recall that b is a standard integer.

We now introduce the notion of p,q,b;r-structure, which is a level r approximation to a p,q,b-structure.

DEFINITION 4.4.4. Let p,q,b,r ≥ 1. A p,q,b;r-structure is a system of the form

M* = (N*,0*,1*,<*,+*,f*,g*,c_0*,...)

such that the following holds.

a. Clauses 1,2,3 in the definition of p,q,b-structure, without change.
b. All instantiations of the universal sentences under clauses 4-7, by closed terms of length ≤ r. Here length counts the total number of occurrences of constant and function symbols that appear.

In particular, we are using the following specialization of clause 7 in the definition of p,q,b-structure:

7'. The c*'s form a strictly increasing set of indiscernibles for the atomic sentences of M* whose terms are of length ≤ r.

Again, we do not require that every element of N* be the value of a closed term.

DEFINITION 4.4.5. A p,q,b;r;n-special structure is a p,q,b;r-structure M* where there exist infinite $D_1 \subseteq \ldots \subseteq D_n \subseteq M^*[r/(p+q)]$ such that
i. For all $1 \leq i < n$, $f^*D_i \subseteq D_{i+1} \cup. g^*D_{i+1}$.
ii. $D_1 \subseteq \{c_j{:}^*\ j \geq 0\}$.

We use M*[r/(p+q)] instead of M*[r] since in clause i, we are applying f*,g* to p,q, terms, respectively, and want all relevant terms to have length at most r.

DEFINITION 4.4.6. The r-type of a p,q,b;r-structure M* is the set of all closed atomic sentences, whose terms have length ≤ r, involving only the constants $0,1,c_0,\ldots,c_{2r}$, which hold in M*. Thus r-types are finite sets.

DEFINITION 4.4.7. A p,q,b;r-type is the r-type of a p,q,b;r-structure. A p,q,b;r;n-special type is the r-type of a p,q,b;r;n-special structure.

LEMMA 4.4.2. Let M* be a p,q,b;r-structure. Then M* is a p,q,b;r;n-special structure if and only if the r-type of M* is a p,q,b;r;n-special type.

Proof: Let M* be a p,q,b;r-structure. First suppose that M* is a p,q,b;r;n-special structure. Then by definition, the r-type of M* is a p,q,b;r;n-special type.

Conversely, suppose the r-type **τ** of M* is a p,q,b;r;n-special type. Let M*′ be a p,q,b;r;n-special structure of r-type **τ**.

Let $D_1 \subseteq \ldots \subseteq D_n \subseteq M^{*\prime}[r/(p+q)]$ be infinite, where
i. For all $1 \leq i < n$, $f^*D_i \subseteq D_{i+1} \cup. g^*D_{i+1}$.
ii. $D_1 \subseteq \{c_j{}^*{:}\ j \geq 0\}$.

We can obviously come up with an infinite list of atomic sentences whose terms are of length ≤ r, whose truth in M*′ witnesses that M*′ is a p,q,b;r;n-special structure. These include the atomic sentences with terms of length ≤ r that justify that M*' is a p,q,b;r-structure, and the atomic sentences with terms of length ≤ r that justify the special clauses i,ii just above. This uses the fact that the lengths of $f(s_1,\ldots,s_p)$, $g(t_1,\ldots,t_q)$ are ≤ r provided the lengths of $s_1,\ldots,s_p,t_1,\ldots,t_q$ are ≤ r/(p+q). But since M* and M*′ have the same r-type, they agree on all such statements. Hence M* is a p,q,b;r;n-special structure. QED

We can view the following as a uniform version of Lemma 4.4.1.

LEMMA 4.4.3. Let p,q,b,n ≥ 1. The following is provable in SMAH. There exist r ≥ 1 such that every p,q,b;r-structure is p,q,b;r;n-special. Furthermore, this entire Lemma, starting with "Let p..." is provable in RCA_0.

Proof: Fix p,q,b,n ≥ 1. We now argue in SMAH. Suppose this is false. Let T be the following theory in the language of p,q,b-structures.

i. Let r ≥ 1. Assert the axioms for being a p,q,b;r-structure.
ii. Let r ≥ 1 and **τ** be a p,q,b;r;n-special type. Assert that **τ** is not the r-type of the p,q,b;r-structure.

We claim that every finite subset of T is satisfiable. To see this, let r be an upper bound on the r's used in the finite subset. By hypothesis, there exists a p,q,b;r-structure M* that is not a p,q,b;r;n-special structure. Fix r,M*.

We claim that M* satisfies the finite subset of T. Let **τ** be the r-type of the p,q,b;r-structure M*.

Obviously M* satisfies all instances of i) for r′ ≤ r. Now let 1 ≤ r′ ≤ r and **τ**′ be a p,q,b;r′;n-special type. Suppose that **τ**′ is the correct r′-type of M*. I.e., M* has r′-type **τ**′. By Lemma 4.4.2, M* is a p,q,b;r′;n-special structure. Since M* is a p,q,b;r-structure, M* is a p,q,b;r;n-special structure. This is a contradiction.

By the compactness theorem, T is satisfiable. Let M* satisfy T. By Lemma 4.4.1, let r be such that M* is p,q,b;r;n-special. Let **τ** be the r-type of M*. Then **τ** is a p,q,b;r;n-special type. By axioms ii) above, **τ** is not the r-type of M*. This is a contradiction. QED

LEMMA 4.4.4. There is a presentation of a primitive recursive function Q(p,q,b,r,**τ**) such that the following is provable in RCA_0. Q(p,q,b,r,**τ**) = 1 if and only if **τ** is a p,q,b;r-type (as a Gödel number).

Proof: We give the following necessary and sufficient finitary condition for **τ** to be a p,q,b;r-type.

1. τ is a set of atomic sentences in $0,1,<,+,f,g,c_0,...,c_{2r}$ whose terms have length $\leq r$, involving only the constants $0,1,c_0,...,c_{2r}$.

2. There is a system $V^* = (D,E,0^*,1^*,<^*,+^*,f^*,g^*,c_0^*,...,c_{2r}^*)$ which obeys the following conditions.

i. D,E have cardinality at least 1 and at most some specific iterated exponential in p,q,r.
ii. $0^*,1^* \in D$.
iii. $+^*:D^2 \to E$.
iv. $f^*:D^p \to E$.
v. $g^*:D^q \to E$.
vi. D is the set of values of the closed terms of length $\leq$ r.
vii. E is D union the values of $+^*,f^*,g^*$.
vii. All axioms in clause b in the definition of p,q,b;r-structure hold in V*.
viii. All sentences in τ hold in V*.
ix. All atomic sentences in $0,1,<,+,f,g,c_0,...,c_{2r}$ outside τ, with terms of length $\leq$ r, fail in V*.

This condition is necessary because such a structure V* can be obtained from any p,q,b;r-structure M* of r-type τ by taking D to be the set of values of closed terms in M* of length $\leq$ r, restricting M* in the obvious way. The atomic sentences in $0,1,<,+,f,g,c_0,...,c_{2r}$ that hold in V* are the same as those that hold in M*, which are the elements of τ.

For the other direction, let τ,V* be given as above. Using the indiscernibility in ix, we can canonically stretch V* to

$$W^* = (D',E',0^*,1^*,<^{*\prime},+^{*\prime},f^{*\prime},g^{*\prime},c_0^{*\prime},c_1^{*\prime},...)$$

which obviously obeys clause 1 and clauses 2i-2ix above, modified to incorporate all constant symbols $c_0,c_1,...$. We now have all of the conditions we need for being a p,q,b;r-structure except that we only have $D' \subseteq E'$. However, this is easily remedied without affecting the properties of W* by taking the domain to be E', and extending $+^{*\prime},f^{*\prime},g^{*\prime}$ arbitrarily to the tuples from E' that are not tuples from D', into E'. This resulting modification of W* is a p,q,b,r-structure with r-type τ. QED

Let τ be a p,q,b;r-type. We want to express

1) τ is a p,q,b;r;n-special type

as a sentence $\lambda(k,n,p+q+2,R_1,...,R_{n-1})$ of section 4.3, and then apply Theorem 4.3.8.

Recall that 1) is equivalent to the condition

2) there exists a p,q,b;r-structure M* of r-type τ and infinite sets $D_1 \subseteq ... \subseteq D_n \subseteq M^*[r/(p+q)]$ such that
i. For all $1 \leq i < n$, $f^*D_i \subseteq D_{i+1} \cup. g^*D_{i+1}$.
ii. $D_1 \subseteq \{c_j^*: j \geq 0\}$.

We now put this in a more syntactic form.

DEFINITION 4.4.8. A p,q,r-term is a closed term in 0,1,+,f,g and constants $c_0,c_1,...$ of length at most r.

We identify M*[r] with the set of all p,q,r-terms. Of course, a given element of M*[r] may be the value of many p,q,r-terms.

DEFINITION 4.4.9. We let τ^* be the set of all atomic sentences obtained from elements of τ by replacing c's by c's in an order preserving way.

3) there exist infinite sets $T_1 \subseteq ... \subseteq T_n$ of p,q,r/(p+q)-terms such that
i. For any two distinct elements t,t' of T_n, $t = t' \notin \tau^*$.
ii. Every $t \in T_1$ is some c_k.
iii. Let $1 \leq i < n$ and $t_1,...,t_p \in T_i$. Then there exists $t \in T_{i+1}$ such that $f(t_1,...,t_p) = t \in \tau^*$, or there exist $t_1',...,t_q' \in T_{i+1}$ such that $f(t_1,...,t_p) = g(t_1',...,t_q') \in \tau^*$.
iv. Let $t,t_1,...,t_q \in T_n$. Then $g(t_1,...,t_q) = t \notin \tau^*$.
v. For all $k \geq 0$ and $t_1,...,t_p \in T_n$, $f(t_1,...,t_p) = c_k \notin \tau^*$.

LEMMA 4.4.5. The following is provable in RCA_0. Let $p,q,b,n,r \geq 1$ and τ be a p,q,b;r-type. Then conditions 1)-3) are equivalent.

Proof: Let τ be a p,q,b;r-type. It is obvious that 1),2) are equivalent. So assume 2) holds. We derive 3). Let M* be a p,q,b;r-structure of r-type τ, and $D_1 \subseteq ... \subseteq D_n \subseteq M^*[r/(p+q)]$ be infinite sets such that

i. For all $1 \leq i < n$, $fD_i \subseteq D_{i+1} \cup. gD_{i+1}$.
ii. $D_1 \subseteq \{c_j^*: j \geq 1\}$.

For each $x \in D_n$, pick a p,q,r/(p+q)-term x# of least possible length whose value in M* is x. If x is some c_i* then make sure that x# is c_i. Set T_i = {x#: $x \in D_i$}.

Since $D_1 \subseteq ... \subseteq D_n$, clearly $T_1 \subseteq ... \subseteq T_n$. Since every $x \in D_n$ lies in M*[r/(p+q)], clearly every x# $\in T_n$ has length ≤ r/(p+q).

Let t,t' $\in T_n$ be distinct. Write t = x#, t' = y#. Then x# ≠ y#, and so t = t' is false. Hence t = t' $\notin$ **τ***. Let $t \in T_1$. Write t = x#, $x \in D_1$. Then x is some c_k*. Therefore x# = c_k. This establishes 3i and 3ii.

To verify 3iii, let 1 ≤ i < n and x_1#,...,x_p# $\in T_i$. Then $x_1,...,x_p \in D_i$. Hence f*($x_1,...,x_p$) $\in$ f*$D_i \subseteq D_{i+1}$ ∪. g*D_{i+1}.

case 1. f*($x_1,...,x_p$) $\in D_{i+1}$. Let the p,q,r/(p+q)-term t $\in T_{i+1}$ have the value f*($x_1,...,x_p$) in M*. Then f(x_1#,...,x_p#) = t holds in M*, and both terms in this equation have length ≤ r. Hence f(x_1*,...,x_p*) = t $\in$ **τ***.

case 2. f*($x_1,...,x_p$) $\in$ gD_{i+1}. Let f*($x_1,...,x_p$) = g*($y_1,...,y_q$), where $y_1,...,y_q \in D_{i+1}$. Then y_1#,...,y_q# $\in T_{i+1}$. Also f(x_1*,...,x_p*) = g(y_1*,...,y_q*) holds in M*, and both terms in this equation have length ≤ r. Hence f(x_1*,...,x_p*) = g(y_1*,...,y_q*) $\in$ **τ***.

To verify 3iv, let x#,x_1#,...,x_q# $\in T_n$. Then g(x_1#,...,x_q#) = x# $\notin$ **τ*** because g*($x_1,...,x_q$) ≠ x in M*.

To verify 3v, let k ≥ 0 and x_1#,...,x_p# $\in T_n$. Then f(x_1#,...,x_p#) = c_k $\notin$ **τ*** because f*($x_1,...,x_p$) ≠ c_k* in M*.

Now assume that 3) holds. We establish 2). Let $T_1 \subseteq ... \subseteq T_n$ be infinite sets of p,q,r/(p+q)-terms such that

i. For any two distinct elements t,t' of T_n, t = t' $\notin$ **τ***.
ii. For all $t \in T_1$ there exists k ≥ 0 such that t is c_k.
iii. Let 1 ≤ i < n and $t_1,...,t_p \in T_i$. Then there exists t $\in T_{i+1}$ such that f($t_1,...,t_p$) = t $\in T_{i+1}$, or there exist $t_1',...,t_q' \in T_{i+1}$ such that f($t_1,...,t_p$) = g($t_1',...,t_q'$) $\in$ **τ***.
iv. Let t,$t_1,...,t_q \in T_n$. Then g($t_1,...,t_q$) = t $\notin$ **τ***.
v. For all k ≥ 0 and $t_1,...,t_p \in T_n$, f($t_1,...,t_p$) = c_k $\notin$ **τ***.

Let M* be any p,q,b;r-structure of r-type **τ**. For each 1 ≤ i ≤ n, let D_i be the set of values of terms in T_i. Then $D_1 \subseteq ... \subseteq D_n \subseteq$ M*[r/(p+q)].

Let $1 \leq i < n$ and $x \in f^*D_i$. We claim that $x \in D_{i+1} \cup g^*D_{i+1}$.

To see this, write $x = f^*(x_1,\ldots,x_p)$, $x_1,\ldots,x_p \in D_i$, and let $t_1,\ldots,t_p \in T_i$ have values $x_1,\ldots,x_p$, respectively. By 3iii, let $t \in T_{i+1}$, where $f(t_1,\ldots,t_p) = t \in \tau^*$, or there exists $t_1',\ldots,t_q' \in T_{i+1}$ such that $f(t_1,\ldots,t_p) = g(t_1',\ldots,t_q') \in \tau^*$.

case 1. $f(t_1,\ldots,t_p) = t \in \tau^*$. Then $f^*(x_1,\ldots,x_p) = x \in D_{i+1}$.

case 2. Let $t_1',\ldots,t_q' \in T_{i+1}$, where $f(t_1,\ldots,t_p) = g(t_1',\ldots,t_q') \in \tau^*$. Let the values of $t_1',\ldots,t_q'$ be $y_1,\ldots,y_q \in D_{i+1}$, respectively. Then $f^*(x_1,\ldots,x_p) = g^*(y_1,\ldots,y_q)$.

Now suppose $x \in D_{i+1} \cap gD_{i+1}$. Let x be the value of $t \in T_{i+1}$, and write $x = g(y_1,\ldots,y_q)$, $y_1,\ldots,y_q \in D_{i+1}$. Let $t_1,\ldots,t_q \in T_{i+1}$ have values $y_1,\ldots,y_q$, respectively. By 3iv, $g(t_1,\ldots,t_q) = t \notin \tau^*$. Since both terms in this equation have length $\leq r$, we see that $g(t_1,\ldots,t_q) = t$ is false in M^*. Hence $g^*(y_1,\ldots,y_q) \neq x$. This is a contradiction.

Finally, let $x \in D_1$. Then x is the value of a term $t \in T_1$. By 3ii, t is some c_k. Hence x is some c_k^*. QED

We can conveniently represent the p,q,r-terms as elements of N^k in the following way. This integer k will be set below.

DEFINITION 4.4.10. Two p,q,r-terms have the same shape if and only if the second can be obtained from the first by replacing c's by c's, where we do not require that equal c's be replaced by equal c's.

Let e be the number of shapes of the p,q,r-terms.

We represent the p,q,r-term σ as follows. Let the shape of σ be $1 \leq i \leq e$. Here the shapes have been arbitrarily indexed without repetition, by $1 \leq i \leq e$.

DEFINITION 4.4.9. The representations of σ are obtained as follows. First write down a sequence of e elements of N, where exactly i of these elements are the same as the first of these elements. Follow this by the sequence of subscripts of the c's that appear from left to right. If this sequence of c's is of length < r then fill it out to length r by repeating the last argument. This results in a representation of σ as an element of N^{e+r}. Obviously, σ will have infinitely many representations.

Set k = e+r. We will use the above representation of p,q,r-terms to write 3) in the form of a sentence $\lambda(k,n,p+q+2,R_1,...,R_{n-1})$, as in section 4.3.

4) There exist infinite sets $B_1 \subseteq ... \subseteq B_n \subseteq N^k$ of p,q,r/(p+q)-representations such that
a. Distinct elements of B_n represent distinct p,q,r/(p+q)-terms.
b. For each $1 \leq i \leq n$, let T_i be the p,q,r/(p+q)-terms represented by the elements of B_i. Then $T_1,...,T_n$ obeys 3) above.

Note the use of τ* in 3). We represent elements of τ* as a p,q,r-representation followed by two equal elements of N (indicating <), or followed by two unequal elements of N (indicating =), followed by a p,q,r-representation. Keep in mind that the lengths of p,q,r-representations are fixed at k = e+r. Hence representations of elements of τ* are fixed at length k+2+k = 2k+2. If τ is a p,q,b;r-type, then τ is finite and τ* is order invariant.

LEMMA 4.4.6. The following is provable in RCA_0. Let p,q,b,n,r ≥ 1 and τ be a p,q,b;r-type. Conditions 1)-4) are each equivalent to $\lambda(k,n,p+q+2,R_1,...,R_{n-1})$, for some order invariant relations $R_1,...,R_{n-1} \subseteq N^{2k(p+q+2)}$ obtained explicitly from p,q,b,n,r,τ.

Proof: We argue in RCA_0. Let p,q,b,n,r ≥ 1 and τ be a p,q,b;r-type. It is clear that 3) is equivalent to 4), and hence by Lemma 4.4.5, 1)-4) are equivalent. We now exclusively use clause 4.

$B_1 \subseteq ... \subseteq B_n$ asserts, for each $1 \leq i < n$, that $(\forall x \in B_i)(\exists y \in B_{i+1})(x = y)$.

"Distinct elements of B_n represent distinct p,q,r/(p+q)-terms" is of the form $(\forall x,y \in B_n)(S(x,y))$.

"Distinct elements t,t' of the corresponding T_n have $t = t' \notin \tau^*$" is of the form $(\forall x,y \in B_n)(S(x,y))$.

Clause 3ii for the corresponding T_1 is of the form $(\forall x \in B_1)(S(x))$.

Clause 3iii for the corresponding T's is of the form $(\forall i \in [1,n))(\forall x_1,\ldots,x_p \in B_i)(\exists y_1,\ldots,y_q \in B_{i+1})(S(x_1,\ldots,x_p, y_1,\ldots,y_q))$.

Clause 3iv for the corresponding T_n is of the form $(\forall x_1,\ldots,x_{q+1} \in B_n)(S(x_1,\ldots,x_{q+1}))$.

Clause 3v for the corresponding T_n is of the form $(\forall x_1,\ldots,x_{p+1} \in B_n)(S(x_{p+1}) \rightarrow S'(x_1,\ldots,x_{p+1}))$.

Here all the S's are order invariant relations. QED

LEMMA 4.4.7. There is a presentation of a primitive recursive function H such that the following is provable in ACA'. Let $p,q,b,n,r \geq 1$ and τ be a p,q,b;r-type. Then $H(p,q,b,r,n,\tau) = 1$ if and only if τ is a p,q,b;r;n-special type (as a Gödel number).

Proof: Let p,q,b,r,n,τ be given, where τ is a p,q,b;r-type. Apply Lemma 4.4.6 to obtain order invariant $R_1,\ldots,R_{n-1}$. Now apply Theorem 4.3.8. QED

We fix H as given by Lemma 4.4.7.

LEMMA 4.4.8. Let $p,q,b,n \geq 1$. The following is provable in SMAH. $(\exists r)(\forall \tau)(Q(p,q,b,r,\tau) = 1 \rightarrow H(p,q,b,r,n,\tau) = 1)$. Furthermore, this entire Lemma, starting with "Let p...", is provable in RCA_0.

Proof: Let p,q,b,n be as given. By Lemma 4.4.3, SMAH proves the existence of $r \geq 1$ such that every p,q,b;r-type is a p,q,b;r;n-special type. Now apply Lemmas 4.4.4 and 4.4.7. QED

LEMMA 4.4.9. RCA_0 + 1-Con(SMAH) proves $(\forall p,q,b,n \geq 1)(\exists r)(\forall \tau)(Q(p,q,b,r,\tau) = 1 \rightarrow H(p,q,b,r,n,\tau) = 1)$.

Proof: We argue within RCA_0 + 1-Con(SMAH). Let $p,q,b,n \geq 1$ be given. By Lemma 4.4.8,

1) $(\exists r)(\forall \tau)(Q(p,q,b,r,\tau) = 1 \rightarrow H(p,q,b,r,n,\tau) = 1)$

is provable in SMAH. Note that the quantifier $\forall\tau$ in 1) is bounded. Hence by 1-Con(SMAH), this Σ^0_1 sentence is true. QED

LEMMA 4.4.10. The following is provable in ACA' + 1-Con(SMAH). $(\forall p,q,b,n \geq 1)(\exists r)(\forall \tau)(\tau$ is a p,q,b;r-type $\rightarrow \tau$ is a p,q,b;r;n-special type).

Proof: By Lemmas 4.4.4, 4.4.7, and 4.4.9. QED

For Propositions C,D, see Appendix A.

THEOREM 4.4.11. Propositions A,B,C,D are provable in ACA' + 1-Con(SMAH).

Proof: Propositions A,C,D are immediate consequences of Proposition B over RCA_0 (see Lemmas 4.2.1 and 5.1.1). We argue in ACA' + 1-Con(SMAH). Let $p,q,b,n \geq 1$, and $f \in ELG(p,b)$, $g \in ELG(q,b)$. Let r be given by Lemma 4.4.10. By Ramsey's theorem for 2r-tuples in ACA', we can find a p,q,b;r-structure $M = (N,0,1,<,+,f,g,c_0,c_1,...)$. Let τ be its r-type. By Lemma 4.4.10, τ is a p,q,b;n;r-special type. By Lemma 4.4.2, M is a p,q,b;r;n-special structure. Let $D_1 \subseteq ... \subseteq D_n \subseteq N$, where $D_1 \subseteq \{c_0,c_1,...\}$, and each $fD_i \subseteq D_{i+1} \cup. gD_{i+1}$, and $D_1 \cap fD_n = \emptyset$. This is Proposition B, thus concluding the proof. QED

CHAPTER 5
INDEPENDENCE OF EXOTIC CASE

5.1. Proposition C and length 3 towers.

In sections 5.1 - 5.9 we show that Proposition A implies the 1-consistency of SMAH (ZFC with strongly Mahlo cardinals of every specific finite order). The derivation is obviously conducted in ZFC. With some detailed examination, we see that this derivation can be carried out in the system ACA' used in Chapter 4. For a detailed discussion of RCA_0 and other subsystems of second order arithmetic, see [Si99].

We actually show that the specialization of Proposition A to rather concrete functions implies the 1-consistency of SMAH.

We use the following very basic functions on the set of all nonnegative integers N.

DEFINITION 5.1.1. We define +,-,•,↑,log as follows.
1. Addition. x+y is the usual addition.
2. Subtraction. Since we are in N, x-y is defined by the usual x-y if x ≥ y; 0 otherwise.
3. Multiplication. x•y is the usual multiplication.
4. Base 2 exponentiation. x↑ is the usual base 2 exponentiation.
5. Base 2 logarithm. Since we are in N, log(x) is the floor of the usual base 2 logarithm, with log(0) = 0.

DEFINITION 5.1.2. TM(0,1,+,-,•,↑,log) is the set of all terms built up from 0,1,+,-,•,↑,log, and variables $v_1,v_2,...$.

DEFINITION 5.1.3. Each t ∈ TM(0,1,+,-,•,↑,log) gives rise to infinitely many functions, one of each arity that is at least as large as all subscripts of variables appearing in t, as follows. Let the variables of t be among $v_1,...,v_k$, $k \geq 1$. Then we associate the function $f:N^k \to N$ given by

$$f(v_1,...,v_k) = t(v_1,...,v_k)$$

where t is interpreted according to Definition 5.1.1.

DEFINITION 5.1.4. BAF (basic functions) is the set of all functions given by terms in 0,1,+,-,•,↑,log, according to Definition 5.1.3.

It is very convenient to extend TM(0,1,+,-,•,↑,log) with definition by cases, to get an alternative description of BAF.

DEFINITION 5.1.5. ETM(0,1,+,-,•,↑,log) is the set of "extended terms" of the following form:

$$\begin{array}{c} t_1 \text{ if } \varphi_1; \\ t_2 \text{ if } \varphi_2 \wedge \neg\varphi_1; \\ \ldots \\ t_n \text{ if } \varphi_n \wedge \neg\varphi_1 \wedge \ldots \wedge \neg\varphi_{n-1}; \\ t_{n+1} \text{ if } \neg\varphi_1 \wedge \ldots \wedge \neg\varphi_n. \end{array}$$

where $n \geq 1$, each $t_i \in TM(0,1,+,-,\bullet,\uparrow,\log)$, and each φ_i is a propositional combination of atomic formulas of the forms $s < t$, $s = t$, where $s,t \in TM(0,1,+,-,\bullet,\uparrow,\log)$.

DEFINITION 5.1.6. As in Definition 5.1.3, each $t \in ETM(0,1,+,-,\bullet,\uparrow,\log)$ gives rise to infinitely many functions, one of each arity at least as large as all subscripts of variables appearing in t.

DEFINITION 5.1.7. EBAF (extended basic functions) is the set of all functions arising in this manner from $ETM(0,1,+,-,\bullet,\uparrow,\log)$.

We now show that EBAF = BAF.

DEFINITION 5.1.8. We use L for the language in first order predicate calculus with equality based on the nonlogical symbols $<,0,1,+,-,\bullet,\uparrow,\log$.

Thus $TM(0,1,+,-,\bullet,\uparrow,\log)$ is the set of all terms in L. Also the formulas φ_i used in the extended terms above are exactly the quantifier free formulas in L.

LEMMA 5.1.1. BAF $\subseteq$ EBAF.

Proof: Let $t \in TM(0,1,+,-,\bullet,\uparrow,\log)$, whose variables are among $v_1,\ldots,v_k$, $k \geq 1$. The function $f(v_1,\ldots,v_k) = t(v_1,\ldots,v_k)$ is also defined by

$$\begin{array}{c} t \text{ if } v_1 = v_1; \\ t \text{ if } \neg v_1 = v_1. \end{array}$$

which places f in EBAF. QED

LEMMA 5.1.2. The following functions lie in BAF.
i. $neg(x) = 1$ if $x = 0$; 0 otherwise.
ii. $\alpha(x) = 1$ if $x \geq 1$; 0 otherwise.
iii. $conj(x,y) = 1$ if $x \geq 1 \wedge y \geq 1$; 0 otherwise.
iv. $disj(x,y) = 1$ if $x \geq 1 \vee y \geq 1$; 0 otherwise.
v. $les(x,y) = 1$ if $x < y$; 0 otherwise.
vi. $eq(x,y) = 1$ if $x = y$; 0 otherwise.

Proof: Note that

$$neg(x) = 1-x.$$
$$\alpha(x) = 1-(1-x).$$
$$conj(x,y) = \alpha(x)\bullet\alpha(y).$$
$$disj(x,y) = neg(conj(neg(x),neg(y)).$$
$$les(x,y) = \alpha(y-x).$$
$$eq(x,y) = 1-((x-y)+(y-x)).$$

QED

LEMMA 5.1.3. Let φ be a quantifier free formula in L whose variables are among $v_1,\ldots,v_k$, $k \geq 1$. Then the function $f_\varphi(x_1,\ldots,x_k) = 1$ if $\varphi(x_1,\ldots,x_k)$; 0 otherwise, lies in BAF.

Proof: Fix $k \geq 1$. We can assume that φ uses only the connectives $\neg,\wedge$. We prove this by induction on φ obeying the hypotheses.

case 1. φ is $s = t$. Then $f_\varphi(v_1,\ldots,v_k) = eq(s(v_1,\ldots,v_k),t(v_1,\ldots,v_k))$.
case 2. φ is $s < t$. Then $f_\varphi(v_1,\ldots,v_k) = les(s(v_1,\ldots,v_k),t(v_1,\ldots,v_k))$.
case 3. φ is $\neg\psi$. Then $f_\varphi(v_1,\ldots,v_k) = neg(f_\psi(v_1,\ldots,v_k))$.
case 4. φ is $\psi \wedge \rho$. Then $f_\varphi(v_1,\ldots,v_k) = conj(f_\psi(v_1,\ldots,v_k),f_\rho(v_1,\ldots,v_k))$.

By Lemmas 5.1.1, 5.1.2, and the induction hypothesis, in each case the function constructed lies in BAF. QED

THEOREM 5.1.4. EBAF = BAF.

Proof: By Lemma 5.1.1, it suffices to prove EBAF $\subseteq$ BAF. Now let $f:N^k \rightarrow N$ be the function in EBAF given by $f(v_1,\ldots,v_k) =$

$$t_1 \text{ if } \varphi_1;$$
$$t_2 \text{ if } \varphi_2 \wedge \neg\varphi_1;$$
$$\ldots$$
$$t_n \text{ if } \varphi_n \wedge \neg\varphi_1 \wedge \ldots \wedge \neg\varphi_{n-1};$$
$$t_{n+1} \text{ if } \neg\varphi_1 \wedge \ldots \wedge \neg\varphi_n.$$

where the variables in $t_1,\ldots,t_{n+1},\varphi_1,\ldots,\varphi_{n+1}$ are among $x_1,\ldots,x_k$, $k \geq 1$.

Then $f:N^k \rightarrow N$ is given by $f(v_1,\ldots,v_k) =$

$$f_{\varphi\_1}\bullet t_1 + \ldots + f_{\varphi\_n\wedge\neg\varphi\_1\wedge\ldots\wedge\neg\varphi\_n-1}\bullet t_n + f_{\neg\varphi\_1\wedge\ldots\wedge\neg\varphi\_n}\bullet t_{n+1}$$

using the notation of Lemma 5.1.3, with + associated to the left. Hence f ∈ BAF by Lemma 5.1.3. QED

It is useful to know that certain functions lie in BAF. The powers of 2 are taken to be the integers 1,2,4,... .

THEOREM 5.1.5. The following functions lie in BAF.
i. All constant functions of every arity.
ii. n^x, where n is a given power of 2.
iii. The greatest power of 2 that is ≤ x if x > 0; 0 otherwise.

Proof: i. This is obvious using the term 1+...+1.
ii. Let $n = 2^k$, k ≥ 0. Write $n^x = 2^{kx}$ = (kx)↑ = (x+...+x)↑.
iii. log(x)↑ is the greatest power of 2 that is ≤ x if x > 0; 1 otherwise. To fix this, take log(x)↑-(1-x).

QED

In this Chapter, we will show that the following specialization of Proposition A to these rather concrete functions implies the consistency of SMAH. Specifically,

PROPOSITION C. For all f,g ∈ ELG ∩ SD ∩ BAF, there exist A,B,C ∈ INF such that

A ∪. fA ⊆ C ∪. gB
A ∪. fB ⊆ C ∪. gC.

We have carefully chosen BAF so that we can choose A,B,C to be (primitive) recursive sets. Accordingly, Proposition C becomes an explicitly Π^0_3 sentence. See Theorem 6.2.20.

We use ELG ∩ SD ∩ BAF instead of ELG ∩ BAF because expansive linear growth is an asymptotic condition, and so ELG ∩ BAF is not included in SD. In BRT, the best course is to include both asymptotic and non asymptotic classes, as they behave differently. E.g., A ∪. fA = U is correct in EBRT in A,fA on SD, but incorrect in EBRT in A,fA on ELG. The function f(x) = 2n, which lies in ELG\SD, is a counterexample.

In the remainder of this chapter, we will assume Proposition C. Our aim is to construct a model of the system

SMAH = ZFC + $\{$there exists a strongly k-Mahlo cardinal$\}_k$.

Our construction will take place well within ZFC. (In section 5.9, we will analyze just what axioms are used for this entire development.) This will establish that none of Propositions A,B,C are provable in SMAH, provided SMAH is consistent. For otherwise, SMAH would prove its own consistency, and hence would be inconsistent by Gödel's second incompleteness theorem.

DEFINITION 5.1.9. The $\Pi^0_1(L)$ sentences are the sentences in L which begin with zero or more universal quantifiers, followed by a formula ψ in which all quantifiers are bounded. I.e., all quantifiers in ψ appear, in abbreviated form, as

$$(\forall x < t)$$
$$(\exists x < t)$$

where x is a variable, t is a term in which x does not appear, and where the intended range of all variables is N.

DEFINITION 5.1.10. We use $TR(\Pi^0_1,L)$ for the set of all $\Pi^0_1(L)$ sentences that are true in N, using the interpretation in Definition 5.1.1.

We will actually establish a stronger result. Using Proposition C, we will construct a model of the system

$$SMAH + TR(\Pi^0_1,L).$$

Strictly speaking, Π^0_1 sentences are obviously not in the language of set theory. However, in weak fragments of set theory, there is the standard version of $N,<,0,1,+,\bullet,\uparrow,\log$, where N is the set theoretic ω, 0 is $\emptyset$, 1 is $\{\emptyset\}$, and $<,+,-,\bullet,\uparrow,\log$ are treated as sets of 2-tuples, 3-tuples, 3-tuples, 3-tuples, 2-tuples, and 2-tuples, respectively.

Accordingly, we view the system $SMAH + TR(\Pi^0_1,L)$ as a set theory that extends the system SMAH. The axioms of $SMAH + TR(\Pi^0_1,L)$ do not form a recursive set. However, this will not cause any difficulties.

DEFINITION 5.1.11. For $x \in N^r$, $|x|$ denotes the maximum term of x.

DEFINITION 5.1.12. For $E \subseteq N$, we write E^* for $E\backslash\{\min(E)\}$. If $E = \emptyset$ then we take $E^* = \emptyset$.

The reader should not confuse our E^* with the set of all finite sequences from E.

Recall Definition 1.1.3.

DEFINITION 5.1.13. For $S \subseteq N$ and $p,q \in N$, we define

$$pS+q = \{pn+q: n \in S\}.$$

LEMMA 5.1.6. Let $f,g \in ELG \cap SD \cap BAF$. There exist $f',g' \in ELG \cap SD \cap BAF$ such that the following holds. Let $S \subseteq N$.
i) $g'S = g(S^*) \cup 6S+2$;
ii) $f'S = f(S^*) \cup g'S \cup 6f(S^*)+2 \cup 2S^*+1 \cup 3S^*+1$.

Proof: Let $f,g \in ELG \cap SD \cap BAF$, where $f:N^p \to N$ and $g:N^q \to N$. We define $g':N^{q+1} \to N$ as follows. Let $x_1,\ldots,x_q,y \in N$.

case 1. $x_1,\ldots,x_q > y$. Set $g'(x_1,\ldots,x_q,y) = g(x_1,\ldots,x_q)$.

case 2. Otherwise. Set $g'(x_1,\ldots,x_q,y) = 6|x_1,\ldots,x_q,y|+2$.

We define $f':N^{5p+q+1} \to N$ as follows. Let $x_1,\ldots,x_{5p},y_1,\ldots,y_{q+1} \in N$.

case a. $|y_1,\ldots,y_{q+1}| = |x_1,\ldots,x_p| = |x_{p+1},\ldots,x_{2p}| = |x_{2p+1},\ldots,x_{3p}| = |x_{3p+1},\ldots,x_{4p}| = |x_{4p+1},\ldots,x_{5p}|$. Set $f'(x_1,\ldots,x_{5p},y_1,\ldots,y_{q+1}) = g'(y_1,\ldots,y_{q+1})$.

case b. $|y_1,\ldots,y_{q+1}| = |x_1,\ldots,x_p| = |x_{p+1},\ldots,x_{2p}| = |x_{2p+1},\ldots,x_{3p}| = |x_{3p+1},\ldots,x_{4p}| < \min(x_{4p+1},\ldots,x_{5p})$. Set $f'(x_1,\ldots,x_{5p},y_1,\ldots,y_{q+1}) = f(x_{4p+1},\ldots,x_{5p})$.

case c. $|y_1,\ldots,y_{q+1}| = |x_1,\ldots,x_p| = |x_{p+1},\ldots,x_{2p}| = |x_{2p+1},\ldots,x_{3p}| = |x_{4p+1},\ldots,x_{5p}| < \min(x_{3p+1},\ldots,x_{4p})$. Set $f'(x_1,\ldots,x_{5p},y_1,\ldots,y_{q+1}) = 6f(x_{3p+1},\ldots,x_{4p})+2$.

case d. $|y_1,\ldots,y_{q+1}| = |x_1,\ldots,x_p| = |x_{p+1},\ldots,x_{2p}| = |x_{3p+1},\ldots,x_{4p}| = |x_{4p+1},\ldots,x_{5p}| < \min(x_{2p+1},\ldots,x_{3p})$. Set $f'(x_1,\ldots,x_{35},y_1,\ldots,y_{q+1}) = 2|x_{2p+1},\ldots,x_{3p}|+1$.

case e. $|y_1,\ldots,y_{q+1}| = |x_1,\ldots,x_p| = |x_{2p+1},\ldots,x_{3p}| = |x_{3p+1},\ldots,x_{4p}| = |x_{4p+1},\ldots,x_{5p}| < \min(x_{p+1},\ldots,x_{2p})$. Set $f'(x_1,\ldots,x_{5p},y_1,\ldots,y_{q+1}) = 3|x_{p+1},\ldots,x_{2p}|+1$.

case f. Otherwise. Set $f'(x_1,\ldots,x_{5p},y_1,\ldots,y_{q+1}) = 2|x_1,\ldots,x_{5p},y_1,\ldots,y_{q+1}|+1$.

Note that in case 1, $|x_1,...,x_q,y| = |x_1,...,x_q|$. Also note that in cases a)-e),

$$|x_1,...,x_{5p},y_1,...,y_{q+1}| = |y_1,...,y_{q+1}|$$
$$|x_1,...,x_{5p},y_1,...,y_{q+1}| = |x_{4p+1},...,x_{5p}|$$
$$|x_1,...,x_{5p},y_1,...,y_{q+1}| = |x_{3p+1},...,x_{4p}|$$
$$|x_1,...,x_{5p},y_1,...,y_{q+1}| = |x_{2p+1},...,x_{3p}|$$
$$|x_1,...,x_{5p},y_1,...,y_{q+1}| = |x_{p+1},...,x_{2p}|$$

respectively. Hence f',g' ∈ ELG ∩ SD ∩ BAF.

Let S ⊆ N. From S, case 1 produces exactly g(S*). Case 2 produces exactly 6S+2. This establishes i).

Case a) produces exactly g'S. Case b) produces exactly f(S*). Case c) produces exactly 6f(S*)+2. Case d produces exactly 2S*+1. Case e produces exactly 3S*+1.

Case f) produces exactly 2S*+1 since 2min(S)+1 is not produced. This is because 2min(S)+1 can only be produced from case f) if all of the arguments are min(S), which can only happen under case a). This establishes ii). QED

LEMMA 5.1.7. Let f,g ∈ ELG ∩ SD ∩ BAF and rng(g) ⊆ 6N. There exist infinite A ⊆ B ⊆ C ⊆ N\{0} such that
i) fA ∩ 6N ⊆ B ∪ gB;
ii) fB ∩ 6N ⊆ C ∪ gC;
iii) fA ∩ 2N+1 ⊆ B;
iv) fA ∩ 3N+1 ⊆ B;
v) fB ∩ 2N+1 ⊆ C;
vi) fB ∩ 3N+1 ⊆ C;
vii) C ∩ gC = ∅;
viii) A ∩ fB = ∅.

Proof: Let f,g be as given. Let f',g' be given by Lemma 5.1.6. Let A,B,C ⊆ N be given by Proposition C for f',g'. We have

A ∪. f'A ⊆ C ∪. g'B
A ∪. f'B ⊆ C ∪. g'C.

Let n ∈ B. Then 6n+2 ∈ g'B ⊆ f'B, and so 6n+2 ∈ C ∨ 6n+2 ∈ g'C. Now 6n+2 ∉ C by C ∩ g'B = ∅. Hence 6n+2 ∈ g'C. By Lemma 5.1.6 i) and rng(g) ⊆ 6N, we have 6n+2 ∈ 6C+2. Therefore n ∈ C. So we have established that B ⊆ C.

Let n ∈ A. Then n ∈ C ∨ n ∈ g'B. Now n ∉ f'B by A ∩ f'B = ∅. Also g'B ⊆ f'B. Hence n ∉ g'B, n ∈ C. Also 6n+2 ∈ g'A ⊆

f'A, and so 6n+2 ∈ C ∨ 6n+2 ∈ g'B. Since n ∈ C, we have 6n+2 ∈ g'C. By C ∩ g'C = ∅, we have 6n+2 ∉ C. Hence 6n+2 ∈ g'B. Since rng(g) ⊆ 6N, we have 6n+2 ∈ 6B+2. Hence n ∈ B. So we have established that A ⊆ B.

We have thus shown that A ⊆ B ⊆ C ⊆ N.

We now verify all of the required conditions i)-viii) above using the three sets A*,B*,C*.

Firstly note that A* ⊆ B* ⊆ C* ⊆ N\{0}. To see this, let n ∈ A*. Then n ∈ A ∧ n > min(A). Hence n ∈ B ∧ n > min(B), and so n ∈ B*. By the same argument, n ∈ B* → n ∈ C*.

We now claim that A* ∩ f(B*) = ∅. This follows from A* ⊆ A and f(B*) ⊆ f'B.

Next we claim that C* ∩ g(C*) = ∅. This follows from C* ⊆ C and g(C*) ⊆ g'C.

Now we claim that f(A*) ∩ 6N ⊆ B* ∪ g(B*). To see this, let n ∈ f(A*) ∩ 6N. Then n ∈ f'A. Hence n ∈ C ∪ g'B.

case 1. n ∈ C. Now 6n+2 ∈ g'C and 6n+2 ∈ 6f(A*)+2 ⊆ f'A. Since C ∩ g'C = ∅, we have 6n+2 ∉ C. Also 6n+2 ∈ C ∪ g'B. Hence 6n+2 ∈ g'B. Since rng(g) ⊆ 6N, we have 6n+2 ∈ 6B+2, and so n ∈ B. Since n ∈ f(A*) and f is strictly dominating, we have n > min(A) ≥ min(B). Hence n ∈ B*.

case 2. n ∈ g'B. Since n ∈ 6N, n ∈ g(B*). This establishes the claim.

Next we claim that f(B*) ∩ 6N ⊆ C* ∪ g(C*). To see this, let n ∈ f(B*) ∩ 6N. Then n ∈ f'B. Hence n ∈ C ∪ g'C.

case 1'. n ∈ C. Since n ∈ f(B*) and f is strictly dominating, we have n > min(B) ≥ min(C). Hence n ∈ C*.

case 2'. n ∈ g'C. Since n ∈ 6N, n ∈ g(C*). This establishes the claim.

Now we claim that f(A*) ∩ 2N+1, f(A*) ∩ 3N+1 ⊆ B*. To see this, let n ∈ f(A*), n ∈ 2N+1 ∪ 3N+1. Then n ∈ f'A, and so n ∈ C ∪ g'B. Recall that rng(g) ⊆ 6N. Since n ∈ 2N+1 ∪ 3N+1, we see that n ∉ g'B, and so n ∈ C. Now 6n+2 ∈ g'C and 6n+2 ∈ 6f(A*)+2 ⊆ f'A. Since C ∩ g'C = ∅, we have 6n+2 ∉ C. Also 6n+2 ∈ f'A ⊆ C ∪ g'B. Hence 6n+2 ∈ g'B. Since rng(g) ⊆ 6N, we have 6n+2 ∈ 6B+2, and so n ∈ B. Since n ∈

f(A*) and f is strictly dominating on A, we have n > min(A) ≥ min(B). Hence n ∈ B*.

Finally we claim that f(B*) ∩ 2N+1, f(B*) ∩ 3N+1 ⊆ C*. To see this, let n ∈ f(B*), n ∈ 2N+1 ∪ 3N+1. Then n ∈ f'B, and so n ∈ C ∪ g'C. Since n ∈ 2N+1 ∪ 3N+1, we have n ∉ 6N ∪ 6N+2. Hence n ∉ g'C, n ∈ C. Since n ∈ f(B*) and f is strictly dominating, n > min(B) ≥ min(C). Hence n ∈ C*. QED

The phrase "length 3 towers" mentioned in the title of this section refers to the A ⊆ B ⊆ C in Lemma 5.1.7.

5.2. From length 3 towers to length n towers.

In this section, we obtain a variant of Lemma 5.1.7 (Lemma 5.2.12) involving length n towers rather than length 3 towers of infinite sets. However, we only assert that the sets in the length n tower have at least r elements, for any r ≥ 1. Thus we pay a real cost for lengthening the towers.

Because the sets in the tower are finite and not infinite, certain indiscernibility properties of the first set in the tower must now be stated explicitly as additional conditions. See Lemma 5.2.12, iii), viii). These indiscernibility properties can of course be obtained from the usual infinite Ramsey theorem by taking a subset of the infinite A ⊆ N from Lemma 5.1.7 - but then we would only have a tower of length 3.

We will apply Lemma 5.1.7 with f arising from term assignments. Thus Lemma 5.2.12 uses g and not f.

Recall the definition of the language L (Definition 5.1.8). In order to avoid having to write too many parentheses in terms and formulas of L, we use the following two standard precedence tables.

↑
•
+,−

¬
∧,∨
→,↔

DEFINITION 5.2.1. Let t be a term of L. We write #(t) for the maximum of: the subscripts of variables in t, and the number of occurrences of the symbols

$$01+-\bullet\uparrow()v_1v_2,\ldots\log$$

We count log as a single symbol. Note that for all $n \geq 0$, $\{t: \#(t) \leq n\}$ is finite.

DEFINITION 5.2.2. Let φ be a quantifier free formula in L. We write #(φ) for the maximum of: the subscripts of variables in φ, and the number of occurrences of the symbols

$$01+-\bullet\uparrow()=<\neg\wedge\vee\rightarrow\leftrightarrow v_1v_2,\ldots,v_r\ \log$$

in φ. Note that for all $n \geq 0$, $\{\varphi: \#(\varphi) \leq n\}$ is finite.

DEFINITION 5.2.3. For all $r \geq 1$, let $\beta(r)$ be the number of terms t in L with $\#(t) \leq r$. We fix a doubly indexed sequence t[i,r] of terms in L, which is defined if and only if $r \geq 1$ and $1 \leq i \leq \beta(r)$. For each $r \geq 1$, the sequence t[i,r], $1 \leq i \leq \beta(r)$, enumerates the terms t with $\#(t) \leq r$, without repetition.

DEFINITION 5.2.4. For all $r \geq 1$, let $\gamma(r)$ be the number of quantifier free formulas φ in L with $\#(\varphi) \leq r$. We fix a doubly indexed sequence φ[i,r] of quantifier free formulas in L, which is defined if and only if $r \geq 1$ and $1 \leq i \leq \gamma(r)$. For each $r \geq 1$, the sequence φ[i,r], $1 \leq i \leq \gamma(r)$, enumerates the quantifier free formulas φ with $\#(\varphi) \leq r$, without repetition.

We adhere to the convention of displaying all free variables (and possibly additional variables). Thus $t(v_1,\ldots,v_n)$ and $\varphi(v_1,\ldots,v_m)$ respectively indicate that all variables in the term t are among the first n variables $v_1,\ldots,v_n$, and all variables in the quantifier free formula φ are among the first m variables $v_1,\ldots,v_m$.

Note that all terms t[i,r] have variables among $v_1,\ldots,v_r$, and all formulas φ[i,r] have variables among $v_1,\ldots,v_r$.

We want to be more specific about the enumerations of terms and formulas in Definitions 5.2.3, 5.2.4.

DEFINITION 5.2.5. Let $r \geq 1$. The enumeration t[1,r],...,t[$\beta(r)$,r] in Definition 5.2.3 is the enumeration of all terms t of L with #(t) ≤ r, ordered first by #(t), and second by the lexicographic ordering of strings of symbols, where, for specificity, the symbols are ordered by

$$01+-\bullet\uparrow()v_1v_2...v_r \log$$

DEFINITION 5.2.6. Let r ≥ 1. The enumeration φ[1,r],...,φ[γ(r),r] in Definition 5.2.4 is the enumeration of all quantifier free formulas φ of L with #(φ) ≤ r, ordered first by #(φ), and second by the lexicographic ordering of strings of symbols, where the symbols are ordered by

$$01+-\bullet\uparrow()=<\neg\wedge\vee\rightarrow\leftrightarrow v_1v_2...v_r \log$$

An important consequence of the way we have enumerated terms and formulas is the following.

$$1 \leq i \leq \beta(r) \wedge 1 \leq r \leq r' \rightarrow t[i,r] = t[i,r'].$$
$$1 \leq i \leq \gamma(r) \wedge 1 \leq r \leq r' \rightarrow \varphi[i,r] = \varphi[i,r'].$$

DEFINITION 5.2.7. For E ⊆ N and r ≥ 1, we write α(r,E) for the set of values of all terms t[i,r], at assignments f to the variables in t, with rng(f) ⊆ E, including t[i,r] that are closed.

DEFINITION 5.2.8. For E ⊆ N and integers p,q ≥ 0, we write α(r,E;p,q) for the set of all nonnegative integers x such that the following holds. There is a term t[i,r] that is not closed, and an assignment f to its variables, with rng(f) ⊆ E, such that x is the value of t[i,r] under f, and x ∈ [pmax(rng(f)),qmax(rng(f))]. We refer to p,q as the lower and upper coefficients, respectively.

Note that for E ⊆ N, r ≥ 1, p,q ≥ 0, α(r,E;p,q) ⊆ [pmin(E),∞).

Here is a version of Lemma 5.1.7, where the role of f is taken up by α. Recall Definition 5.1.12.

LEMMA 5.2.1. Let r ≥ 1 and g ∈ ELG ∩ SD ∩ BAF, rng(g) ⊆ 6N. There exist infinite A ⊆ B ⊆ C ⊆ N\{0} such that
i) 6α(r,A*;1,r) ⊆ B ∪ gB;
ii) 6α(r,B*;1,r) ⊆ C ∪ gC;
iii) 2α(r,A*;1,r)+1 ⊆ B;
iv) 3α(r,A*;1,r)+1 ⊆ B;
v) 2α(r,B*;1,r)+1 ⊆ C;
vi) 3α(r,B*;1,r)+1 ⊆ C;

vii) $C \cap gC = \emptyset$;
viii) $A \cap \alpha(r,B^*;2,r) = \emptyset$.

Proof: Let r,g be as given. We define $f \in ELG \cap SD \cap BAF$ of arity $\beta(r)+12+r$ as follows. Let $x^* =$

$$(y_1,\ldots,y_{\beta(r)},z_1,\ldots,z_6,w_1,\ldots,w_6,x_1,\ldots,x_r) \in N^{\beta(r)+12+r}.$$

Let i,j,k be greatest such that

$$y_1 = \ldots = y_i$$
$$z_1 = \ldots = z_j$$
$$w_1 = \ldots = w_k$$

respectively.

Define $f(x^*) =$

$$jt[i,r](x_1,\ldots,x_r)+k-1 \text{ if } |x^*|+1,2|x^*| \leq jt[i,r](x_1,\ldots,x_r)+k-1 \leq r|x^*|;$$
$$\max(|x^*|+1,2|x^*|) \text{ otherwise.}$$

Clearly $f \in ELG \cap SD \cap BAF$. We claim that for any $D \subseteq N$, $2 \leq p \leq 6$, and $0 \leq q \leq 5$,

$$\alpha(r,D^*;2,r) \cup p\alpha(r,D^*;1,r)+q \subseteq fD.$$

To see this, let $u \in \alpha(r,D^*;2,r)$, $v \in p\alpha(r,D^*;1,r)+q$, and write

$$u = t[i,r](x_1,\ldots,x_r)$$
$$v = pt[i',r](x_1,\ldots,x_r)+q$$

where $x_1,\ldots,x_r \in D^*$, $1 \leq i,i' \leq \beta(r)$, $2|x_1,\ldots,x_r| \leq u \leq r|x_1,\ldots,x_r|$, $|x_1,\ldots,x_r| \leq v \leq r|x_1,\ldots,x_r|$, and $t[i,r],t[i',r]$ are not closed.

First let $y_1 = \ldots = y_i = \min(D)$, $y_{i+1} = \ldots = y_{\beta(r)} = |x_1,\ldots,x_r|$, $z_1 = w_1 = \min(D)$, $z_2 = \ldots = z_6 = w_2 = \ldots = w_6 = |x_1,\ldots,x_r|$. Then $f(y_1,\ldots,y_{\beta(r)},z_1,\ldots,z_6,w_1,\ldots,w_6,x_1,\ldots,x_r) = u \in fD$.

Now let $y_1 = \ldots = y_i = \min(D)$, $y_{i+1} = \ldots = y_{\beta(r)} = |x_1,\ldots,x_r|$, $z_1 = \ldots = z_p = \min(D)$, $z_{p+1} = \ldots = z_6 = |x_1,\ldots,x_r|$, $w_1 = \ldots = w_{q+1} = \min(D)$, $w_{q+2} = \ldots = w_6 = |x_1,\ldots,x_r|$.

It is obvious that
$f(y_1,...,y_{\beta(r)},z_1,...,z_6,w_1,...,w_6,x_1,...,x_r) = v \in fD$.

Now apply Lemma 5.1.7 to f,g to obtain $A,B,C \subseteq N\backslash\{0\}$ with the properties i)-viii) cited there.

From the demonstrated claim, we have

$$6\alpha(r,A^*;1,r) \subseteq fA.$$
$$6\alpha(r,B^*;1,r) \subseteq fB.$$
$$2\alpha(r,A^*;1,r)+1 \subseteq fA.$$
$$3\alpha(r,A^*;1,r)+1 \subseteq fA.$$
$$2\alpha(r,B^*;1,r)+1 \subseteq fB.$$
$$3\alpha(r,B^*;1,r)+1 \subseteq fB.$$
$$\alpha(r,B^*;2,r) \subseteq fB.$$

We now obtain i)- viii) here immediately from the i)-viii) of Lemma 5.1.7. QED

We are now going to define three properties of finite length towers of sets, of increasing strength: r,g-good for aN, r,g-great for aN, and r,g-terrific for aN. The notion of r-good generalizes some properties from Lemma 5.2.1.

DEFINITION 5.2.9. Let $n \geq 3$, $r,a \geq 1$, and $g \in ELG \cap SD \cap BAF$. We say that $(D_1,...,D_n)$ is r,g-good for aN if and only if

i) $D_1 \subseteq ... \subseteq D_n \subseteq N\backslash\{0\}$;
ii) for all $x < y$ from D_1, $x\uparrow < y$;
iii) for all $1 \leq i \leq n-1$, $a\alpha(r,D_i^*;1,r) \subseteq D_{i+1} \cup gD_{i+1}$;
iv) for all $1 \leq i \leq n-1$, $2\alpha(r,D_i^*;1,r)+1 \subseteq D_{i+1}$;
v) for all $1 \leq i \leq n-1$, $3\alpha(r,D_i^*;1,r)+1 \subseteq D_{i+1}$;
vi) $D_n \cap gD_n = \emptyset$;
vii) $D_1 \cap \alpha(r,D_2^*;2,r) = \emptyset$.

The following proves the existence of length 3 towers that are r,g-good for 6N.

LEMMA 5.2.2. Let $r \geq 1$ and $g \in ELG \cap SD \cap BAF$, $rng(g) \subseteq 6N$. There exists (A,B,C) which is r,g-good for 6N, where A is infinite.

Proof: Let r,g be as given, and let $A,B,C \subseteq N\backslash\{0\}$ be as given by Lemma 5.2.1. Set $D_1 = A$, $D_2 = B$, $D_3 = C$. Obviously i),iii)- vii) hold in the definition of r,g-good for 6N. However ii) may fail. We can obviously shrink A so that ii) holds, keeping A infinite, and retaining i),iii)-vii). QED

We now want to define certain $g \in ELG \cap SD \cap BAF$ so that any r,g-good sequence for N codes up the truth values of existential closures of quantifier free formulas $\varphi[i,r]$, $1 \le i \le \gamma(r)$, in a convenient uniform way. This introduces a kind of quantifier elimination.

DEFINITION 5.2.10. Let $r \ge 1$ and $g \in ELG \cap SD \cap BAF$, where $rng(g) \subseteq 24N$. We define $\boldsymbol{\tau}(g,r) \in ELG \cap SD \cap BAF$ as follows. $\boldsymbol{\tau}(g,r)$ has arity $\gamma(r)+k+r+1$, where k is the arity of g. Let $x^* = (y_1,\ldots,y_{\gamma(r)},z_1,\ldots,z_k,x_1,\ldots,x_r,w) \in N^{\gamma(r)+k+r+1}$. Let $i \in [1,\gamma(r)]$ be greatest such that $1 \le i \le \gamma(r)$ and $y_1 = \ldots = y_i$.

case 1. $|x^*| = w \wedge x_1,\ldots,x_r < w \wedge \varphi[i,r](x_1,\ldots,x_r)$. Define $\boldsymbol{\tau}(g,r)(x^*) = 24\gamma(r)w+24i+6$.

case 2. $|x^*| = |z_1,\ldots,z_k| \wedge x_1 = \ldots = x_r = w$. Define $\boldsymbol{\tau}(g,r)(x^*) = g(z_1,\ldots,z_k)$.

case 3. Otherwise. Define $\boldsymbol{\tau}(g,r)(x^*) = 24|x^*|+12$.

We now establish some useful coding properties of $\boldsymbol{\tau}(g,r)$.

LEMMA 5.2.3. $\boldsymbol{\tau}(g,r) \in ELG \cap SD \cap BAF$. The values arising out of the above three cases are mutually disjoint, and lie in 6N. Let $E \subseteq N$. For all $w \in E$ and $1 \le i \le \gamma(r)$, $24\gamma(r)w+24i+6 \in \boldsymbol{\tau}(g,r)E \leftrightarrow (\exists v_1,\ldots,v_r \in E)(v_1,\ldots,v_r < w \wedge \varphi[i,r](v_1,\ldots,v_r))$. $gE = \boldsymbol{\tau}(g,r)E \cap 24N$.

Proof: Note that in case 1, $\gamma(r),w \ge 1$, and $24w \le 24\gamma(r)w+24i+6 \le 100\gamma(r)w$. Hence

$$|x^*|+1,24|x^*| \le \boldsymbol{\tau}(g,r)(x^*) \le 100\gamma(r)|x^*|.$$

In case 2,

$$|x^*| = |z_1,\ldots,z_k|$$
$$|\boldsymbol{\tau}(g,r)(x^*)| = |g(z_1,\ldots,z_k)|.$$

In case 3, $|x^*| \ge 1$, and

$$24|x^*| < \boldsymbol{\tau}(g,r)(x^*) \le 36|x^*|.$$

Therefore $\boldsymbol{\tau}(g,r) \in ELG \cap SD \cap BAF$.

Since $rng(g) \subseteq 24N$, the values arising out of the three cases are mutually disjoint. Also note that the w,i used in case 1 can be recovered from any value of $\tau(g,r)$ obtained by case 1. This is because $1 \le i \le \gamma(r)$ in case 1.

Let $E \subseteq N$ and $w \in E$. First suppose $24\gamma(r)w+24i+6 \in \tau(g,r)E$. Then $24\gamma(r)w+24i+6$ must arise out of case 1, with, say, $x^* \in E^{\gamma(r)+k+r+1}$. Then the w,i used in case 1 must be this w,i. Hence the $x_1,\ldots,x_r$ used in case 1 must be $< w$, and $\varphi[i,r](x_1,\ldots,x_r)$.

Conversely, suppose $x_1,\ldots,x_r \in E \cap [0,w)$ and $\varphi[i,r](x_1,\ldots,x_r)$. Then we can choose $y_1 = \ldots = y_i = x_1$ and $y_{i+1} = \ldots = y_{\gamma(r)} = z_1 = \ldots = z_k = w$. Then case 1 applies, $y_1,\ldots,y_{\gamma(r)},z_1,\ldots,z_k,w \in E$, and i is greatest such that $y_1 = \ldots = y_i$. Hence $\tau(g,r)(y_1,\ldots,y_{\gamma(r)},z_1,\ldots,z_k,x_1,\ldots,x_r,w) = 24\gamma(r)w+24i+6$.

For the final claim, note that every element of gE arises out of case 2, since we can set $y_1 = \ldots = y_{\gamma(r)} = x_1 = \ldots = x_r = w = z_1$, taking $z_1,\ldots,z_k$ to be arbitrary elements of E. On the other hand, all elements of $\tau(g,r)E$ lying in 24N must arise out of case 2, in which case they must lie in gE. QED

DEFINITION 5.2.11. Throughout the book, we will use the logical construction

$$\varphi_1 \leftrightarrow \ldots \leftrightarrow \varphi_k$$

for

$$(\varphi_1 \leftrightarrow \varphi_2) \wedge (\varphi_2 \leftrightarrow \varphi_3) \wedge \ldots \wedge (\varphi_{k-1} \leftrightarrow \varphi_k).$$

LEMMA 5.2.4. Let $r \ge 1$, $g \in ELG \cap SD \cap BAF$, $rng(g) \subseteq 24N$, and (A,B,C) be $100\gamma(r),\tau(g,r)$-good for 6N. Then

i) for all $1 \le i \le \gamma(r)$ and $x \in B^*$,

$$(\exists v_1,\ldots,v_r \in C)(v_1,\ldots,v_r < x \wedge \varphi[i,r](v_1,\ldots,v_r)) \leftrightarrow 24\gamma(r)x+24i+6 \notin C;$$

ii) for all $1 \le i \le \gamma(r)$ and $x \in A^*$,

$$(\exists v_1,\ldots,v_r \in B)(v_1,\ldots,v_r < x \wedge \varphi[i,r](v_1,\ldots,v_r)) \leftrightarrow (\exists v_1,\ldots,v_r \in C)(v_1,\ldots,v_r < x \wedge \varphi[i,r](v_1,\ldots,v_r)) \leftrightarrow 24\gamma(r)x+24i+6 \notin B \leftrightarrow 24\gamma(r)x+24i+6 \notin C.$$

iii) (A,B,C) is r,g-good for 24N.

Proof: Let r,g,A,B,C be as given. For claim i), let $1 \leq i \leq \gamma(r)$, $x \in B^*$. Then $4\gamma(r)x+4i+1 \in \alpha(100\gamma(r),B^*;1,100\gamma(r))$. To see this, note that $\gamma(r),x \geq 1$, $2x \leq 4\gamma(r)x+4i+1 \leq 100\gamma(r)x$. Also $4\gamma(r)x+4i+1$ is a term $t(x)$ with $\#(t) \leq 100\gamma(r)$.

By clauses iii),vi) in the definition of $100\gamma(r),\tau(g,r)$-good for 6N, we have

$$24\gamma(r)x+24i+6 \in C \cup \tau(g,r)C.$$
$$C \cap \tau(g,r)C = \emptyset.$$

By the above and Lemma 5.2.3,

$$(\exists v_1,\ldots,v_r \in C)(v_1,\ldots,v_r < x \wedge \varphi[i,r](v_1,\ldots,v_r)) \leftrightarrow$$
$$24\gamma(r)x+24i+6 \in \tau(g,r)C \leftrightarrow 24\gamma(r)x+24i+6 \notin C.$$

For claim ii), let $1 \leq i \leq \gamma(r)$ and $x \in A^*$. Then $4\gamma(r)x+4i+1 \in \alpha(100\gamma(r),A^*;1,100\gamma(r))$. By clauses iii),iv),vi) in the definition of $100\gamma(r),\tau(g,r)$-good for 6N, we have

$$24\gamma(r)x+24i+6 \in B \cup \tau(g,r)B$$
$$B \cap \tau(g,r)B = \emptyset.$$

By the above and Lemma 5.2.3,

$$(\exists v_1,\ldots,v_r \in B)(v_1,\ldots,v_r < x \wedge \varphi[i,r](v_1,\ldots,v_r)) \leftrightarrow$$
$$24\gamma(r)x+24i+6 \in \tau(g,r)B \leftrightarrow 24\gamma(r)x+24i+6 \notin B.$$

Hence

$$(\exists v_1,\ldots,v_r \in C)(v_1,\ldots,v_r < x \wedge \varphi[i,r](v_1,\ldots,v_r)) \rightarrow$$
$$24\gamma(r)x+24i+6 \notin C \rightarrow$$
$$24\gamma(r)x+24i+6 \notin B \rightarrow$$
$$(\exists v_1,\ldots,v_r \in B)(v_1,\ldots,v_r < x \wedge \varphi[i,r](v_1,\ldots,v_r)) \rightarrow$$
$$(\exists v_1,\ldots,v_r \in C)(v_1,\ldots,v_r < x \wedge \varphi[i,r](v_1,\ldots,v_r))$$

and so all of the above $\rightarrow$ are also $\leftrightarrow$.

For claim iii), by the definition of $100\gamma(r),\tau(g,r)$-good for 6N, we have

$$6\alpha(100\gamma(r),A^*;1,100\gamma(r)) \subseteq B \cup \tau(g,r)B$$
$$6\alpha(100\gamma(r),B^*;1,100\gamma(r)) \subseteq C \cup \tau(g,r)C$$
$$2\alpha(100\gamma(r),A^*;1,100\gamma(r))+1 \subseteq B$$
$$3\alpha(100\gamma(r),A^*;1,100\gamma(r))+1 \subseteq B$$
$$2\alpha(100\gamma(r),B^*;1,100\gamma(r))+1 \subseteq C$$
$$3\alpha(100\gamma(r),B^*;1,100\gamma(r))+1 \subseteq C$$
$$C \cap \tau(g,r)C = \emptyset$$

$$A \cap \alpha(100\gamma(r),B^*;2,100\gamma(r)) = \emptyset$$
for all x < y from A, x↑ < y.

By Lemma 5.2.3, $gB = \tau(g,r)B \cap 24N$ and $gC = \tau(g,r)C \cap 24N$. Hence the conditions

$$24\alpha(r,A^*;1,r) \subseteq B \cup gB$$
$$24\alpha(r,B^*;1,r) \subseteq C \cup gC$$
$$2\alpha(r,A^*;1,r)+1 \subseteq B$$
$$3\alpha(r,A^*;1,r)+1 \subseteq B$$
$$2\alpha(r,B^*;1,r)+1 \subseteq C$$
$$3\alpha(r,B^*;1,r)+1 \subseteq C$$
$$C \cap gC = \emptyset$$
$$A \cap \alpha(r,B^*;2,r) = \emptyset$$
for all x < y from A, x↑ < y

follow immediately. Therefore (A,B,C) is r,g-good for 24N. QED

We now define r,g-great towers, which feature a special form of indiscernibility for terms. We also define r,g-terrific towers, which feature a special form of indiscernibility for quantifier free formulas. We will only use r,g-terrific towers of length 3.

DEFINITION 5.2.12. Let $n \geq 3$, $r,a \geq 1$, and $g \in ELG \cap SD \cap BAF$. We say that $(D_1,\ldots,D_n)$ is r,g-great for aN if and only if

i) $(D_1,\ldots,D_n)$ is r,g-good for aN;
ii) Let $1 \leq i \leq \beta(2r)$, $x_1,\ldots,x_{2r} \in D_1$, $y_1,\ldots,y_r \in \alpha(r,D_2)$, where $(x_1,\ldots,x_r),(x_{r+1},\ldots,x_{2r})$ have the same order type and min, and $y_1,\ldots,y_r \leq \min(x_1,\ldots,x_r)$. Then
$t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in D_3^* \leftrightarrow$
$t[i,2r](x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \in D_3^*$.

DEFINITION 5.2.13. Let $r,a \geq 1$, and $g \in ELG \cap SD \cap BAF$. We say that (A,B,C) is r,g-terrific for aN if and only if

i) (A,B,C) is r,g-great for aN;
ii) A is infinite;
iii) for all $1 \leq i \leq \gamma(r)$,

$$(\exists v_1,\ldots,v_r \in B)(\varphi[i,r](v_1,\ldots,v_r)) \leftrightarrow$$
$$(\exists v_1,\ldots,v_r \in C)(\varphi[i,r](v_1,\ldots,v_r)).$$

We now derive an essentially well known infinitary combinatorial lemma. E.g., see [Sc74].

LEMMA 5.2.5. Let D be an infinite subset of N and $r \geq 1$. Let $f:N \to N$, and $R_1,...,R_s$ be a finite list of subsets of N^{2r}. There exists an infinite $D' \subseteq D$ such that the following holds. Let $1 \leq i \leq s$, $x_1,...,x_{2r} \in D'$, and $y_1,...,y_r \in N$, where $(x_1,...,x_r)$ and $(x_{r+1},...,x_{2r})$ have the same order type and min, and $y_1,...,y_r \leq f(\min(x_1,...,x_r))$. Then $R_i(x_1,...,x_r,y_1,...,y_r) \leftrightarrow R_i(x_{r+1},...,x_{2r},y_1,...,y_r)$.

Proof: Let $D,r,f,R_1,...,R_s$ be as given. Here we write $R_i(z_1,...,z_{2r})$ for $(z_1,...,z_{2r}) \in R_i$. We will partition the ordered 2r tuples from N into finitely many pieces as follows. Let $x_1,...,x_{2r} \in N$ be given. We partition $(x_1,...,x_{2r})$

a. first according to the order type of $(x_1,...,x_{2r})$.
b. second according to the set of all $i \in [1,s]$ such that for all $y_1,..,y_r \leq f(\min(x_1,...,x_{2r}))$, $R_i(x_1,...,x_r,y_1,...,y_r) \leftrightarrow R_i(x_{r+1},...,x_{2r},y_1,...,y_r)$.

By Ramsey's theorem, let $D' \subseteq D$ be infinite, where any two $(x_1,...,x_{2r}) \in D'^{2r}$ with the same order type lie in the same partition.

Let $1 \leq i \leq s$ and μ be the order type of an element of N^r. We say that $(x_1,...,x_{2r})$ is μ-special if and only if

i) $(x_1,...,x_r)$ and $(x_{r+1},...,x_{2r})$ have order type μ;
ii) $\min(x_1,...,x_r) = \min(x_{r+1},...,x_{2r})$;
iii) if $x_{r+j} > \min(x_1,...,x_r)$, then $|x_1,...,x_r| < x_{r+j}$.

The μ-special tuples are exactly the 2r-tuples of some particular order type depending on μ. Hence for each μ,i, we have

1) for all μ-special $(x_1,...,x_{2r}) \in D'^{2r}$, we have: for all $y_1,...,y_{2r} \leq f(\min(x_1,...,x_{2r}))$, $R_i(x_1,...,x_r,y_1,...,y_r) \leftrightarrow R_i(x_{r+1},...,x_{2r},y_1,...,y_r)$; or

2) for all μ-special $(x_1,...,x_{2r}) \in D'^{2r}$, we have: $\neg$(for all $y_1,...,y_r \leq f(\min(x_1,...,x_{2r}))$, $R_i(x_1,...,x_r,y_1,...,y_r) \leftrightarrow R_i(x_{r+1},...,x_{2r},y_1,...,y_r)$).

Suppose 2) holds for μ. Let $\alpha_1,\alpha_2,...$ be elements of N^r where each 2r-tuple (α_j,α_{j+1}) is μ-special. For each $j < k$ from $[1,\infty)$, let $h(j,k)$ be some counterexample $(y_1,...,y_r)$ given by 2) for $(x_1,...,x_{2r}) = (\alpha_j,\alpha_k)$.

Obviously h is bounded by $f(\min(\alpha_1))$. By Ramsey's theorem, h is constant on the $j < k$ drawn from some infinite subset of N. But $h(j,k) = h(j,p) = h(k,p)$ is obviously impossible for $j < k < p$. We conclude that 2) fails. Hence 1) holds for μ.

We have thus shown that for all μ,i, 1) holds. To complete the argument, let $1 \leq i \leq s$, $x_1,\ldots,x_{2r} \in D'$, and $y_1,\ldots,y_r \in N$, where $(x_1,\ldots,x_r)$ and $(x_{r+1},\ldots,x_{2r})$ have the same order type and min, and $y_1,\ldots,y_r \leq f(\min(x_1,\ldots,x_r))$. Let the order type of $(x_1,\ldots,x_r)$ be μ. Choose $x_1',\ldots,x_r' \in D'$ such that $(x_1,\ldots,x_r,x_1',\ldots,x_r')$ and $(x_{r+1},\ldots,x_{2r},x_1',\ldots,x_r')$ are μ-special. By 1),

$$R_i(x_1,\ldots,x_r,y_1,\ldots,y_r) \leftrightarrow R_i(x_1',\ldots,x_r',y_1,\ldots,y_r).$$
$$R_i(x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \leftrightarrow R_i(x_1',\ldots,x_r',y_1,\ldots,y_r).$$

Hence

$$R_i(x_1,\ldots,x_r,y_1,\ldots,y_r) \leftrightarrow R_i(x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r)$$

as required. QED

We now prove the existence of r,g-terrific towers.

LEMMA 5.2.6. Let $r \geq 1$ and $g \in ELG \cap SD \cap BAF$, where $rng(g) \subseteq 24N$. There exists (A,B,C) which is r,g-terrific for 24N.

Proof: Let r,g be as given. By Lemma 5.2.2, there exists (A,B,C) which is $100\gamma(r),\tau(g,r)$-good for 6N, where A is infinite. By Lemma 5.2.4, (A,B,C) is r,g-good for 24N, and satisfies clauses i) and ii) in Lemma 5.2.4.

For all $1 \leq i \leq \beta(2r)$, let $R_i \subseteq N^{2r}$ be given by

$$R_i(x_1,\ldots,x_{2r}) \leftrightarrow t[i,2r](x_1,\ldots,x_{2r}) \in C^*.$$

Apply Lemma 5.2.5 to these R_i with D = A to obtain $A' \subseteq A$, A' infinite, such that (A',B,C) is r,g-great for 24N.

To see that (A',B,C) is r,g-terrific for 24N, we need only verify clause iii) in that definition. Since (A,B,C) satisfies clause ii) in Lemma 5.2.4, we have that for all $1 \leq i \leq \gamma(r)$ and $x \in A^*$,

$$(\exists v_1,\ldots,v_r \in B)(v_1,\ldots,v_r < x \wedge \varphi[i,r](v_1,\ldots,v_r)) \leftrightarrow$$
$$(\exists v_1,\ldots,v_r \in C)(v_1,\ldots,v_r < x \wedge \varphi[i,r](v_1,\ldots,v_r)).$$

Since A* is infinite, we have

$$(\exists v_1,\ldots,v_r \in B)(\varphi[i,r](v_1,\ldots,v_r)) \leftrightarrow$$
$$(\exists v_1,\ldots,v_r \in C)(\varphi[i,r](v_1,\ldots,v_r)).$$

QED

We remark that, using Lemma 5.2.5, we can obtain ii) in the definition of r,g-great with $\alpha(r,D_2)$ replaced by N. However, if we formulated r,g-greatness in such a strong form, we would not be able to push down from C to B in Lemma 5.2.8.

LEMMA 5.2.7. For all $n \geq 3$ and $k,p,r \geq 1$, there exists $m \geq 1$ such that the following holds. Let $g \in ELG \cap SD \cap BAF$ be k-ary, $a \geq 1$, and $(D_1,\ldots,D_n)$ be r,g-great for aN, $|D_1| = p$. There exists $(D_1',\ldots,D_n')$ which is r,g-great for aN, where $D_1' = D_1$, each $D_i' \subseteq D_i$, and $|D_n'| \leq m$.

Proof: Let n,k,p,r,a be as given. Let $g,D_1,\ldots,D_n$ also be as given. We will construct the required $D_1',\ldots,D_n'$ by induction on $1 \leq j \leq n$, in such a way that there is an obvious bound on the cardinality of each D_{j+1}' that depends only on j,k,p,r and not on $a,n,g,D_1,\ldots,D_n$.

Suppose $D_1 = D_1' \subseteq \ldots \subseteq D_j'$ have been defined, $1 \leq j < n$, such that $(\forall i \in [1,j])(D_i' \subseteq D_i)$. We now construct $D_{j+1}' \subseteq D_{j+1}$.

First throw all elements of D_j' into D_{j+1}', and also $\min(D_{j+1})$ into D_{j+1}'. Then for each $x \in a\alpha(r,D_j'^*;1,r)$, throw x into D_{j+1}' if $x \in D_{j+1}$; otherwise find a k-tuple y from D_{j+1} such that $g(y) = x$ and throw $y_1,\ldots, y_k$ into D_{j+1}'. Next, throw all elements of $2\alpha(r,D_j'^*;1,r)+1$, $3\alpha(r,D_j'^*;1,r)+1$, into D_{j+1}'. Note that these elements are in D_{j+1}, because $(D_1,\ldots,D_n)$ is r,g-good.

Finally, if $j = 2$ then let $1 \leq i \leq \beta(2r)$, $x_1,\ldots,x_r \in D_1$, and $y_1,\ldots,y_r \in \alpha(r,D_2')$, $y_1,\ldots,y_r \leq \min(x_1,\ldots,x_r)$. If $t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in D_3^*$, then throw $t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r)$ in D_3'. Otherwise, take no action.

It is clear that $(D_1',\ldots,D_n')$ is r,g-good for aN. We have to verify clause ii) in the definition of r,g-great for aN.

Let $1 \le i \le \beta(2r)$, $x_1,\ldots,x_r \in D_1$, $y_1,\ldots,y_r \in \alpha(r,D_2')$, where $y_1,\ldots,y_r \le \min(x_1,\ldots,x_r)$. We claim that

$$t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in D_3'^* \leftrightarrow t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in D_3^*.$$

The forward direction is immediate. For the reverse direction, first note that $\min(D_3) = \min(D_3')$ by construction. If the right side holds, then $t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r)$ has been thrown into D_3', and since $t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) > \min(D_3) = \min(D_3')$, the left side follows.

Now let $1 \le i \le \beta(2r)$, $x_1,\ldots,x_{2r} \in D_1$, $y_1,\ldots,y_r \in \alpha(r,D_2')$, where $(x_1,\ldots,x_r)$ and $(x_{r+1},\ldots,x_{2r})$ have the same order type and min, and $y_1,\ldots,y_r \le \min(x_1,\ldots,x_r)$. We must verify that

$$t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in D_3'^* \leftrightarrow t[i,2r](x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \in D_3'^*.$$

By the above, this is equivalent to

$$t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in D_3^* \leftrightarrow t[i,2r](x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \in D_3^*$$

which follows from the hypothesis on $(D_1,\ldots,D_n)$ - in particular, from ii) in the definition of r,g-great.

It is clear that we can write m as a specific iterated exponential in n,k,p,r. QED

We show that, at the cost of increasing r to much larger s, we can guarantee that for any s,g-terrific tower (A,B,C), any r,g-great tower contained in C can be shrunk to an r,g-great tower contained in B.

LEMMA 5.2.8. Let $n \ge 3$, $k,p,r \ge 1$, and $g \in ELG \cap SD \cap BAF$ be k-ary. There exists $s \ge 1$ such that the following holds. Let (A,B,C) be s,g-terrific for 24N. Let $(D_1,\ldots,D_n)$ be r,g-great for 24N, $|D_1| = p$, and $D_n \subseteq C$. Then some $(D_1',\ldots,D_n')$ is r,g-great for 24N, where $|D_1'| = p$ and $D_n' \subseteq B$ is finite.

Proof: Let n,k,p,r,g be as given. Let $m \ge 1$ be given by Lemma 5.2.7, with $a = 24$, which depends only on n,k,p,r. Let $s \gg n,k,p,r,m$ and the presentation of g. (Some specific iterated exponential in n,k,p,r,m, and the size of the presentation of g, will suffice). Let (A,B,C) be s,g-terrific for 24N. Let $(D_1,...,D_n)$ be r,g-great for 24N, $|D_1| = p$, and $D_n \subseteq C$.

By Lemma 5.2.7, the following statement is true:

*) there exists $(D_1,...,D_n)$ which is r,g-great for 24N, where $|D_1| = p$ and $D_n = \{x_1,...,x_m\} \subseteq C$.

We claim that *) asserts the existence of $x_1,...,x_m \in C$ such that a quantifier free formula $\varphi(x_1,...,x_m)$ in L holds. This crucially depends on the fact that $g \in BAF$. The actual formula depends on n,k,p,r, and the function g.

To see this, $\varphi(x_1,...,x_m)$ asserts that $x_1,...,x_m$ can be arranged into sets $D_1 \subseteq ... \subseteq D_n = \{x_1,...,x_m\}$, where $(D_1,...,D_n)$ is r,g-great for 24N. We have to put clauses i),ii) in Definition 5.2.12, with a = 24, in quantifier free form.

Each arrangement of $x_1,...,x_m$ into sets $D_1 \subseteq ... \subseteq D_n = \{x_1,...,x_m\}$ is given by a double sequence x_{ij}, $1 \leq i \leq n$, $1 \leq j \leq m$, where the x_{ij} are among the variables $x_1,...,x_m$. So we disjunct over the finitely many such double sequences of variables.

According to Definition 5.2.12, we assert

i. $(\{x_{11},...,x_{1m}\},...,\{x_{n1},...,x_{nm}\})$ is r,g-good for 24N.
ii. Let $1 \leq i \leq \beta[2r]$, $x_1,...,x_{2r} \in \{x_{11},...,x_{1m}\}$, $y_1,...,y_r \in \alpha(r,\{x_{21},...,x_{2m}\})$, where $(x_1,...,x_r)$, $(x_{r+1},...,x_{2r})$ have the same order type and min, and $y_1,...,y_r \leq \min(x_1,...,x_r)$. Then

$$t[i,2r](x_1,...,x_r,y_1,...,y_r) \in \{x_{31},...,x_{3m}\}\backslash\{0\} \leftrightarrow$$
$$t[i,2r](x_{r+1},...,x_{2r},y_1,...,y_r) \in \{x_{31},...,x_{3m}\}\backslash\{0\}.$$

It is clear that ii) is given by a quantifier free formula in L.

As for i), it asserts

i'. $\{x_{11},...,x_{1m}\} \subseteq ... \subseteq \{x_{n1},...,x_{nm}\} \subseteq N\backslash\{0\}$.
ii'. $x_{1i} < x_{1j} \rightarrow x_{1i}\uparrow < x_{1j}$.
iii'. For all $1 \leq i \leq n-1$, $24\alpha(r,\{x_{i1},...,x_{im}\}\backslash\{0\};1,r) \subseteq \{x_{i+1,1},...,x_{i+1,m}\} \cup g\{x_{i+1,1},...,x_{i+1,m}\}$.
iv'. For all $1 \leq i \leq n-1$, $2\alpha(r,\{x_{i1},...,x_{im}\}\backslash\{0\};1,r)+1 \subseteq \{x_{i+1,1},...,x_{i+1,m}\}$;
v'. Same as iv' with 2 replaced by 3.
vi'. $\{x_{n1},...,x_{nm}\} \cap g\{x_{n1},...,x_{nm}\} = \emptyset$.

vii'. $\{x_{11},\ldots,x_{1m}\} \cap \alpha(r,\{x_{21},\ldots,x_{2m}\};2,r) = \emptyset$.

It is now clear that i) is also given by a quantifier free formula.

By the choice of s, write $\varphi = \varphi[i,s]$, where $1 \leq i \leq \gamma(s)$.

By Lemma 5.2.7, we have

$$(\exists v_1,\ldots,v_m \in C)(\varphi[i,s](v_1,\ldots,v_m)).$$

By clause iii) in the definition of s,g-terrific for 24N,

$$(\exists v_1,\ldots,v_m \in B)(\varphi[i,s](v_1,\ldots,v_m)).$$

Hence

$$(\exists v_1,\ldots,v_m \in B)(\exists D_1,\ldots,D_n)((D_1,\ldots,D_n) \text{ is } r,g\text{-great for } 24N \wedge |D_1| = p \wedge D_n = \{v_1,\ldots,v_m\}).$$

I.e., some $(D_1',\ldots,D_n')$ is r,g-great for 24N, where $|D_1'| = p$ and $D_n' \subseteq B$ has at most m elements. QED

DEFINITION 5.2.14. Let s(n,k,p,r,g) be an s given by Lemma 5.2.8.

LEMMA 5.2.9. Let $n \geq 3$, $k,p,r \geq 1$, and $g \in ELG \cap SD \cap BAF$ be k-ary. There exists $t \geq 1$ such that the following holds. Let (A,B,C) be t,g-terrific for 24N. Then some $(D_1,\ldots,D_n)$ is r,g-great for 24N, where $|D_1| = p$ and $D_n \subseteq B$ is finite.

Proof: Let n,k,p,r,g be as given. Let $t = \max\{s(q,k,p,r,g): 3 \leq q \leq n)\}$. Let (A,B,C) be t,g-terrific for 24N. We prove by induction on $3 \leq q \leq n$ that some $(D_1,\ldots,D_q)$ is r,g-great for 24N, where $|D_1| = p$ and $D_n \subseteq B$ is finite.

For the basis case q = 3, apply Lemma 5.2.8 to (D_1,D_2,D_3), where D_1 is any subset of A of cardinality p, and $D_2 = B$, $D_3 = C$. Note that $t \geq s(3,k,p,r,g)$.

Let $3 \leq q < n$ and $(D_1,\ldots,D_q)$ be r,g-great for 24N, where $|D_1| = p$ and $D_q \subseteq B$ is finite.

We claim that $(D_1,\ldots,D_q,C)$ is r,g-great for 24N.

We first verify that $(D_1,\ldots,D_q,C)$ is r,g-good for 24N. In light of the fact that $(D_1,\ldots,D_q)$ is r,g-good for 24N and $q \geq 3$, it suffices to show that

$$24\alpha(r,D_q^*;2,r) \subseteq C \cup gC$$
$$2\alpha(r,D_q^*;2,r)+1 \subseteq C$$
$$3\alpha(r,D_q^*;2,r)+1 \subseteq C$$
$$C \cap gC = \emptyset.$$

These are immediate since $D_q \subseteq B$ and (A,B,C) is r,g-good for 24N.

Clause ii) in the definition of $(D_1,...,D_q,C)$ is immediate since $q \geq 3$ and $(D_1,...,D_q)$ is r,g-great for 24N.

Now apply Lemma 5.2.8 to $(D_1,...,D_q,C)$ to obtain a sequence $(D_1',...,D_{q+1}')$ that is r,g-great for 24N, where $|D_1| = p$ and $D_{q+1}' \subseteq B$ is finite. Note that $t \geq s(q+1,k,p,r,g)$. QED

LEMMA 5.2.10. Let $n \geq 3$, $p,r \geq 1$, and $g \in ELG \cap SD \cap BAF$, where $rng(g) \subseteq 24N$. There exists $(D_1,...,D_n)$ which is r,g-great for 24N, where $|D_1| = p$ and D_n is finite.

Proof: Let n,p,r,g be as given. Let g be k-ary. Let t be given by Lemma 5.2.9. By Lemma 5.2.6, let (A,B,C) be t,g-terrific for 24N. By Lemma 5.2.9, let $(D_1,...,D_n)$ be r,g-great for 24N, where $|D_1| = p$ and D_n is finite. QED

LEMMA 5.2.11. Let $r \geq 3$ and $g \in ELG \cap SD \cap BAF$, where $rng(g) \subseteq 24N$. There exists $(D_1,...,D_r)$ such that
i) $D_1 \subseteq ... \subseteq D_r \subseteq N\backslash\{0\}$;
ii) $|D_1| = r$ and D_r is finite;
iii) for all $x < y$ from D_1, $x\uparrow < y$;
iv) for all $1 \leq i \leq r-1$, $24\alpha(r,D_i^*;1,r) \subseteq D_{i+1} \cup gD_{i+1}$;
v) for all $1 \leq i \leq r-1$, $2\alpha(r,D_i^*;1,r)+1$, $3\alpha(r,D_i^*;1,r)+1 \subseteq D_{i+1}$;
vi) $D_r \cap gD_r = \emptyset$;
vii) $D_1 \cap \alpha(r,D_2^*;2,r) = \emptyset$;
viii) Let $1 \leq i \leq \beta(2r)$, $x_1,...,x_{2r} \in D_1$, $y_1,...,y_r \in \alpha(r,D_2)$, where $(x_1,...,x_r)$ and $(x_{r+1},...,x_{2r})$ have the same order type and min, and $y_1,...,y_r \leq \min(x_1,...,x_r)$. Then
$t[i,2r](x_1,...,x_r,y_1,...,y_r) \in D_3^* \leftrightarrow$
$t[i,2r](x_{r+1},...,x_{2r},y_1,...,y_r) \in D_3^*$.

Proof: Immediate from Lemma 5.2.10 and the definition of r,g-great for 24N, setting n,p,r there to be r here. QED

We now eliminate the use of the D_i^*.

LEMMA 5.2.12. Let $r \geq 3$ and $g \in ELG \cap SD \cap BAF$, where $rng(g) \subseteq 48N$. There exists $(D_1,...,D_r)$ such that

i) $D_1 \subseteq \ldots \subseteq D_r \subseteq N\backslash\{0\}$;
ii) $|D_1| = r$ and D_r is finite;
iii) for all $x < y$ from D_1, $x\uparrow < y$;
iv) for all $1 \le i \le r-1$, $48\alpha(r,D_i;1,r) \subseteq D_{i+1} \cup gD_{i+1}$;
v) for all $1 \le i \le r-1$, $2\alpha(r,D_i;1,r)+1$, $3\alpha(r,D_i;1,r)+1 \subseteq D_{i+1}$;
vi) $D_r \cap gD_r = \emptyset$;
vii) $D_1 \cap \alpha(r,D_2;2,r) = \emptyset$;
viii) Let $1 \le i \le \beta(2r)$, $x_1,\ldots,x_{2r} \in D_1$, $y_1,\ldots,y_r \in \alpha(r,D_2)$, where $(x_1,\ldots,x_r)$ and $(x_{r+1},\ldots,x_{2r})$ have the same order type and min, and $y_1,\ldots,y_r \le \min(x_1,\ldots,x_r)$. Then
$t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in D_3 \leftrightarrow$
$t[i,2r](x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \in D_3$.

Proof: Let r,g be as given. Let $g:N^k \to 48N$.

Define $g':N^{k+1} \to 24N$ by $g'(x_1,\ldots,x_{k+1}) = g(x_1,\ldots,x_k)$ if $x_{k+1} < x_1,\ldots,x_k$; $48|x_1,\ldots,x_{k+1}|+24$ otherwise.

Note that $rng(g') \subseteq 24N$, and $g' \in ELG \cap SD \cap BAF$. Let $D_1,\ldots,D_n \subseteq N$ be given by Lemma 5.2.11 applied to $r+1,g'$. In particular, $|D_1| = r+1$.

We now verify that $D_1^*,\ldots,D_r^*$ is as required.

For claim i), since $D_1 \subseteq \ldots \subseteq D_r$, we have $\min(D_1) \ge \ldots \ge \min(D_r)$. We claim that $D_1^* \subseteq \ldots \subseteq D_r^*$. To see this, let $n \in D_i^*$. Then $n \in D_{i+1}$, $n > \min(D_i) \ge \min(D_{i+1})$, $n \in D_{i+1}^*$.

For claim ii), since $|D_1| = r+1$, we have $|D_1^*| = r$. since D_r is finite, D_r^* is finite.

Claim iii) is immediate from iii) of Lemma 5.2.11.

For claim iv), let $1 \le i \le r-1$, $x \in 48\alpha(r,D_i^*;1,r)$. Then $x > \min(D_i) \ge \min(D_{i+1})$. By Lemma 5.2.11 iv), $x \in D_{i+1} \cup g'D_{i+1}$. If $x \in D_{i+1}$ then $x \in D_{i+1}^*$. If $x \in g'D_{i+1}$ then $x \in g(D_{i+1}^*)$, because x must arise from the first clause in the definition of g'.

For claim v), let $1 \le i \le r-1$, $x \in 2\alpha(r,D_i^*;1,r)+1 \cup 3\alpha(r,D_i^*;1,r)+1$. Then $x > \min(D_i) \ge \min(D_{i+1})$. By Lemma 5.2.11 v), $x \in D_{i+1}$. Hence $x \in D_{i+1}^*$.

For vi), we have $D_r \cap g'D_r = \emptyset$. Since $g(D_r^*) \subseteq g'(D_r)$, we have $D_r^* \cap g(D_r^*) = \emptyset$.

Claim vii) is the same as vii) of Lemma 5.2.11.

For claim viii), let $1 \leq i \leq \beta(2r)$. Let $1 \leq i' \leq \beta(2r+2)$ be such that t[i',2r+2] is the result of replacing the variables $v_{r+1},\ldots,v_{2r}$ in t[i,2r] with the variables $v_{r+2},\ldots,v_{2r+1}$.

Let $x_1,\ldots,x_{2r} \in D_1^*$, $y_1,\ldots,y_r \in \alpha(r,D_2^*)$, where $(x_1,\ldots,x_r)$ and $(x_{r+1},\ldots,x_{2r})$ have the same order type and min, and $y_1,\ldots,y_r \leq \min(x_1,\ldots,x_r)$. Clearly

$$t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) = \\ t[i',2r+2](x_1,\ldots,x_r,x_r,y_1,\ldots,y_r,y_r).$$

$$t[i,2r](x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) = \\ t[i',2r+2](x_{r+1},\ldots,x_{2r},x_{2r},y_1,\ldots,y_r,y_r).$$

By Lemma 5.2.11 viii),

$$t[i',2r+2](x_1,\ldots,x_r,x_r,y_1,\ldots,y_r,y_r) \in D_3^* \leftrightarrow \\ t[i',2r+2](x_{r+1},\ldots,x_{2r},x_{2r},y_1,\ldots,y_r,y_r) \in D_3^*.$$

$$t[i,r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in D_3^* \leftrightarrow \\ t[i,r](x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \in D_3^*.$$

QED

5.3. Countable nonstandard models with limited indiscernibles.

LEMMA 5.3.1. There exist positive integers $\sigma_1,\tau_1,\sigma_2,\tau_2,\ldots$, each divisible by 96, such that for all $n \geq 1$ and $x,y \in N$,

$$\sigma_n x + \tau_n = \sigma_m y + \tau_m \rightarrow (n = m \wedge x = y).$$
$$\sigma_n,\tau_n \geq 96n.$$

Proof: For $n \geq 1$, let $\sigma_n = 96(p_n!)$ and $\tau_n = 96p_n$, where p_n is the n-th prime. Suppose $96(p_n!)x + 96p_n = 96(p_m!)y + 96p_m$. Then $p_n!x + p_n = p_m!y + p_m$. If $n \leq m$ then p_n clearly divides the left side and the first term of the right side. Hence p_n divides p_m. Therefore $n = m$. If $m \leq n$ then also $n = m$. Hence $n = m$. Therefore $x = y$. QED

DEFINITION 5.3.1. We fix σ_n,τ_n, $n \geq 1$, as given by Lemma 5.3.1.

Recall the standard pairing function P (Definition 3.2.1). We have $P(n,m) \geq n,m$. We use the extension $P(x,y,z) =$

$P(P(x,y),z)$. We have $P(n,m,r) \geq n,m,r$, and P is strictly increasing in each argument.

The following Lemma adjoins r predicates $E_1,\ldots,E_r \subseteq N$ to our basic standard countable structure $(N,<,0,1,+,-,\bullet,\uparrow,\log)$.

LEMMA 5.3.2. Let $r \geq 3$. There exists a structure $(N,<,0,1,+,-,\bullet,\uparrow,\log,E_1,\ldots,E_r)$ such that the following holds.
i) $E_1 \subseteq \ldots \subseteq E_r \subseteq N\backslash\{0\}$;
ii) $|E_1| = r$ and E_r is finite;
iii) For all $x < y$ from E_1, $x\uparrow < y$;
iv) Let $1 \leq i \leq \gamma(r)$, $1 \leq j < r$, $0 \leq a,b < r$, and $x \in \alpha(r,E_j;1,r)$. Then $(\exists v_2,\ldots,v_r \in E_{j+1})(v_2,\ldots,v_r \leq ax+b \wedge \varphi[i,r](x,v_2,\ldots,v_r)) \leftrightarrow \sigma_{P(i,a,b)}x+\tau_{P(i,a,b)} \notin E_{j+1}$;
v) For all $1 \leq j \leq r-1$, $2\alpha(r,E_j;1,r)+1$, $3\alpha(r,E_j;1,r)+1 \subseteq E_{j+1}$;
vi) $E_1 \cap \alpha(r,E_2;2,r) = \emptyset$;
vii) Let $1 \leq i \leq \beta(2r)$, $x_1,\ldots,x_{2p} \in E_1$, $y_1,\ldots,y_r \in \alpha(r,E_2)$, where $(x_1,\ldots,x_r)$ and $(x_{r+1},\ldots,x_{2r})$ have the same order type and min, and $y_1,\ldots,y_r \leq \min(x_1,\ldots,x_r)$. Then $t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in E_3 \leftrightarrow t[i,2r](x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \in E_3$.

Proof: Let $r \geq 3$, and let $r' >> r$. We define $\gamma(r)+3r$-ary $g \in$ BAF with $rng(g) \subseteq 48N$, as follows. Let $x\# = (y_1,\ldots,y_{\gamma(r)},z_1,\ldots,z_r,w_1,\ldots,w_r,x,x_2,\ldots,x_r) \in N^{\gamma(r)+3r}$. Let i be greatest such that $y_1 = \ldots = y_{i+1}$. Let a be greatest such that $z_1 = \ldots = z_{a+1}$. Let b be greatest such that $w_1 = \ldots = w_{b+1}$. (It will prove to be convenient to write x here instead of x_1.)

case 1. $0 < |x\#| \leq (3+a+b)x \wedge |x_2,\ldots,x_r| \leq ax+b \wedge \varphi[i,r](x,x_2,\ldots,x_r)$. Set $g(x\#) = \sigma_{P(i,a,b)}x+\tau_{P(i,a,b)}$.

case 2. Otherwise. Set $g(x\#) = 96|x\#|+48$.

In case 1, $g(x\#) \geq 96P(i,a,b)x \geq 96P(1,a,b)x \geq 96\max(1,a,b)x \geq 32(1+a+b)x \geq 8(3+a+b)x \geq 8|x\#| > |x\#|$. Also $g(x\#) \leq \sigma_{P(i,a,b)}|x\#|+\tau_{P(i,a,b)} \leq (\sigma_{P(i,a,b)}+\tau_{P(i,a,b)})|x\#|$.

In case 2, $|x\#| < g(x\#) \leq 192|x\#|$. Hence $g \in$ ELG $\cap$ SD $\cap$ BAF.

Clearly rng(g) $\subseteq$ 48N. So we can apply Lemma 5.2.12 with r'. Let $D_1,...,D_{r'} \subseteq$ N be given by Lemma 5.2.12. For all $1 < i \leq r$, set $E_i = D_i$. Set E_1 to be the first r elements of D_1.

Claims i),ii),iii),v),vi) for $E_1,...,E_r$ follow immediately from clauses i),ii),iii),v),vii) for $D_1,...,D_{r'}$ in Lemma 5.2.12.

For claim iv), let $1 \leq i \leq \gamma(r)$, $1 \leq j < r$, $0 \leq a,b < r$, and $x \in \alpha(r,E_j;1,r)$. We claim that

$$\sigma_{P(i,a,b)}x+\tau_{P(i,a,b)} \in 48\alpha(r',E_j;1,r').$$

To see this, write

$$|d_1,...,d_k| \leq x = t[i,r](d_1,...,d_k) \leq r|d_1,...,d_k|,$$

where $k \geq 1$ and $d_1,...,d_k \in E_j$. Since $96|\sigma_{P(i,a,b)}, 96|\tau_{P(i,a,b)}$, let $p = \sigma_{P(i,a,b)}/48$ and $q = \tau_{P(i,a,b)}/48$. Then we have

$$px+q \in \alpha(r',E_j;1,r')$$

since r' >> r and p,q > 0. This establishes the claim.

Since $r' \geq r$, by Lemma 5.2.12 iv),vi),

$$\sigma_{P(i,a,b)}x+\tau_{P(i,a,b)} \in E_{j+1} \cup. gE_{j+1}.$$

First assume that

$$\sigma_{P(i,a,b)}x+\tau_{P(i,a,b)} \notin E_{j+1}.$$

Then $\sigma_{P(i,a,b)}x+\tau_{P(i,a,b)} \in gE_{j+1}$. Write

$$\sigma_{P(i,a,b)}x+\tau_{P(i,a,b)} = g(y_1,...,y_{\gamma(r)},z_1,...,z_r,w_1,...,w_r,u,u_2,...,u_r),$$

where $y_1,...,y_{\gamma(r)},z_1,...,z_r,w_1,...,w_r,u,u_2,...,u_r \in E_{j+1}$.

Since 96 divides $\sigma_{P(i,a,b)}x+\tau_{P(i,a,b)}$, $\sigma_{(i,a,b,)}x+\tau_{P(i,a,b)}$ can only arise from case 1 in the definition of g.

Let i' be greatest such that $y_1 = ... = y_{i'+1}$, a' be greatest such that $z_1 = ... = z_{a'+1}$, and b' be greatest such that $w_1 = ... = w_{b'+1}$. Then

$$0 < |y_1,...,y_{\gamma(r)},z_1,...,z_r,w_1,...,w_r,u,u_2,...,u_r| \leq (3+a'+b')x.$$
$$u_2,...,u_r \leq a'u+b'.$$

$$\varphi[i',r](u,u_2,...,u_r).$$
$$g(y_1,...,y_{\gamma(r)},z_1,...,z_r,w_1,...,w_r,u,u_2,...,u_r) =$$
$$\sigma_{P(i',a',b')}u + \tau_{P(i',a',b')} = \sigma_{P(i,a,b)}x + \tau_{P(i,a,b)}.$$

By Lemma 5.3.1,

$$i = i' \wedge a = a' \wedge \wedge b = b' \wedge u = x.$$

Hence

$$u_2,...,u_r \leq ax+b.$$
$$\varphi[i,r](x,u_2,...,u_r).$$

In particular,

$$(\exists v_2,...,v_r \in E_{j+1})$$
$$(v_2,...,v_r \leq ax+b \wedge \varphi[i,r](x,v_2,...,v_r)).$$

Now assume that

$$(\exists v_2,...,v_r \in E_{j+1})$$
$$(v_2,...,v_r \leq ax+b \wedge \varphi[i,r](x,v_2,...,v_r)).$$

Let

$$x_2,...,x_r \in E_{j+1}.$$
$$x_2,...,x_r \leq ax+b.$$
$$\varphi[i,r](x,x_2,...,x_r).$$

By Lemma 5.2.12 v), $2x+1 \in 2\alpha(r';E_j,1,r')+1 \subseteq D_{j+1} = E_{j+1}$.
Note that

$$0 < |x,...,x,2x+1,...,2x+1,x,...,x,2x+1,...,2x+1,$$
$$x,...,x,2x+1,...,2x+1,x,x_2,...,x_r| \leq$$
$$\max(2x+1,ax+b) \leq (3+a+b)x.$$
$$x_2,...,x_r \leq ax+b.$$
$$\varphi[i,r](x,x_2,...,x_r).$$

Here the first group of x's has length i, the second group of x's has length a, and the third group of x's has length b.

Hence case 1 applies, and so

$$g(x,...,x,2x+1,...,2x+1,x,...,x,2x+1,...,2x+1,$$
$$x,...,x,2x+1,...,2x+1,x,x_2,...,x_r) =$$
$$\sigma_{P(i,a,b)}x+\tau_{P(i,a,b)}.$$

Hence $\sigma_{P(i,a,b)}x+\tau_{P(i,a,b)} \in gE_{j+1}$. By Lemma 5.2.12, vi), $E_{j+1} \cap gE_{j+1} = \emptyset$. Hence $\sigma_{P(i,a,b)}x+\tau_{P(i,a,b)} \notin E_{j+1}$ as required. This establishes claim iv).

Claim vii) is immediate from Lemma 5.2.12 vii). QED

We now work with countable structures whose domain is not N. These structures must interpret the language L, so that we work with structures of the form (A,<,0,1,+,-,•,log,...). In fact, this is why we wrote (N,<,0,1,+,-,•,↑,log,E_1,...,E_r) in Lemma 5.3.2.

Let M = (A,<,0,1,+,-,•,↑,log,...) be given. In all such M that we consider, M will satisfy a certain amount of arithmetic. In particular, M will satisfy TR(Π^0_1,L). See the discussion below.

DEFINITION 5.3.2. Let E ⊆ A and p ∈ N. We write α(E;p,<∞) for the set of x ∈ A such that the following holds. There is a term t in L that is not closed, and an assignment f to its variables, with rng(f) ⊆ E, such that x is the value of t under f, and a nonnegative integer k, such that x ∈ [pmax(rng(f)),kmax(rng(f))].

In the above, the value of t under f is computed using the interpretation M of L. It is important to note that here both p and k serve as standard integers.

DEFINITION 5.3.3. We let α(E) be the set of all values of terms t in L under an assignment of elements of E to the variables in t, computed according to M. For α(E), we allow closed terms.

DEFINITION 5.3.4. We also let α(r,E) be the set of all values of terms t in L with #(t) ≤ r, under an assignment of elements of E to the variables in t, computed according to M. For α(r,E), we also allow closed terms.

Recall the theory TR(Π^0_1,L) from Definition 5.1.10. It is clear that (N,<,0,1,+,-,•,↑,log) satisfies PA(L) + TR(Π^0_1,L), where PA(L) is Peano Arithmetic, formulated in L. See Definition 5.6.6.

LEMMA 5.3.3. There exists a countable structure M = (A,<,0,1,+,-,•,↑,log,E_1,E_2,...) obeying the following conditions.
i) (A,<,0,1,+,-,•,↑,log) satisfies TR(Π^0_1,L);
ii) $E_1 \subseteq E_2 \subseteq \ldots \subseteq A\backslash\{0\}$;

iii) E_1 has order type ω, and has no upper bound in A;
iv) For all $x < y$ from E_1, $x\uparrow < y$;
v) Let $r \geq 1$, $\varphi(v_1,...,v_r)$ be a quantifier free formula of L, and $a,b \in N$. There exists $d,e \in N\backslash\{0\}$ such that for all $j \geq 1$ and $x \in \alpha(E_j;1,<\infty)$, $(\exists v_2,...,v_r \in E_{j+1})(v_2,...,v_r \leq ax+b \wedge \varphi(x,v_2,...,v_r)) \leftrightarrow dx+e \notin E_{j+1}$;
vi) For all $j \geq 1$, $2\alpha(E_j;1,<\infty)+1$, $3\alpha(E_j;1,<\infty)+1 \subseteq E_{j+1}$;
vii) $E_1 \cap \alpha(E_2;2,<\infty) = \emptyset$;
viii) Let $r \geq 1$ and $t(v_1,...,v_{2r})$ be a term of L. Let $x_1,...,x_{2r} \in E_1$, $y_1,...,y_r \in \alpha(E_2)$, where $(x_1,...,x_r)$ and $(x_{r+1},...,x_{2r})$ have the same order type and min, and $y_1,...,y_r \leq \min(x_1,...,x_r)$. Then $t(x_1,...,x_r,y_1,...,y_r) \in E_3 \leftrightarrow t(x_{r+1},...,x_{2r},y_1,...,y_r) \in E_3$.

Proof: We apply the compactness theorem for predicate calculus with equality, to Lemma 5.3.2.

For the purposes of the proof of this Lemma only, we use the language L' which augments the language L with infinitely many unary relation symbols E_i, $i \geq 1$, and infinitely many constant symbols, c_i, $i \geq 1$.

Let T be the following set of axioms in L'.

1. $TR(\Pi^0_1,L)$.
2. For all $i \geq 1$, we take $c_i < c_{i+1} \wedge c_i \in E_1$.
3. For all $i \geq 1$, we take $E_i \subseteq E_{i+1} \wedge 0 \notin E_i$.
4. $(\forall x,y \in E_1)(x < y \rightarrow x\uparrow < y)$.
5. Let $1 \leq i \leq \gamma(r)$, $1 \leq j < r$, and $0 \leq a,b < r$. $(\forall v_1 \in \alpha(E_j;1,<\infty))((\exists v_2,...,v_r \in E_{j+1})(v_2,...,v_r \leq av_1+b \wedge \varphi[i,r](v_1,...,v_r)) \leftrightarrow \sigma_{P(i,a,b)}v_1+\tau_{P(i,a,b)} \notin E_{j+1})$. Here we index over r,i,j,a,b, and also non closed terms and standard integer upper coefficients for $\alpha(E_j;1,<\infty)$. The latter is used to create infinitely many conditional members of $\alpha(E_j;1,<\infty)$).
6. Let $j \geq 1$. We take the schemes $2\alpha(E_j;1,<\infty)+1 \subseteq E_{j+1}$, $3\alpha(E_j;1,<\infty)+1 \subseteq E_{j+1}$. Here we index over j, and also non closed terms and standard integer upper coefficients for $\alpha(E_j;1,<\infty)$. The latter is used to create infinitely many conditional members of $\alpha(E_j;1,<\infty)$.
7. We take the scheme $E_1 \cap \alpha(E_2;2,<\infty) = \emptyset$. Here we index over non closed terms and also standard integer upper coefficients for $\alpha(E_2;2,<\infty)$. The latter is used to create infinitely many conditional members of $\alpha(E_j;2,<\infty)$.
8. Let $r \geq 1$ and t be a term in L with at most the variables $v_1,...,v_{2r}$. Let $x_1,...,x_{2r} \in E_1$, $y_1,...,y_r \in \alpha(r,E_2)$, where $(x_1,...,x_r)$ and $(x_{r+1},...,x_{2r})$ have the same order type and

min, and $y_1,...,y_r \leq \min(x_1,...,x_r)$. Then $t(x_1,...,x_r,y_1,...,y_r) \in E_3 \leftrightarrow t(x_{r+1},...,x_{2r},y_1,...,y_r) \in E_3$. Here we index over r,t, and terms for $\alpha(r,E_2)$. The latter is used to create finitely many conditional elements of $\alpha(r,E_2)$.

These axioms have very robust formulations in light of axioms 1. It suffices to remark that in 5, we take av+b to be

$$(1+...+1)\bullet v_i+(1+...+1)$$

where the 1's are associated to the left, and where there are a 1's in the first sum, and b 1's in the second sum. We take 0 1's to mean 0.

Let $T_0 \subseteq T$ be finite. Let $s \geq 3$ be so large that all of the i,r,j+1, values of β at # of terms, and upper coefficients used, are at most s.

Let $M_s = (N,<,0,1,+,-,\bullet,\uparrow,\log,E_1,...,E_s)$ be given by Lemma 5.3.2, with r = s. We now show that M_s satisfies T_0 + $TR(\Pi^0{}_1,L)$, where for all $1 \leq i \leq s$, c_i is interpreted as the i-th element of E_1 (c_1 is interpreted as $\min(E_1)$). Obviously, M_s satisfies 1,2 of T_0 by construction.

The axioms in T_0 from 3-4,6,7 obviously hold in M_s using Lemma 5.3.2 i)-iii),v),vi).

For the axioms in T_0 from 5, we have to handle several different r's at once. This is because of the different lengths of the existential quantifiers that appear in 5.

We use our convenient coding setup whereby if $1 \leq i \leq \gamma(r)$ and $1 \leq r \leq s$, then $\varphi[i,r] = \varphi[i,s]$.

For 5, let $1 \leq i \leq \gamma(r)$, $1 \leq j < r$, and $0 \leq a,b < r$. The axioms in T_0 from 5 must have $r \leq s$. By Lemma 5.3.2 iv), M_s satisfies

$$(\forall v_1 \in \alpha(s,E_j;1,s))((\exists v_2,...,v_s \in E_{j+1})$$
$$(v_2,...,v_s \leq av_1+b \wedge \varphi[i,s](v_1,...,v_s)) \leftrightarrow$$
$$\sigma_{P(i,a,b,)}v_1+\tau_{P(i,a,b)} \notin E_{j+1}).$$

It is clear that M_s satisfies

$$(\forall v_1 \in \alpha(r,E_j;1,r))((\exists v_2,...,v_r \in E_{j+1})$$
$$(v_2,...,v_r \leq av_1+b \wedge \varphi[i,r](v_1,...,v_r)) \leftrightarrow$$

$\sigma_{P(i,a,b)}v_1+\tau_{P(i,a,b)} \notin E_{j+1})$

since $1 \leq r \leq s$. In particular, all variables in $\varphi[i,s] = \varphi[i,r]$ are among $v_1,...,v_r$, so the extra existential quantifiers, $v_{r+1},...,v_s$, are dummy quantifiers. Therefore M_s satisfies the axioms in T_0 from 5.

We now come to the verification of 8 in M_s. Let $r \geq 1$, t be a term in L with at most the variables v1,...,v2r, $x_1,...,x_{2r} \in E_1$, $y_1,...,y_r \in \alpha(r,E_2)$, where $(x_1,...,x_r)$ and $(x_{r+1},...,x_{2r})$ have the same order type and min, and $y_1,...,y_r \leq \min(x_1,...,x_r)$.

The axioms in T_0 from 8 must have $r \leq s$. Also we can let $1 \leq i \leq \beta(2s)$ be such that t[i,2s] is the result of replacing the variables $v_{r+1},...,v_{2r}$ in t by the variables $v_{s+1},...,v_{s+r}$. By Lemma 5.3.2 vii), M_s satisfies

$$t[j,2s](x_1,...,x_r,...,x_r,y_1,...,y_r,...,y_r) \in E_3 \leftrightarrow$$
$$t[j,2s](x_{r+1},...,x_{2r},...,x_{2r},y_1,...,y_r,...,y_r) \in E_3.$$

Note that

$$t[j,2s](x_1,...,x_r,...,x_r,y_1,...,y_r,...,y_r) = t(x_1,...,x_r,y_1,...,y_r).$$
$$t[j,2s](x_{r+1},...,x_{2r},...,x_{2r},y_1,...,y_r,...,y_r) = t(x_{r+1},...,x_{2r},y_1,...,y_r).$$

Hence M_s satisfies

$$t(x_1,...,x_r,y_1,...,y_r) \in E_3 \leftrightarrow$$
$$t(x_{r+1},...,x_{2r},y_1,...,y_r) \in E_3.$$

By the compactness theorem for first order predicate calculus with equality, T has a countable model $M = (A,<,0,1,+,-,\bullet,\uparrow,\log,E_1,E_2,...)$. We now verify clauses i)-viii) of Lemma 5.3.3, except for clause iii). In order to verify clause iii), we must adjust M.

Claim i) is immediate from axioms 1 of T.

Claim ii) is immediate from axioms 3 of T.

Claim iv) is immediate from axioms 4 of T.

For claim v), let $r \geq 1$, $\varphi(x_1,...,x_r)$ be a quantifier free formula of L, $a,b \in N$. By axiom 5 of T, M satisfies

$$(\forall v_1 \in \alpha(E_j;1,<\infty))$$
$$((\exists v_2,\ldots,v_r \in E_{j+1})(v_2,\ldots,v_r \leq ax_1+b \wedge \varphi[i,r](v_1,\ldots,v_r)) \leftrightarrow$$
$$\sigma_{P(i,a,b)}v_1+\tau_{P(i,a,b)} \notin E_{j+1}).$$

Set $d = \sigma_{P(i,a,b)}$ and $e = \tau_{P(i,a,b)}$.

For claim vi), let $r,j \geq 1$. By axiom 6 of T, M satisfies

$$2\alpha(r,E_j,1,r)+1 \subseteq E_{j+1}.$$
$$3\alpha(r,E_j,1,r)+1 \subseteq E_{j+1}.$$

Since r is arbitrary, M satisfies

$$2\alpha(E_j;1,<\infty)+1 \subseteq E_{j+1}.$$
$$3\alpha(E_j;1,<\infty)+1 \subseteq E_{j+1}.$$

Claim vii) follows immediately from axioms 7 of T.

Claim viii) also follows immediately from axioms 8 of T.

Now M may not satisfy iii). We will instead use an initial segment of M so that iii) holds. We need to check that the above verifications in M are still valid in our initial segment of M (defined below).

By axioms 2 of T, let $E_1' \subseteq E_1$ be of order type ω. Let

$$A' = \{x \in dom(M): (\exists y \in E_1')(x < y)\}.$$

Note that by axioms 1,4 of T, A' is closed under all of the primitive operations of L. Hence we let M' be M restricted to A', where the E_1 of M' is E_1', and the E_j of M', $j \geq 2$, is $E_j \cap A'$.

We now show that M' satisfies all of the claims i)-viii).

For i), note that M' is still a model of $TR(\Pi^0{}_1,L)$ because M' is an initial segment of M that is closed under the operations of M.

Claims ii),iii) are immediate by the definitions of the E_i of M'.

The remaining claims are all immediate since all of the quantifiers are bounded, the initial segment A' is closed under all of the primitive operations of M, and E_1 has been shrunk to $E_1' \subseteq E_1$. QED

We fix $M = (A,<,0,1,+,-,\bullet,\uparrow,\log,E_1,E_2,...)$ as given by Lemma 5.3.3.

DEFINITION 5.3.5. We will use the notation $|y_1,...,y_r|$ for the maximum of $y_1,...,y_r \in A$ in the sense of M.

LEMMA 5.3.4. Every element of E_1 is nonstandard.

Proof: Fix a standard element k of E_1. Let t(x) be a term of L such that

$$t(x) = k \text{ if } x = k;\ 0 \text{ otherwise.}$$

By Lemma 5.3.3 iii), let $k < n$, $n \in E_1$. By Lemma 5.3.3 viii),

$$t(k) \in E_3 \leftrightarrow t(n) \in E_3.$$
$$k \in E_3 \leftrightarrow 0 \in E_3.$$

This is a contradiction since $k \in E_3$ and $0 \notin E_3$, by Lemma 5.3.3 ii). QED

LEMMA 5.3.5. Let $r,j \geq 1$, $\varphi(v_1,...,v_r)$ be a quantifier free formula of L, $a,b \in N$, and $x \in \alpha(E_1;1,<\infty)$ Then $(\exists v_2,...,v_r \in E_{j+1})(v_2,...,v_r \leq ax+b \wedge \varphi(x,v_2,...,v_r)) \leftrightarrow$ $(\exists v_2,...,v_r \in E_2)(v_2,...,v_r \leq ax+b \wedge \varphi(x,v_2,...,v_r))$.

Proof: Let $r \geq 1$, $\varphi(v_1,...,v_r)$ be a quantifier free formula of L, and $a,b \in N$. By Lemma 5.3.3 v), let $d,e \in N\backslash\{0\}$ be such that the following holds. For all $j \geq 1$ and $x_1 \in \alpha(E_1;1,<\infty)$,

$$(\exists v_2,...,v_r \in E_{j+1})(v_2,...,v_r \leq ax+b \wedge \varphi(x,v_2,...,v_r)) \leftrightarrow dx+e \notin E_{j+1}.$$

Now let $j \geq 1$ and $x \in \alpha(E_1;1,<\infty)$. Then

$$(\exists v_2,...,v_r \in E_{j+1})(v_2,...,v_r \leq ax+b \wedge \varphi(x,v_2,...,v_r)) \rightarrow$$
$$dx+e \notin E_{j+1} \rightarrow dx+e \notin E_2 \rightarrow$$
$$(\exists v_2,...,v_r \in E_2)(v_2,...,v_r \leq ax+b \wedge \varphi(x,v_2,...,v_r)).$$

QED

LEMMA 5.3.6. For all $j \geq 1$, $E_1 \cap \alpha(E_j;2,<\infty) = \emptyset$.

Proof: By Lemma 5.3.3 vii), this is true for $j = 1,2$. Suppose this is false for some fixed $j \geq 3$. Let $y \in E_1$, p,r

≥ 1, $t(v_2,\ldots,v_r)$ be a term of L, $x_2,\ldots,x_r \in E_j$, $y = t(x_2,\ldots,x_r)$, and $2|x_2,\ldots,x_r| \leq y \leq p|x_2,\ldots,x_k|$. Then

$$(\exists v_2,\ldots,v_r \in E_j)(v_2,\ldots,v_r \leq y \wedge 2|v_2,\ldots,v_r| \leq y \leq p|v_1,\ldots,v_r| \wedge y = t(v_2,\ldots,v_r)).$$

By Lemma 5.3.5,

$$(\exists v_2,\ldots,v_r \in E_2)(v_2,\ldots,v_r \leq y \wedge 2|v_2,\ldots,v_r| \leq y \leq p|v_2,\ldots,v_r| \wedge y = t(v_2,\ldots,v_r)).$$

Therefore $y \in \alpha(E_2;2,<\infty)$. Since $y \in E_1$, this contradicts Lemma 5.3.3 vii). QED

LEMMA 5.3.7. Let $r \geq 1$ and $\varphi(v_1,\ldots,v_{2r})$ be a quantifier free formula of L. Let $x_1,\ldots,x_{2r} \in E_1$, $y_1,\ldots,y_r \in \alpha(E_2)$, where $(x_1,\ldots,x_r)$ and $(x_{r+1},\ldots,x_{2r})$ have the same order type and min, and $y_1,\ldots,y_r \leq \min(x_1,\ldots,x_r)$. Then $\varphi(x_1,\ldots,x_r,y_1,\ldots,y_r) \leftrightarrow \varphi(x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r)$.

Proof: Let r,φ be as given. Let $f:N^{2r} \to N$ be defined by

$$f(x_1,\ldots,x_{2r}) = 0 \text{ if } \varphi(x_1,\ldots,x_{2r});\ x_1 \text{ otherwise.}$$

Obviously, f is given by a term $t(x_1,\ldots,x_{2r})$ of L.

Let $x_1,\ldots,x_{2r},y_1,\ldots,y_r$ be as given. Since $0 \notin E_3$ and $x_1,\ldots,x_{2r} \in E_1$, we have

$$\varphi(x_1,\ldots,x_r,y_1,\ldots,y_r) \leftrightarrow t(x_1,\ldots,x_r,y_1,\ldots,y_r) \notin E_3.$$
$$\varphi(x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \leftrightarrow t(x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \notin E_3.$$

By Lemma 5.3.3 viii),

$$t(x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \in E_3 \leftrightarrow t(x_1,\ldots,x_r,y_1,\ldots,y_r) \in E_3.$$
$$\varphi(x_1,\ldots,x_r,y_1,\ldots,y_r) \leftrightarrow \varphi(x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r).$$

QED

DEFINITION 5.3.6. For x in A and $k \geq 0$, we write $\uparrow k(x)$ for $x\uparrow\ldots\uparrow$, where there are k $\uparrow$'s. We take $\uparrow 0(x) = x$.

DEFINITION 5.3.7. By Lemma 5.3.4 and Lemma 5.3.3 iii), we fix $c_1 < c_2 < \ldots$ to be the strictly increasing ω enumeration of E_1, which consists entirely of nonstandard elements. The c's are unbounded in A.

LEMMA 5.3.8. Let $r \geq 1$ and $t(v_1,\ldots,v_r)$ be a term of L. There exists $p \in N$ such that for all $x_1,\ldots,x_r$, $t(x_1,\ldots,x_r) \leq \uparrow p(|x_1,\ldots,x_r|)$. Furthermore, if $x_1,\ldots,x_r \leq c_n$ then $t(x_1,\ldots,x_r) < c_{n+1}$.

Proof: Let $r \geq 1$. The first claim is easily proved by induction on the term $t(v_1,\ldots,v_r)$.

We now show that for all $p \in N$ and $n \geq 1$, $\uparrow p(c_n) < c_{n+1}$. Suppose $\uparrow p(c_n) \geq c_{n+1}$. By Lemma 5.3.7, for all $m \geq n+1$, $\uparrow p(c_n) \geq c_m$. But this contradicts Lemma 5.3.3 iii), that the c's have no upper bound in A.

For the second claim, we use p from the first claim, which depends only on r,t. Let $x_1,\ldots,x_r \leq c_n$. Then $t(x_1,\ldots,x_r) \leq \uparrow p(|x_1,\ldots,x_r|) \leq \uparrow p(c_n) < c_{n+1}$. QED

LEMMA 5.3.9. For all $a,b \in N$ there exist $c,d \in N\backslash\{0\}$ such that the following holds. Let $j \geq 1$ and $x \in \alpha(E_j;1,<\infty)$. Then $ax+b \in E_{j+1} \leftrightarrow cx+d \notin E_{j+1}$.

Proof: Let $a,b \in N$. By Lemma 5.3.3 v), let $c,d \in N\backslash\{0\}$ be such that the following holds. Let $j \geq 1$ and $x \in E_j$. Then

$$(\exists v_2 \in E_{j+1})(v_2 \leq ax+b \wedge v_2 = ax+b) \leftrightarrow cx+d \notin E_{j+1}.$$

I.e.,

$$ax+b \in E_{j+1} \leftrightarrow cx+d \notin E_{j+1}.$$

QED

LEMMA 5.3.10. Let $r \geq 1$, $a,b \in N$, and $\varphi(x_1,\ldots,x_r)$ be a quantifier free formula in L. There exist $d,e,f,g \in N\backslash\{0\}$ such that the following holds. Let $j \geq 1$ and $x \in \alpha(E_j;1,<\infty)$. Then $(\exists v_2,\ldots,v_r \in E_{j+1})(v_2,\ldots,v_r \leq ax+b \wedge \varphi(x,v_2,\ldots,v_r)) \leftrightarrow dx+e \notin E_{j+1} \leftrightarrow fx+g \in E_{j+1}$.

Proof: Let r,φ,a,b be as given. By Lemma 5.3.3 v), let $d,e \in N\backslash\{0\}$ be such that the following holds. Let $j \geq 1$ and $x \in \alpha(E_j;1,<\infty)$. Then

$$(\exists v_2,\ldots,v_r \in E_{j+1})(v_2,\ldots,v_r \leq ax+b \wedge \varphi(x,v_2,\ldots,v_r)) \leftrightarrow dx+e \notin E_{j+1}.$$

By Lemma 5.3.9, let $f,g \in N\backslash\{0\}$ be such that for all $j \geq 1$ and $x \in \alpha(E_j;1,<\infty)$,

$$dx+e \in E_{j+1} \leftrightarrow fx+g \notin E_{j+1}.$$

$$(\exists v_2,\ldots,v_r \in E_{j+1})(v_2,\ldots,v_r \leq ax+b \wedge \varphi(v_1,\ldots,v_r)) \leftrightarrow$$
$$dx+e \notin E_{j+1} \leftrightarrow px+q \in E_{j+1}.$$

QED

We view Lemma 5.3.10 as a form of quantifier elimination without parameters. We need to develop a workable form of this kind of quantifier elimination with parameters. This requires that we have a mechanism for coding up tuples.

DEFINITION 5.3.8. We adapt the standard pairing function of Definition 3.2.1 to map A^2 onto A, for our structure M. I.e., for all $x,y \in A$,

$$P(x,y) = (x+y)(x+y+1)/2 + y = (x^2+y^2+2xy+x+3y)/2.$$

By Lemma 5.3.3 i, M satisfies $TR(\Pi^0{}_1,L)$. Hence $P:A^2 \rightarrow A$ is one-one, onto, P is strictly increasing in each argument, and for all $x,y \in A$, $P(x,y) \geq x,y$.

DEFINITION 5.3.9. We extend P naturally to any finite number of arguments by $P(x) = x$, and for $k \geq 3$, $P(x_1,\ldots,x_k) = P(P(x_1,x_2),x_3,\ldots,x_k)$.

Note that for each $k \geq 1$, P is a bijection from A^k onto A, P is strictly increasing in each argument, and for all $x_1,\ldots,x_k \in A$, $P(x_1,\ldots,x_k) \geq x_1,\ldots,x_k$.

DEFINITION 5.3.10. We also define, in M,

$$x \div y = \text{the unique } z \text{ such that } y \bullet z \leq x < (y+1) \bullet z \text{ if } y \neq 0;$$
$$0 \text{ otherwise.}$$

Let $x_1,\ldots,x_k \leq c_n$, where $x_1,\ldots,x_k \in E_j$. Suppose we want to code $x_1,\ldots,x_k$. The natural choice is of course $P(x_1,\ldots,x_k)$. However, at this point, we don't know that $P(x_1,\ldots,x_k) \in E_j$, or even $P(x_1,\ldots,x_k) \in E_{j+1}$, $2P(x_1,\ldots,x_k) \in E_{j+1}$, or $3P(x_1,\ldots,x_k)+1 \in E_{j+1}$, which severely limits the usefulness of $P(x_1,\ldots x_k)$.

Our approach is to use $c_m > c_n$ to give a code for $x_1,\ldots,x_k \leq c_n$ that we can really use. For each $m > n$, a useful code for $x_1,\ldots,x_k \leq c_n$ is

$$CODE(c_m;x_1,\ldots,x_k) = 8((\log(c_m))\uparrow+P(x_1,\ldots,x_k))+1.$$

We make a more general definition.

DEFINITION 5.3.11. We define

$$\text{CODE}(w;x_1,\ldots,x_k) = 8((\log(w))\uparrow+P(x_1,\ldots,x_k))+1.$$
$$\text{INCODE}(x) = (x-(\log(x))\uparrow-1)\div 8.$$

Here ÷8 is the floor of the result of dividing by 8. Also, the - here is associated to the left: a-b-c = (a-b)-c.

Note that CODE is given by a term in L. However, INCODE (inverse code) is not given by a term in L. So we have to be careful how we use INCODE. This issue arises in the proof of Lemma 5.3.13, statement 1). But note that

$$y\div 8 = z \leftrightarrow 8z \leq y < 8z+8.$$
$$\text{INCODE}(x) = z \leftrightarrow 8z \leq x-(\log(x))\uparrow-1 < 8z+8.$$

Thus the associated graphs are expressible as quantifier free formulas of L. This supports careful use of INCODE.

Recall that from the proof of Theorem 5.1.5, $\log(w)\uparrow$ is the greatest power of 2 that is $\leq w$ if $w > 0$; 1 otherwise.

LEMMA 5.3.11. Let $k,n,m \geq 1$, and $x_1,\ldots,x_k \leq c_n < c_m$, where $x_1,\ldots,x_k \in \alpha(E_j;1,<\infty)$. Then $\text{CODE}(c_m;x_1,\ldots,x_k) \in \alpha(E_j;2,<\infty) \cap E_{j+1}$. Separately, let $k \geq 1$ and $8P(x_1,\ldots,x_k)+1 < \log(w)$. Then $\text{INCODE}(\text{CODE}(w;x_1,\ldots,x_k)) = P(x_1,\ldots,x_k)$.

Proof: Let $k,n,m,x_1,\ldots,x_k$ be as given. Note that

$$(c_m\div 2)+1 \leq (\log(c_m))\uparrow \leq c_m.$$
$$2c_m \leq 4(\log(c_m))\uparrow+P(x_1,\ldots x_k)) \leq 5c_m.$$

$$4((\log(c_m))\uparrow+P(x_1,\ldots x_k)) \in \alpha(E_j;2,<\infty).$$
$$\text{CODE}(c_m;x_1,\ldots,x_k) \in 2\alpha(E_j;2,<\infty)+1.$$

We have $\text{CODE}(c_m;x_1,\ldots,x_k) \in E_{j+1}$ by Lemma 5.3.3 vi).

Now let $k,x_1,\ldots,x_k,w$ be as given. We claim that

1) $\log(\text{CODE}(w;x_1,\ldots,x_k)) = \log(w)+3.$

To see this, note that

$$\log(\text{CODE}(w;x_1,\ldots,x_k)) =$$
$$\log(8((\log(w))\uparrow + P(x_1,\ldots,x_k))+1) =$$
$$\log(8(\log(w))\uparrow + 8P(x_1,\ldots,x_k) + 1) =$$

$$\log((\log(w)+3)\uparrow + 8P(x_1,...,x_k) + 1) \leq$$
$$\log((\log(w)+3)\uparrow + \log(w)) = \log(w)+3 \leq$$
$$\log((\log(w)+3)\uparrow + 8P(x_1,...,x_k) + 1).$$

Using 1),

$$\text{INCODE}(\text{CODE}(w;x_1,...,x_k)) = z \leftrightarrow$$
$$8z \leq \text{CODE}(w;x_1,...,x_k)-(\log(\text{CODE}(w;x_1,...,x_k)))\uparrow-1 < 8z+8 \leftrightarrow$$
$$8z \leq \text{CODE}(w;x_1,...,x_k)-(\log(w)+3)\uparrow-1 < 8z+8 \leftrightarrow$$
$$8z \leq \text{CODE}(w;x_1,...,x_k)-8((\log(w))\uparrow)-1 < 8z+8 \leftrightarrow$$
$$8z \leq 8P(x_1,...,x_k) < 8z+8.$$

Hence

$$\text{INCODE}(\text{CODE}(w;x_1,...,x_k)) = P(x_1,...,x_k).$$

QED

LEMMA 5.3.12. Let $x \in \alpha(E_j;1,<\infty)$. There exist $y,z \in E_{j+1} \cap [0,4x]$ such that $x = y-z$.

Proof: Let x be as given. By Lemma 5.3.3 vi), $2x+1$, $3x+1 \in E_{j+1}$. Write $x = (3x+1)-(2x+1)$. QED

LEMMA 5.3.13. Let $r \geq 1$, $p \geq 2$, and $\varphi(v_1,...,v_{2r})$ be a quantifier free formula of L. There exist $a,b,d,e \in N\backslash\{0\}$ such that the following holds. Let $j,n \geq 1$ and $x_1,...,x_r \in \alpha(E_j;1,<\infty) \cap [0,c_n]$. Then

$$(\exists v_{r+1},...,v_{2r} \in E_{j+1})(v_{r+1},...,v_{2r} \leq \uparrow p(|x_1,...,x_r|) \wedge$$
$$\varphi(x_1,...,x_r,v_{r+1},...,v_{2r})) \leftrightarrow$$
$$a\text{CODE}(c_{n+1};x_1,...,x_r)+b \notin E_{j+1} \leftrightarrow$$
$$d\text{CODE}(c_{n+1};x_1,...,x_r)+e \in E_{j+1}.$$

Proof: Let r,p,φ be as given. By Lemma 5.3.10, let $a,b,d,e \in N\backslash\{0\}$ be such that the following holds. Let $j \geq 1$ and $x \in \alpha(E_j;1,<\infty)$. Then

1) $(\exists v_1,...,v_{3r} \in E_{j+1})(v_1,...,v_{3r} \leq x \wedge v_{r+1},...,v_{2r} \leq \uparrow p(|v_{2r+1}-v_1,...,v_{3r}-v_r|) \wedge \text{INCODE}(x) = P(v_{2r+1}-v_1,...,v_{3r}-v_r) \wedge \varphi(v_{2r+1}-v_1,...,v_{3r}-v_r,v_{r+1},...,v_{2r})) \leftrightarrow ax+b \notin E_{j+1} \leftrightarrow dx+e \in E_{j+1}$.

We have used the fact that $\text{INCODE}(v) = P(v_1,...,v_r)$ can be expanded out as a formula of L in variables $v,v_1,...,v_r$, as observed just before Lemma 5.3.11.

Now let $j,n \geq 1$, $x_1,\ldots,x_r \in \alpha(E_j;1,<\infty) \cap [0,c_n]$. By Lemma 5.3.11, $CODE(c_{n+1};x_1,\ldots,x_r) \in \alpha(E_j;1,<\infty)$. Hence we can set $x = CODE(c_{n+1};x_1,\ldots,x_r)$ and obtain the following.

2) $(\exists v_1,\ldots,v_{3r} \in E_{j+1})(v_1,\ldots,v_{3r} \leq CODE(c_{n+1};x_1,\ldots,x_r) \wedge v_{r+1},\ldots,v_{2r} \leq \uparrow p(|v_{2r+1}-v_1,\ldots,v_{3r}-v_r|) \wedge INCODE(CODE(c_{n+1};x_1,\ldots,x_r)) = P(v_{2r+1}-v_1,\ldots,v_{3r}-v_r) \wedge \varphi(v_{2r+1}-v_1,\ldots,v_{3r}-v_r,v_{r+1},\ldots,v_{2r})) \leftrightarrow aCODE(c_{n+1};x_1,\ldots,x_r)+b \notin E_{j+1} \leftrightarrow dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E_{j+1}$.

By Lemma 5.3.8, $8P(x_1,\ldots,x_r)+1 < \log(c_{n+1})$. Using Lemma 5.3.11,

3) $(\exists v_1,\ldots,v_{3r} \in E_{j+1})(v_1,\ldots,v_{2r} \leq CODE(c_{n+1};x_1,\ldots,x_r) \wedge v_{r+1},\ldots,v_{2r} \leq \uparrow p(|v_{2r+1}-v_1,\ldots,v_{3r}-v_r|) \wedge P(x_1,\ldots,x_r) = P(v_{2r+1}-v_1,\ldots,v_{3r}-v_r) \wedge \varphi(v_{2r+1}-v_1,\ldots,v_{3r}-v_r,v_{r+1},\ldots,v_{2r})) \leftrightarrow aCODE(c_{n+1};x_1,\ldots,x_r)+b \notin E_{j+1} \leftrightarrow dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E_{j+1}$.

4) $(\exists v_1,\ldots,v_{3r} \in E_{j+1})(v_1,\ldots,v_{2r} \leq CODE(c_{n+1};x_1,\ldots,x_r) \wedge v_{r+1},\ldots,v_{2r} \leq \uparrow p(|v_{2r+1}-v_1,\ldots,v_{3r}-v_r|) \wedge x_1 = v_{2r+1}-v_1 \wedge \ldots \wedge x_r = v_{3r}-v_r \wedge \varphi(v_{2r+1}-v_1,\ldots,v_{3r}-v_r,v_{r+1},\ldots,v_{2r})) \leftrightarrow aCODE(c_{n+1};x_1,\ldots,x_r)+b \notin E_{j+1} \leftrightarrow dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E_{j+1}$.

By Lemma 5.3.12,

5) $(\exists v_{r+1},\ldots,v_{2r} \in E_{j+1})(v_{r+1},\ldots,v_{2r} \leq CODE(c_{n+1};x_1,\ldots,x_r) \wedge v_{r+1},\ldots,v_{2r} \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,v_{r+1},\ldots,v_{2r})) \leftrightarrow aCODE(c_{n+1};x_1,\ldots,x_r)+b \notin E_{j+1} \leftrightarrow dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E_{j+1}$.

Note that the application of Lemma 5.3.12 to the $x = 1$ requires $1 = 4-3$, and $4 \leq \uparrow 1(1)$ is false. However, $4 \leq \uparrow 2(1)$ is true. This explains why we require $p \geq 2$.

By $x_1,\ldots,x_r \leq c_n$ and Lemma 5.3.8,

6) $(\exists v_{r+1},\ldots,v_{2r} \in E_{j+1})(v_{r+1},\ldots,v_{2r} \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,v_{r+1},\ldots,v_{2r})) \leftrightarrow aCODE(c_{n+1};x_1,\ldots,x_r)+b \notin E_{j+1} \leftrightarrow dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E_{j+1}$.

QED

LEMMA 5.3.14. Let $r \geq 1$, $i_1,\ldots,i_r \geq 1$, and $\varphi(x_1,\ldots,x_{2r})$ be a quantifier free formula of L. Suppose $(\forall v_1,\ldots,v_r \in E_2)(\varphi(c_{i\_1},\ldots,c_{i\_r},v_1,\ldots,v_r))$. Then for all $j \geq 1$, $(\forall v_1,\ldots,v_r \in E_j)(\varphi(c_{i\_1},\ldots,c_{i\_r},v_1,\ldots,v_r))$.

Proof: Let $r,\varphi,i_1,\ldots,i_r$ be as given. Fix $n > i_1,\ldots,i_r$.

We apply Lemma 5.3.13. Let a,b,d,e $\in$ N\{0} be such that the following holds. For all j $\geq$ 1,

$$(\exists v_1,\ldots,v_{r+1} \in E_{j+1})(v_1,\ldots,v_r \leq |c_{i\_1},\ldots,c_{i\_r},c_n|\uparrow\uparrow \wedge v_1,\ldots,v_r \leq c_n \wedge \neg\varphi(c_{i\_1},\ldots,c_{i\_r},v_1,\ldots,v_r)) \leftrightarrow \text{aCODE}(c_{n+1};c_{i\_1},\ldots,c_{i\_r},c_n)+b \notin E_{j+1} \leftrightarrow \text{dCODE}(c_{n+1};c_{i\_1},\ldots,c_{i\_r},c_n)+e \in E_{j+1}.$$

$$(\exists v_1,\ldots,v_r \in E_{j+1})(v_1,\ldots,v_r \leq c_n \wedge \neg\varphi(c_{i\_1},\ldots,c_{i\_r},v_1,\ldots,v_r)) \leftrightarrow \text{aCODE}(c_{n+1};c_{i\_1},\ldots,c_{i\_r},c_n)+b \notin E_{j+1} \leftrightarrow \text{dCODE}(c_{n+1};c_{i\_1},\ldots,c_{i\_r},c_n)+e \in E_{j+1}.$$

By hypothesis,

$$\neg(\exists v_1,\ldots,v_r \in E_2)(v_1,\ldots,v_r \leq c_n \wedge \neg\varphi(c_{i\_1},\ldots,c_{i\_r},v_1,\ldots,v_r)).$$

$$\text{aCODE}(c_{n+1};c_{i\_1},\ldots,c_{i\_r},c_n)+b \in E_2.$$

Now let j $\geq$ 1. Then

$$\text{aCODE}(c_{n+1};c_{i\_1},\ldots,c_{i\_r},c_n)+b \in E_{j+1}.$$

Hence

$$\neg(\exists v_1,\ldots,v_r \in E_{j+1})(v_1,\ldots,v_r \leq c_n \wedge \neg\varphi(c_{i\_1},\ldots,c_{i\_r},v_1,\ldots,v_r)).$$

I.e.,

$$(\forall v_1,\ldots,v_r \in E_{j+1})(v_1,\ldots,v_r \leq c_n \rightarrow \varphi(c_{i\_1},\ldots,c_{i\_r},v_1,\ldots,v_r)).$$

Since $n \geq i_1,\ldots,i_r$ is arbitrary and the c's have no upper bound in A, we have

$$(\forall v_1,\ldots,v_r \in E_{j+1})(\varphi(c_{i\_1},\ldots,c_{i\_r},v_1,\ldots,v_r)).$$

QED

DEFINITION 5.3.12. We say that $t(v_1,\ldots,v_r)$ is a $(p,<\infty)$ term of L if and only if

i. $t(v_1,\ldots,v_r)$ is a term of L.
ii. p is a positive standard integer.
iii. There exists a standard integer q such that for all $x_1,\ldots,x_r \in A$, $p|x_1,\ldots,x_r| \leq t(x_1,\ldots,x_r) \leq q|x_1,\ldots,x_r|$.

LEMMA 5.3.15. Let $r \geq 1$, $t(v_1,...,v_{2r})$ be a $(1,<\infty)$ term of L, and $i_1,...,i_{2r} \geq 1$, where $(i_1,...,i_r)$ and $(i_{r+1},...,i_{2r})$ have the same order type and min. For all $j \geq 1$, $y_1,...,y_r \in E_j$, $y_1,...,y_r \leq \min(c_{i\_1},...,c_{i\_r})$,

$$t(c_{i\_1},...,c_{i\_r},y_1,...,y_r) \in E_{j+1} \leftrightarrow t(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r) \in E_{j+1}.$$

Proof: By Lemma 5.3.3 viii), this holds for $j = 2$. In fact, in the case $j = 2$, we have the equivalence for any term t.

We will use Lemma 5.3.14 to argue that it holds for any $j \geq 1$. But there are many details that need to be checked.

By Lemma 5.3.9, let $a,b \in N\backslash\{0\}$ be such that the following holds. For all $j \geq 1$ and $x \in \alpha(E_j;1,<\infty)$,

$$1)\ x \in E_{j+1} \leftrightarrow ax+b \notin E_{j+1}.$$

Let $r,t,i_1,...,i_{2r}$ be as given. Fix $n = \min(i_1,...,i_{2r})$.

Since t is a $(1,<\infty)$ term, for all $j \geq 1$ and $y_1,...,y_r \in E_j$,

$$2)\ t(c_{i\_1},...,c_{i\_r},y_1,...,y_r),\ t(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r) \in \alpha(E_j;1,<\infty).$$

By 1),2), for all $j \geq 1$ and $y_1,...,y_r \in E_j$,

$$3)\ t(c_{i\_1},...,c_{i\_r},y_1,...,y_r) \in E_{j+1} \rightarrow at(c_{i\_1},...,c_{i\_r},y_1,...,y_r)+b \notin E_{j+1}$$
$$\wedge$$
$$t(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r) \in E_{j+1} \rightarrow at(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r)+b \notin E_{j+1}.$$

By Lemma 5.3.3 viii), for all $y_1,...,y_r \in \alpha(E_2) \cap [0,c_n]$,

$$4)\ t(c_{i\_1},...,c_{i\_r},y_1,...,y_r) \in E_3 \rightarrow t(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r) \in E_3$$
$$\wedge$$
$$t(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r) \in E_3 \rightarrow t(c_{i\_1},...,c_{i\_r},y_1,...,y_r) \in E_3.$$

By 1),2),4), for all $y_1,...,y_r \in E_2 \cap [0,c_n]$,

$$5)\ t(c_{i\_1},...,c_{i\_r},y_1,...,y_r) \in E_3 \rightarrow at(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r)+b \notin E_3$$
$$\wedge$$
$$t(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r) \in E_3 \rightarrow$$

$$at(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)+b \notin E_3.$$

By elementary logical manipulations from 5, for all $y_1,\ldots,y_r \in E_2 \cap [0,c_n]$,

$$t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \notin E_3 \lor$$
$$at(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)+b \notin E_3$$
$$\land$$
$$t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \notin E_3 \lor$$
$$at(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)+b \notin E_3.$$

$$(\forall u,v \in E_3)(t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \neq u \lor$$
$$at(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)+b \neq v)$$
$$\land$$
$$(\forall u,v \in E_3)(t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \neq u \lor$$
$$at(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)+b \neq v).$$

$$6)\ (\forall u_1,u_2,u_3,u_4 \in E_3)$$
$$(t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \neq u_1 \lor$$
$$at(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)+b \neq u_2$$
$$\land$$
$$t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \neq u_3 \lor$$
$$at(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)+b \neq u_4).$$

Write 6) in the form

$$7)\ (\forall v_{3r+1},v_{3r+2},v_{3r+3},v_{3r+4} \in E_3)$$
$$\psi(c_{i\_1},\ldots,c_{i\_2r},v_{2r+1},\ldots,v_{3r+4}).$$

where ψ is given by

$$8)\ \psi(v_1,\ldots,v_{3r+4}) =$$
$$(t(v_1,\ldots,v_r,v_{2r+1},\ldots,y_{3r}) \neq v_{3r+1} \lor$$
$$at(v_{r+1},\ldots,v_{2r},v_{2r+1},\ldots,v_{3r})+b \neq v_{3r+2}$$
$$\land$$
$$t(v_{r+1},\ldots,v_{2r},\ v_{2r+1},\ldots,y_{3r}) \neq v_{3r+3} \lor$$
$$at(v_1,\ldots,v_r,v_{2r+1},\ldots,y_{3r})+b \neq v_{3r+4}).$$

To recapitulate, we have

$$9)\ (\forall v_{2r+1},\ldots,v_{3r} \in E_2)(v_{2r+1},\ldots,v_{3r} \leq c_n \rightarrow$$
$$(\forall v_{3r+1},v_{3r+2},v_{3r+3},v_{3r+4} \in E_3)$$
$$(\psi(c_{i\_1},\ldots,c_{i\_2r},v_{2r+1},\ldots,y_{3r+4}))).$$

We can weaken 9) to

$$10)\ (\forall v_{2r+1},\ldots,y_{3r+4} \in E_2)$$
$$(v_{2r+1},\ldots,y_{3r} \leq c_n \rightarrow \psi(c_{i\_1},\ldots,c_{i\_2r},v_{2r+1},\ldots,v_{3r+4})).$$

We now want to apply Lemma 5.3.14 to obtain 10) with E_2 replaced by any E_j, $j \geq 1$. Lemma 5.3.14 requires that we quantify over $v_1,\ldots,v_{r'}$, and use r' constants, where $r' \geq 1$. We can set $r' = 3r+4$ and add $2r+3$ dummy constants.

Hence for all $j \geq 1$,

$$11)\ (\forall v_{2r+1},\ldots,y_{3r+4} \in E_{j+1})$$
$$(v_{2r+1},\ldots,y_{3r} \leq c_n \rightarrow \psi(c_{i\_1},\ldots,c_{i\_2r},v_{2r+1},\ldots,v_{3r+4})).$$

We can now perform the above rewriting in reverse. By 11), for all $j \geq 1$ and $v_{2r+1},\ldots,y_{3r} \in E_j \cap [0,c_n]$,

$$12)\ (\forall v_{3r+1},v_{3r+2},v_{3r+3},v_{3r+4} \in E_{j+1})$$
$$(\psi(c_{i\_1},\ldots,c_{i\_2r},v_{2r+1},\ldots,y_{3r+4})).$$

By 8),12), for all $j \geq 1$ and $v_{2r+1},\ldots,y_{3r} \in E_j \cap [0,c_n]$,

$$13)\ (\forall v_{3r+1},v_{3r+2},v_{3r+3},v_{3r+4} \in E_{j+1})$$
$$(t(c_{i\_1},\ldots,c_{i\_r},v_{2r+1},\ldots,v_{3r}) \neq v_{3r+1} \vee$$
$$at(c_{i\_r+1},\ldots,c_{i\_2r},v_{2r+1},\ldots,v_{3r})+b \neq v_{3r+2}$$
$$\wedge$$
$$t(c_{i\_r+1},\ldots,c_{i\_2r},v_{2r+1},\ldots,v_{3r}) \neq v_{3r+3} \vee$$
$$at(c_{i\_1},\ldots,c_{i\_r},v_{2r+1},\ldots,v_{3r})+b \neq v_{3r+4}).$$

By logical manipulations, for all $j \geq 1$ and $v_{2r+1},\ldots,v_{3r} \in E_j \cap [0,c_n]$,

$$14)\ (\forall v_{3r+1},v_{3r+2} \in E_{j+1})(t(c_{i\_1},\ldots,c_{i\_r},v_{2r+1},\ldots,v_{3r}) \neq v_{3r+1} \vee$$
$$at(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)+b \neq v_{3r+2})$$
$$\wedge$$
$$(\forall v_{3r+3},v_{3r+4} \in E_{j+1})(t(c_{i\_r+1},\ldots,c_{i\_2r},v_{2r+1},\ldots,v_{3r}) \neq v_{3r+3} \vee$$
$$at(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)+b \neq v_{3r+4}).$$

$$15)\ t(c_{i\_1},\ldots,c_{i\_r},v_{2r+1},\ldots,v_{3r}) \notin E_{j+1} \vee$$
$$at(c_{i\_r+1},\ldots,c_{i\_2r},v_{2r+1},\ldots,v_{3r})+b \notin E_{j+1}$$
$$\wedge$$
$$t(c_{i\_r+1},\ldots,c_{i\_2r},v_{2r+1},\ldots,v_{3r}) \notin E_{j+1} \vee$$
$$at(c_{i\_1},\ldots,c_{i\_r},v_{2r+1},\ldots,v_{3r})+b \notin E_{j+1}.$$

$$16)\ t(c_{i\_1},\ldots,c_{i\_r},v_{2r+1},\ldots,v_{3r}) \in E_{j+1} \rightarrow$$
$$at(c_{i\_r+1},\ldots,c_{i\_2r},v_{2r+1},\ldots,v_{3r})+b \notin E_{j+1}$$
$$\wedge$$
$$t(c_{i\_r+1},\ldots,c_{i\_2r},v_{2r+1},\ldots,v_{3r}) \in E_{j+1} \rightarrow$$
$$at(c_{i\_1},\ldots,c_{i\_r},v_{2r+1},\ldots,v_{3r})+b \notin E_{j+1}.$$

By 1),2),16),

17) $t(c_{i\_1},...,c_{i\_r},v_{2r+1},...,v_{3r}) \in E_{j+1} \rightarrow$
$t(c_{i\_r+1},...,c_{i\_2r},v_{2r+1},...,v_{3r}) \in E_{j+1}$
$\wedge$
$t(c_{i\_r+1},...,c_{i\_2r},v_{2r+1},...,v_{3r}) \in E_{j+1} \rightarrow$
$t(c_{i\_1},...,c_{i\_r},v_{2r+1},...,v_{3r}) \in E_{j+1}$.

18) $t(c_{i\_1},...,c_{i\_r},v_{2r+1},...,v_{3r}) \in E_{j+1} \leftrightarrow$
$t(c_{i\_r+1},...,c_{i\_2r},v_{2r+1},...,v_{3r}) \in E_{j+1}$

as required. QED

LEMMA 5.3.16. Let $r \geq 1$ and $t(v_1,...,v_r)$ be a term of L. There exists a $(1,<\infty)$ term $t'(v_1,...,v_{r+1})$ such that the following holds. Let $n,j \geq 1$ and $x_1,...,x_r \in \alpha(E_j;1,<\infty) \cap [0,c_n]$. Then $t(x_1,...,x_r) \in E_{j+1} \leftrightarrow t'(x_1,...,x_r,c_{n+1}) \in E_{j+1}$.

Proof: Let r,t be as given. By Lemma 5.3.8, let $p \geq 2$ be such that for all $n \geq 1$, $x_1,...,x_r \leq c_n$, we have $t(x_1,...,x_r) \leq \uparrow p(c_n)$. By Lemma 5.3.13, let $a,b \in N\backslash\{0\}$ be such that the following holds. Let $j,n \geq 1$ and $x_1,...,x_r \in \alpha(E_j;1,<\infty) \cap [0,c_n]$. Then

$$(\exists y \in E_{j+1})(y \leq \uparrow p(|x_1,...,x_r|) \wedge y = t(x_1,...,x_r)) \leftrightarrow aCODE(c_{n+1};x_1,...,x_r)+b \in E_{j+1}.$$

By the choice of p and $|x_1,...,x_r| \leq c_n$, we have

$$t(x_1,...,x_r) \in E_{j+1} \leftrightarrow aCODE(c_{n+1};x_1,...,x_r)+b \in E_{j+1}.$$

So we can set $t'(v_1,...,v_{r+1}) = aCODE(v_{r+1};v_1,...,v_r)+b$ if $|v_1,...,v_{r+1}| \leq aCODE(v_{r+1};v_1,...,v_r)+b \leq 16a|v_1,...,v_{r+1}|$; $|v_1,...,v_{r+1}|$ otherwise. Obviously t' is a $(1,<\infty)$ term, and for all $x_1,...,x_r \leq c_n$, $t'(x_1,...,x_r,c_{n+1}) = aCODE(c_{n+1};x_1,...,x_r)+b \in [c_{n+1},16ac_{n+1}]$. QED

LEMMA 5.3.17. Let $r,j \geq 1$ and $t(v_1,...,v_{2r})$ be a term of L. Let $i_1,...,i_{2r} \geq 1$, and $y_1,...,y_r \in E_j$, where $(i_1,...,i_r)$ and $(i_{r+1},...,i_{2r})$ have the same order type and min, and $y_1,...,y_r \leq \min(c_{i\_1},...,c_{i\_r})$. Then

$$t(c_{i\_1},...,c_{i\_r},y_1,...,y_r) \in E_{j+1} \leftrightarrow t(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r) \in E_{j+1}.$$

Proof: Let $r,t(v_1,...,v_{2r})$ be as given. Let $t'(x_1,...,x_{2r+1})$ be as given by Lemma 5.3.16. Let $j,i_1,...,i_{2r},y_1,...,y_r$ be as given. Let $n > \max(i_1,...,i_{2r})$. Obviously, $y_1,...,y_r \leq c_n$. By Lemma 5.3.16,

$$t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \in E_{j+1} \leftrightarrow$$
$$t'(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r,c_{n+1}) \in E_{j+1}.$$

$$t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \in E_{j+1} \leftrightarrow$$
$$t'(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r,c_{n+1}) \in E_{j+1}.$$

Since t' is a $(1,<\infty)$ term, we see that by Lemma 5.3.15,

$$t'(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r,c_{n+1}) \in E_{j+1} \leftrightarrow$$
$$t'(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r,c_{n+1}) \in E_{j+1}.$$

Hence

$$t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \in E_{j+1} \leftrightarrow$$
$$t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \in E_{j+1}.$$

QED

LEMMA 5.3.18. There exists a countable structure M = $(A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,\ldots)$ such that the following holds.
i) $(A,<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies $TR(\Pi^0{}_1,L)$;
ii) $E \subseteq A\backslash\{0\}$;
iii) The c_n, $n \geq 1$, form a strictly increasing sequence of nonstandard elements in $E\backslash\alpha(E;2,<\infty)$ with no upper bound in A;
iv) Let $r,n \geq 1$, $t(v_1,\ldots,v_r)$ be a term of L, and $x_1,\ldots,x_r \leq c_n$. Then $t(x_1,\ldots,x_r) < c_{n+1}$;
v) $2\alpha(E;1,<\infty)+1,\ 3\alpha(E;1,<\infty)+1 \subseteq E$;
vi) Let $r \geq 1$, $a,b \in N$, and $\varphi(v_1,\ldots,v_r)$ be a quantifier free formula of L. There exist $d,e,f,g \in N\backslash\{0\}$ such that for all $x_1 \in \alpha(E;1,<\infty)$, $(\exists x_2,\ldots,x_r \in E)(x_2,\ldots,x_r \leq ax_1+b \wedge \varphi(x_1,\ldots,x_r)) \leftrightarrow dx_1+e \notin E \leftrightarrow fx_1+g \in E$;
vii) Let $r \geq 1$, $p \geq 2$, and $\varphi(v_1,\ldots,v_{2r})$ be a quantifier free formula of L. There exist $a,b,d,e \in N\backslash\{0\}$ such that the following holds. Let $n \geq 1$ and $x_1,\ldots,x_r \in \alpha(E;1,<\infty) \cap [0,c_n]$. Then
$(\exists y_1,\ldots,y_r \in E)(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,y_1,\ldots,y_r)) \leftrightarrow$
$a\text{CODE}(c_{n+1};x_1,\ldots,x_r)+b \notin E \leftrightarrow$
$d\text{CODE}(c_{n+1};x_1,\ldots,x_r)+e \in E$. Here CODE is as defined just before Lemma 5.3.11;
viii) Let $k,n,m \geq 1$, and $x_1,\ldots,x_k \leq c_n < c_m$, where $x_1,\ldots,x_k \in \alpha(E;1,<\infty)$. Then $\text{CODE}(c_m;x_1,\ldots,x_k) \in E$;
ix) Let $r \geq 1$ and $t(v_1,\ldots,v_{2r})$ be a term of L. Let $i_1,\ldots,i_{2r} \geq 1$ and $y_1,\ldots,y_r \in E$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$

have the same order type and min, and $y_1,...,y_r \le \min(c_{i\_1},...,c_{i\_r})$. Then
$t(c_{i\_1},...,c_{i\_r},y_1,...,y_r) \in E \leftrightarrow$
$t(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r) \in E$.

Proof: Let this M be the same as the M given by Lemma 5.3.3, except that instead of using $E_1,E_2,...$, we use $E = \bigcup\{E_n: n \ge 1\}$. We also use the enumeration $c_1 < c_2 < ...$ of E_1.

Claim i) is the same as Lemma 5.3.3 i).

Claim ii) is immediate from Lemma 5.3.3 ii).

Claim iii) is from Lemmas 5.3.3 iii), 5.3.4, 5.3.6, and the definition of the c's.

Claim iv) is from Lemma 5.3.8.

Claim v) is immediate from Lemma 5.3.3 vi).

For claim vi), let $r,a,b,\varphi(v_1,...,v_r)$ be as given. By Lemma 5.3.10, let $d,e,f,g \in N\backslash\{0\}$ be such that the following holds. Let $j \ge 1$ and $x_1 \in \alpha(E_j;1,<\infty)$. Then

$$(\exists x_2,...,x_r \in E_{j+1})(x_2,...,x_r \le ax_1+b \wedge \varphi(x_1,...,x_r)) \leftrightarrow dx_1+e \notin E_{j+1} \leftrightarrow fx_1+g \in E_{j+1}.$$

Let $x_1 \in \alpha(E;1,<\infty)$. For all $j \ge 1$, if $x_1 \in \alpha(E_j;1,<\infty)$, then

1) $(\exists x_2,...,x_r \in E_{j+1})(x_2,...,x_r \le ax_1+b \wedge \varphi(x_1,...,x_r)) \leftrightarrow dx_1+e \notin E_{j+1} \leftrightarrow fx_1+g \in E_{j+1}$.

We must verify that

$$(\exists x_2,...,x_r \in E)(x_2,...,x_r \le ax_1+b \wedge \varphi(x_1,...,x_r)) \leftrightarrow dx_1+e \notin E \leftrightarrow fx_1+g \in E.$$

First assume

2) $(\exists x_2,...,x_r \in E)(x_2,...,x_r \le ax_1+b \wedge \varphi(x_1,...,x_r))$.

Let j be such that

3) $x_1 \in \alpha(E_j;1,<\infty)$.
$(\exists x_2,...,x_r \in E_{j+1})(x_2,...,x_r \le ax_1+b \wedge \varphi(x_1,...,x_r))$.

By 1),3),

$$dx_1+e \notin E_{j+1}.$$
$$fx_1+g \in E_{j+1}.$$

Since j can be raised arbitrarily,

$$dx_1+e \notin E.$$
$$fx_1+g \in E.$$

Next assume

$$4)\ dx_1+e \notin E.$$

By 1),4), for all $j \geq 1$, if $x_1 \in \alpha(E_j;1,<\infty)$ then

$$(\exists x_2,\ldots,x_r \in E_{j+1})(x_2,\ldots,x_r \leq ax_1+b \wedge \varphi(x_1,\ldots,x_r)).$$
$$fx_1+g \in E_{j+1}.$$
$$(\exists x_2,\ldots,x_r \in E)(x_2,\ldots,x_r \leq ax_1+b \wedge \varphi(x_1,\ldots,x_r)).$$
$$fx_1+g \in E.$$

Finally assume

$$5)\ fx_1+g \in E.$$

By 1), for all $j \geq 1$, if $fx_1+g \in E_{j+1}$ and $x_1 \in \alpha(E_j;1,<\infty)$, then

$$(\exists x_2,\ldots,x_r \in E_{j+1})(x_2,\ldots,x_r \leq ax_1+b \wedge \varphi(x_1,\ldots,x_r)).$$
$$dx_1+e \notin E_{j+1}.$$

Since we can choose such a j to be arbitrarily large,

$$(\exists x_2,\ldots,x_r \in E)(x_2,\ldots,x_r \leq ax_1+b \wedge \varphi(x_1,\ldots,x_r)).$$
$$dx_1+e \notin E.$$

For claim vii), let $r,p,\varphi(v_1,\ldots,v_{2r})$ be as given. By Lemma 5.3.13, let $a,b,d,e \in N\backslash\{0\}$ be such that the following holds. For all $j,n \geq 1$ and $x_1,\ldots,x_r \in \alpha(E_j;1,<\infty) \cap [0,c_n]$,

$$(\exists y_1,\ldots,y_r \in E_{j+1})(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge$$
$$\varphi(x_1,\ldots,x_r,y_1,\ldots,y_r) \leftrightarrow$$
$$a\mathrm{CODE}(c_{n+1};x_1,\ldots,x_r)+b \notin E_{j+1} \leftrightarrow$$
$$d\mathrm{CODE}(c_{n+1};x_1,\ldots,x_r)+e \in E_{j+1}.$$

Fix $n \geq 1$ and $x_1,\ldots.,x_r \in \alpha(E;1,<\infty) \cap [0,c_n]$. Then for all $j \geq 1$ and $x_1,\ldots,x_r \in \alpha(E_j;1,<\infty) \cap [0,c_n]$,

$$6)\ (\exists y_1,\ldots,y_r \in E_{j+1})(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,y_1,\ldots,y_r) \leftrightarrow aCODE(c_{n+1};x_1,\ldots,x_r)+b \notin E_{j+1} \leftrightarrow dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E_{j+1}.$$

We must verify that

$$(\exists y_1,\ldots,y_r \in E)(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,y_1,\ldots,y_r)) \leftrightarrow aCODE(c_{n+1};x_1,\ldots,x_r)+b \notin E \leftrightarrow dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E.$$

First assume

$$7)\ (\exists y_1,\ldots,y_r \in E)(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,y_1,\ldots,y_r)).$$

Let $j \geq 1$ be such that

$$x_1,\ldots,x_r \in \alpha(E_j;1,<\infty).$$
$$(\exists y_1,\ldots,y_r \in E_{j+1})(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,y_1,\ldots,y_r)).$$

By 6),7),

$$aCODE(c_{n+1};x_1,\ldots,x_r)+b \notin E_{j+1}.$$
$$dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E_{j+1}.$$

Since j can be raised arbitrarily,

$$aCODE(c_{n+1};x_1,\ldots,x_r)+b \notin E.$$
$$dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E.$$

Now assume

$$8)\ aCODE(c_{n+1};x_1,\ldots,x_r)+b \notin E.$$

By 6),8), for all $j \geq 1$ and $x_1,\ldots,x_r \in \alpha(E_j;1,<\infty) \cap [0,c_n]$,

$$(\exists y_1,\ldots,y_r \in E_{j+1})(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,y_1,\ldots,y_r)).$$
$$dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E_{j+1}.$$
$$(\exists y_1,\ldots,y_r \in E)(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,y_1,\ldots,y_r)).$$
$$dCODE(c_{n+1};x_1,\ldots,x_r)+e \in E.$$

Finally assume

$$9)\ d\mathrm{CODE}(c_{n+1};x_1,\ldots,x_r)+e \in E.$$

By 6), for all $j \geq 1$ such that $x_1,\ldots,x_r \in \alpha(E_j;1,<\infty) \cap [0,c_n]$ and $d\mathrm{CODE}(c_{n+1};x_1,\ldots,x_r)+e \in E_{j+1}$,

$$(\exists y_1,\ldots,y_r \in E_{j+1})(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,y_1,\ldots,y_r).$$
$$a\mathrm{CODE}(c_{n+1};x_1,\ldots,x_r)+b \notin E_{j+1}.$$

Since we can choose arbitrarily large such j,

$$(\exists y_1,\ldots,y_r \in E)(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,y_1,\ldots,y_r).$$
$$a\mathrm{CODE}(c_{n+1};x_1,\ldots,x_r)+b \notin E.$$

For claim viii), let $k,n,m,x_1,\ldots,x_k$ be as given. Let $j \geq 1$ be such that $x_1,\ldots,x_k \in \alpha(E_j;1,<\infty)$. By Lemma 5.3.11, $\mathrm{CODE}(c_m;x_1,\ldots,x_k) \in E_{j+1}$. Hence $\mathrm{CODE}(c_m;x_1,\ldots,x_k) \in E$.

For claim ix), let $r,t,i_1,\ldots,i_{2r},y_1,\ldots,y_r$ be as given. By Lemma 5.3.17, for all $j \geq 1$, if $y_1,\ldots,y_r \in E_j$ then

$$10)\ t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \in E_{j+1} \leftrightarrow t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \in E_{j+1}.$$

We must verify that

$$t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \in E \leftrightarrow t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \in E.$$

First assume $t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \in E$. Let $j \geq 1$ be such that

$$11)\ y_1,\ldots,y_r \in E_j.$$
$$t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \in E_{j+1}.$$

By 10),11),

$$t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \in E_{j+1}.$$
$$t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \in E.$$

Finally, assume $t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \in E$. Let $j \geq 1$ be such that

$$12)\ y_1,\ldots,y_r \in E_j.$$
$$t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \in E_{j+1}.$$

By 10),12),

$$t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \in E_{j+1}.$$
$$t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \in E.$$

QED

5.4. Limited formulas, limited indiscernibles, x-definability, normal form.

We fix $M = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,\ldots)$ as given by Lemma 5.3.18.

DEFINITION 5.4.1. Let L(E) be the first order predicate calculus with equality, using $<,0,1,+,-,\bullet,\uparrow,\log,E$, where E is 1-ary. The c's are not included in L(E). We will always write $t \in E$ instead of $E(t)$.

We follow the convention that $\varphi(v_1,\ldots,v_k)$ represents a formula of L(E) whose free variables are among $v_1,\ldots,v_k$. This does not require that v_k be free or even appear in φ. Recall that all variables are of the form v_n, where $n \geq 1$.

In this section, we will only be concerned with what we call the E formulas of L(E).

DEFINITION 5.4.2. The E formulas of L(E) are inductively defined as follows.

i) Every atomic formula of L(E) is an E formula;
ii) If φ,ψ are E formulas then $(\neg\varphi)$, $(\varphi\wedge\psi)$, $(\varphi\vee\psi)$, $(\varphi\rightarrow\psi)$, $(\varphi\leftrightarrow\psi)$ are E formulas;
iii) If φ is an E formula and $n \geq 1$, then $(\exists v_n \in E)(\varphi)$, $(\forall v_n \in E)(\varphi)$ are E formulas.

DEFINITION 5.4.3. We take

$$(\exists v_n \in E)(\varphi),\ (\forall v_n \in E)(\varphi)$$

to be abbreviations of

$$(\exists v_n)(v_n \in E \wedge \varphi),\ (\forall v_n)(v_n \in E \rightarrow \varphi).$$

Although general formulas of L(E) will arise in this section, attention will be focused on their relativizations, which are E formulas of L(E).

DEFINITION 5.4.4. Let $\varphi(v_1,...,v_k)$ be a formula of L(E) and v be a variable not among $v_1,...,v_k$. We let $\varphi(v_1,...,v_k)^v$ be the result of bounding all quantifiers in $\varphi(v_1,...,v_k)$ to

$$E \cap [0,v].$$

I.e., we replace each quantifier

$$(\forall u) \text{ by } (\forall u \in E \cap [0,v])$$
$$(\exists u) \text{ by } (\exists u \in E \cap [0,v]).$$

These bounded quantifiers should be expanded in the usual way to create an actual formula in L(E).

We now define a very important 6-ary relation.

DEFINITION 5.4.5. We define $A(r,n,m,\varphi,a,b)$ if and only if

i) $r,n,m,a,b \in N\backslash\{0\}$, $n < m$;
ii) $\varphi = \varphi(v_1,...,v_r)$ is a formula of L(E); i.e., all free variables of φ are among $v_1,...,v_r$;
iii) Let $x_1,...,x_r \in E \cap [0,c_n]$. Then $\varphi(x_1,...,x_r)^{c\_n} \leftrightarrow$ $aCODE(c_m;c_n,...,c_{m-1},x_1,...,x_r)+b \in E$.

LEMMA 5.4.1. Let $r,n \geq 1$ and $\varphi(v_1,...,v_r)$ be a quantifier free formula of L. There exist a,b such that $A(r,n,n+1,\varphi,a,b)$.

Proof: Let r,n,φ be as given. Note that $\varphi^{c\_n} = \varphi$.

By Lemma 5.3.18 vii), let $a,b \in N\backslash\{0\}$ be such that the following holds. Let $n \geq 1$ and $x_1,...,x_r \in E \cap [0,c_n]$.

$(\exists y \in E)(y \leq |c_n,x_1,...,x_r|\uparrow\uparrow \wedge y \leq |x_1,...,x_r| \wedge$
$\varphi(c_n,x_1,...,x_r,y))$

$$\leftrightarrow$$

$$(\exists y \in E)(y \leq |c_n,x_1,...,x_r|\uparrow\uparrow \wedge \rho(c_n,x_1,...,x_r,y))$$

$$\leftrightarrow$$

$$aCODE(c_{n+1};c_n,x_1,...,x_r)+b \in E.$$

$$\varphi(x_1,...,x_r) \leftrightarrow$$
$$aCODE(c_{n+1};c_n,x_1,...,x_r)+b \in E.$$

Hence $A(r,n,n+1,\varphi,a,b)$. QED

Note that in the proof of Lemma 5.4.1, the second displayed formula is subject to Lemma 5.3.18 vii). The formula ρ used can be read off easily from the first displayed formula. We will be using this style of exposition throughout this section.

LEMMA 5.4.2. Let $r \geq 1$ and φ be $t \in E$, where $t(v_1,...,v_r)$ is a term of L. There exist a,b such that the following holds. Let $n \geq 1$. Then $A(r,n,n+1,\varphi,a,b)$.

Proof: Let r,φ,t be as given.

Let $p \geq 2$ be such that for all $x_1,...,x_r \in A$, $t(x_1,...,x_r) \leq \uparrow p(|x_1,...,x_r|)$. By Lemma 5.3.18 vii), let $a,b \in N\backslash\{0\}$ be such that the following holds. Let $n \geq 1$ and $x_1,...,x_r \in E \cap [0,c_n]$. Then

$$(\exists y \in E)(y \leq \uparrow p(|c_n,x_1,...,x_r|) \wedge y = t(x_1,...,x_r))$$
$$\leftrightarrow$$
$$(\exists y \in E)(y \leq \uparrow p(|c_n,x_1,...,x_r|) \wedge \rho(c_n,x_1,...,x_r,y))$$
$$\leftrightarrow$$
$$a\mathrm{CODE}(c_{n+1};c_n,x_1,...,x_r)+b \in E.$$

$$t(x_1,...,x_r) \in E \leftrightarrow$$
$$a\mathrm{CODE}(c_{n+1};c_n,x_1,...,x_r)+b \in E.$$

Hence $A(r,n,n+1,\varphi,a,b)$. QED

LEMMA 5.4.3. Let $A(r,n,m,\varphi,a,b)$. There exist d,e such that $A(r,n,m,\neg\varphi,d,e)$.

Proof: Let $A(r,n,m,\varphi,a,b)$. By Lemma 5.3.18 vi), fix $i,j \in N\backslash\{0\}$ such that the following holds. Let $x_1 \in \alpha(E;1,<\infty)$. Then

$$(\exists x_2 \in E)(x_2 \leq x_1 \wedge x_2 = x_1) \leftrightarrow$$
$$ix_1+j \notin E.$$

Clearly for all $x_1 \in \alpha(E;1,<\infty)$,

$$1)\ x_1 \in E \leftrightarrow ix_1+j \notin E.$$

Now let $x_1,...,x_r \in E \cap [0,c_n]$. By $A(r,n,m,\varphi,a,b)$,

$$2)\ \varphi(x_1,...,x_r)^{c\_n} \leftrightarrow$$
$$a\mathrm{CODE}(c_m;c_n,...,c_{m-1},x_1,...,x_r)+b \in E.$$

By Lemma 5.3.18 viii),

$$\mathrm{CODE}(c_m;c_n,...,c_{m-1},x_1,...,x_r) \in E.$$

By 1),

$$3)\ a(\mathrm{CODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r))+b \in E \leftrightarrow$$
$$ia(\mathrm{CODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r))+ib+j \notin E.$$

By 2),3),

$$\neg\varphi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow$$
$$ia(\mathrm{CODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r))+ib+j \in E.$$

Therefore $A(r,n,m,\neg\varphi,ia,ib+j)$. QED

LEMMA 5.4.4. Let $a,b,d,e \in N\backslash\{0\}$. There exist $f,g \in N\backslash\{0\}$ such that the following holds. Let $w \in \alpha(E;1,<\infty)$. Then $(aw+b \in E \wedge dw+e \in E) \leftrightarrow fw+g \in E$.

Proof: Let $a,b,d,e \in N\backslash\{0\}$. Let $p = \max(a,b,d,e)$.

By Lemma 5.3.18 vi), let $f,g \in N\backslash\{0\}$ such that the following holds. Let $w \in \alpha(E;1,<\infty)$. Then

$$(\exists y,z \in E)(y,z \leq pw+p \wedge y = aw+b \wedge z = cw+d) \leftrightarrow$$
$$fw+g \in E.$$

$$(\exists y,z \in E)(y = aw+b \wedge z = cw+d) \leftrightarrow$$
$$fw+g \in E.$$

$$(aw+b \in E \wedge cw+d \in E) \leftrightarrow$$
$$fw+g \in E.$$

QED

LEMMA 5.4.5. Let $A(r,n,m,\varphi,a,b)$ and $A(r,n,m,\psi,d,e)$. There exist f,g such that $A(r,n,m,\varphi\wedge\psi,f,g)$.

Proof: Assume $A(r,n,m,\varphi,a,b)$, $A(r,n,m,\psi,d,e)$. Let $x_1,\ldots,x_r \in E \cap [0,c_n]$, Then

$$1)\ \varphi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow$$
$$a\mathrm{CODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b \in E.$$

$$\psi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow$$
$$d\mathrm{CODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_e)+e \in E.$$

Let f,g be given by Lemma 5.4.4 using a,b,d,e. By Lemma 5.3.18 viii),

$$\mathrm{CODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r) \in E.$$

Hence by Lemma 5.4.4,

$$2)\ \text{aCODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b \in E \wedge \text{dCODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+e \in E \leftrightarrow \text{fCODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+g \in E.$$

By 1),2),

$$((\varphi\wedge\psi)(x_1,\ldots,x_r))^{c\_n} \leftrightarrow \varphi(x_1,\ldots,x_r)^{c\_n} \wedge \psi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow \text{fCODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+g \in E.$$

QED

LEMMA 5.4.6. Let $1 \leq i \leq r$ and $A(r,n,m,\varphi,a,b)$. There exists d,e such that $A(r,n,m+1,(\exists v_i)(\varphi),d,e)$.

Proof: Let $1 \leq i \leq r$ and $A(r,n,m,\varphi,a,b)$. Let $x_1,\ldots,x_r \in E \cap [0,c_n]$. Then

$$1)\ \varphi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow \text{aCODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b \in E.$$

By Lemma 5.3.18 vii), let $d,e \in N\backslash\{0\}$ be such that the following holds, using m for n. Let $x_1,\ldots,x_r \in E \cap [0,c_n]$. Then

$$(\exists x_i,w \in E)(x_i,w \leq c_m\uparrow\uparrow \wedge x_i \leq c_n \wedge w = \text{aCODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b)) \leftrightarrow$$
$$(\exists z,w \in E)(z,w \leq c_m\uparrow\uparrow \wedge z \leq c_n \wedge w = \text{aCODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_{i-1},z,x_{i+1},\ldots x_r)+b)) \leftrightarrow$$
$$(\exists z,w \in E)(z,w \leq c_m\uparrow\uparrow \wedge \rho(c_n,\ldots,c_m,x_1,\ldots,x_r,z,w)) \leftrightarrow$$
$$\text{dCODE}(c_{m+1};c_n,\ldots,c_m,x_1,\ldots,x_r)+e \in E.$$

$$(\exists x_i,w \in E)(x_i \leq c_n \wedge w = \text{aCODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b)) \leftrightarrow \text{dCODE}(c_{m+1};c_n,\ldots,c_m,x_1,\ldots,x_r)+e \in E.$$

$$2)\ (\exists x_i \in E)(x_i \leq c_n \wedge \text{aCODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b \in E)$$

$$\leftrightarrow$$

$$dCODE(c_{m+1};c_n,\ldots,c_m,x_1,\ldots,x_r)+e \in E.$$

By 1),2),

$$(\exists x_i \in E)(x_i \leq c_n \wedge \varphi(x_1,\ldots,x_r)^{c\_n}) \leftrightarrow$$
$$dCODE(c_{m+1};c_n,\ldots,c_m,x_1,\ldots,x_r)+e \in E.$$

$$(\exists x_i)(\varphi(x_1,\ldots,x_r))^{c\_n}$$
$$\leftrightarrow$$
$$dCODE(c_{m+1};c_n,\ldots,c_m,x_1,\ldots,x_r)+e \in E.$$

Hence $A(r,n,m+1,(\exists v_i)(\varphi),d,e)$. QED

LEMMA 5.4.7. Let $m \leq m'$ and $A(r,n,m,\varphi,a,b)$. There exist d,e such that $A(r,n,m',\varphi,d,e)$.

Proof: Let $m < m'$ and $A(r,n,m,\varphi,a,b)$. Let $x_1,\ldots,x_r \in E \cap [0,c_n]$. Then

$$1)\ \varphi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow$$
$$aCODE(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b \in E.$$

By Lemma 5.3.18 vii), let $d,e \in N\backslash\{0\}$ be such that the following holds. Let $x_1,\ldots,x_r \in E \cap [0,c_n]$. Then

$$(\exists y \in E)(y \leq c_{m'}\uparrow\uparrow \wedge y = aCODE(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b)$$
$$\leftrightarrow$$
$$(\exists y \in E)(y \leq c_{m'}\uparrow\uparrow \wedge \rho(c_n,\ldots,c_{m'-1},x_1,\ldots,x_r,y)$$
$$\leftrightarrow$$
$$dCODE(c_{m'};c_n,\ldots,c_{m'-1},x_1,\ldots,x_r)+e \in E.$$

$$(\exists y \in E)(y = aCODE(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b) \leftrightarrow$$
$$dCODE(c_{m'};c_n,\ldots,c_{m'-1},x_1,\ldots,x_r)+e \in E.$$

$$2)\ aCODE(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b \in E \leftrightarrow$$
$$dCODE(c_{m'};c_n,\ldots,c_{m'-1},x_1,\ldots,x_r)+e \in E.$$

By 1),2),

$$\varphi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow$$
$$dCODE(c_{m'};c_n,\ldots,c_{m'-1},x_1,\ldots,x_r)+e \in E.$$

Therefore $A(r,n,m',\varphi,d,e)$. QED

LEMMA 5.4.8. Let $r \leq r'$ and $A(r',n,m,\varphi,a,b)$, where all free variables of φ are among $v_1,\ldots,v_r$. There exist d,e such that $A(r,n,m+1,\varphi,d,e)$.

Proof: Let $r,r'n,m,\varphi,a,b$ be as given. By $A(r',n,m,\varphi,a,b)$, for all $x_1,\ldots,x_{r'} \in E \cap [0,c_n]$,

$$1)\ \varphi(x_1,\ldots,x_{r'})^{c\_n} \leftrightarrow$$
$$aCODE(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_{r'})+b \in E.$$

Note that $\varphi(x_1,\ldots,x_{r'})^{c\_n} = \varphi(x_1,\ldots,x_r)^{c\_n}$. Hence for all $x_1,\ldots,x_r \in E \cap [0,c_n]$,

$$2)\ \varphi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow$$
$$aCODE(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r,x_r,\ldots,x_r)+b \in E.$$

By Lemma 5.3.18 vii), let $d,e \in N\backslash\{0\}$ be such that the following holds. Let $x_1,\ldots,x_r \in E \cap [0,c_n]$. Then

$$(\exists z \in E)(z \leq c_m\uparrow\uparrow \wedge z = aCODE(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r,x_r,\ldots,x_r))$$
$$\leftrightarrow$$
$$(\exists z \in E)(z \leq c_n\uparrow\uparrow \wedge \rho(c_n,\ldots,c_m,x_1,\ldots,x_r,z)$$
$$\leftrightarrow$$
$$dCODE(c_{m+1};c_n,\ldots,c_m,x_1,\ldots,x_r)+e \in E.$$

$$3)\ aCODE(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r,x_r,\ldots,x_r)+b \in E \leftrightarrow$$
$$dCODE(c_{m+1};c_n,\ldots,c_m,x_1,\ldots,x_r)+e \in E.$$

By 2),3), for all $x_1,\ldots,x_r \in E \cap [0,c_n]$,

$$\varphi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow$$
$$dCODE(c_{m+1};c_n,\ldots,c_m,x_1,\ldots,x_r)+e \in E.$$

Hence $A(r,n,m+1,\varphi,d,e)$. QED

LEMMA 5.4.9. Let $r,n \geq 1$ and $\varphi(x_1,\ldots,x_r)$ be a formula of L(E). There exists m,a,b such that $A(r,n,m,\varphi,a,b)$.

Proof: By induction on the complexity of φ. Without loss of generality, we can assume that φ uses only the connectives $\neg,\wedge$, and only the quantifier $\exists$. For our purposes, we define $c(\varphi)$ as the total number of occurrences of connectives and quantifiers in φ.

We prove the following by induction on $p \geq 0$. Let $r,n \geq 1$ and $\varphi(v_1,\ldots,v_r)$ be a formula of L(E) with $c(\varphi) \leq p$. There exist m,a,b such that $A(r,n,m,\varphi,a,b)$.

We first handle the basis case $p = 0$. Let r,n,φ be as given. Then φ has no connectives and no quantifiers, and so

φ is an atomic formula of L(E). Now use Lemmas 5.4.1 and 5.4.2 with m = n+1.

Now assume that the statement holds of $p \geq 0$. Let $r,n \geq 1$ and $\varphi(v_1,\ldots,v_r)$ be a formula of L(E) with $c(\varphi) = p+1$.

case 1. $\varphi(v_1,\ldots,v_r) = \neg\psi(v_1,\ldots,v_r)$. By the induction hypothesis, let $A(r,n,m,\psi,a,b)$. By Lemma 5.4.3, there exist d,e such that $A(r,n,m,\varphi,d,e)$.

case 2. $\varphi(v_1,\ldots,v_r) = \psi(v_1,\ldots,v_r) \wedge \rho(v_1,\ldots,v_r)$. By the induction hypothesis, let $A(r,n,m,\psi,a,b)$,$A(r,n,m',\rho,d,e)$. By Lemma 5.4.7, let $A(r,n,\max(m,m'),\psi,a',b')$, $A(r,n,\max(m,m'),\rho,d',e')$. By Lemma 5.4.5, there exists f,g such that $A(r,n,\max(m,m'),\varphi,f,g)$.

case 3. $\varphi(v_1,\ldots,v_r) = (\exists v_i)(\psi)$, $1 \leq i \leq r$. Then we can write $\psi = \psi(v_1,\ldots,v_r)$ because has all free variables of φ are among $v_1,\ldots,v_r$. By the induction hypothesis, let $A(r,n,m,\psi,a,b)$. By Lemma 5.4.6, there exist d,e such that $A(r,n,m+1,\varphi,d,e)$.

case 4. $\varphi(v_1,\ldots,v_r) = (\exists v_i)(\psi)$, $i > r$. Then ψ has all free variables among $v_1,\ldots,v_i$, and we an write $\psi = \psi(v_1,\ldots,v_i)$. By the induction hypothesis, let $A(i,n,m,\psi,a,b)$. By Lemma 5.4.6, let $A(i,n,m+1,\varphi,d,e)$. By Lemma 5.4.8, there exists f,g such that $A(r,n,m+2,\varphi,f,g)$.

QED

We now extend the indiscernibility in Lemma 5.3.18 iv) to formulas.

LEMMA 5.4.10. Let $r \geq 1$ and $\varphi(v_1,\ldots,v_{2r})$ be a formula in L(E). Let $1 \leq i_1,\ldots,i_{2r} < n$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and the same min. Let $y_1,\ldots,y_r \in E$, $y_1,\ldots,y_r \leq \min(c_{i\_1},\ldots,c_{i\_r})$. Then $\varphi(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)^{c\_n} \leftrightarrow \varphi(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)^{c\_n}$.

Proof: Let $r,\varphi,i_1,\ldots,i_{2r}$ be as given. Let $n > i_1,\ldots,i_{2r}$. By Lemma 5.4.9, let m,a,b be such that the following holds. For all $x_1,\ldots,x_{2r} \in E \cap [0,c_n]$,

$$\varphi(x_1,\ldots,x_{2r})^{c\_n} \leftrightarrow$$
$$a\mathrm{CODE}(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_{2r})+b \in E.$$

Let $y_1,\ldots,y_r$ be as given. Then

$$1)\ \varphi(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)^{c\_n} \leftrightarrow$$
$$aCODE(c_m:c_n,\ldots,c_{m-1},c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)+b \in E.$$

$$\varphi(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)^{c\_n} \leftrightarrow$$
$$aCODE(c_m;c_n,\ldots,c_{m-1},c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)+b \in E.$$

By Lemma 5.3.18 ix),

$$2)\ aCODE(c_m;c_n,\ldots,c_{m-1},c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)+b \in E \leftrightarrow$$
$$aCODE(c_m;c_n,\ldots,c_{m-1},c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)+b \in E.$$

By 1),2),

$$\varphi(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)^{c\_n} \leftrightarrow$$
$$\varphi(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)^{c\_n}.$$

QED

LEMMA 5.4.11. Let $k,n \geq 1$ and $\varphi(v_1,\ldots,v_k)$ be a formula of L(E). There exist $m,a,b \in N\backslash\{0\}$, $n < m$, and $y_n,\ldots,y_m \in E \cap [0,c_{n+1}]$ such that for all $x_1,\ldots,x_k \in E \cap [0,c_n]$,

$$\varphi(x_1,\ldots,x_k)^{c\_n} \leftrightarrow$$
$$aCODE(y_m;y_n,\ldots,y_{m-1},x_1,\ldots,x_k)+b \in E.$$

Proof: Let k,n,φ be as given. By Lemma 5.4.9, there exist $m,a,b \in N\backslash\{0\}$ such that

$$1)\ (\forall x_1,\ldots,x_k \in E \cap [0,c_n])(\varphi(x_1,\ldots,x_r)^{c\_n}$$

$$\leftrightarrow$$

$$aCODE(c_m;c_n,\ldots,c_{m-1},x_1,\ldots,x_r)+b \in E).$$

$$2)\ (\exists y_n,\ldots,y_m \in E)(\forall x_1,\ldots,x_k \in E \cap [0,c_n])$$
$$(\varphi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow aCODE(y_m;y_n,\ldots,y_{m-1},x_1,\ldots,x_r)+b \in E).$$

$$3)\ (\exists y_n,\ldots,y_m \in E)(\forall x_1,\ldots,x_k \in E \cap [0,c_n])$$
$$(\varphi(x_1,\ldots,x_r)^{c\_n} \leftrightarrow (\exists z \in E)(z = aCODE(y_m;y_n,\ldots,y_{m-1},x_1,\ldots,x_r)+b)).$$

By Lemma 5.3.18 iii), choose t so large that

$$4)\ (\exists y_n,\ldots,y_m \in E \cap [0,c_t])(\forall x_1,\ldots,x_k \in E \cap [0,c_n])(\varphi(x_1,\ldots,x_r)^{c\_n}$$

$$\leftrightarrow$$

$(\exists z \in E \cap [0,c_{t+1}])(z = aCODE(y_m;y_n,...,y_{m-1},x_1,...,x_r)+b))$.

By Lemma 5.4.10,

5) $(\exists y_n,...,y_m \in E \cap [0,c_{n+1}])(\forall x_1,...,x_k \in E \cap [0,c_n])(\varphi(x_1,...,x_r)^{c\_n} \leftrightarrow$

$(\exists z \in E \cap [0,c_{n+2}])(z = aCODE(y_m;y_n,...,y_{m-1},x_1,...,x_r)+b))$.

6) $(\exists y_n,...,y_m \in E \cap [0,c_{n+1}])(\forall x_1,...,x_k \in E \cap [0,c_n])(\varphi(x_1,...,x_r)^{c\_n} \leftrightarrow$

$(\exists z \in E)(z = aCODE(y_m;y_n,...,y_{m-1},x_1,...,x_r)+b))$.

7) $(\exists y_n,...,y_m \in E \cap [0,c_{n+1}])(\forall x_1,...,x_k \in E \cap [0,c_n])(\varphi(x_1,...,x_r)^{c\_n} \leftrightarrow$

$aCODE(y_m;y_n,...,y_{m-1},x_1,...,x_r)+b \in E)$.

QED

Recall that $\alpha(E)$ is the set of all values of terms in L at arguments from E (Definition 5.3.3).

LEMMA 5.4.12. $\alpha(E) = E-E$. Let $n \geq 1$. $\alpha(E \cap [0,c_n]) \subseteq (E \cap [0,c_{n+1}]) - (E \cap [0,c_{n+1}])$.

Proof: Since $E-E \subseteq \alpha(E)$, it suffices to prove $\alpha(E) \subseteq E-E$. Let $t(v_1,...,v_k)$ be a term in L, and let $x_1,...,x_k \in E$. Let n be such that $x_1,...,x_k < c_n$.

Note that by Lemma 5.3.18 iv),v),

$$t(x_1,...,x_k) < c_{n+1}.$$
$$2c_{n+1}+t(x_1,...,x_k),3c_{n+1}+t(x_1,...,x_k) \in \alpha(E;1,<\infty).$$
$$3(2c_{n+1}+t(x_1,...,x_k))+1,\ 2(3c_{n+1}+t(x_1,...,x_k))+1 \in E.$$
$$6c_{n+1}+3t(x_1,...,x_k)+1,\ 6c_{n+1}+2t(x_1,...,x_k)+1 \in E.$$
$$(6c_{n+1}+3t(x_1,...,x_k)+1)-(6c_{n+1}+2t(x_1,...,x_k)+1) = t(x_1,...,x_k) \in E-E.$$

Thus we have written $t(x_1,...,x_k)$ as the difference between two elements of E. This establishes the first claim.

For the second claim, let $n \geq 1$. Let $t(v_1,...,v_k)$ be a term in L. By the proof of the first claim,

1) $(\forall x_1,...,x_k \in E \cap [0,c_n])(\exists y,z \in E \cap [0,c_{n+2}])(t(x_1,...,x_k) = y-z)$.

By Lemma 5.4.10,

2) $(\forall x_1,\ldots,x_k \in E \cap [0,c_n])(\exists y,z \in E \cap [0,c_{n+1}])$
$(t(x_1,\ldots,x_k) = y-z)$.

QED

LEMMA 5.4.13. Let $k,r \geq 1$ and $x_1,\ldots,x_k,y_1,\ldots,y_r \in A$. Then $P(y_1,\ldots,y_r,x_1,\ldots,x_k) = P(P(y_1,\ldots,y_r),x_1,\ldots,x_k)$.

Proof: Recall the definition of P in section 5.3, right after the proof of Lemma 5.3.10. We prove the following by induction on $r \geq 1$:

for all $k \geq 1$ and $x_1,\ldots,x_k,y_1,\ldots,y_r \in A$,
$P(y_1,\ldots,y_r,x_1,\ldots,x_k) = P(P(y_1,\ldots,y_r),x_1,\ldots,x_k)$.

For the basis case $r = 1$, this asserts that for all $k \geq 1$

$$P(y_1,x_1,\ldots,x_k) = P(P(y_1),x_1,\ldots,x_k)$$

which follows from $P(y_1) = y_1$.

Fix $r \geq 1$. Suppose that for all $k \geq 1$ and $x_1,\ldots,x_k,y_1,\ldots,y_r$,

1) $P(y_1,\ldots,y_r,x_1,\ldots,x_k) =$
$P(P(y_1,\ldots,y_r),x_1,\ldots,x_k)$.

We want to verify that for all $k \geq 1$ and $x_1,\ldots,x_k,y_1,\ldots,y_{r+1}$,

$P(y_1,\ldots,y_{r+1},x_1,\ldots,x_k) =$
$P(P(y_1,\ldots,y_{r+1}),x_1,\ldots,x_k)$.

Let $k \geq 1$ and $x_1,\ldots,x_k,y_1,\ldots,y_{r+1} \in A$. By the induction hypothesis 1) using $k = k+1$,

2) $P(y_1,\ldots,y_{r+1},x_1,\ldots,x_k) =$
$P(P(y_1,\ldots,y_r),y_{r+1},x_1,\ldots,x_k)$.

By the definition of P,

3) $P(P(y_1,\ldots,y_r),y_{r+1},x_1,\ldots,x_k) =$
$P(P(P(y_1,\ldots,y_r),y_{r+1}),x_1,\ldots,x_k)$.

By the induction hypothesis 1) using $k = 1$,

4) $P(P(y_1,\ldots,y_r),y_{r+1}) =$

$$P(y_1,...,y_{r+1}).$$

By 2),3),4),

$$P(y_1,...,y_{r+1},x_1,...,x_k) = P(P(y_1,...,y_{r+1}),x_1,...,x_k)$$

as required. QED

LEMMA 5.4.14. Let $k,n,r \geq 1$, and $\varphi(v_1,...,v_{r+k})$ be a formula of L(E). Let $y_1,...,y_r \in E \cap [0,c_n]$. There exist $d,e,f,g,h,i,j,p \in E \cap [0,c_{n+1}]$ such that for all $x_1,...,x_k \in E \cap [0,c_n]$,

$$\varphi(y_1,...,y_r,x_1,...,x_k)^{c\_n} \leftrightarrow (d-e)\text{CODE}(f-g;h-i,x_1,...,x_k)+(j-p) \in E.$$

Proof: Let k,n,r,φ be as given. By Lemma 5.4.11, let $m,a,b \in N\backslash\{0\}$, $n < m$, and $z_n,...,z_m \in E \cap [0,c_{n+1}]$, be such that for all $y_1,...,y_r,x_1,...,x_k \in E \cap [0,c_n]$,

$$\varphi(y_1,...,y_r,x_1,...,x_k)^{c\_n} \leftrightarrow a\text{CODE}(z_m;z_n,...,z_{m-1},y_1,...,y_r,x_1,...,x_k)+b \in E.$$

By the definition of CODE introduced right after the proof of Lemma 5.3.10,

$$1)\ \varphi(y_1,...,y_r,x_1,...,x_k)^{c\_n} \leftrightarrow a(8((\log(z_m))\uparrow+P(z_n,...,z_{m-1},y_1,...,y_r,x_1,...,x_k))+1)+b \in E.$$

Now fix $y_1,...,y_r$ as given. These are in addition to the already fixed $z_n,...,z_m \in E$.

By Lemma 5.4.13 and 1), for all $x_1,...,x_k \in E \cap [0,c_n]$,

$$\varphi(y_1,...,y_r,x_1,...,x_k)^{c\_n} \leftrightarrow a(8((\log(z_m))\uparrow+P(P(z_n,...,z_{m-1},y_1,...,y_r),x_1,...,x_k))+1)+b \in E.$$

$$2)\ \varphi(y_1,...,y_r,x_1,...,x_k)^{c\_n} \leftrightarrow a\text{CODE}(z_m;P(z_n,...,z_{m-1},y_1,...,y_r),x_1,...,x_k)+b \in E.$$

By Lemma 5.4.12, let $a = d-e$, $z_m = f-g$, $P(z_n,...,z_{m-1},y_1,...,y_r) = h-i$, $b = j-p$, where $d,e,f,g,h,i,j,p \in E \cap [0,c_{n+2}]$. Make these substitutions for $a,z_m,P(z_n,...,z_{m-1},y_1,...,y_r),b$, respectively, in 2).

The Lemma requires that $d,e,f,g,h,i,j,p \in E \cap [0,c_{n+1}]$, and we only have $d,e,f,g,h,i,j,p \in E \cap [0,c_{n+2}]$. However, we can apply Lemma 5.4.10 in the obvious way to reduce to $E \cap [0,c_{n+1}]$. QED

LEMMA 5.4.15. For all $k \geq 1$ there exists a term $t(v_1,\ldots,v_{k+8})$ of L(E) such that the following holds. Let $n,r \geq 1$, $\varphi(v_1,\ldots,v_{r+k})$ be a formula of L(E), and $y_1,\ldots,y_r \in E \cap [0,c_n]$. There exists $w_1,\ldots,w_8 \in E \cap [0,c_{n+1}]$ such that for all $x_1,\ldots,x_k \in E \cap [0,c_n]$,

$$\varphi(y_1,\ldots,y_r,x_1,\ldots,x_k)^{c\_n} \leftrightarrow t(x_1,\ldots,x_k,w_1,\ldots,w_8) \in E.$$

Proof: Let $k \geq 1$. Let $t(v_1,\ldots,v_{k+8})$ be the obvious term of L(E) such that for all $x_1,\ldots,x_k,w_1,..,w_8 \in A$,

$$t(x_1,\ldots,x_k,w_1,\ldots,w_8) = (w_1-w_2)\mathrm{CODE}(w_3-w_4;w_5-w_6,x_1,\ldots,x_k)+(w_7-w_8).$$

Let $n,r,\varphi,y_1,\ldots,y_r$ be as given. By Lemma 5.4.14, there exist $w_1,\ldots,w_8 \in E \cap [0,c_{n+1}]$ such that for all $x_1,\ldots,x_k \in E \cap [0,c_n]$,

$$\varphi(y_1,\ldots,y_r,x_1,\ldots,x_k)^{c\_n} \leftrightarrow (w_1-w_2)\mathrm{CODE}(w_3-w_4;w_5-w_6,x_1,\ldots,x_k)+(w_7-w_8) \in E.$$

QED

DEFINITION 5.4.6. Let $k \geq 1$ and $x \in E$. An x-definable k-ary relation is a relation R of the form

$$R = \{(x_1,\ldots,x_k) \in E^k \cap [0,x]^k\colon \varphi(x_1,\ldots,x_p)^x\}$$

where $p \geq k$, $\varphi(v_1,\ldots,v_p)$ is a formula of L(E), and $x_{k+1},\ldots,x_p \in E \cap [0,x]$.

It is essential that x-definability requires boundedness. These are the internal relations, and this requirement is in analogy with the set/class distinct in set (class) theory.

LEMMA 5.4.16. Let $k,n \geq 1$ and R be a c_n-definable k-ary relation. Let t_k is the term of L(E) given by Lemma 5.4.15. There exists $y_1,\ldots,y_8 \in E \cap [0,c_{n+1}]$ such that $R = \{(x_1,\ldots,x_k) \in E^k \cap [0,c_n]^k\colon t_k(x_1,\ldots,x_k,y_1,\ldots,y_8) \in E\}$.

Proof: Let $n \geq 1$ and R be a c_n-definable k-ary relation. Write

$$R = \{(x_1,\ldots,x_k) \in E^k \cap [0,c_n]^k\colon \varphi(x_1,\ldots,x_p)^{c\_n}\}$$

where $p \geq k \geq 1$, $\varphi(v_1,\ldots,v_p)$ is a formula of L(E), and $x_{k+1},\ldots,x_p \in E \cap [0,c_n]$.

We now apply Lemma 5.4.15 to the formula

$$\varphi'(v_1,\ldots,v_p) = \varphi(v_{p-k+1},\ldots,v_p,v_1,\ldots,v_{p-k}).$$

We use the present $x_{k+1},\ldots,x_p$ for the parameters $y_1,\ldots,y_r$ in Lemma 5.4.15.

Let $y_1,\ldots,y_8 \in E \cap [0,c_{n+1}]$, where for all $x_1,\ldots,x_k \in E \cap [0,c_n]$,

$$\varphi'(x_{k+1},\ldots,x_p,x_1,\ldots,x_k)^{c\_n} \leftrightarrow \varphi(x_1,\ldots,x_p)^{c\_n} \leftrightarrow$$
$$R(x_1,\ldots,x_k) \leftrightarrow t_k(x_1,\ldots,x_k,z_1,\ldots,z_8) \in E.$$

QED

Below, the new features over Lemma 5.3.18 are items vi) and vii).

LEMMA 5.4.17. There exists a countable structure $M = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,\ldots)$, and terms $t_1,t_2,\ldots$ of L, where for all i, t_i has variables among $v_1,\ldots,v_{i+8}$, such that the following holds.
i) $(A,<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies $TR(\Pi^0{}_1,L)$;
ii) $E \subseteq A\backslash\{0\}$;
iii) The c_n, $n \geq 1$, form a strictly increasing sequence of nonstandard elements in $E\backslash\alpha(E;2,<\infty)$ with no upper bound in A;
iv) Let $r,n \geq 1$ and $t(v_1,\ldots,v_r)$ be a term of L, and $x_1,\ldots,x_r \leq c_n$. Then $t(x_1,\ldots,x_r) < c_{n+1}$;
v) $2\alpha(E;1,<\infty)+1$, $3\alpha(E;1,<\infty)+1 \subseteq E$;
vi) Let $k,n \geq 1$ and R be a c_n-definable k-ary relation. There exists $y_1,\ldots,y_8 \in E \cap [0,c_{n+1}]$ such that $R = \{(x_1,\ldots,x_k) \in E^k \cap [0,c_n]^k\colon t_k(x_1,\ldots,x_k,y_1,\ldots,y_8) \in E\}$;
vii) Let $r \geq 1$ and $\varphi(v_1,\ldots,v_{2r})$ be a formula of L(E). Let $1 \leq i_1,\ldots,i_{2r} < n$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and the same min. Let $y_1,\ldots,y_r \in E$, $y_1,\ldots,y_r \leq \min(c_{i\_1},\ldots,c_{i\_r})$. Then $\varphi(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r)^{c\_n} \leftrightarrow \varphi(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)^{c\_n}$.

Proof: The t's are given by Lemma 5.4.15. i)-v) are from Lemma 5.3.18 i)-v). vi) is by Lemma 5.4.16. vii) is by Lemma 5.4.10. QED

5.5. Comprehension, indiscernibles.

We fix $M = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,...)$ and terms $t_1,t_2,...$ of L(E) be given as in Lemma 5.4.17.

We now consider unbounded quantifiers. Below, Q indicates either ∀ or ∃. All formulas of L(E) are interpreted in M.

LEMMA 5.5.1. Let $n,m \geq 0$, $r \geq 1$, and $\varphi(v_1,...,v_{n+m})$ be a quantifier free formula of L(E). Let $x_{n+1},...,x_{n+m} \in E \cap [0,c_r]$. Then
$(Q_n x_n \in E)...(Q_1 x_1 \in E)(\varphi(x_1,...,x_{n+m})) \leftrightarrow$
$(Q_n x_n \in E \cap [0,c_{r+1}])...(Q_1 x_1 \in E \cap [0,c_{r+n}])(\varphi(x_1,...,x_{n+m}))$.

Proof: We prove the following statement by induction on $n \geq 0$.

Let $m \geq 0$, $r \geq 1$, $\varphi(x_1,...,x_{n+m})$ be a quantifier free formula in L(E), $Q_1,...,Q_n$ be quantifiers, and $x_{n+1},...,x_{n+m} \in E \cap [0,c_r]$. Then

$$(Q_n x_n \in E)...(Q_1 x_1 \in E)(\varphi(x_1,...,x_{n+m})) \leftrightarrow$$
$$(Q_n x_n \in E \cap [0,c_{r+1}])...(Q_1 x_1 \in E \cap [0,c_{r+n}])(\varphi(x_1,...,x_{n+m})).$$

The basis case n = 0 is trivial. Assume this is true for a given $n \geq 0$. Let $m \geq 0$, $r \geq 1$, and $\varphi(x_1,...,x_{n+1+m})$ be a quantifier free formula in L(E). Let $x_{n+2},...,x_{n+1+m} \in E \cap [0,c_r]$. We wish to verify that

$$(Q_{n+1} x_{n+1} \in E)...(Q_1 x_1 \in E)(\varphi(x_1,...,x_{n+1+m})) \leftrightarrow$$
$$(Q_{n+1} x_{n+1} \in E \cap [0,c_{r+1}])...(Q_1 x_1 \in E \cap [0,c_{r+n+1}])$$
$$(\varphi(x_1,...,x_{n+1+m})).$$

By duality, we may assume that Q_{n+1} is ∃. Thus we wish to verify that

$$1)\quad (\exists x_{n+1} \in E)(Q_n x_n \in E)...(Q_1 x_1 \in E)(\varphi(x_1,...,x_{n+1+m}))$$
$$\leftrightarrow$$
$$(\exists x_{n+1} \in E \cap [0,c_{r+1}])(Q_n x_n \in E \cap [0,c_{r+2}])...$$
$$(Q_1 x_1 \in E \cap [0,c_{r+n+1}])(\varphi(x_1,...,x_{n+1+m})).$$

Let $x_{n+1} \in E \cap [0,c_{r+1}]$ witness the right side of 1). I.e.,

2) $(Q_n x_n \in E \cap [0,c_{r+2}])\ldots(Q_1 x_1 \in E \cap [0,c_{r+n+1}])(\varphi(x_1,\ldots,x_{n+1+m}))$.

According to the induction hypothesis applied to $m+1,r+1,\varphi(x_1,\ldots,x_{n+1+m}),Q_1,\ldots,Q_n$, and $x_{n+1},\ldots,x_{m+1+m}, \in E \cap [0,c_{r+1}]$, we have

3) $(Q_n x_n \in E)\ldots(Q_1 x_1 \in E)(\varphi(x_1,\ldots,x_{n+1+m})) \leftrightarrow (Q_n x_n \in E \cap [0,c_{r+2}])\ldots(Q_1 x_1 \in E \cap [0,c_{r+n+1}])(\varphi(x_1,\ldots,x_{n+1+m}))$.

By 2),3),

$$(Q_n x_n \in E)\ldots(Q_1 x_1 \in E)(\varphi(x_1,\ldots,x_{n+1+m})),$$

which is the left side of 1) instantiated with x_{n+1}.

Finally, let $x_{n+1} \in E$ witness the left side of 1). I.e.,

4) $(Q_n x_n \in E)\ldots(Q_1 x_1 \in E)(\varphi(x_1,\ldots,x_{n+1+m}))$.

Let $x_{n+1} \leq c_s$, $s \geq r+1$. According to the induction hypothesis applied to $m+1,s,\varphi(x_1,\ldots,x_{n+1+m}),Q_1,\ldots,Q_n$, and $x_{n+2},\ldots,x_{n+1+m}, \in E \cap [0,c_s]$, we have

5) $(Q_n x_n \in E)\ldots(Q_1 x_1 \in E)(\varphi(x_1,\ldots,x_{n+1+m})) \leftrightarrow (Q_n x_n \in E \cap [0,c_{s+1}])\ldots(Q_1 x_1 \in E \cap [0,c_{s+n}])(\varphi(x_1,\ldots,x_{n+1+m}))$.

By 4),5),

$$(\exists x_{n+1} \in E \cap [0,c_s])(Q_n x_n \in E \cap [0,c_{s+1}])\ldots(Q_1 x_1 \in E \cap [0,c_{s+n}])(\varphi(x_1,\ldots,x_{n+1+m})).$$

By Lemma 5.4.17 vii), since $x_{n+2},\ldots,x_{n+1+m} \in E \cap [0,c_r]$, we have

$$(\exists x_{n+1} \in E \cap [0,c_{r+1}])(Q_n x_n \in E \cap [0,c_{r+2}])\ldots(Q_1 x_1 \in E \cap [0,c_{r+n+1}])(\varphi(x_1,\ldots,x_{n+1+m}))$$

which is the right side of 1). QED

Note that Lemmas 5.4.17 and 5.5.1 concern only the E formulas of L(E). I.e., all of the quantifiers are relativized to E. This is clear for Lemma 5.4.17 by Definitions 5.4.4, 5.4.5. Lemma 5.5.1 only involves quantifier free formulas which are inside quantifiers relativized to E.

DEFINITION 5.5.1. Let $k \geq 1$ and $R \subseteq A^k$. We say that R is M,E definable if and only if $R \subseteq E^k$, and R is definable by an E formula of L(E) with parameters from E. I.e., there exists $m \geq 1$, an E formula $\varphi(x_1,\ldots,x_{k+m})$, and $x_{k+1},\ldots,x_{k+m} \in E$, such that

$$R = \{(x_1,\ldots,x_k) \in E^k: \varphi(x_1,\ldots,x_{k+m})\}.$$

Recall the definition of x-definability (Definition 5.4.6).

DEFINITION 5.5.2. We say that R is bounded if and only if there exists $x \in E$ such that $R \subseteq [0,x]^k$.

DEFINITION 5.5.3. For all $k \geq 1$, we write X_k for the set of all bounded M,E definable k-ary relations.

LEMMA 5.5.2. Let $k \geq 1$ and $R \subseteq A^k$. The following are equivalent.
i) $R \in X_k$;
ii) R is c_n-definable for some $n \geq 1$;
iii) R is x-definable for some $x \in E$.

Proof: Let k,R be as given. We have ii) → iii) → i). So we need only prove i) → ii). Let $R \in X_k$. By choosing r to be sufficiently large, we can write

$$R = \{(x_1,\ldots,x_k) \in E^k \cap [0,c_r]: \varphi(x_1,\ldots,x_{k+m})\}$$

where $\varphi(x_1,\ldots,x_{k+m})$ is an E formula of L(E), $r \geq 1$, and $x_{k+1},\ldots,x_{k+m} \in E \cap [0,c_r]$. We can assume that φ is in prenex form. By a change of bound variables, we can assume that φ is in the form

$$(Q_1x_{k+m+1} \in E)\ldots(Q_nx_{k+m+n} \in E)(\psi(x_1,\ldots,x_{k+m+n}))$$

where $\psi(x_1,\ldots,x_{k+m+n})$ is a quantifier free formula of L(E).

Let $x_1,\ldots,x_k \in E \cap [0,c_r]$. By Lemma 5.5.1,

$$R(x_1,\ldots,x_k) \leftrightarrow \varphi(x_1,\ldots,x_{k+m}) \leftrightarrow$$
$$(Q_1x_{k+m+1} \in E)\ldots(Q_nx_{k+m+n} \in E)(\psi(x_1,\ldots,x_{k+m+n})) \leftrightarrow$$
$$(Q_1x_{k+m+1} \in E \cap [0,c_{r+1}])\ldots(Q_nx_{k+m+n} \in E \cap [0,c_{r+n}])(\psi(x_1,\ldots,x_{k+m+n})).$$

Since $R \subseteq E^k \cap [0,c_r]^k$, this provides a c_{r+n}-definition of R. QED

Lemma 5.5.2 reveals a considerable amount of robustness.

DEFINITION 5.5.4. We say that a k-ary relation $R \subseteq E^k$ is internal (to M) if and only if R obeys any (all) of conditions i) - iii) in Lemma 5.5.2.

DEFINITION 5.5.5. Let $k \geq 1$ and $R \subseteq A^k$. We say that $y_1,\ldots,y_9$ codes R if and only if $y_1,\ldots,y_9 \in E$ and

$$R = \{(x_1,\ldots,x_k) \in E^k \cap [0,y_9]^k: t_k(x_1,\ldots,x_k,y_1,\ldots,y_8) \in E\}.$$

LEMMA 5.5.3. Every internal R is coded by some $y_1,\ldots,y_9$. For $k \geq 1$, every $y_1,\ldots,y_9 \in E$ codes some unique $R \subseteq A^k$, which must be internal.

Proof: Let R be internal. Let $n \geq 1$, where R is c_n-definable. By Lemma 5.4.17 vi), write

$$R = \{(x_1,\ldots,x_k) \in E^k \cap [0,c_n]^k: t_k(x_1,\ldots,x_k,y_1,\ldots,y_8) \in E\}$$

where $y_1,\ldots,y_8 \in E$. Then R is coded by $y_1,\ldots,y_8,c_n$.

Now let $k \geq 1$, and $y_1,\ldots,y_9 \in E$. Then $y_1,\ldots,y_9$ codes

$$R = \{(x_1,\ldots,x_k) \in E^k \cap [0,y_9]^k: t_k(x_1,\ldots,x_k,y_1,\ldots,y_8) \in E\}.$$

R is obviously unique (given k), bounded, and M,E definable. I.e., R is internal. QED

We now work with the second order expansion M* of M, where $M^* = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,\ldots,X_1,X_2,\ldots)$. Recall the definition of X_k (Definition 5.5.3).

We use the following language L*(E) suitable for M*.

DEFINITION 5.5.6. The first order terms of L*(E) are exactly the terms of L(E). The second order variables of L*(E) are written $V^k{}_n$, k,n, ≥ 1.
The atomic formulas of L*(E) are of the form

$$t \in E$$
$$V^k{}_n(t_1,\ldots,t_k)$$
$$s = t$$
$$s < t$$

where $s,t,t_1,...,t_k$ are first order terms of L*(E) and $k,n \geq 1$. We view E as a unary predicate symbol, rather than a second order object.

DEFINITION 5.5.7. The formulas of L*(E) are inductively defined as follows.

i) every atomic formula of L*(E) is a formula of L*(E);
ii) if φ,ψ are formulas of L*(E) then $(\neg\varphi),(\varphi\wedge\psi),(\varphi\vee\psi),(\varphi\rightarrow\psi),(\varphi\leftrightarrow\psi)$ are formulas of L*(E);
iii) if φ is a formula of L*(E) and $k,n \geq 1$, then $(\forall v_n)(\varphi)$, $(\exists v_n)(\varphi)$, $(\forall V^k{}_n)(\varphi)$, $(\exists V^k{}_n)(\varphi)$ are formulas of L*(E).

As was the case with L(E), it is the E formulas of L*(E) that we focus on.

DEFINITION 5.5.8. The E formulas of L*(E) are inductively defined as follows.

1) every atomic formula of L*(E) is a formula of L*(E);
ii) if φ,ψ are formulas of L*(E) then $(\neg\varphi),(\varphi\wedge\psi),(\varphi\vee\psi),(\varphi\rightarrow\psi),(\varphi\leftrightarrow\psi)$ are formulas of L*(E);
iii) if φ is a formula of L*(E) and $k,n \geq 1$, then $(\forall v_n \in E)(\varphi)$, $(\exists v_n \in E)(\varphi)$, $(\forall V^k{}_n)(\varphi)$, $(\exists V^k{}_n)(\varphi)$ are formulas of L*(E).

DEFINITION 5.5.9. We use

$$(\forall v_n \in E)(\varphi),\ (\exists v_n \in E)(\varphi)$$

as abbreviations for

$$(\forall v_n)(v_n \in E \rightarrow \varphi),\ (\exists v_n)(v_n \in E \wedge \varphi).$$

DEFINITION 5.5.10. The intended interpretation of L*(E) is the structure M* introduced above, where the first order quantifiers range over A, and the second order quantifiers $V^k{}_n$ range over X_k.

Note that in M*, if a second order object holds at any arguments, then those arguments must have the attribute E. That is, all elements of all second order objects are tuples of elements of E.

DEFINITION 5.5.11. A relation is said to be M*,E definable if and only if it is a relation on E that is M* definable by an E formula of L*(E) with second order parameters from the various X_k and first order parameters from E only.

In practice, we will allow flexibility of notation in presenting formulas of L*(E). In particular we will often drop the subscripts or superscripts on the second order variables.

We also take advantage of the added flexibility of notation that comes from sometimes treating k-ary relations as sets of k-tuples, with the ∈ notation.

LEMMA 5.5.4. Let $k \geq 1$ and $R \subseteq A^k$. The following are equivalent.
i) $R \in X_k$;
ii) R is c_n-definable for some $n \geq 1$;
iii) R is x-definable for some $x \in E$;
iv) R is M*,E definable and bounded.

Proof: Let k,R be as given. In light of Lemma 5.5.2, we have only to verify that iv) implies i). Let

$$R = \{(x_1,\ldots,x_k) \in E^k \cap [0,c_r]^k: \varphi(x_1,\ldots,x_{k+m},R_1,\ldots,R_n) \text{ holds in } M^*\},$$

where $k,m,n,r \geq 1$, $\varphi(V_1,\ldots,v_{k+m},V_1,\ldots,V_n)$ is an E formula of L*(E) whose free variables are among the variables $v_1,\ldots,v_{k+m},V_1,\ldots,V_n$, $x_{k+1},\ldots,x_{k+m} \in E \cap [0,c_r]$, and $R_1,\ldots,R_k$ are internal.

We can remove $R_1,\ldots,R_n$ using definitions of $R_1,\ldots,R_n$ in the form given by Lemma 5.4.17 vi).

We can also remove second order quantifiers by appropriately quantifying over codes, as can be seen from Lemma 5.5.3. This involves quantifying over nine variables. Since each second order quantifier has a definite arity, k, we are only using the fixed term t_k. We then obtain a definition of R by an E formula of L(E). Hence R is internal. QED

DEFINITION 5.5.12. The bounded comprehension axioms of L*(E) consist of all E formulas of L*(E) of the form

$$x_{k+1},\ldots,x_{k+m+1} \in E \rightarrow (\exists R)(\forall x_1,\ldots,x_k \in E)(R(x_1,\ldots,x_k) \leftrightarrow (x_1,\ldots,x_k \leq x_{k+m+1} \wedge \varphi))$$

where $k \geq 1$, $m \geq 0$, φ is an E formula of L*(E) in which R is not free, and all first order variables free in φ are among $x_1,\ldots,x_{k+m+1}$.

LEMMA 5.5.5. The bounded comprehension axioms of L*(E) hold in M*.

Proof: Let a bounded comprehension axiom of L*(E)

$$1)\ x_{k+1},\ldots,x_{k+m+1} \in E \rightarrow (\exists R)(\forall x_1,\ldots,x_k \in E)(R(x_1,\ldots,x_k) \leftrightarrow (x_1,\ldots,x_k \leq x_{k+m+1} \wedge \varphi))$$

be given, subject to the required syntactic conditions above. Write $\varphi = \varphi(x_1,\ldots,x_{k+m+1},V_1,\ldots,V_n)$, where $V_1,\ldots,V_n$ are distinct second order variables of L*(E), and all free variables of φ are among $x_1,\ldots,x_{k+m+1},V_1,\ldots,V_n$.

Let $x_{k+1},\ldots,x_{k+m+1} \in E$ and $R_1,\ldots,R_n \in X$ have the same respective arities as $V_1,\ldots,V_n$. Set

$$R = \{(x_1,\ldots,x_k) \in E^k\text{: } x_1,\ldots,x_k \leq x_{k+1} \wedge \varphi(x_1,\ldots,x_{k+m+1},R_1,\ldots,R_n)\}.$$

Then R is a bounded M*,E definable relation. By Lemma 5.5.4, $R \in X_k$. Therefore R witnesses the consequent of 1). QED

LEMMA 5.5.6. Let $r \geq 1$, and $\varphi(v_1,\ldots,v_{2r})$ be an E formula of L(E). Let $1 \leq i_1,\ldots,i_{2r}$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and the same min. Let $x_1,\ldots,x_r \in E$, $x_1,\ldots,x_r \leq \min(c_{i\_1},\ldots,c_{i\_r})$. Then $\varphi(c_{i\_1},\ldots,c_{i\_r},x_1,\ldots,x_r) \leftrightarrow \varphi(c_{i\_r+1},\ldots,c_{i\_2r},x_1,\ldots,x_r)$.

Proof: Let $r,\varphi,i_1,\ldots,i_{2r}$ be as given. Let $t = \max(i_1,\ldots,i_{2r})$. We can assume that φ is in prenex form:

$$(Q_n v_{2r+1} \in E)\ldots(Q_1 v_{2r+n} \in E)(\psi(v_1,\ldots,v_{2r+n})).$$

where ψ is a quantifier free formula of L(E). By Lemma 5.5.1, for all $v_1,\ldots,v_{2r} \in E \cap [0,c_t]$,

$$(Q_n v_{2r+1} \in E)\ldots(Q_1 v_{2r+n} \in E)(\psi(v_1,\ldots,v_{2r+n}))$$
$$\leftrightarrow$$
$$(Q_n v_{2r+1} \in E \cap [0,c_{t+1}])\ldots(Q_1 v_{2r+n} \in E \cap [0,c_{t+n}])(\psi(v_1,\ldots,v_{2r+n})).$$

In particular, for all $x_1,\ldots,x_r \in E$, $x_1,\ldots,x_r \leq \min(c_{i\_1},\ldots,c_{i\_r})$,

$$1)\ (Q_n v_{2r+1} \in E)\ldots(Q_1 v_{2r+n} \in E)(\psi(c_{i\_1},\ldots,c_{i\_r},x_1,\ldots,x_r,v_{2r+1},\ldots,v_{2r+n}))$$

$$\leftrightarrow$$

$$(Q_n v_{2r+1} \in E \cap [0,c_{t+1}])\ldots(Q_1 v_{2r+n} \in E \cap [0,c_{t+n}])$$
$$(\psi(c_{i\_1},\ldots,c_{i\_r},x1,\ldots,xr,v_{2r+1},\ldots,v_{2r+n})).$$

$$2)\ (Q_n v_{2r+1} \in E)\ldots(Q_1 v_{2r+n} \in E)$$
$$(\psi(c_{i\_r+1},\ldots,c_{i\_2r},x_1,\ldots,x_r,v_{2r+1},\ldots,v_{2r+n}))$$
$$\leftrightarrow$$
$$(Q_n v_{2r+1} \in E \cap [0,c_{t+1}])\ldots(Q_1 v_{2r+n} \in E \cap [0,c_{t+n}])$$
$$(\psi(c_{i\_r+1},\ldots,c_{i\_2r},x_1,\ldots,x_r,v_{2r+1},\ldots,v_{2r+n})).$$

Hence

$$3)\ \varphi(c_{i\_1},\ldots,c_{i\_r},x_1,\ldots,x_r) \leftrightarrow$$
$$(Q_n v_{2r+1} \in E \cap [0,c_{t+1}])\ldots(Q_1 v_{2r+n} \in E \cap [0,c_{t+n}])$$
$$(\psi(c_{i\_1},\ldots,c_{i\_r},x_1,\ldots,x_r,v_{2r+1},\ldots,v_{2r+n}))^{c\_t+n}.$$

$$4)\ \varphi(c_{i\_r+1},\ldots,c_{i\_2r},x_1,\ldots,x_r) \leftrightarrow$$
$$(Q_n v_{2r+1} \in E \cap [0,c_{t+1}])\ldots(Q_1 v_{2r+n} \in E \cap [0,c_{t+n}])$$
$$(\psi(c_{i\_r+1},\ldots,c_{i\_2r},x_1,\ldots,x_r,v_{2r+1},\ldots,v_{2r+n}))^{c\_t+n}.$$

The right sides of 3),4) are $\psi_{c\_t+n},\rho_{c\_t+n}$, respectively, where ρ,ψ begin with the quantifier Q_n. ρ,ψ are first expanded out to formulas of L(E) in the obvious way. Then the displayed quantifiers are relativized to $E \cap [0,c_{t+n}]$.

By Lemma 5.4.17 vii), for all $x_1,\ldots,x_r \in E$, $x_1,\ldots,x_r \leq \min(c_{i\_1},\ldots,c_{i\_r})$,

$$\varphi(c_{i\_1},\ldots,c_{i\_r},x_1,\ldots,x_r) \leftrightarrow \varphi(c_{i\_r+1},\ldots,c_{i\_2r},x_1,\ldots,x_r)$$

QED

LEMMA 5.5.7. Let $r \geq 1$, and $\varphi(v_1,\ldots,v_{2r})$ be an E formula of L*(E), with no free second order variables. Let $1 \leq i_1,\ldots,i_{2r}$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and the same min. Let $x_1,\ldots,x_r \in E$, $x_1,\ldots,x_r \leq \min(c_{i\_1},\ldots,c_{i\_r})$. Then $\varphi(c_{i\_1},\ldots,c_{i\_r},x_1,\ldots,x_r) \leftrightarrow \varphi(c_{i\_r+1},\ldots,c_{i\_2r},x_1,\ldots,x_r)$.

Proof: By the same argument that we used in the proof of Lemma 5.5.4, using codes, we can remove all second order quantifiers in φ, thereby reducing φ to an equivalent E formula $\psi(v_1,\ldots,v_{2r})$ of L(E). No new parameters are introduced in this process. Then apply Lemma 5.5.6. QED

LEMMA 5.5.8. There exists a countable second order structure $M^* = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,\ldots,X_1,X_2,\ldots)$, where for all $i \geq 1$, X_i is the set of all i-ary relations on

A that are c_n-definable for some $n \geq 1$; and terms $t_1,t_2,...$ of L, where for all i, t_i has variables among $x_1,...,x_{i+8}$, such that the following holds.
i) $(A,<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies $TR(\Pi^0_1,L)$;
ii) $E \subseteq A\backslash\{0\}$;
iii) The c_n, $n \geq 1$, form a strictly increasing sequence of nonstandard elements of $E\backslash\alpha(E;2,<\infty)$ with no upper bound in A;
iv) For all $r,n \geq 1$, $\uparrow r(c_n) < c_{n+1}$;
v) $2\alpha(E;1,<\infty)+1$, $3\alpha(E;1,<\infty)+1 \subseteq E$;
vi) Let $k,n \geq 1$ and R be a c_n-definable k-ary relation. There exist $y_1,...,y_8 \in E \cap [0,c_{n+1}]$ such that $R = \{(x_1,...,x_k) \in E^k \cap [0,c_n]^k\colon t_k(x_1,...,x_k,y_1,...,y_8) \in E\}$;
vii) Let $k \geq 1$, $m \geq 0$, and φ be an E formula of $L^*(E)$ in which R is not free, where all first order variables free in φ are among $x_1,...,x_{k+m+1}$. Then $x_{k+1},...,x_{k+m+1} \in E \rightarrow (\exists R)(\forall x_1,...,x_k \in E)(R(x_1,...,x_k) \leftrightarrow (x_1,...,x_k \leq x_{k+m+1} \wedge \varphi))$;
viii) Let $r \geq 1$, and $\varphi(x_1,...,x_{2r})$ be an E formula of $L^*(E)$ with no free second order variables. Let $1 \leq i_1,...,i_{2r}$, where $(i_1,...,i_r)$ and $(i_{r+1},...,i_{2r})$ have the same order type and the same min. Let $x_1,...,x_r \in E$, $x_1,...,x_r \leq \min(c_{i\_1},...,c_{i\_r})$. Then $\varphi(c_{i\_1},...,c_{i\_r},x_1,...,x_r) \leftrightarrow \varphi(c_{i\_r+1},...,c_{i\_2r},x_1,...,x_r)$.

Proof: i),ii),iii),v),vi) are identical to i),ii),iii),v),vi) of Lemma 5.4.17. iv) follows immediately from iv) of Lemma 5.4.17. vii) is from Lemma 5.5.5. viii) is from Lemma 5.5.7. QED

5.6. Π^0_1 correct internal arithmetic, simplification.

We fix $M^* = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,...,X_1,X_2,...)$ from Lemma 5.5.8. Let $M = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,...)$. We can view the main point of this section as the derivation of a suitable form of the axiom of infinity.

Note that we have yet to use that the c's lie outside $\alpha(E;2,<\infty)$, from Lemma 5.5.8 iii). In this section, we use this in an essential way. This condition is needed in order to obtain any useable form of the axiom of infinity.

The one and only use of the fact that the c's lie outside $\alpha(E;2,<\infty)$, in this Chapter, is in the proof of Lemma 5.6.6. There we use that $c_5 \notin \alpha(E;2,<\infty)$.

We first prove the existence of a least internal set I containing 1, and closed under + $2c_1$ (see Lemma 5.6.7 and Definition 5.6.3). We then define natural arithmetic operations on I (see Lemma 5.6.10), resulting in the structure M(I) which satisfies PA(L) (see Lemma 5.6.11). Then we define a natural external isomorphism h from M(I) into M. We then show that M(I) satisfies PA(L) + TR(Π^0_1,L) using the solution to Hilbert's 10th Problem (see Lemma 5.6.14).

At this point, we only care that M(I) satisfies TR(Π^0_1,L), and that I is internally well ordered. The external h is used only to take advantage of the fact that M satisfies TR(Π^0_1,L). We think of h as external because its range is not a subset of E.

M(I) will provide us with the arithmetic part of the structure M# in Lemma 5.6.18.

We remind the reader that for $x,y \in A$, x-y always means

$$x-y \text{ if } x \geq y;\ 0 \text{ if } x < y.$$

Recall that $\alpha(E)$ is the set of all values of terms in L at arguments from E (Definition 5.3.3).

LEMMA 5.6.1. $\alpha(E) = E-E$.

Proof: According to Lemma 5.4.12, $\alpha(E) = E-E$ holds in the structure M given by Lemma 5.3.18, which is the same as the structure M given by Lemma 5.4.17. Therefore $\alpha(E) = E-E$ also holds in the structure M* given by Lemma 5.5.8, which is an expansion of M. QED

DEFINITION 5.6.1. We say that x is critical if and only if $x \in E-E \wedge 2xc_1+1 \in E$.

LEMMA 5.6.2. Let $p,x > 0$, where $p \in N$ and x is critical. Then p,2x+p are critical.

Proof: Let p,x be as given. By Lemma 5.6.1, $p,2x+p \in E-E$. Note that $pc_1 \in \alpha(E;1,<\infty)$. Hence by Lemma 5.5.8 v), $2pc_1+1 \in 2\alpha(E;1,<\infty)+1 \subseteq E$. Hence p is critical.

By $2xc_1+1 \in E$ and Lemma 5.5.8 v),

$$|2xc_1+1,c_1| \leq (2xc_1+1)+(pc_1-1) \leq 4p|2xc_1,c_1|.$$
$$(2xc_1+1)+(pc_1-1) = 2xc_1+pc_1 = (2x+p)c_1 \in \alpha(E;1,<\infty).$$

$$2(2x+p)c_1+1 \in 2\alpha(E;1,<\infty)+1 \subseteq E.$$

Hence 2x+p is critical. QED

LEMMA 5.6.3. Let $x \geq 1$ be critical. Suppose that for all critical $y \in [2,x]$, there is a critical z such that $y \in \{2z,2z+1\}$. Then x+1 is critical and there is a critical z such that $x+1 \in \{2z,2z+1\}$.

Proof: Let $x \geq 1$, and assume the hypothesis. If x = 1 then by Lemma 5.6.2, x+1 = 2 is critical and z = 1 is critical and $x+1 \in \{2z,2z+1\}$. So we can assume $x \geq 2$. Hence $x \in [2,x]$. By hypothesis, let z be critical and $x \in \{2z,2z+1\}$. Then $z \geq 1$ and $z < x$.

Suppose z = 1. Then $x \in \{2,3\}$, and so x+1 is critical by Lemma 5.6.2. If x = 2 then $x+1 \in \{2(1),2(1)+1\}$ and 1 is critical. If x = 3 then $x+1 \in \{2(2),2(2)+1\}$ and 2 is critical.

We may suppose $z \geq 2$. By hypothesis, let w be critical, where $z \in \{2w,2w+1\}$. Then $w \geq 1$, and

$$x \in \{4w,4w+1,4w+2,4w+3\}.$$
$$(x+1)c_1 \in \{4wc_1+c_1,4wc_1+2c_1,4wc_1+3c_1,4wc_1+4c_1\}.$$

$$(x+1)c_1 \in \{2(2wc_1+1)+c_1-2,2(2wc_1+1)+2c_1-2, 2(2wc_1+1)+3c_1-2,2(2wc_1+1)+4c_1-2\}$$

Now each of these four terms lies in $[2wc_1+1,4(2wc_1+1)]$, and $2wc_1+1 \in E$ (since w is critical). Therefore all four terms lie in $\alpha(E;1,<\infty)$. Hence $(x+1)c_1 \in \alpha(E;1,<\infty)$. So by Lemma 5.5.8 v), $2(x+1)c_1+1 \in 2\alpha(E;1,<\infty)+1 \subseteq E$.

Since x is critical, $x \in E-E$. By Lemma 5.6.1, $x+1 \in E-E$. Hence x+1 is critical.

Note that $z+1 \in \{2w+1,2w+2\}$. Since w is critical, by Lemma 5.6.2, z+1 is critical.

Using $z \in \{2w,2w+1\}$, $x \in \{4w,4w+1,4w+2,4w+3\}$, we see that $x+1 \in \{2z+1,2(z+1)\} = \{4w+1,4w+2,4w+3,4w+4\}$. We have that z,z+1 are critical.

case 1. x+1 = 2z+1. Then there is a critical u such that $x+1 \in \{2u,2u+1\}$, by taking u = z.

case 2. $x+1 = 2(z+1)$. Then there is a critical u such that $x+1 \in \{2u,2u+1\}$, by taking $u = z+1$.

QED

DEFINITION 5.6.2. Let C be the set of all $2xc_1+1$ such that

i) x is critical $\wedge$ $x \geq 1$;
ii) for all critical $y \in [2,x]$, there exists critical z such that $y \in \{2z,2z+1\}$.

LEMMA 5.6.4. $\min(C) = 2c_1+1$. $C \subseteq E \cap \alpha(E;2,<\infty)$. $(\forall u \in C)(u+2c_1 \in C)$. C is M,E definable, with only the parameter c_1.

Proof: 1 is critical by Lemma 5.6.2. Hence $2c_1+1 \in C$, and $2c_1+1$ is the least element of C.

For the second claim, let $y \in C$, and write $y = 2xc_1+1$, x critical, $x \geq 1$. Hence $y = 2xc_1+1 \in E$. Therefore, it suffices to verify that $y \in \alpha(E;2,<\infty)$.

If $x = 1$ then $y \in \alpha(E;2,<\infty)$. Assume $x \geq 2$. Therefore $x \in [2,x]$. Let $x \in \{2z,2z+1\}$, where z is critical. If $z = 1$ then again $y \in \alpha(E;2,<\infty)$.

Assume $z \geq 2$. Then $z \in [2,x]$. Let $z \in \{2w,2w+1\}$, where w is critical. Then $x \in \{4w,4w+2,4w+1,4w+3\}$. Also $2wc_1+1 \in E$. Clearly $w \geq 1$. We have

$$y = 2xc_1+1 \in \{8wc_1+1,8wc_1+4c_1+1,\\ 8wc_1+2c_1+1,8wc_1+6c_1+1\}.$$
$$y \in \{4(2wc_1+1)-3,4(2wc_1+1)+4c_1-3,\\ 4(2wc_1+1)+2c_1-3,4(2wc_1+1)+6c_1-3\}.$$

Therefore $y \in \alpha(E;2,<\infty)$, using $2wc_1+1 \in E$ and c_1 as the parameters, and noting that $w \geq 1$. This establishes the second claim.

For the third claim, let $u \in C$. Write $u = 2xc_1+1$. Then $x \geq 1$ is critical. Also, for all critical $y \in [2,x]$, there exists critical z such that $y \in \{2z,2z+1\}$. Hence by Lemma 5.6.3, $x+1$ is critical and there exists critical z such that $x+1 \in \{2z,2z+1\}$.

We must verify that $u+2c_1 = 2xc_1+1+2c_1 = 2(x+1)c_1+1 \in C$. We have only to verify clause ii) in the definition of C with $x+1$ instead of x. Let $y \in [2,x+1]$ be critical. If $y \leq x$

then there exists critical z such that $y = \{2z,2z+1\}$, since $2xc_1+1 \in C$. Now suppose $y = x+1$. We have already established that $x+1$ is critical and there is a critical z such that $x+1 \in \{2z,2z+1\}$. This establishes the third claim.

For the fourth claim, we must check that $C \subseteq E$ can be defined by an E formula of L(E), using only the parameter c_1. Note that $v \in C$ if and only if $v \in E$ and

$$(\exists x)(v = 2xc_1+1 \wedge x \text{ is critical} \wedge x \geq 1 \wedge (\forall y \in [2,x])(y \text{ critical} \rightarrow (\exists z)(z \text{ is critical} \wedge y \in \{2z,2z+1\}))).$$

$$(\exists x)(v = 2xc_1+1 \wedge x \text{ is critical} \wedge x \geq 1 \wedge (\forall \text{ critical } y)(y \in [2,x] \rightarrow (\exists z)(z \text{ is critical} \wedge y \in \{2z,2z+1\}))).$$

$$(\exists x \in E-E)(v = 2xc_1+1 \wedge x \geq 1 \wedge (\forall y \in E-E)(2yc_1+1 \in E \wedge y \in [2,x] \rightarrow (\exists z \in E-E)(2zc_1+1 \in E \wedge y \in \{2z,2z+1\}))).$$

$$(\exists x_1,x_2 \in E)(v = 2(x_1-x_2)c_1+1 \wedge x_1-x_2 \geq 1 \wedge (\forall y_1,y_2 \in E)(2(y_1-y_2)c_1+1 \in E \wedge y_1-y_2 \in [2,x] \rightarrow (\exists z_1,z_2 \in E)(2(z_1-z_2)c_1+1 \in E \wedge y_1-y_2 \in \{2(z_1-z_2),2(z_1-z_2)+1\}))).$$

QED

LEMMA 5.6.5. Suppose $2(E-E)c_1+1 \neg\subseteq C \cup \{1\}$. There exists an internal subset of $C \cup \{1\}$, containing 1, and closed under $+2c_1$.

Proof: Let $x \in E-E$, $2xc_1+1 \notin C \cup \{1\}$. Then $x > 1$. By Lemma 5.6.4, $C \cap [0,2xc_1+1]$ is internal, and contains $2c_1+1$.

We claim that $C \cap [0,2xc_1+1]$ is closed under $+2c_1$. To see this, let $u \in C \cap [0,2xc_1+1]$. By Lemma 5.6.4, $u+2c_1 \in C$. Write $u = 2yc_1+1$.

If $y < x$ then $u+2c_1 = 2yc_1+1+2c_1 = 2(y+1)c_1+1 \leq 2xc_1+1$.

If $y = x$ then $u = 2xc_1+1$. This contradicts $u \in C$, $2xc_1+1 \notin C$.

If $y \geq x+1$ then $u \geq 2(x+1)c_1+1 > 2xc_1+1$. This contradicts $u \leq 2xc_1+1$. This establishes the claim.

It is now clear that $(C \cap [0,2xc_1+1]) \cup \{1\}$ contains 1, and is closed under $+2c_1$, and is internal. QED

LEMMA 5.6.6. Suppose $2(E-E)c_1+1 \subseteq C \cup \{1\}$. There exists an internal subset of $C \cup \{1\}$, containing 1, and closed under $+2c_1$.

Proof: Assume $2(E-E)c_1+1 \subseteq C \cup \{1\}$.

Suppose $C \cap [0,c_5]$ has no greatest element. Note that by Lemma 5.6.4, $(C \cap [0,c_5]) \cup \{1\}$ is an internal subset of E, containing 1.

We claim that $(C \cap [0,c_5]) \cup \{1\}$ is closed under $+2c_1$. To see this, let $u \in (C \cap [0,c_5]) \cup \{1\}$. Let $u = 2zc_1+1$. Since u is not the greatest element of $(C \cap [0,c_5])$, let $2zc_1+1 < 2wc_1+1 \in (C \cap [0,c_5]) \cup \{1\}$. By Lemma 5.6.4, $2zc_1+1+2c_1 = 2(z+1)c_1+1 \in C$. Since $w \geq z+1$, we see that $2zc_1+1+2c_1 \leq 2wc_1+1$. Hence $2zc_1+1+2c_1 \in (C \cap[0,c_5]) \cup \{1\}$. This establishes the claim.

By the claim, it suffices to assume that $C \cap [0,c_5]$ has a greatest element. Let u be the greatest element of $C \cap [0,c_5]$. We will derive a contradiction.

Since C is closed under $+2c_1$, $u+2c_1 \in C$, $u+2c_1 > c_5$, $c_5-u < 2c_1$. Since $c_5-u \in E-E$, we have $v = 2(c_5-u)c_1+1 \in 2(E-E)c_1+1 \subseteq C \cup \{1\}$.

Note that $v < 2(2c_1)c_1+1 < c_2$, by Lemma 5.5.8 iv).

Consider the following true statement about v,c_1.

$$(\exists x,y \in E)(y \leq x \wedge v = 2(x-y)c_1+1).$$

By Lemma 5.5.8 iii), let $n \geq 3$ be so large that

$$(\exists x,y \in E)(y \leq x < c_n \wedge v = 2(x-y)c_1+1).$$

By Lemma 5.5.8 viii),

$$(\exists x,y \in E)(y \leq x < c_3 \wedge v = 2(x-y)c_1+1).$$

Fix $x,y \in E$, $y \leq x < c_3$, $v = 2(x-y)c_1+1$. Then $2(x-y)c_1+1 = 2(c_5-u)c_1+1$, $x-y = c_5-u$. Hence

$$c_5 = u+(x-y).$$

By Lemma 5.6.4, $u \in \alpha(E;2,<\infty)$. Since $x-y = c_5-u < 2c_1$, we have $u > c_5-2c_1 > c_4$, using Lemma 5.5.8 iv).

We claim that $c_5 \in \alpha(E;2,<\infty)$. To see this, write

$$u = t(w_1,\ldots,w_k),\ w_1,\ldots,w_k \in E,\ k \geq 1.$$
$$2|w_1,\ldots,w_k| \leq u \leq p|w_1,\ldots,w_k|,\ p \in N.$$

By Lemma 5.5.8 iv), since $u > c_4$, we have

$$x,y < c_3 < |w_1,\ldots,w_k|$$
$$|w_1,\ldots,w_k,x,y| = |w_1,\ldots,w_k|$$
$$2|w_1,\ldots,w_k,x,y| \leq u \leq u+(x-y) = t(w_1,\ldots,w_k)+(x-y)$$
$$\leq 2p|w_1,\ldots,w_k,x,y|.$$
$$c_5 \in \alpha(E;2,<\infty).$$

using the representation $c_5 = t(w_1,\ldots,w_k)+(x-y)$ in the parameters $w_1,\ldots,w_k,x,y \in E$. But this contradicts Lemma 5.5.8 iii). QED

LEMMA 5.6.7. There exists an internal subset of $C \cup \{1\}$, containing 1, and closed under $+2c_1$. $C \subseteq E \cap (2(E-E)c_1+1)$.

Proof: The first claim is by Lemmas 5.6.5 and 5.6.6. For the second claim, $C \subseteq E$ by Lemma 5.6.4. Let $u \in C$. Write $u = 2xc_1+1$, x critical. Then $x \in E-E$. Hence $u \in 2(E-E)c_1+1$. QED

DEFINITION 5.6.3. Let I be the intersection of all internal sets containing 1, and closed under $+2c_1$.

By Lemma 5.6.7, I exists.

LEMMA 5.6.8. The following hold.
i. I is the least internal set which is closed under $+2c_1$ and contains 1.
ii. $I \subseteq C \cup \{1\}$.
iii. The immediate successor in I of any $x \in I$ is $x+2c_1$.
iv. Every internal nonempty subset of I has a least element.
v. I is defined by an E formula of L*(E) with only the parameter c_1.
vi. $I \subseteq [0,c_2)$.

Proof: By Lemma 5.5.8 vii), I is an internal set. By definition, it is closed under $+2c_1$ and contains 1. Hence i) follows from the definition of I.

ii) follows from Lemma 5.6.7.

For iii), it follows from ii) that every element of I is of the form $2xc_1+1$. Let $u \in I$. Write $u = 2xc_1+1$. Now $2xc_1+1+2c_1 = 2(x+1)c_1+1 \in I$. There is no room for any element of I strictly between $2xc_1+1$ and $2(x+1)c_1+1 = u+2c_1$.

For iv), let $S \subseteq I$ be nonempty and internal. If S has no least element then let $S^* = \{x \in I$: x is below every element of $S\}$. Obviously $S^* \subseteq I$ is a nonempty internal set containing 1 with no greatest element. Let $u \in S^*$. Let $u < v \in S^*$. Then $u+2c_1 \in I$ and $u+2c_1 \leq v$. Therefore $u+2c_1 \in S$. Thus we have shown that S^* is closed under $+2c_1$, and contains 1. Therefore $S^* = I$. This contradicts the definition of S^*.

For v), the natural formalization of the definition of I results in an E formula of L*(E) with only the parameter c_1.

For vi), by Lemma 5.5.8 iii), since the c's are unbounded in A, and I is bounded in A, let $n \geq 2$ be such that $I \subseteq [0,c_n]$. We view this inclusion as a statement about c_1,c_n. By Lemma 5.5.8 viii), the corresponding statement about c_1,c_2 holds. I.e., $I \subseteq [0,c_2]$. QED

LEMMA 5.6.9. Every element of I is of the form $2xc_1+1$, with $x \in E\text{-}E$. $x \in I \wedge x > 1 \rightarrow x-2c_1 \in I$.

Proof: For the first claim, let $u \in I$. By Lemma 5.6.8, $u \in C \cup \{1\}$. If $u = 1$ then set $x = 0$. If $u \in C$, apply the second claim of Lemma 5.6.7.

For the second claim, let $x \in I$, $x > 1$, $x-2c_1 \notin I$. Then $I \cap [0,x)$ is an internal set which contains 1.

We claim that $I \cap [0,x)$ is closed under $+2c_1$. To see this, write $x = 2c_1z+1$. Let $u = 2c_1w+1 \in I \cap [0,x)$. Then $w < z$ and $2c_1(w+1)+1 \in I$.

It remains to show that $2c_1(w+1)+1 < x$. I.e., $w+1 < z$. From $w < z$, we have $w+1 \leq z$. So we merely have to eliminate the case $w+1 = z$.

Suppose $w+1 = z$. Then $w = z-1$, $u = 2c_1(z-1)+1 = x-2c_1 \in I$. This contradicts $x-2c_1 \notin I$.

We now see that $I \cap [0,x)$ is an internal set closed under $+2c_1$, containing 1. By Lemma 5.6.8, $I \cap [0,x) = I$, contradicting $x \in I$. QED

LEMMA 5.6.10. The following hold.
i. If $2xc_1+1, 2yc_1+1 \in I$ then $2(x+y)c_1+1 \in I$.
ii. If $2xc_1+1, 2yc_1+1 \in I$ then $2xyc_1+1 \in I$.
iii. If $2xc_1+1, 2yc_1+1 \in I$ then $2(x-y)c_1+1 \in I$.
iv. If $2xc_1+1 \in I$ then $2x\uparrow c_1+1 \in I$.
v. If $2xc_1+1 \in I$ then $2\log(x)c_1+1 \in I$.

Proof: For i), fix $u = 2xc_1+1 \in I$. We can assume that $x > 0$. Let

$$S = \{v \in I: (\exists y)(v = 2yc_1+1 \wedge 2(x+y)c_1+1 \notin I)\} = \{v \in I: (\exists y \in E-E)(v = 2yc_1+1 \wedge 2(x+y)c_1+1 \notin I)\}.$$

This equality holds by Lemma 5.6.9.

By Lemma 5.6.8, S is internal. Assume S is nonempty. By Lemma 5.6.8, let $v = 2yc_1+1$ be the least element of S. Clearly $v > 1$, $y > 0$, and so by Lemma 5.6.9, $v-2c_1 = 2(y-1)c_1+1 \in I$. By the choice of v, $v-2c_1 \notin S$. Hence $2(x+y-1)c_1+1 \in I$. By Lemma 5.6.8, $2(x+y-1)c_1+1+2c_1 = 2c_1(x+y)+1 \in I$. This contradicts $v \in S$.

For ii), fix $u = 2xc_1+1 \in I$. We can assume that $x > 0$. Let

$$S' = \{v \in I: (\exists y)(v = 2yc_1+1 \wedge 2(xy)c_1+1 \notin I)\} = \{v \in I: (\exists y \in E-E)(v = 2yc_1+1 \wedge 2(xy)c_1+1 \notin I)\}.$$

This equality holds by Lemma 5.6.9.

By Lemma 5.6.8, S' is internal. Assume S' is nonempty. By Lemma 5.6.8, let $v = 2yc_1+1$ be the least element of S'. Clearly $v > 1$, $y > 0$, and so by Lemma 5.6.9, $v-2c_1 = 2(y-1)c_1+1 \in I$. By the choice of v, $v-2c_1 \notin S'$. Hence $2x(y-1)c_1+1 \in I$. By the first claim, since $2xc_1+1 \in I$, we have $2(x+x(y-1))c_1+1 = 2c_1(xy)+1 \in I$. This contradicts $v \in S'$.

For iii), fix $u = 2yc_1+1 \in I$, and let

$$S'' = \{v \in I: (\exists x)(v = 2xc_1+1 \wedge 2(x-y)c_1+1 \notin I)\} = \{v \in I: (\exists x \in E-E)(v = 2xc_1+1 \wedge 2(x-y)c_1+1 \notin I)\}$$

This equality holds by Lemma 5.6.9.

By Lemma 5.6.8, S′′ is internal. Assume S′′ is nonempty. By Lemma 5.6.8, let $v = 2xc_1+1$ be the least element of S′′. Clearly $v > 1$, $x > y$, and so by Lemma 5.6.9, $v-2c_1 = 2(x-1)c_1+1 \in I$. By the choice of v, $v-2c_1 \notin S''$. Hence $2((x-1)-y)c_1+1 \in I$. Now $(x-1)-y = (x-y)-1 < x-y$. Hence $2((x-y)-1)c_1+1 \in I$. By Lemma 5.6.8, $2(x-y)c_1+1 \in I$. This contradicts $v \in S''$.

For iv), let

$$S^* = \{v \in I: (\exists x)(v = 2xc_1+1 \wedge 2x\uparrow c_1+1 \notin I)\} = \{v \in I: (\exists x \in E-E)(v = 2xc_1+1 \wedge 2x\uparrow c_1+1 \notin I)\}$$

This equality holds by Lemma 5.6.9.

By Lemma 5.6.8, S* is internal. Assume S* is nonempty. By Lemma 5.6.8, let $v = 2xc_1+1$ be the least element of S*. Clearly $v > 1$, $x > 0$, and so by Lemma 5.6.9, $v-2c_1 = 2(x-1)c_1+1 \in I$. By the choice of v, $v-2c_1 \notin S^*$. Hence $2(x-1)\uparrow c_1+1 \in I$. By the first claim, $2((x-1)\uparrow+(x-1)\uparrow)c_1+1 = 2x\uparrow c_1+1 \in I$. This contradicts $v \in S^*$.

For v), let

$$S^{**} = \{v \in I: (\exists x)(v = 2xc_1+1 \wedge 2\log(x)c_1+1 \notin I)\} = \{v \in I: (\exists x \in E-E)(v = 2xc_1+1 \wedge 2\log(x)c_1+1 \notin I)\}$$

This equality holds by Lemma 5.6.9.

By Lemma 5.6.8, S** is internal. Assume S** is nonempty, By Lemma 5.6.8, let $v = 2xc_1+1$ be the least element of S**. Clearly $v > 1$, $x > 0$, and so by Lemma 5.6.19, $v-2c_1 = 2(x-1)c_1+1 \in I$. By the choice of v, $v-2c_1 \notin S^{**}$. Hence $2\log(x-1)c_1+1 \in I$. Clearly $\log(x-1) \in \{\log(x)-1,\log(x)\}$. Since $2\log(x)c_1+1 \notin I$, we have $\log(x-1) = \log(x)-1$. Hence $2(\log(x)-1)c_1+1 \in I$. by Lemma 5.6.8, $2\log(x)c_1+1 \in I$. This contradicts $v \in S^{**}$. QED

We use Lemmas 5.6.9, 5.6.10 to impose an arithmetic structure on I. We define $0' = 1$, $1' = 2c_1+1$. Let $x,y \in I$, $x = 2zc_1+1$, $y = 2wc_1+1$. We define $x +' y = 2(z+w)c_1+1$, $x -' y = 2(z-w)c_1+1$, $x \bullet' y = 2zwc_1+1$, $x\uparrow' = 2z\uparrow c_1+1$, $\log'(x) = 2\log(z)c_1+1$.

DEFINITION 5.6.4. We introduce the relational structure

$$M(I) = (I,<,0',1',+',-',\bullet',\uparrow',\log').$$

It is essential to note that by Lemma 5.6.8, M(I) is internal. I.e., the domain and component relations of M(I) are internal as relations.

DEFINITION 5.6.5. Let $h:I \rightarrow E-E$ be the one-one function defined by

$$h(2c_1x+1) = x.$$

Note that h may not be internal, because, for example, its values may not all lie in E. But h is a perfectly good external isomorphism from M(I) onto the structure

$$M|rng(h) = (rng(h),<,0,1,+,-,\bullet,\uparrow,log)$$

which is a substructure of (a reduct of) M*. Note also that M|rng(h) may not be internal, because rng(h) $\subseteq$ E-E may not be a subset of E.

Recall from section 5.1 that TR(Π^0_1,L) is defined to be the set of all true Π^0_1 sentences in the language based on <,0,1,+,-,•,↑,log. Here bounded quantifiers are allowed.

It is immediate that M|rng(h) satisfies the true Π^0_1 sentences of L with **no bounded quantifiers allowed**. We have to bridge this gap.

DEFINITION 5.6.6. Let PA(L) be the usual system of Peano arithmetic for the language L. Its nonlogical axioms are as follows.

1. $x+1 \neq 0$.
2. $x+1 = y+1 \rightarrow x = y$.
3. $0+1 = 1$.
4. $x+0 = x$.
5. $x+(y+1) = (x+y)+1$.
6. $x\bullet 0 = 0$.
7. $x\bullet(y+1) = x\bullet y + x$.
8. $\neg x < 0$.
9. $x < y+1 \leftrightarrow (x < y \vee x = y)$.
10. $x \leq y \rightarrow x < y \vee x = y$.
11. $0\uparrow = 1$.
12. $(x+1)\uparrow = x\uparrow+x\uparrow$.
13. $\log(0) = 0$.
14. $y\uparrow \leq x \wedge x < (y+1)\uparrow \rightarrow \log(x) = y$.
15. $\varphi[x/0] \wedge (\forall x)(\varphi \rightarrow \varphi[x/x+1]) \rightarrow \varphi$, where φ is a formula in L.

DEFINITION 5.6.7. A strict Π^0_1 sentence is a Π^0_1 sentence without bounded quantifiers.

LEMMA 5.6.11. TR(Π^0_1,L) logically implies PA(L) without 15. M|rng(h) satisfies PA(L). M(I) satisfies PA(L).

Proof: The axioms of PA(L) without 15 are clearly true strict Π^0_1 sentences, and so by Lemma 5.5.8 i), they hold in M. Hence they also hold in the substructure M|rng(h) of M. By the external isomorphism h, they hold in M(I).

For 15, first note that by Lemma 5.6.10, M(I) satisfies that every element > 0 has an immediate predecessor. Suppose that in M(I), φ defines a subset S of I containing 0′ and closed under the +1 of M(I). Suppose S ≠ I.

Since M(I) is internal, S is internal. Hence by Lemma 5.6.8, I\S has a least element x ∈ I. Since x > 0′, x has an immediate predecessor y ∈ I, with y ∈ S. Hence x ∈ S, which is a contradiction. This establishes the second claim.

The third claim follows by the isomorphism h. QED

LEMMA 5.6.12. For every Π^0_1(L) sentence φ there is a strict Π^0_1(L) sentence ψ such that PA(L) proves φ ↔ ψ.

Proof: By a well known normal form theorem, we fix a Π^0_1(L) formula ρ(x,y) in L with the distinct free variables x,y only, such that the following holds. For all Π^0_1(L) sentences φ, there exists n ∈ N such that PA(L) proves

$$1)\ (\forall x)(\rho(x,n^*)) \leftrightarrow \varphi$$

where n* is 1+1...+1, with n 1's. See, e.g., [Si99], section II.2.

From the work on Hilbert's 10th problem, there exists k ≥ 1 and two polynomials $Q_1(x_1,\ldots,x_k,y)$, $Q_2(x_1,\ldots,x_k,y)$, with nonnegative integer coefficients, such that

$$2)\ (\forall x)(\rho(x,y)) \leftrightarrow (\forall x_1,\ldots,x_k)(Q_1(x_1,\ldots,x_k,y) \neq Q_2(x_1,\ldots,x_k,y)))$$

is true for all y ∈ N. Here all variables range over nonnegative integers. This follows immediately from the sharp form of the negative solution to Hilbert's 10th problem that asserts that every recursively enumerable subset of N is Diophantine. This is due to Y. Matiyasevich, J. Robinson, M. Davis, and H. Putnam. See, e.g., [Da73], [Mat93].

Moreover, it is well known that for a given $\rho(x,y)$, polynomials Q_1,Q_2 can be found such that PA proves: for all y, 2) holds. This is because the entire treatment of Hilbert's 10th problem can be carried out straightforwardly within PA(L). We fix such polynomials Q_1,Q_2.

(In fact, this treatment can be carried out in the very weak fragment of PA called EFA = exponential function arithmetic, which is $I\Sigma_0(\exp)$. See [HP93], p. 37, and [GD82].)

Now let φ be a $\Pi^0{}_1(L)$ sentence. Fix n such that 1) is provable in PA(L). Set y = n* in 2). Then PA(L) proves

$$3)\ \varphi \leftrightarrow (\forall x)(\rho(x,n^*)) \leftrightarrow (\forall x_1,\ldots,x_k)(Q_1(x_1,\ldots,x_k,n^*) \neq Q_2(x_1,\ldots,x_k,n^*))$$

and so we set

$$\psi = (\forall x_1,\ldots,x_k)(Q_1(x_1,\ldots,x_k,n^*) \neq Q_2(x_1,\ldots,x_k,n^*)).$$

QED

LEMMA 5.6.13. PA(L) + strict $TR(\Pi^0{}_1,L)$ logically implies $TR(\Pi^0{}_1,L)$. M|rng(h) and M(I) satisfy PA(L) + $TR(\Pi^0{}_1,L)$.

Proof: For the first claim, let $\varphi \in TR(\Pi^0{}_1,L)$. By Lemma 5.6.12, let ψ be strict $TR(\Pi^0{}_1,L)$, where PA(L) proves $\psi \rightarrow \varphi$. Then PA(L) + strict $TR(\Pi^0{}_1,L)$ proves φ. Hence PA(L) + strict $TR(\Pi^0{}_1,L)$ proves $TR(\Pi^0{}_1,L)$.

For the second claim, by Lemma 5.6.11, M|rng(h) and M(I) satisfy PA(L). Now obviously M|rng(h) satisfies strict $TR(\Pi^0{}_1,L)$) since M does (Lemma 5.5.8 i)), and M|rng(h) is a substructure of M. Hence M(I) also satisfies strict $TR(\Pi^0{}_1,L)$. Hence by the first claim, M|rng(h) and M(I) satisfy $TR(\Pi^0{}_1,L)$. QED

Note that the definitions of CODE and INCODE from section 5.3, apply without modification to the present context.

LEMMA 5.6.14. Let $k,n,m \geq 1$, and $x_1,\ldots,x_k \leq c_n < c_m$, where $x_1,\ldots,x_k \in E$. Then $CODE(c_m;x_1,\ldots,x_k) \in E$, and $INCODE(CODE(c_m;x_1,\ldots,x_k)) = P(x_1,\ldots,x_k)$.

Proof: We essentially repeat the proof of Lemma 5.3.11, slightly adapted to the present context.

Let $k,n,m,x_1,\ldots,x_k$ be as given. Note that

$$(c_m \div 2)+1 \le (\log(c_m))\uparrow \le c_m.$$
$$2c_m \le 4(\log(c_m))\uparrow+P(x_1,\ldots x_k)) \le 5c_m.$$

$$4((\log(c_m))\uparrow+P(x_1,\ldots x_k)) \in \alpha(E;2,<\infty).$$
$$\mathrm{CODE}(c_m;x_1,\ldots,x_k) \in 2\alpha(E;2,<\infty)+1.$$

Hence $\mathrm{CODE}(c_m;x_1,\ldots,x_k) \in E$ by Lemma 5.5.8 v).

We claim that

$$1)\ \log(\mathrm{CODE}(c_m;x_1,\ldots,x_k)) = \log(c_m)+3.$$

To see this, note that

$$\log(\mathrm{CODE}(c_m;x_1,\ldots,x_k)) =$$
$$\log(8((\log(c_m))\uparrow + P(x_1,\ldots,x_k))+1) =$$
$$\log(8(\log(c_m))\uparrow + 8P(x_1,\ldots,x_k) + 1) =$$
$$\log((\log(c_m)+3)\uparrow + 8P(x_1,\ldots,x_k) + 1) \le$$
$$\log((\log(c_m)+3)\uparrow + \log(c_m)) = \log(c_m)+3 \le$$
$$\log((\log(c_m)+3)\uparrow + 8P(x_1,\ldots,x_k) + 1).$$

Using 1),

$$\mathrm{INCODE}(\mathrm{CODE}(c_m;x_1,\ldots,x_k)) = z \leftrightarrow$$
$$8z \le \mathrm{CODE}(c_m;x_1,\ldots,x_k)-(\log(\mathrm{CODE}(c_m;x_1,\ldots,x_k)))\uparrow-1 < 8z+8 \leftrightarrow$$
$$8z \le \mathrm{CODE}(c_m;x_1,\ldots,x_k)-(\log(c_m)+3)\uparrow-1 < 8z+8 \leftrightarrow$$
$$8z \le \mathrm{CODE}(c_m;x_1,\ldots,x_k)-8((\log(c_m))\uparrow)-1 < 8z+8 \leftrightarrow$$
$$8z \le 8P(x_1,\ldots,x_k) < 8z+8.$$

Hence

$$\mathrm{INCODE}(\mathrm{CODE}(c_m;x_1,\ldots,x_k)) = P(x_1,\ldots,x_k).$$

QED

The following will be used to give an interpretation of the $\in$ relation in the set theory $K(\Pi)$ introduced below.

LEMMA 5.6.15. There is an E formula $\sigma(x_1,x_2)$ of $L(E)$ such that the following holds. Let S be an internal set. There exist arbitrarily large $y \in E$ such that $S = \{x \in E: \sigma(x,y)\}$.

Proof: Let $S \subseteq E$ be internal. Let $n \geq 1$ be such that S is c_n-definable (see Lemma 5.5.4). By Lemma 5.5.8 vi), write

$$1)\ S = \{x \in E \cap [0,c_n]: t_1(x,y_1,...,y_8) \in E\}$$

where $y_1,...,y_8 \in E$. This definition of S has the parameters $c_n,y_1,...,y_8$. Here t_1 is among the terms t1,t2,... given at the beginning of Lemma 5.5.8. Here t_1 is defined independently of S.

We now show that instead of using the 9 parameters $c_n,y_1,...,y_8 \in E$ above, we can use a single parameter $y \in E$. In particular, we claim that there are arbitrarily large y $\in$ E such that

$$2)\ S = \{x \in E: (\exists z_0,...,z_8 \in E)(\text{INCODE}(y) = P(z_0,...,z_8) \wedge x \leq z_0 \wedge t_k(x,z_1,...,z_8) \in E\}.$$

To see this, first let $x \in S$. Then 1) holds with $c_n,y_1,...,y_8 \in E$. Set $y = \text{CODE}(c_m;c_n,y_1,...,y_8)$, where $y_1,...,y_8,c_n < c_m$. By Lemma 5.6.15, $y \in E$. Obviously $y \geq c_m$. We have

$$x \in E \cap [0,c_n] \wedge t_1(x,y_1,...,y_8) \in E.$$

Set $z_0,...,z_8 = c_n,y_1,...,y_8$, respectively. By Lemma 5.6.14,

$$\text{INCODE}(y) = \text{INCODE}(\text{CODE}(c_m;c_n,y_1,...,y_8)) = P(z_0,...,z_8).$$

Also $x \leq z_0$, $t_1(x,z_1,...,z_8) \in E$.

On the other hand, suppose

$$x \in E \wedge (\exists z_0,...,z_8 \in E)(\text{INCODE}(y) = P(z_0,...,z_8) \wedge x \leq z_0 \wedge t_1(x,z_1,...,z_8) \in E\})$$

where $y = \text{CODE}(c_m;c_n,y_1,...y_8)$.

Let $z_0,...,z_8 \in E$ be such that

$$\text{INCODE}(y) = P(z_0,...,z_8) \wedge x \leq z_0 \wedge t_1(x,z_1,...,z_8) \in E.$$

By Lemma 5.6.14, $\text{INCODE}(y) = P(c_n,y_1,...,y_8)$. Hence $c_n = z_0$, $y_1 = z_1$, ..., $y_8 = z_8$, $x \leq c_n$, and $t_1(x,y_1,...,y_8) \in E$. Hence by 1), $x \in S$.

It remains to see that S has been defined by an E formula of L(E) in x,y. It suffices to write

$$\mathrm{INCODE}(y) = P(z_0,\ldots,z_8)$$

as a quantifier free formula in L. This is clear from

$$\mathrm{INCODE}(y) = u \leftrightarrow$$
$$8u \leq y-(\log(y))\uparrow-1 < 8u+8.$$

QED

We are now prepared to streamline the structure M*, retaining only what is needed to complete the construction of a model of SMAH + TR($\Pi^0{}_1$,L).

We have built quite a bit of complexity in M* in order to carry out the construction of arithmetic in M* via the internal structure M(I), and have related that arithmetic to the arithmetic of M on (a subset of) A in order to obtain $\Pi^0{}_1$ correctness for M(I).

Now that we have this machinery in place, we no longer need to work with any objects outside of E.

Our simplification will be formulated in terms of a first order linearly ordered set theory. We will convert M* to a model of this linearly ordered set theory whose domain is a subset of E.

We now present the language L# for linearly ordered set theory.

DEFINITION 5.6.8. The language L# is based on the following primitives.

i) variables v_n, $n \geq 1$;
ii) the constant symbols d_n, $n \geq 1$;
iii) the unary relation symbol NAT;
iv) the binary relation symbols $\in$,<;
v) the constant symbols 0,1;
vi) the unary function symbols $\uparrow$,log;
vii) the binary function symbols +,-,•;
viii) = (equality).

Note that L# includes constant symbols d_n, $n \geq 1$, whereas L, L(E), and L*(E) do not include constant symbols c_n, $n \geq 1$.

The constants c_n appeared only as distinguished elements of our interpretations of the languages L, L(E), and L*(E).

DEFINITION 5.6.9. The terms of L# are built from the variables and the constant symbols of L#, using the function symbols. The atomic formulas of L# are of the form $s = t$, $s < t$, $s \in t$, where s,t are terms of L#. Formulas of L# are defined in the usual way using the usual connectives $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$, and the usual quantifiers $\forall,\exists$.

We now introduce the linearly ordered set theory K(Π) in the language L#.

DEFINITION 5.6.10. K(Π) consists of the following axioms.

1. < is a linear ordering (irreflexive, transitive, connected).
2. $x \in y \rightarrow x < y$.
3. Let $1 \leq n < m$. Then $d_n < d_m$.
4. Let φ be a formula of L# in which v_1 is not free. Then $(\exists v_1)(\forall v_2)(v_2 \in v_1 \leftrightarrow (v_2 \leq v_3 \wedge \varphi))$.
5. Let $r \geq 1$ and $\varphi(v_1,\ldots,v_{2r})$ be a formula of L#. Let $1 \leq i_1,\ldots,i_{2r}$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and min. Let $y_1,\ldots,y_r \leq \min(d_{i\_1},\ldots,d_{i\_r})$. Then $\varphi(d_{i\_1},\ldots,d_{i\_r},y_1,\ldots,y_r) \leftrightarrow \varphi(d_{i\_r+1},\ldots,d_{i\_2r},y_1,\ldots,y_r)$.
6. NAT defines a nonempty initial segment under <, with no greatest element, and no limit point, where all points are $< d_1$, and whose first two elements are $0 < 1$, such that $+,-,\bullet,\uparrow,\log$ map NAT into NAT.
7. $(\forall x)$(if x has an element in NAT then x has a < least element).
8. Let $\varphi \in TR(\Pi^0_1,L)$. Take the relativization of φ to NAT.
9. $+,-,\bullet,\uparrow,\log$ have the default value 0 in case one or more arguments lie outside NAT.

DEFINITION 5.6.11. We now define the structure $M\# = (D,<,\in,NAT,0,1,+,-,\bullet,\uparrow,\log,d_1,d_2, \ldots)$ as follows. Recall that we have been using the structure $M^* = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,\ldots,X_1,X_2,\ldots)$.

By Lemma 5.6.8, $I \subseteq E \cap [0,c_2)$. Let J be the initial segment of (E,<) determined by I. Take $D = E\backslash J \cup I$. I.e., D is the result of cutting down J to I in E.

Define < in M# to be the restriction of < in M* to D. Take $NAT(x) \leftrightarrow x \in I$.

Define 0,1,+,−,•,↑,log of M# as follows. The 0,1 of M# are the same as the 0,1 of the structure M(I). The +,−,•,↑,log of M# restricted to I are the same as the +,−,•,↑,log of M(I). Finally, if one or more arguments lie outside I, then the +,−,•,↑,log of M# return the 0 of M(I).

Let $x,y \in D$. Define

$$x \in y \leftrightarrow (\sigma(x,y) \wedge x < y)$$

where σ is given by Lemma 5.6.15.

Finally, for $n \geq 1$, define $d_n = c_{n+1}$.

LEMMA 5.6.16. Let $k \geq 1$, $\varphi(v_1,\ldots,v_k)$ be a formula of L# without any d's. There exists an E formula $\varphi'(x_1,\ldots,x_{k+1})$ of L*(E) such that the following holds. Let $x_1,\ldots,x_k \in D$. Then

$$\varphi(x_1,\ldots,x_k) \text{ holds in M\# } \leftrightarrow$$
$$\varphi'(x_1,\ldots,x_k,c_1) \text{ holds in M*.}$$

Proof: Let φ be as given. First, formally restrict the scope of all quantifiers to the formal property $x \in E \wedge (x \in I \vee (\forall v \in I)(v < x))$. The extension of this property is D.

Now replace all subformulas NAT(t) by $(\exists v)(v = t \wedge v \in I)$.

Next unravel all subformulas $s = t$, $s < t$, by using new existential quantifiers relativized to I for subterms with 0,1,+,−,•,↑,log. We can straightforwardly do this so that

i. there is at most one occurrence of a function symbol in every remaining equation.
ii. there are no occurrences of function symbols in every remaining inequality.

Now replace $v+w = z$, $v-w = z$, $v \bullet w = z$, $v\uparrow = z$, $\log(v) = z$, respectively, by

$(v \notin I \vee w \notin I \wedge z = 0) \vee (v \in I \wedge w \in I \wedge v+'w = z)$.
$(v \notin I \vee w \notin I \wedge z = 0) \vee (v \in I \wedge w \in I \wedge v-'w = z)$.
$(v \notin I \vee w \notin I \wedge z = 0) \vee (v \in I \wedge w \in I \wedge v\bullet'w = z)$.
$(v \notin I \wedge z = 0) \vee (v \in I \wedge v\uparrow' = z)$.
$(v \notin I \wedge z = 0) \vee (v \in I \wedge \log'(v) = z)$.

Then replace $v+'w = z$, $v-'w = z$, $v\bullet'w = z$, $v\uparrow' = z$, $\log'(v) = z$, respectively, by their definitions given right after the proof of Lemma 5.6.10.

Now replace 0 by 1 and 1 by $2c_1+1$.

Next replace atomic subformulas $z \in w$ by $\sigma(z,w)$, given by Definition 5.6.3.

Finally, replace all $v \in I$ by the definition of I in Definition 5.6.3.

The parameter c_1, only, appears in the definition of I, and the definitions of $1,+,-,\bullet,\uparrow,\log$. QED

LEMMA 5.6.17. $M\# = (D,<,\in,NAT,0,1,+,-,\bullet,\uparrow,\log,d_1,d_2,\ldots)$ satisfies $K(\Pi)$, where $d_1,d_2,\ldots$ forms a strictly increasing sequence from D without an upper bound.

Proof: Axioms 1,2,3,9 are evident by construction.

For axiom 4, let $\varphi(v_2,\ldots,v_k)$ be as given, $k \geq 1$. Let $x_2,\ldots,x_k \in D$. Define

$$S = \{x_2 \in D: x_2 \leq x_3 \wedge \varphi(x_2,\ldots,x_k) \text{ holds in } M\#\}.$$

By Lemma 5.6.16, we can write S in the form

$$S = \{x_2 \in D: x_2 \leq x_3 \wedge \varphi'(x_2,\ldots,x_k,c_1) \text{ holds in } M^*\}$$

where $\varphi'(v_2,\ldots,v_{k+1})$ is an E formula of $L^*(E)$. Hence S is internal. By Lemma 5.6.15, let $y \in E$, $y > x_3,c_2$, be such that

$$S = \{x \in E: \sigma(x,y)\}.$$

Note that since $y \in E$ and $y > c_2$, we have $y \in D$.

Since $S \subseteq D$, $y \in D$, and S is strictly bounded above by y, we have

$$S = \{x \in D: x \in_{M\#} y\}.$$

We now claim that

$$(\forall x_2)(x_2 \in y \leftrightarrow (x_2 \leq x_3 \wedge \varphi(x_2,\ldots,x_k)))$$

holds in M#. To see this, let $x_2 \in D$, $x_2 \in_{M\#} y$. Then $x_2 \in S$, and so $x_2 \leq x_3$, and $\varphi(x_2,\ldots,x_k)$ holds in M#.

Conversely, suppose $x_2 \in D$, $x_2 \leq x_3$, and $\varphi(x_2,\ldots,x_k)$ holds in M#. Then $x_2 \in S$, and so $x_2 \in_{M\#} y$.

For axiom 5, let $r \geq 1$, $\varphi(v_1,\ldots,v_{2r})$ be a formula in L#. Let $1 \leq i_1,\ldots,i_{2r}$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and the same min. Let $x_{r+1},\ldots,x_{2r} \in D$, $x_{r+1},\ldots,x_{2r} \leq \min(d_{i\_1},\ldots,d_{i\_r})$.

Let $\varphi'(x_1,\ldots,x_{2r+1})$ be given by Lemma 5.6.16. Then for all $x_1,\ldots,x_{2r} \in D$,

$$\varphi(d_{i\_1},\ldots,d_{i\_r},x_{r+1},\ldots,x_{2r}) \text{ holds in M\#} \leftrightarrow \varphi'(c_{i\_1\ +1},\ldots,c_{i\_r\ +1},x_{r+1},\ldots,x_{2r},c_1) \text{ holds in M*}.$$

$$\varphi(d_{i\_r+1},\ldots,d_{i\_2r},x_{r+1},\ldots,x_{2r}) \text{ holds in M\#} \leftrightarrow \varphi'(c_{i\_r+1\ +1},\ldots,c_{i\_2r\ +1},x_{r+1},\ldots,x_{2r},c_1) \text{ holds in M*}.$$

By Lemma 5.5.8 viii), the right sides of the above two equivalences are equivalent. Hence the left sides of the above two equivalences are equivalent.

For axiom 6, NAT defines a nonempty initial segment under < by construction, and is I. I has no greatest element, and no limit point by Lemmas 5.6.8, 5.6.9. NAT lives below d_1 since $I \subseteq [0,c_2)$, according to Lemma 5.6.8, and $d_1 = c_2$. The first two elements of NAT are the 0,1 of M# by construction.

For axiom 7, by Lemma 5.6.8, I is internally well ordered in M*. By Lemma 5.6.16, NAT = I remains internally well ordered in M#.

For axiom 8, NAT with the 0,1,<,+,-,•,↑,log of M# is the same as M(I). By Lemma 5.6.13, M(I) satisfies TR($\Pi^0{}_1$,L). Hence NAT with the 0,1,<,+,-,•,↑,log of M# satisfies the sentences in TR($\Pi^0{}_1$,L).

The d's are unbounded in M# because the c's are unbounded in M*. QED

We now put Lemma 5.6.17 into our usual format to be used in the next section.

LEMMA 5.6.18. There exists a countable structure $M\# = (D,<,\in,NAT,0,1,+,-,\bullet,\uparrow,\log,d_1,d_2,...)$ such that the following holds.
i) < is a linear ordering (irreflexive, transitive, connected);
ii) $x \in y \rightarrow x < y$;
iii) The d_n, $n \geq 1$, form a strictly increasing sequence of elements of D with no upper bound in D;
iv) Let φ be a formula of L# in which v_1 is not free. Then $(\exists v_1)(\forall v_2)(v_2 \in v_1 \leftrightarrow (v_2 \leq v_3 \wedge \varphi))$;
v) Let $r \geq 1$ and $\varphi(v_1,...,v_{2r})$ be a formula of L# not mentioning any constants d_n, $n \geq 1$. Let $1 \leq i_1,...,i_{2r}$, where $(i_1,...,i_r)$ and $(i_{r+1},...,i_{2r})$ have the same order type and min. Let $y_1,...,y_r \leq \min(d_{i\_1},...,d_{i\_r})$. Then $\varphi(d_{i\_1},...,d_{i\_r},y_1,...,y_r) \leftrightarrow \varphi(d_{i\_r+1},...,d_{i\_2r},y_1,...,y_r)$;
vi) NAT defines a nonempty initial segment under <, with no greatest element, and no limit point, where all points are $< d_1$, and whose first two elements are 0,1, respectively;
vii) $(\forall x)$(if x has an element obeying NAT then x has a < least element);
viii) Let $\varphi \in TR(\Pi^0_1,L)$. The relativization of φ to NAT holds.
ix) $+,-,\bullet,\uparrow,\log$ have the default value 0 in case one or more arguments lie outside NAT.

Proof: This is immediate from Lemma 5.6.17. QED

5.7. Transfinite induction, comprehension, indiscernibles, infinity, Π^0_1 correctness.

We now fix $M\# = (D,<,\in,NAT,0,1,+,-,\bullet,\uparrow,\log,d_1,d_2,...)$ as given by Lemma 5.6.18.

While working in M#, we must be cautious.

a. The linear ordering < may not be internally well ordered. In fact, there may not even be a < minimal element above the initial segment given by NAT.
b. We may not have extensionality.

Note that we have lost the internally second order nature of M* as we passed from M* to the present M# in section 5.6. The goal of this section is to recover this internally second order aspect, and gain internal well foundedness of <.

To avoid confusion, we use the three symbols =, ≡, ≈. Here = is the standard identity relation we have been using throughout the book.

DEFINITION 5.7.1. We use ≡ for extensionality equality in the form

$$x \equiv y \leftrightarrow (\forall z)(z \in x \leftrightarrow z \in y).$$

DEFINITION 5.7.2. We use ≈ as a special symbol in certain contexts.

DEFINITION 5.7.3. We write $x \approx \emptyset$ if and only if x has no elements.

We avoid using the notation $\{x_1,...,x_k\}$ out of context, as there may be more than one set represented in this way.

DEFINITION 5.7.4. Let $k \geq 1$. We write $x \approx \{y_1,...,y_k\}$ if and only if

$$(\forall z)(z \in x \leftrightarrow (z = y_1 \vee ... \vee z = y_k)).$$

LEMMA 5.7.1. Let $k \geq 1$. For all $y_1,...,y_k$ there exists $x \approx \{y_1,...,y_k\}$. Here x is unique up to ≡.

Proof: Let $y = \max(y_1,...,y_k)$. By Lemma 5.6.18 iv),

$$(\exists x)(\forall z)(z \in x \leftrightarrow (z \leq y \wedge (z = y_1 \vee ... \vee z = y_k))).$$

The last claim is obvious. QED

DEFINITION 5.7.5. We write $x \approx \langle y,z \rangle$ if and only if there exists a,b such that

i) $x \approx \{a,b\}$;
ii) $a \approx \{y\}$;
iii) $b \approx \{y,z\}$.

LEMMA 5.7.2. If $x \approx \langle y,z \rangle \wedge w \in x$, then $w \approx \{y\} \vee w \approx \{y,z\}$. If $x \approx \langle y,z \rangle \wedge x \approx \langle u,v \rangle$, then $y = u \wedge z = v$. For all y,z, there exists $x \approx \langle y,z \rangle$.

Proof: For the first claim, let x,y,z,w be as given. Let a,b be such that $x \approx \{a,b\}$, $a \approx \{y\}$, $b \approx \{y,z\}$. Then $w = a \vee w = b$. Hence $w \approx \{y\} \vee w \approx \{y,z\}$.

For the second claim, let $x \approx \langle y,z \rangle$, $x \approx \langle u,v \rangle$. Let

$x \approx \{a,b\}$, $a \approx \{y\}$, $b \approx \{y,z\}$
$x \approx \{c,d\}$, $c \approx \{u\}$, $d \approx \{u,v\}$.

Then

$(a = c \vee a = d) \wedge (b = c \vee b = d) \wedge (c = a \vee c = b) \wedge (d = a \vee d = b)$.

Since $a = c \vee a = d$, we have $y = u \vee (y = u = v)$. Hence $y = u$.

We have $b \approx \{y,z\}$, $d \approx \{y,v\}$. If $b = d$ then $z = v$. So we can assume $b \neq d$. Hence $b = c$, $d = a$. Therefore $u = y = z$, $y = u = v$.

For the third claim, let y,z. By Lemma 5.7.1, let $a \approx \{y\}$ and $b \approx \{y,z\}$. Let $x \approx \{a,b\}$. Then $x \approx \langle y,z\rangle$. QED

DEFINITION 5.7.6. Let $k \geq 2$. We inductively define $x \approx \langle y_1,\ldots,y_k\rangle$ as follows. $x \approx \langle y_1,\ldots,y_{k+1}\rangle$ if and only if $(\exists z)(x \approx \langle z,y_3,\ldots,y_{k+1}\rangle \wedge z \approx \langle y_1,y_2\rangle)$. In addition, we define $x \approx \langle y\rangle$ if and only if $x = y$.

LEMMA 5.7.3. Let $k \geq 1$. If $x \approx \langle y_1,\ldots,y_k\rangle$ and $x \approx \langle z_1,\ldots,z_k\rangle$, then $y_1 = z_1 \wedge \ldots \wedge y_k = z_k$. For all $y_1,\ldots,y_k$, there exists x such that $x \approx \langle y_1,\ldots,y_k\rangle$.

Proof: The first claim is by external induction on $k \geq 2$, the case $k = 1$ being trivial. The basis case $k = 2$ is by Lemma 5.7.2. Suppose this is true for a fixed $k \geq 2$. Let $x \approx \langle y_1,\ldots,y_{k+1}\rangle$, $x \approx \langle z_1,\ldots,z_{k+1}\rangle$. Let u,v be such that $x \approx \langle u,y_3,\ldots,y_{k+1}\rangle$, $x \approx \langle v,z_3,\ldots,z_{k+1}\rangle$, $u \approx \langle y_1,y_2\rangle$, $v \approx \langle z_1,z_2\rangle$. By induction hypothesis, $u = v \wedge y_3 = z_3 \wedge \ldots \wedge y_{k+1} = z_{k+1}$. By Lemma 5.7.2, since $u = v$, we have $y_1 = z_1 \wedge y_2 = z_2$.

The second claim is also by external induction on $k \geq 2$, the case $k = 1$ being trivial. The basis case $k = 2$ is by Lemma 5.7.2. Suppose this is true for a fixed $k \geq 2$. Let $y_1,\ldots,y_{k+2}$. By Lemma 5.7.2, let $z \approx \langle y_1,y_2\rangle$. By induction hypothesis, let $x \approx \langle z,y_3,\ldots,y_{k+2}\rangle$. Then $x \approx \langle y_1,\ldots,y_{k+2}\rangle$. QED

DEFINITION 5.7.7. Let $k \geq 1$. We say that R is a k-ary relation if and only if $(\forall x \in R)(\exists y_1,\ldots,y_k)(x \approx \langle y_1,\ldots,y_k\rangle)$. If R is a k-ary relation then we define $R(y_1,\ldots,y_k)$ if and only if

$$(\exists x \in R)(x \approx \langle y_1,\ldots,y_k\rangle).$$

Note that if R is a k-ary relation with $R(y_1,\ldots,y_k)$, then there may be more than one $x \in R$ with $x \approx \langle y_1,\ldots,y_k\rangle$.

We use set abstraction notation with care.

DEFINITION 5.7.8. We write

$$x \approx \{y: \varphi(y)\}$$

if and only if

$$(\forall y)(y \in x \leftrightarrow \varphi(y)\}.$$

If there is such an x, then x is unique up to $\equiv$.

Let R,S be k-ary relations. The notion $R \equiv S$ is usually too strong for our purposes.

DEFINITION 5.7.9. We define $R \equiv' S$ if and only if

$$(\forall x_1,\ldots,x_k)(R(x_1,\ldots,x_k) \leftrightarrow S(x_1,\ldots,x_k)).$$

DEFINITION 5.7.10. We define $R \subseteq' S$ if and only if

$$(\forall x_1,\ldots,x_k)(R(x_1,\ldots,x_k) \rightarrow S(x_1,\ldots,x_k).$$

We now prove comprehension for relations. To do this, we need a bounding lemma.

LEMMA 5.7.4. Let $n,k \geq 1$, and $x_1,\ldots,x_k \leq d_n$. There exists $y \approx \{x_1,\ldots,x_k\}$ such that $y \leq d_{n+1}$. There exists $z \approx \langle x_1,\ldots,x_k\rangle$ such that $z \leq d_{n+1}$.

Proof: Let $k,n,x_1,\ldots,x_k$ be as given. By Lemmas 5.7.1 and 5.7.3,

$$(\exists y)(y \approx \{x_1,\ldots,x_k\}).$$
$$(\exists z)(z \approx \langle x_1,\ldots,x_k\rangle).$$

By Lemma 5.6.18 iii), let $r > n$ be such that

$$(\exists y \leq d_r)(y \approx \{x_1,\ldots,x_k\}).$$
$$(\exists z \leq d_r)(z \approx \langle x_1,\ldots,x_k\rangle).$$

By Lemma 5.6.18 v),

$$(\exists y \leq d_{n+1})(y \approx \{x_1,\ldots,x_k\}).$$
$$(\exists z \leq d_{n+1})(z \approx <x_1,\ldots,x_k>).$$

QED

LEMMA 5.7.5. Let $k,n \geq 1$ and $\varphi(v_1,\ldots,v_{k+n})$ be a formula of L#. Let $y_1,\ldots,y_n,z$ be given. There is a k-ary relation R such that $(\forall x_1,\ldots,x_k)(R(x_1,\ldots,x_k) \leftrightarrow (x_1,\ldots,x_k \leq z \wedge \varphi(x_1,\ldots,x_k,y_1,\ldots,y_n)))$.

Proof: Let $k,n,m,\varphi,y_1,\ldots,y_n,z$ be as given. By Lemma 5.6.18 iii), let $r \geq 1$ be such that $y_1,\ldots,y_n,z \leq d_r$. By Lemma 5.6.18 iv), let R be such that

$$1)\ (\forall x)(x \in R \leftrightarrow (x \leq d_{r+1} \wedge (\exists x_1,\ldots,x_k \leq z)(x \approx <x_1,\ldots,x_k> \wedge \varphi(x_1,\ldots,x_k,y_1,\ldots,y_n)))).$$

Obviously R is a k-ary relation. We claim that

$$(\forall x_1,\ldots,x_k)(R(x_1,\ldots,x_k) \leftrightarrow (x_1,\ldots,x_k \leq z \wedge \varphi(x_1,\ldots,x_k,y_1,\ldots,y_n))).$$

To see this, fix $x_1,\ldots,x_k$. First assume $R(x_1,\ldots,x_k)$. Let $x \approx <x_1,\ldots,x_k>$, $x \in R$. By 1),

$$x \leq d_{r+1} \wedge (\exists x_1^*,\ldots,x_k^* \leq z)(x = <x_1^*,\ldots,x_k^*> \wedge \varphi(x_1^*,\ldots,x_k^*,y_1,\ldots,y_n)).$$

Let $x_1^*,\ldots,x_k^*$ be as given by this statement. By Lemma 5.7.3, $x_1^* = x_1, \ldots, x_k^* = x_k$. Hence $x_1,\ldots,x_k \leq z \wedge \varphi(x_1,\ldots,x_k,y_1,\ldots,y_n)$.

Now assume

$$x_1,\ldots,x_k \leq z \wedge \varphi(x_1,\ldots,x_k,y_1,\ldots,y_n).$$

By Lemma 5.7.4, let

$$x \approx <x_1,\ldots,x_k> \wedge x \leq d_{r+1}.$$

By 1), $x \in R$. Hence $R(x_1,\ldots,x_k)$. QED

LEMMA 5.7.6. If $x \approx \{y_1,\ldots,y_k\}$ then each $y_i < x$. If $x \approx <y_1,\ldots,y_k>$, $k \geq 2$, then each $y_i < x$. If $x \approx <y_1,\ldots,y_k>$, $k \geq 1$, then each $y_i \leq x$. If $R(x_1,\ldots,x_k)$ then each $x_i < R$.

Proof: The first claim is evident from Lemma 5.6.18 ii). The second claim is by external induction on $k \geq 2$. For the basis case k = 2, note that if $x \approx \langle y,z\rangle$ then y,z are both elements of elements of x, and apply Lemma 5.6.18 ii). Now assume true for fixed $k \geq 2$. Let $x \approx \langle y_1,\ldots,y_{k+1}\rangle$, and let $z \approx \langle y_1,y_2\rangle$, $x \approx \langle z,y_3,\ldots,y_{k+1}\rangle$, By induction hypothesis, $z,y_3,\ldots,y_{k+1} < x$, and also $y_1,y_2 < x$.

The third claim involves only the new case k = 1, which is trivial.

For the final claim, let $R(x_1,\ldots,x_k)$. Let $x \approx \langle x_1,\ldots,x_k\rangle$, $x \in R$. By the second claim and Lemma 5.6.18 iii), $x_1,\ldots,x_k \leq x < R$. QED

DEFINITION 5.7.11. A binary relation is defined to be a 2-ary relation. Let R be a binary relation. We "define"

$$\mathrm{dom}(R) \approx \{x\colon (\exists y)(R(x,y))\}.$$
$$\mathrm{rng}(R) \approx \{x\colon (\exists y)(R(y,x))\}.$$
$$\mathrm{fld}(R) \approx \{x\colon (\exists y)(R(x,y) \vee R(y,x)\}.$$

Note that this constitutes a definition of dom(R), rng(R), fld(R) up to ≡.

LEMMA 5.7.7. For all binary relations R, dom(R) and rng(R) and fld(R) exist.

Proof: Let R be a binary relation. By Lemma 5.6.18 iv), let A,B,C be such that

$$(\forall x)(x \in A \leftrightarrow (x \leq R \wedge (\exists y)(R(x,y))).$$
$$(\forall x)(x \in B \leftrightarrow (x \leq R \wedge (\exists y)(R(y,x))).$$
$$(\forall x)(x \in C \leftrightarrow (x \leq R \wedge (\exists y)(R(x,y) \vee R(y,x)))).$$

By Lemma 5.7.6,

$$(\forall x)(x \in A \leftrightarrow (\exists y)(R(x,y)).$$
$$(\forall x)(x \in B \leftrightarrow (\exists y)(R(y,x)).$$
$$(\forall x)(x \in C \leftrightarrow (\exists y)(R(x,y) \vee R(y,x))).$$

QED

DEFINITION 5.7.12. A pre well ordering is a binary relation R such that

i) $(\forall x \in \mathrm{fld}(R))(R(x,x))$;
ii) $(\forall x,y,z \in \mathrm{fld}(R))((R(x,y) \wedge R(y,z)) \rightarrow R(x,z))$;
iii) $(\forall x,y \in \mathrm{fld}(R))(R(x,y) \vee R(y,x))$;
iv) $(\forall x \subseteq \mathrm{fld}(R))(\neg(x \approx \emptyset) \rightarrow (\exists y \in x)(\forall z \in x)(R(y,z)))$.

Note that R is a pre well ordering if and only if R is reflexive, transitive, connected, and every nonempty subset of its field (or domain) has an R least element.

Note that all pre well orderings are reflexive. Clearly for pre well orderings R, dom(R) ≡ rng(R) ≡ fld(R).

Let R be a reflexive and transitive relation.

DEFINITION 5.7.13. It will be convenient to write R(x,y) as $x \leq_R y$, and write $x =_R y$ for $x \leq_R y \wedge y \leq_R x$. We also define $x \geq_R y \leftrightarrow y \leq_R x$, $x <_R y \leftrightarrow x \leq_R y \wedge \neg y \leq_R x$, $x >_R y \leftrightarrow y <_R x$, and $x \neq_R y \leftrightarrow \neg x =_R y$.

DEFINITION 5.7.14. Let R be a pre well ordering and x ∈ fld(R). We "define" the binary relations R|<x by

$$(\forall y,z)(R|<x(y,z) \leftrightarrow y \leq_R z <_R x)).$$

Note that R|<x is unique up to ≡'. Also note that by Lemma 5.7.5, R|<x exists. Furthermore, it is easy to see that R|<x is a pre well ordering.

When we write R|<x, we require that x ∈ fld(R).

DEFINITION 5.7.15. Let R,S be pre well orderings. We say that T is an isomorphism from R onto S if and only if

i) T is a binary relation;
ii) dom(T) ≡ dom(R), rng(T) ≡ dom(S);
iii) Let T(x,y), T(z,w). Then $x \leq_R z \leftrightarrow y \leq_S w$;
iv) Let $x =_R u$, $y =_S v$. Then $T(x,y) \leftrightarrow T(u,v)$.

LEMMA 5.7.8. Let R,S be pre well orderings, and T be an isomorphism from R onto S. Let T(x,y), T(z,w). Then $x <_R z \leftrightarrow y <_S w$, and $x =_R z \leftrightarrow y =_S w$.

Proof: Let R,S,T,x,y,z,w be as given. Suppose $x <_R z$. Then $y \leq_S w$. If $w \leq_S y$ then $z \leq_R x$. Hence $y <_R w$. Suppose $y <_S w$. Then $x \leq_R z$. If $z \leq_R x$ then $w \leq_S y$. Hence $x <_R z$. Suppose $x =_R z$. Then $y \leq_S w$ and $w \leq_S y$. Hence $y =_S w$. Suppose $y =_S w$. Then $x \leq_R z$ and $z \leq_R x$. Hence $x =_R z$. QED

LEMMA 5.7.9. Let R,S be pre well orderings. Let a,b ∈ dom(S). Let T be an isomorphism from R onto S|<a, and T* be an isomorphism from R onto S|<b. Then $a =_S b$ and T ≡' T*.

Proof: Let R,S,a,b,T,T* be as given. Suppose there exists x ∈ dom(R) such that for some y, ¬(T(x,y) ↔ T*(x,y)). By Lemma 5.6.18 iv), let x be R least with this property.

case 1. (∃y)(T(x,y) ∧ ¬T*(x,y)). Let T(x,y), ¬T*(x,y). Also let T*(x,y*). If y $=_S$ y* then by clause iv) in the definition of isomorphism, T*(x,y). Hence ¬y $=_S$ y*.

case 1a. y $<_S$ y*. Then y $<_S$ b. Let T*(x*,y).

Suppose x* $<_R$ x. If ¬T(x*,y), then we have contradicted the choice of x. Hence T(x*,y). But this contradicts T(x,y) by Lemma 5.7.8.

Suppose x $\leq_R$ x*. By T*(x,y*), T*(x*,y) and Lemma 5.7.8, y* $\leq_S$ y. This is a contradiction.

case 1b. y* $<_S$ y. Then y* $<_S$ a. Let T(x*,y*). By T(x,y) and Lemma 5.7.8, x* $<_R$ x. By the choice of x, since T(x*,y*), we have T*(x*,y*). By Lemma 5.7.8, since T*(x,y*), we have x $=_R$ x*. Since T(x,y), by Lemma 5.7.8 we have y $=_S$ y*. This is a contradiction.

case 2. (∃y)(¬T(x,y) ∧ T*(x,y)). Let ¬T(x,y), T*(x,y). This is the same as case 1, interchanging a,b, and T,T*.

We have now established that T ≡′ T*. If a $<_S$ b then a ∈ rng(T*) but a ∉ rng(T). This contradicts T ≡′ T*. If b $<_S$ a then b ∈ rng(T) but b ∉ rng(T*). This also contradicts T ≡′ T*. Therefore a $=_S$ b. QED

DEFINITION 5.7.16. Let R,S be pre well orderings. Let T be an isomorphism from R onto S. Let x ∈ dom(R). We write T|<x for "the" restriction of T to first arguments u $<_R$ x. We write T|≤x for "the" restriction of T to first arguments u $\leq_R$ x. Note that T|<x, T|≤x are each unique up to ≡'.

LEMMA 5.7.10. Let R,S be pre well orderings. Let T be an isomorphism from R onto S, and T(x,y). Then T|<x is an isomorphism from R|<x onto S|<y.

Proof: Let R,S,T,x,y be as given. It suffices to show that rng(T|<x) ≡ {b: b $<_S$ y}. Let b $<_S$ y. Let T(a,b). By Lemma 5.7.8, a $<_R$ x. Hence b ∈ rng(T|<x). QED

LEMMA 5.7.11. Let R,S be pre well orderings, T be an isomorphism from R onto S, and T* be an isomorphism from R|<x onto S|<y. Then T* ≡' T|<x and T(x,y).

Proof: Let R,S,T,T*,x,y be as given. Let T(x,y*). By Lemma 5.7.10, T|<x is an isomorphism from R|<x onto S|<y*. By Lemma 5.7.9, y $=_S$ y* and T|<x ≡' T*. Hence T(x,y). QED

DEFINITION 5.7.17. Let T be a binary relation. We write T^{-1} for the binary relation given by T^{-1}(x,y) ↔ T(y,x). By Lemma 5.7.5, T^{-1} exists. Obviously T^{-1} is unique up to ≡'.

LEMMA 5.7.12. Let R,S be pre well orderings, and T be an isomorphism from R onto S. Then T^{-1} is an isomorphism from S onto R.

Proof: Let R,S,T be as given. Obviously dom(T^{-1}) ≡ dom(S) and rng(T^{-1}) ≡ dom(R). Let T^{-1}(x,y), T^{-1}(z,w). Then T(y,x), T(w,z). Hence y $\leq_R$ w ↔ x $\leq_S$ z.

Finally, let T^{-1}(x,y), x $=_R$ u, y $=_S$ v. Then T(y,x), T(v,u), T^{-1}(u,v). QED

DEFINITION 5.7.18. Let R be a pre well ordering. We can append a new point ∞ on top and form the extended pre well ordering R^+. The canonical way to do this is to use R itself as the new point. This defines R^+ uniquely up to ≡'.

Clearly R^+|<∞ ≡' R.

LEMMA 5.7.13. Let R,S be pre well orderings. Exactly one of the following holds.
1. R,S are isomorphic.
2. R is isomorphic to some S|<y, y ∈ dom(S).
3. Some R|<x, x ∈ dom(R), is isomorphic to S.
In case 2, the y is unique up to $=_S$. In case 3, the x is unique up to $=_R$. In all three cases, the isomorphism is unique up to ≡'.

Proof: We first prove the uniqueness claims. For case 1, let T,T* be isomorphisms from R onto S. Then T,T* are isomorphisms from R onto S^+|<∞. By Lemma 5.7.9, T ≡' T*.

For case 2, Let T be an isomorphism from R onto S|<y, and T* be an isomorphism from R onto S|<y*. Apply Lemma 5.7.9.

For case 3, Let T be an isomorphism from R|<x onto S, and T* be an isomorphism from R|<x* onto S. By Lemma 5.7.12, T^{-1} is an isomorphism from S onto R|<x, and T^{*-1} is an isomorphism from S onto R|<x*. Apply Lemma 5.7.9.

For uniqueness, it remains to show that at most one case applies. Suppose cases 1,2 apply. Let T be an isomorphism from R onto S, and T* be an isomorphism from R onto S|<y. Then T is an isomorphism from R onto S^+|<∞, and T* is an isomorphism from R onto S^+|<y. By Lemma 5.7.9, y is ∞, which is a contradiction.

Suppose cases 1,3 hold. Let T be an isomorphism from R onto S, and T* be an isomorphism from R|<x onto S. Then T^{-1} is an isomorphism from S onto R^+|<∞, and T^{*-1} is an isomorphism from S onto R^+|<x. By Lemma 5.7.9, x is ∞, which is a contradiction.

Suppose cases 2,3 hold. Let T be an isomorphism from R onto S|<y and T* be an isomorphism from R|<x onto S. By Lemma 5.7.10, T|<x is an isomorphism from R|<x onto S|<z, where T(x,z). Hence T|<x is an isomorphism from R|<x onto S^+|<z. Also T* is an isomorphism from R|<x onto S^+|<∞. Hence by Lemma 5.7.9, z is ∞. This is a contradiction.

We now show that at least one of 1-3 holds. Consider all isomorphisms from some R^+|<x onto some S^+|<y, x ∈ dom(R^+), y ∈ dom(S^+). We call these the local isomorphisms.

We claim the following, concerning these local isomorphisms. Let T be an isomorphism from R^+|<x onto S^+|<y, and T* be an isomorphism from R^+|<x* onto S^+|<y*. If x $=_{R+}$ x* then y $=_{S+}$ y* and T ≡' T*. If x $<_{R+}$ x* then y $<_{S+}$ y* and T ≡' T*|<x. If x* $<_{R+}$ x then y* $<_{S+}$ y and T* ≡' T|<x*.

To see this, let T,T*,x,y be as given.

case 1. x $=_{R+}$ x*. Apply Lemma 5.7.9.

case 2. x* $<_{R+}$ x. Suppose y $\leq_{S+}$ y*. Let T(x*,z), z $<_{S+}$ y. By Lemma 5.7.10, T|<x* is an isomorphism from R^+|<x* onto S^+|<z. By Lemma 5.7.9, T* ≡' T|<x* and z $=_{S+}$ y*. This is a contradiction. Hence y* $<_{S+}$ y. By Lemma 5.7.10, T|<x* is an isomorphism from R^+|<x* onto S^+|<w, where T(x*,w), w $<_{S+}$ y. By Lemma 5.7.9, T* ≡' T|<x*.

case 3. x $<_{R+}$ x*. Symmetric to case 2.

By Lemma 5.7.5, we can form the union T of all of the local isomorphisms, since the underlying arguments are all in dom(R^+) or dom(S^+), both of which are bounded.

By the pairwise compatibility of the local isomorphisms, T obeys conditions iii),iv) in the definition of isomorphism. It is also clear that the domain of T is closed downward in R^+, and the range of T is closed downward in S^+. Hence dom(T) ≈ {u: u $<_{R+}$ x}, rng(T) ≈ {v: v $<_{S+}$ y}, for some x ∈ dom(R^+), y ∈ dom(S^+). Hence T is an isomorphism from R^+|<x onto S^+|<y.

We now argue by cases.

case 1. x,y are ∞. Then T is an isomorphism from R onto S.

case 2. x is ∞, y ∈ dom(S). Then T is an isomorphism from R onto S|<y*, y^ defined below.

case 3. x ∈ dom(R), y is ∞. Then T is an isomorphism from R|<x* onto S, x^ defined below.

case 4. x ∈ dom(R), y ∈ dom(S). Then T is an isomorphism from R|<x onto S|<y. Using Lemma 5.7.5, let T* be defined by

$$T^*(u,v) \leftrightarrow$$
$$T(u,v) \vee (u =_R x \wedge v =_S y).$$

Then T* is an isomorphism from R|<x^ onto S|<y^, where x^,y^ are respective immediate successors of x,y in R^+,S^+. This contradicts the definition of T. QED

LEMMA 5.7.14. Let R,S,S* be pre well orderings. Let T be an isomorphism from R onto S, and T* be an isomorphism from S onto S*. Define T**(x,y) ↔ (∃z)(T(x,z) ∧ T*(z,y)), by Lemma 5.7.5. Then T** is an isomorphism from R onto S*.

Proof: Let R,S,S*,T,T*,T** be as given. Note that T** is defined up to ≡′. Obviously dom(T**) ≡ dom(R), rng(T**) ≡ dom(S*).

Suppose T**(x,y), T**(x*,y*). Let T(x,z), T*(z,y), T(x*,w), T*(w,y*). Then $x \leq_R x^* \leftrightarrow z \leq_S w$, $z \leq_R w \leftrightarrow y \leq_S y^*$. Therefore $x \leq_R x^* \leftrightarrow y \leq_S y^*$.

Suppose T**(x,y), $x =_R u$, $y =_{S'} v$. Let T(x,z), T*(z,y). Then T(u,z), T*(z,v). Hence T**(u,v). QED

We introduce the following notation in light of Lemma 5.7.13.

DEFINITION 5.7.19. Let R,S be pre well orderings. We define

R =** S ↔
R,S are pre well orderings and R,S are isomorphic.

R <** S ↔
R,S are pre well orderings and there exists y ∈ fld(S) such that R and S|<y are isomorphic.

R ≤** S ↔
R <** S ∨ R =** S.

LEMMA 5.7.15. In <**, the y is unique up to $=_S$. <** is irreflexive and transitive on pre well orderings. =** is an equivalence relation on pre well orderings. ≤** is reflexive and transitive and connected on pre well orderings. Let R,S,S* be pre well orderings. (R ≤** S ∧ S <** S*) → R <** S*. (R <** S ∧ S ≤** S*) → R <** S*. R <** S ∨ S <** R ∨ R =** S, with exclusive ∨. R ≤** S ∨ S ≤** R. (R ≤** S ∧ S ≤** R) → R =** S.

Proof: We apply Lemmas 5.7.13 and 5.7.14. For the first claim, if R <** S then we are in case 2 of Lemma 5.7.13, and the y is unique up to $=_S$.

For the second claim, <** is irreflexive since R <** R implies that cases 1,2 both hold in Lemma 5.7.13 for R,R. Also, suppose R <** S, S <** S*. Let T be an isomorphism from R onto S|<y, and T* be an isomorphism from S onto S*|<z. By Lemma 5.7.10, Let T** be an isomorphism from S|<y onto S*|<w. By Lemma 5.7.14, there is an isomorphism from R onto S*|<w. Hence R <** S*.

For the third claim, note that R =** R because there is an isomorphism from R onto R by defining T(x,y) ↔ x $=_R$ y. Now suppose R =** S, and let T be an isomorphism from R onto S. By Lemma 5.7.12, T^{-1} is an isomorphism from S onto R. Hence S =** R. Finally, suppose R =** S, S =** S*, and let T be an isomorphism from R onto S, T* be an isomorphism from S onto S*. By Lemma 5.7.14, R =** S*.

For the fourth claim, since R =** R, we have R ≤** R. For transitivity, let R ≤** S, S ≤** S*. If R <** S, S <** S*, then by the second claim, R <** S*, and so R ≤** S*. If R =** S, S =** S*, then by Lemma 5.7.14, R =** S*, and so R ≤** S*. The remaining two cases for transitivity follow from the fifth and sixth claims. Connectivity of ≤** is by Lemma 5.7.13.

For the fifth claim, let R ≤** S and S <** S*. By the second claim, we have only to consider the case R =** S. Let S be isomorphic to S*|<y. Since R is isomorphic to S, by the third claim, R is isomorphic to S*|<y. Hence R <** S*.

For the sixth claim, let R <** S and S ≤** S*. By the second claim, we have only to consider the case S =** S*. Let R be isomorphic to S|<y. By Lemma 5.7.10, S|<y is isomorphic to S*|<z, for some z ∈ dom(S*). By the third claim, R is isomorphic to S*|<z. Hence R <** S*.

The seventh and eighth claims are immediate from Lemmas 5.7.12 and 5.7.13.

For the ninth claim, let R ≤** S and S ≤** R. Assume R <** S. By the sixth claim R <** R, which is a contradiction. Assume S <** R. By the sixth claim, S <** S, which is also a contradiction. By the eighth claim, R ≤** S ∨ S ≤** R. Under either disjunct, R =** S. QED

LEMMA 5.7.16. Every nonempty set of pre well orderings has a ≤** least element.

Proof: Let A be a nonempty set of pre well orderings, and fix S ∈ A. We can assume that there exists R ∈ A such that R <** S, for otherwise, S is a ≤** minimal element of A.

By Lemma 5.7.5, define

B ≈ {y ∈ dom(S): (∃R ∈ A)(T =** S|<y)}.

Let y be an S least element of B. Let R ∈ A be isomorphic to S|<y.

We claim that R is a ≤** least element of A. To see this, by trichotomy, let R* <** R, R* ∈ A. Then R* <** S|<y, since R is isomorphic to S|<y.

Let R* be isomorphic to (S|<y)|<z, z $<_S$ y. Then R* is isomorphic to S|<z, z $<_S$ y. This contradicts the choice of y. QED

DEFINITION 5.7.20. For x,y ∈ D, we define x <# y if and only

there exists a pre well ordering S ≤ y such that for every pre well ordering R ≤ x, R <** S.

We caution the reader that the $\leq$ in the above definition is not to be confused with $\leq^{**}$. It is from the $<$ of D in the structure M#. In particular, x,y generally will not be pre well orderings. Thus here we are treating R,S as points.

DEFINITION 5.7.21. We define $x \leq^{\#} y$ if and only if

for all pre well orderings $R \leq x$ there exists a pre well ordering $S \leq y$ such that $R \leq^{**} S$.

LEMMA 5.7.17. $<^{\#}$ is an irreflexive and transitive relation on D. $\leq^{\#}$ is a reflexive and transitive relation on D. Let $x,y \in D$. $x \leq^{\#} y \vee y <^{\#} x$. $x <^{\#} y \rightarrow x \leq^{\#} y$. $(x \leq^{\#} y \wedge y <^{\#} z) \rightarrow x <^{\#} z$. $(x <^{\#} y \wedge y \leq^{\#} z) \rightarrow x <^{\#} z$. $x \leq y \rightarrow x \leq^{\#} y$. $x <^{\#} y \rightarrow x < y$. $x \leq^{\#} y \leftrightarrow \neg y <^{\#} x$. $x <^{\#} y \leftrightarrow \neg y \leq^{\#} x$.

Proof: For the first claim, $<^{\#}$ is irreflexive since $<^{**}$ is irreflexive. Suppose $x <^{\#} y$ and $y <^{\#} z$. Let $S \leq y$ be a pre well ordering such that for all pre well orderings $R \leq x$, $R <^{**} S$. Let $S^* \leq z$ be a pre well ordering such that for all pre well orderings $R \leq y$, $R <^{**} S^*$. Then $S <^{**} S^*$. Hence for all pre well orderings $R \leq x$, $R <^{**} S <^{**} S^*$. Hence for all pre well orderings $R \leq x$, $R <^{**} S^*$, by the transitivity of $<^{**}$. Since $S^* \leq z$, we have $x \leq^{\#} z$.

For the second claim, $x \leq^{\#} x$ since $\leq^{**}$ on pre well orderings is reflexive. Suppose $x \leq^{\#} y$ and $y \leq^{\#} z$. Let $R \leq x$. Let $S \leq y$, $R \leq^{**} S$. Let $S^* \leq z$, $S \leq^{**} S^*$. By the transitivity of $\leq^{**}$, $R \leq^{**} S^*$.

For the third claim, let $\neg(x \leq^{\#} y)$. Let $R \leq x$ be a pre well ordering such that for all pre well orderings $S \leq y$, we have $\neg R \leq^{**} S$. We claim that $y <^{\#} x$. To see this, let $S \leq y$ be a pre well ordering. Then $\neg R \leq^{**} S$. By Lemma 5.7.15, $S <^{**} R$.

For the fourth claim, let $x <^{\#} y$. Let $S \leq y$ be a pre well ordering such that for all pre well orderings $R \leq x$, $R <^{**} S$. Let $R \leq x$ be a pre well ordering. Then $R \leq^{**} S$. Hence $x \leq^{\#} y$.

For the fifth claim, let $x \leq^{\#} y$ and $y <^{\#} z$. Let $S \leq z$ be a pre well ordering such that for all pre well orderings $R \leq y$, $R <^{**} S$. Let $R \leq x$ be a pre well ordering. Let $S^* \leq y$ be a pre well ordering such that $R \leq^{**} S^*$. Then $S^* <^{**} S$. By Lemma 5.7.15, $R <^{**} S$. We have verified that $x <^{\#} z$.

For the sixth claim, let x <# y and y ≤# z. Let S ≤ y be a pre well ordering such that for all pre well orderings R ≤ x, R <** S. Let S* ≤ z be a pre well ordering such that S ≤** S*. By Lemma 5.7.15, for all pre well orderings R ≤ x, R <** S*. Hence x <# z.

The seventh claim is obvious.

For the eight claim, let x <# y. Let S ≤ y be a pre well ordering, where for all pre well orderings R ≤ x, we have R <** S. If y ≤ x then S ≤ x, and so S <** S. This is a contradiction. Hence x < y.

For the ninth claim, the converse is the first claim. Suppose x ≤# y ∧ y <# x. By the third claim, x <# x, which is impossible.

For the tenth claim, the converse is the first claim. Suppose x <# y ∧ y ≤# x. By the third claim, y <# y, which is impossible. QED

We now define x =# y if and only if x ≤# y ∧ y ≤# x.

LEMMA 5.7.18. =# is an equivalence relation on D. Let x,y ∈ D. x ≤# y ↔ (x <# y ∨ x =# y). x <# y ∨ y <# x ∨ x =# y, with exclusive ∨.

Proof: For the first claim, reflexivity and symmetry are obvious, by Lemma 5.7.17. Let x =# y and y =# z. Then x ≤# y and y ≤# z. Hence x ≤# z. Also z ≤# y and y ≤# x. Hence z ≤# x. Therefore x =# z.

For the second claim, let x,y ∈ D. By Lemma 5.7.17, x ≤# y ∨ y <# x. By the first claim, x <#y ∨ y <# x or x =# y.

To see that the ∨ is exclusive, suppose x <# y, y <# x. By Lemma 5.7.17, x <# x, which is a contradiction. Suppose x <# y, x =# y. By Lemma 5.7.17, x <# x, which is a contradiction. Suppose y <# x, x =# y. By Lemma 5.7.17, y <# y, which is a contradiction. QED

DEFINITION 5.7.22. We say that S is x-critical if and only if

i) S is a pre well ordering;
ii) for all pre well orderings R ≤ x, R <** S;
iii) for all y ∈ dom(S), S|<y is ≤** some pre well ordering R ≤ x.

LEMMA 5.7.19. Assume $(\forall y \in x)$(y is a pre well ordering). Then there exists a pre well ordering S such that $(\forall R \in x)(R \leq^{**} S) \wedge (\forall u \in \text{dom}(S))(\exists R \in x)(S|<u <^{**} R)$.

Proof: Let x be as given. Let $x < d_r$, $r \geq 1$. By Lemma 5.7.20 iv), define

$$E \approx \{y \leq d_{r+1}: (\exists R,z)(R \in x \wedge y \text{ is an } R|<z)\}.$$

By Lemma 5.7.5, we define

$$S(u,v) \leftrightarrow u,v \in E \wedge u \leq^{**} v.$$

Then S is uniquely defined up to ≡′. By Lemmas 5.7.15, 5.7.16, S is a pre well ordering.

Let $R \in x$ and $z \in \text{dom}(R)$. By Lemma 5.6.18 iv),

$$(\exists y)(y \text{ is an } R|<z).$$

By Lemma 5.6.18 iii), let $p \geq r+1$ be such that

$$(\exists y < d_p)(y \text{ is an } R|<z).$$

By Lemma 5.7.20 v),

$$(\exists y < d_{r+1})(y \text{ is an } R|<z).$$

Hence every R|<z, $R \in x$, is isomorphic to an element of E.

We claim that we can define an isomorphism T_R from any given $R \in x$, onto S or a proper initial segment of S, as follows. T_R relates each $z \in \text{dom}(R)$ to the elements of E that are isomorphic to R|<z. Note that each $z \in \text{dom}(R)$ gets related by T_R to something; i.e., all of the R|<z lying in E.

To verify the claim, we first show that $\text{rng}(T_R)$ is closed downward under $\leq^{**}$ in E. Fix $T_R(z,w)$. Let w^* be an S least element of E, $w^* <^{**} w$, which is not in $\text{rng}(T_R)$. Then T_R must act as an isomorphism from some proper initial segment J of R|<z onto S|<w*. We can assume $J \in E$ (by taking an isomorphic copy). Hence $T_R(J,w^*)$, contradicting that $w^* \notin \text{rng}(T_R)$.

Since $rng(T_R)$ is closed downward under ≤** in E, we see that $rng(T_R)$ ≡ E, or $rng(T_R)$ ≡ S|<v, for some v ∈ E. From the definition of T_R, T_R is an isomorphism from R onto S or a proper initial segment of S. Hence R ≤** S.

Now let u ∈ dom(S). Then u is some R|<z, R ∈ x. Therefore u <** R, for some R ∈ x. QED

LEMMA 5.7.20. Assume (∀y ∈ x)(y is a pre well ordering). Then there exists a pre well ordering S such that (∀R ∈ x)(R <** S) ∧ (∀R <** S)(∃y ∈ x)(R ≤** y).

Proof: Let x be as given.

case 1. x has a ≤** greatest element R. Set S ≡ R^+.

case 2. Otherwise. Set S to be as provided by Lemma 5.7.19 applied to x.

QED

LEMMA 5.7.21. For all x, there exists an x-critical S. If S is x-critical then x < S.

Proof: Let x be given. By Lemma 5.6.18 iv), define

x* ≈ {R: R ≤ x ∧ R is a pre well ordering}.

Let S be as provided by Lemma 5.7.20. Then S is x-critical.

Now let S be x-critical. If S ≤ x then S <* S, which is impossible by ii) in the definition of x-critical. QED

LEMMA 5.7.22. For all x, all x-critical S are isomorphic. For all x,y, x <# y if and only if (∃R,S)(R is x-critical ∧ S is y-critical ∧ R <** S).

Proof: Let R,S be x-critical. Suppose R <** S, and let R =** S|<y. By clause iii) in the definition of x-critical, let S|<y ≤** R* ≤ x, R* a pre well ordering. By clause ii) in the definition of R is x-critical, R* <** R. Hence R ≤** R* <** R. This is a contradiction. Hence ¬(R <** S). By symmetry, we also obtain ¬(S <** R). Hence R,S are isomorphic.

For the second claim, let x,y ∈ D. First assume x <# y. Let R be x-critical and S be y-critical. Let S* ≤ y be a pre well ordering such that for all pre well orderings R* ≤ x, we have R* <** S*.

We claim that R ≤** S*. To see this, suppose S* <** R, and let S* be isomorphic to R|<z. Since R is x-critical, let R|<z ≤** R* ≤ x, where R* is a pre well ordering. Then S* ≤** R*. Since R* ≤ x, we have R* <** S*, which is a contradiction. Thus R ≤** S*.

Note that S* <** S since S* ≤ y and S is y-critical. Hence R <** S.

For the converse, assume R is x-critical, S is y-critical, and R <** S. Let R be isomorphic to S|<z. Since S is y-critical, let S|<z ≤** R* ≤ y, where R* is a pre well ordering. Then R ≤** R* ≤ y.

We claim that for all pre well orderings S* ≤ x, S* <** R*. To see this, let S* ≤ x be a pre well ordering. Since R is x-critical, S* <** R ≤** R* ≤ y.

We have shown that x <# y using R* ≤ y, as required. QED

LEMMA 5.7.23. Let n ≥ 1. For all x ≤ d_n there exists x-critical S < d_{n+1}. d_n <# d_{n+1}.

Proof: Let n ≥ 1 and x ≤ d_n. By Lemmas 5.7.21 and 5.6.18 ii), there exists m > n such that the following holds.

$$(\exists S < d_m)(S \text{ is x-critical}).$$

By Lemma 5.6.18 v),

$$(\exists S < d_{n+1})(S \text{ is x-critical}).$$

For the second claim, by the first claim let R < d_{n+1}, where R is d_n-critical. Let S be d_{n+1}-critical. Then R <** S. By Lemma 5.7.22, d_n <# d_{n+1}. QED

LEMMA 5.7.24. If y ∈ x then x has a <# least element. Every first order property with parameters that holds of some x, holds of a <# least x. 0 is a <# least element.

Proof: Let y ∈ x. By Lemma 5.6.18 ii), let n ≥ 1 be such that x ≤ d_n. By Lemma 5.7.23, for each y ∈ x there exists a y-critical S < d_{n+1}. By Lemma 5.6.18 iv), we can define

$$B \approx \{S < d_{n+1} : (\exists y \in x)(S \text{ is y-critical})\}$$

uniquely up to ≡.

By Lemma 5.7.16, let S be a <** least element of B. Let S be y-critical, y ∈ x. We claim that y is a <# minimal element of x. Suppose z <# y, z ∈ x. By Lemma 5.7.23, let R be z-critical, R ∈ B. By the choice of S, S ≤** R. By Lemma 5.7.22, let R*,S* be such that R* is z-critical, S* is y-critical, and R* <** S*. By the first claim of Lemma 5.7.22, R <** S. This is a contradiction.

For the second claim, let φ(y). By Lemma 5.6.18 ii), let y < d_n. By Lemma 5.6.18 iv), let x ≈ {y < d_{n+1}: φ(y)}. By the first claim, let y be a <# minimal element of x. Suppose φ(z), z <# y. Since z ∉ x, we have z ≥ d_{n+1}. Since z <# y, we have z < y (Lemma 5.7.17). This contradicts y < d_{n+1} ∧ z ≥ d_{n+1}.

The third claim follows immediately from the last claim of Lemma 5.7.17. QED

LEMMA 5.7.25. If x ≤ y then x ≤# y. If x ≤ y ≤ z and x =# z, then x =# y =# z.

Proof: The first claim is trivial.

For the second claim, let x ≤ y ≤ z, x =# z. Using the first claim and Lemmas 5.7.17, 5.7.18, x ≤# y ≤# z ≤# x. Hence x =# y =# z. QED

From Lemma 5.7.25, we obtain a picture of what <# looks like.

LEMMA 5.7.26. =# is an equivalence relation on D whose equivalence classes are nonempty intervals in D (not necessarily with endpoints). These are called the intervals of =#. x <# y if and only if the interval of =# in which x lies is entirely below the interval of =# in which y lies. There is no highest interval for =#. The d’s lie in different intervals of =#, each entirely higher than the previous.

Proof: For the first claim, =# is an equivalence relation by Lemma 5.7.18. Suppose x < y, x =# y. By Lemma 5.7.25, any x < z < y has x =# z =# y. So the equivalence classes under =# are intervals in <.

For the second claim, let x <# y. Let z lie in the same interval of =# as x. Let w lie in the same interval of =# as y. Then x =* z, y =* w. By Lemma 5.7.18, z <# w. By Lemma 5.7.17, z < w.

Conversely, assume the interval of =# in which x lies is entirely below the interval of =# in which y lies. Then ¬(x =# y). By Lemma 5.7.18, x <# y ∨ y <# x. The later implies y < x, which is impossible. Hence x <# y.

For the final claim, by Lemma 5.7.23, each d_n <# d_{n+1}. By the second claim, the intervals of =# in which d_n lies is entirely below the interval of =# in which d_{n+1} lies. QED

Recall the component NAT in the structure M#.

LEMMA 5.7.27. There is a binary relation RNAT (recursively defined natural numbers) such that
i) dom(RNAT) ≈ {x: NAT(x)};
ii) (∀y)(RNAT(0,y) ↔ y is a <# least element);
iii) (∀x)(NAT(x) → (∀w)(RNAT(x+1,w) ↔ (∃z)(RNAT(x,z) ∧ w is an immediate successor of z in <#)));
iv) RNAT < d_2.
Any two RNAT's (even without iv)) are ≡'. If NAT(x) then {y: RNAT(x,y)} forms an equivalence class under =#.

Proof: We will use the following facts. The set of all <# minimal elements exists and is nonempty. For all y, the set of all immediate successors of y in <# exists and is nonempty. These follow from Lemmas 5.7.24, 5.7.26, and 5.6.18 iv).

DEFINITION 5.7.23. We say that a binary relation R is x-special if and only if

i) NAT(x);
ii) dom(R) ≈ {y: y ≤ x};
iii) (∀y)(R(0,y) ↔ y is a <# minimal element);
iv) (∀y ≤ x)(∀w)(R(y+1,w) ↔ (∃z)(R(y,z) ∧ w is an immediate successor of z in <#)).

We claim that for all x with NAT(x), there exists an x-special R. This is proved by induction, which is supported by Lemma 5.6.18 iv), vi), vii), and Lemma 5.7.5. The basis case x = 0 is immediate.

For the induction case, let R be x-special. By Lemma 5.7.5, define

$$S(y,w) \leftrightarrow R(y,w) \vee (y = x+1 \wedge (\exists z)(R(x,z) \wedge w \text{ is an immediate successor of } z \text{ in } <\#)).$$

uniquely up to ≡'. We claim that S is x+1-special. It is clear that dom(S) ≈ {y: y ≤ x+1} since dom(R) ≈ {y: y ≤ x} and we can find immediate successors in <#. Also the conditions

$$(\forall y)(S(0,y) \leftrightarrow y \text{ is a } <\# \text{ minimal element}).$$
$$(\forall y \leq x)(\forall w)(S(y+1,w) \leftrightarrow (\exists z)(R(y,z) \wedge w \text{ is an immediate successor of } z \text{ in } <\#)).$$

are inherited from R. To see that

$$(\forall w)(S(x+1,w) \leftrightarrow (\exists z)(S(x,z) \wedge w \text{ is an immediate successor of } z \text{ in } <\#))$$

we need to know that {z: R(x,z)} forms an equivalence class under =#. This is proved by induction on x from 0 through x.

We have thus shown that there exists an x-special R for all x with NAT(x). Another induction on NAT shows that

$$\text{1) } NAT(x) \wedge NAT(y) \wedge x \leq y \wedge R \text{ is x-special } \wedge S \text{ is y-special } \wedge z \leq x \rightarrow R(z,w) \leftrightarrow S(z,w).$$

We also claim that

$$NAT(x) \rightarrow \text{there exists an x-special } R < d_2.$$

To see this, let NAT(x). By Lemma 5.6.18 iii), let n > 1 be so large that

$$(\exists y < d_n)(y \text{ is x-special}).$$

By Lemma 5.6.18 vi), x < d_1. Hence by Lemma 5.6.18 v),

$$(\exists y < d_2)(y \text{ is x-special}).$$

Because of this d_2 bound, we an apply Lemma 5.7.5 to form a union RNAT of the x-special relations with NAT(x), uniquely up to ≡'. Claims i)-iii) are easily verified using 1). Thus we have

(∃R)(R is an RNAT ∧ R obeys clauses i)-iii)).

Hence by Lemma 5.6.18 v),

(∃R < d_2)(R is an RNAT ∧ R obeys clauses i)-iii)).
(∃R)(R obeys clauses i)-iv)).

The remaining claims can be proved from properties i)-iii) by induction. QED

DEFINITION 5.7.24. We fix the RNAT of Lemma 5.7.27, which is unique up to ≡′.

The limit point provided by the next Lemma will be used to interpret ω.

LEMMA 5.7.28. There is a <# least limit point of <#. I.e., there exists x such that
i) (∃y)(y <# x);
ii) (∀y <# x)(∃z <# x)(y <# z);
iii) for all x* with properties i),ii), x ≤# x*.
All <# least limit points of <# are =#, and < d_2.

Proof: We say that z is an ω if and only if z is a <# least limit point of <#; i.e., z obeys i)-iii).

By an obvious induction, if NAT(x) then {z: (∃y ≤ x)(RNAT(y,z))} forms an initial segment of <#. Therefore rng(RNAT) forms an initial segment of <#. Since RNAT < d_2, rng(RNAT) ⊆ [0,d_2)). According to Lemma 5.7.24, let z be <# least such that (∀x ∈ rng(RNAT))(x <# z).

It is clear that z obeys claims i),ii). Suppose x* has properties i),ii). By an obvious induction, we see that (∀y ∈ rng(RNAT))(y <# x*). Hence z ≤# x*. Thus we have verified claim iii) for z. I.e., z is an ω.

Suppose z,z* are ω's. By iii), z ≤# z*, z* ≤# z. Hence z =# z*.

By Lemma 5.6.18 iii), let n > 1 be such that

"there exists an ω < d_n".

Hence By Lemma 5.6.18 v),

"there exists an ω < d_2".

Finally, we establish that every ω is < d_2. Suppose

"there exists an $\omega > d_2$".

By Lemma 5.6.18 v),

"there exists an $\omega > d_3$".

Hence the ω's form an interval, with an element < d_2 and an element > d_3. Hence $d_2 =\# d_3$. This contradicts Lemma 5.7.26. QED

We are now prepared to define the system M^.

DEFINITION 5.7.25. $M\hat{} = (C,<,0,1,+,-,\bullet,\uparrow,\log,\omega,c_1,c_2,...,Y_1,Y_2,...)$, where the following components are defined below.

i) (C,<) is a linear ordering;
ii) $c_1,c_2,...$ are elements of C;
iii) for $k \geq 1$, Y_k is a set of k-ary relations on C;
iv) $0,1,\omega$ are elements of C;
v) $+,-,\bullet$ are binary functions from C into C;
vi) $\uparrow$,log are unary functions from C into C.

DEFINITION 5.7.26. For $x \in D$, we write [x] for the equivalence class of x under =#. Recall from Lemma 5.7.26 that each [x] is a nonempty interval in (D,<).

DEFINITION 5.7.27. We define $C = \{[x]; x \in D\}$. We define $[x] < [y] \leftrightarrow x <\# y$. For all $n \geq 1$, we define $c_n = [d_{n+1}]$.

DEFINITION 5.7.28. Let $k \geq 1$. We define Y_k to be the set of all k-ary relations R on C, where there exists a k-ary relation S on D, internal to M#, (i.e., given by a point in D), such that for all $x_1,...,x_k \in C$,

$$R(x_1,...,x_k) \leftrightarrow (\exists y_1,...,y_k \in D)(y_1 \in x_1 \wedge ... \wedge y_k \in x_k \wedge S(y_1,...,y_k)).$$

Since k-ary relations S on D are required to be bounded in D, by Lemma 5.7.26 every $R \in Y_k$ is bounded in C.

DEFINITION 5.7.29. By Lemma 5.7.28, we define the ω of M^ to be [z], where z is an ω of M#, as defined in the first line of the proof of Lemma 5.7.28.

DEFINITION 5.7.30. Define the following function f externally. For each x ∈ D such that NAT(x), let f(x) = {y: RNAT(x,y)}. Note that by Lemma 5.7.27, f(x) ∈ C. Note that the relation y ∈ f(x) is internal to M#. Also by Lemma 5.7.28 and an internal induction argument, f is one-one.

DEFINITION 5.7.31. We define 0 to be f(0) = [0], and 1 to be f(1).

DEFINITION 5.7.32. For x,y such that NAT(x),NAT(y), we define

$$f(x)+f(y) = f(x+y).$$
$$f(x)-f(y) = f(x-y).$$
$$f(x)\bullet f(y) = f(x\bullet y).$$
$$f(x)\uparrow = f(x\uparrow).$$
$$\log(f(x)) = f(\log(x)).$$

Here the operations on the left side are in M^, and the operations on the right side are in M#. Note that the above definitions of +,-,•,log on rng(f) are internal to M#.

DEFINITION 5.7.33. Let u,v ∈ C, where ¬(u,v ∈ rng(f)). We define

$$u+v = u-v = u\bullet v = u\uparrow = \log(u) = [0].$$

We now define the language L^ suitable for M^, without the c's.

DEFINITION 5.7.34. L^ is based on the following primitives.

i) The binary relation symbol <;
ii) The constant symbols 0,1,ω;
iii) The unary function symbols ↑,log;
iv) The binary function symbols +,-,•;
v) The first order variables v_n, n ≥ 1;
vi) The second order variables B^n_m, n,m ≥ 1;

In addition, we use ∀,∃,¬,∧,∨,→,↔,=. Commas and parentheses are also used. "B" indicates "bounded set".

DEFINITION 5.7.35. The first order terms of L^ are inductively defined as follows.

i) The first order variables v_n, n ≥ 1 are first order terms of L^;
ii) The constant symbols 0,1,ω are first order terms of L^;

iii) If s,t are first order terms of L^ then s+t, s-t, s•t, t↑, log(t) are first order terms of L^.

DEFINITION 5.7.36. The atomic formulas of L^ are of the form

$$s = t$$
$$s < t$$
$$B^n_m(t_1,...,t_n)$$

where $s,t,t_1,...,t_n$ are first order terms and $n \geq 1$. The formulas of L^ are built up from the atomic formulas of L^ in the usual way using the connectives and quantifiers.

Note that there is no epsilon relation in L^.

The first order quantifiers range over C. The second order quantifiers B^n_k range over Y_n.

LEMMA 5.7.29. Let $k \geq 1$ and $R \subseteq C^k$ be M^ definable (with first and second order parameters allowed). Then $\{(x_1,...,x_k): R([x_1],...,[x_k])\}$ is M# definable (with parameters allowed). If R is M^ definable without parameters, then $\{(x_1,...,x_k): R([x_1],...,[x_k])\}$ is M# definable without parameters.

Proof: The construction of M^ takes place in M#, where equality in M^ is given by the equivalence relation =# in M#. Note that =# is defined in M# without parameters. The <,0,1,ω of M^ are also defined without parameters.

Let $k \geq 1$. The relations in Y_k are each coded by arbitrary internal k ary relations R in M#, where the application relation "the relation coded by R holds at points $x_1,...,x_k$" is defined in M# without parameters.

Using these considerations, it is straightforward to convert M^ definitions to M# definitions. QED

LEMMA 5.7.30. There exists a structure $M^\wedge = (C,<,0,1,+,-,\bullet,\uparrow,\log,\omega,c_1,c_2,...,Y_1,Y_2,...)$ such that the following holds.
i) (C,<) is a linear ordering;
ii) ω is the least limit point of (C,<);
iii) $(\{x: x < \omega\},<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies $TR(\Pi^0_1,L)$;
iv) For all $x,y \in C$, $\neg(x < \omega \wedge y < \omega) \rightarrow x+y = x\bullet y = x-y = x\uparrow = \log(x) = 0$;

v) The c_n, $n \geq 1$, form a strictly increasing sequence of elements of C, all > ω, with no upper bound in C;
vi) For all $k \geq 1$, Y_k is a set of k-ary relations on C whose field is bounded above;
vii) Let $k \geq 1$, and φ be a formula of L^ in which the k-ary second order variable B^k_n is not free, and the variables B^m_r range over Y_r. Then $(\exists B^k_n \in Y_k)(\forall x_1,\ldots,x_k)(B^k_n(x_1,\ldots,x_k) \leftrightarrow (x_1,\ldots,x_k \leq y \wedge \varphi))$;
viii) Every nonempty M^ definable subset of C has a < least element;
ix) Let $r \geq 1$ and $\varphi(v_1,\ldots,v_{2r})$ be a formula of L^. Let $1 \leq i_1,\ldots,i_{2r}$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and the same min. Let $y_1,\ldots,y_r \in C$, $y_1,\ldots,y_r \leq \min(c_{i\_1},\ldots,c_{i\_r})$. Then $\varphi(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \leftrightarrow \varphi(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r)$.

Proof: We show that the M^ we have constructed obeys these properties. Claim i) is by construction, since <# is irreflexive, transitive, and has trichotomy. Claim ii) is by the definition of ω (see Definition 5.7.29).

For claim iii), note that the f used in the construction of M^ defines an isomorphism from the ({x: NAT(x)},0,1,+,-,•,↑,log) of M# onto the ({x: x < ω},<,0,1,+,-,•,↑,log) of M^. Now apply Lemma 5.6.18 viii).

Claim iv) is by construction.

For claim v), for all $n \geq 1$, $c_n = [d_{n+1}]$. By Lemma 5.7.26, the c_n's are strictly increasing. Let $[x] \in C$. By Lemma 5.6.18 iii), let $x < d_{m+1}$, in M#. By Lemma 5.7.17, $\neg(d_{m+1}$ <# x). Therefore x ≤# d_{m+1}. Hence $[x] \leq [d_{m+1}] = c_m$. Hence the c_n's have no upper bound in C. By Lemma 5.7.27, any ω of M# is <# d2 in M#. Hence $\omega < c_1$ in M^.

Claim vi) is by construction. This uses that there is no <# greatest point in M# (Lemma 5.7.26).

For claim vii), it suffices to show that every M^ definable relation R on C whose field is bounded above (≤ on C) lies in Y_k. By Lemma 5.7.29, the k-ary relation S on D given by

$$S(y_1,\ldots,y_k) \leftrightarrow R([y_1],\ldots,[y_k])$$

is M# definable. Since the field of R is bounded above (≤ on C), the field of S is bounded above (< on D). This uses that < on C has no greatest element (Lemma 5.7.26). Hence we can take S to be internal to M#; i.e., given by a point in D. Therefore $R \in Y_k$.

For claim viii), let R be a nonempty M^ definable subset of C. By Lemma 5.7.29, S ≈ {y: [y] ∈ R} is nonempty and M# definable. By Lemma 5.7.24, let y be a <# least element of S.

We claim that in M^, [y] is the < least element of R. To see this, let [z] ∈ R, [z] < [y]. Then z <# y and z ∈ S, which contradicts the choice of y.

For claim ix), let $\varphi(x_1,\ldots,x_{2r}),i_1,\ldots,i_{2r},y_1,\ldots,y_r$ be as given. Let $i = \min(i_1,\ldots,i_r)$. Since $y_1,\ldots,y_r \leq c_i = [d_{i+1}]$, every element of the equivalence classes $y_1,\ldots,y_r$ is ≤# d_{i+1}. Hence we can write $y_1 = [z_1],\ldots,y_r = [z_r]$, where $z_1,\ldots,z_r \leq d_{i+1}$.

By Lemma 5.7.29, the 2r-ary relation S on D given by

$$S(w_1,\ldots,w_{2r}) \leftrightarrow$$
$$\varphi([w_1],\ldots,[w_{2r}]) \text{ holds in M\^{}}$$

is definable in M# without parameters.

Note that $\min(i_1+1,\ldots,i_{2r}+1) = i+1$. Hence by Lemma 5.6.18 v), we have

$$S(d_{i\_1+1},\ldots,d_{i\_r+1},z_1,\ldots,z_r) \leftrightarrow$$
$$S(d_{i\_r+1+1},\ldots,d_{i\_2r+1},z_1,\ldots,z_r).$$

Hence in M^,

$$\varphi(c_{i\_1},\ldots,c_{i\_r},[z_1],\ldots,[z_r]) \leftrightarrow$$
$$\varphi(c_{i\_r+1},\ldots,c_{i\_2r},[z_1],\ldots,[z_r]).$$

$$\varphi(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \leftrightarrow$$
$$\varphi(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r).$$

QED

5.8. ZFC + V = L, indiscernibles, and Π^0_1 correct arithmetic.

We fix $M\hat{} = (C,<,0,1,+,-,\bullet,\uparrow,\log,\omega,c_1,c_2,\ldots,Y_1,Y_2,\ldots)$ as given by Lemma 5.7.30. We work entirely within M^. E.g., we treat C as the universe of points, and regard the elements of the Y_k as the internal relations.

In particular, if we say that R is an internal relation, then we mean that R is an element of some Y_k. If we say that R is an M^ definable relation (first and second order parameters allowed), then we do not necessarily mean that R is an internal relation. However, by Lemma 5.7.30, vii), if R is an M^ definable relation which is **bounded**, then R is an internal relation; i.e., R is an element of some Y_k. In fact, Y_k is the set of all bounded M^ definable relations on C.

DEFINITION 5.8.1. Functions are always identified with their graphs. We refer to the elements of Y_1 as the internal sets.

An important obstacle is that there is no way of showing, in M^, that the family of all internal subsets of an internal set is in any sense internal. E.g., no way of showing that they are all cross sections of some fixed internal binary relation.

It would appear that this obstacle is fatal, as it indicates an inability to interpret the power set axiom, despite bounded comprehension, indiscernibility, and infinity.

However, in this section, we argue carefully that we can still construct the constructible universe. Because of the explicitness of this construction, we can use indiscernibility to overcome this obstacle within the constructible universe.

We first have to develop a pairing function. By an interval, we mean a set $[x,y)$, where $x,y \in C$.

LEMMA 5.8.1. Let $k \geq 1$ and F be a k-ary M^ definable function, defined without second order parameters. For all x, $\{F(y_1,\ldots,y_k): y_1,\ldots,y_k < x\}$ is bounded above. For all x, the restriction of F to $[0,x)^k$ is an internal function.

Proof: Let k,F be as given, and let $x \in C$. Let $n \geq 1$ be such that x and all parameters used in the definition of F are $< c_n$. Let $y_1,\ldots,y_k < x$. Let $m > n$ be such that $F(y_1,\ldots,y_k) < c_m$. Consider the true statement

$$F(y_1,\ldots,y_k) < c_m.$$

This is a statement involving c_m and certain parameters < c_n. By Lemma 5.7.30 ix),

$$F(y_1,...,y_k) < c_{n+1}.$$

The second claim follows immediately by Lemma 5.7.30 vii). QED

DEFINITION 5.8.2. For all x ∈ C, we write x+1 for the immediate successor of x in <.

The above exists by Lemma 5.7.30 v),viii). This is a slight abuse of notation since x+1 already has a meaning, as + is a primitive of M^. However, note that by Lemma 5.7.30 ii),iii), if x < ω then x+1 is also the immediate successor of x in <.

LEMMA 5.8.2. Let x,y ∈ C, x > 0. There is a unique strictly increasing internal f with dom(f) = [0,x), rng(f) an interval, and f(0) = y.

Proof: We first prove a strong form of uniqueness. Suppose x,x',y ∈ C, x,x' > 0, and let f,g be strictly increasing internal functions, where dom(f) = [0,x), dom(g) = [0,x'), and rng(f),rng(g) are intervals, and f(0) = g(0) = y. Then f,g agree on their common domain. To see this, suppose this is false. By Lemma 5.7.30 viii), let b be < least such that f(b) ≠ g(b). Obviously f(b) is the strict sup of the f(c), c < b, and g(b) is the strict sup of the g(c), c < b. Hence f(b) = g(b), which is a contradiction. Hence f,g agree on their common domain.

For existence, fix x,y ∈ C. We prove that for all 0 < u ≤ x, there exists strictly increasing internal f such that dom(f) = [0,u), rng(f) is an interval, and f(0) = y.

Suppose this is false. By Lemma 5.7.30 viii), let 0 < u ≤ x be < least such that this is false. For each 0 < v < u, let f_v be the unique internal function which is strictly increasing with dom(f_v) = [0,v), rng(f_v) an interval, and f(0) = y.

First suppose u is a limit. By the comparability, the union, f, of the f_v, v < u, is a function M^ definable without second order parameters (but with second order quantifiers). Hence f is strictly increasing, with dom(f) =

[0,u), f(0) = y. By Lemma 5.7.30 viii), rng(f) must be an interval. We have now contradicted the choice of u.

Now suppose u = v+1. If v = 0 then f_u obviously exists. Hence v > 0. Let f_v have range [y,z). Extend f_v to f by setting f(v) = z. Again we have contradicted the choice of u. QED

DEFINITION 5.8.3. We now define (x,y) <* (z,w) if and only if

i) max(x,y) < max(z,w); or
ii) max(x,y) = max(z,w) and (x,y) lexicographically precedes (z,w).

LEMMA 5.8.3. Every M^ definable binary relation R that holds of some (x,y), x,y ∈ C, holds of a <* least (x,y).

Proof: Let R be as given. The set of all max's of pairs at which R holds is obviously a nonempty M^ definable subset of C. By Lemma 5.7.30 viii), let u be its < least element. By Lemma 5.7.30 viii), let x be the < least first term of a pair at which R holds, whose maximum is u. By Lemma 5.7.30 viii), let y be the < least second term of a pair at which R holds, whose maximum is u, and whose first term is x. Then (x,y) is as required. QED

LEMMA 5.8.4. There is an M^ definable binary function $F:C^2 \to C$, defined without parameters, such that for all x,y ∈ C, F(x,y) is the strict sup of all F(z,w) with (z,w) <* (x,y). F is unique.

Proof: Define Q(u,G) if and only if

1) $G:\{x: x < u\}^2 \to C$ is internal, such that for all x,y < u, G(x,y) is the strict sup of all G(z,w), (z,w) <* (x,y).

We claim that for all v,w < u, if Q(v,G) and Q(w,H), then G,H agree on their common domain. This is proved in the obvious way using Lemma 5.8.3.

Define R(u) ↔ (∃G)(Q(u,G)). Suppose (∃u)(¬R(u)).

By Lemma 5.7.30 viii), let u be < least such that ¬R(u). Then for all v < u, there exists G with Q(v,G).

We thus see that for all v < u, there is a unique G_v with $Q(v,G_v)$, and these various G_v, v < u, are comparable.

Obviously R(0), and so u > 0.

Suppose u is a limit. By comparability, the union of the G_v, v < u, is an internal function G according to Lemma 5.8.1. It is obvious that Q(u,G). This contradicts the choice of u.

Now suppose u = v+1. We will extend G_v to G as follows. Since G_v is internal, by Lemma 5.7.30 viii), let u_1 be the strict sup of the values of G_v. By Lemma 5.8.2, let H be a strictly increasing internal function that maps [0,v) onto $[u_1,u_2)$, and J be a strictly increasing internal function that maps [0,v] onto $[u_2,u_3]$. Now extend G_v to G by defining G(w,v) = H(w) and G(v,w) = J(w), where w ≤ v. Clearly Q(u,G). This contradicts the choice of u.

We have thus established that for all u, R(u) holds.

We now define F as follows. Let x,y ∈ C. Let G be the unique internal function given by R(u), with u = max(x,y)+1. Set F(x,y) = G(x,y). It is clear that F is as required. F is unique by Lemma 5.8.3. QED

DEFINITION 5.8.4. We write P for the F constructed in the proof of Lemma 5.8.4.

LEMMA 5.8.5. For all x ∈ C, x ≤ P(0,x). Let x,y ∈ C. x > 0 → x,y < P(x,y). x,y ≤ P(x,y). $P:C^2 \to C$ is a bijection.

Proof: Suppose the first claim is false. By Lemma 5.7.30 viii), let x be < least such that P(0,x) < x. Then for all z < x, z ≤ P(0,z). Hence x ≤ P(0,x), which is a contradiction.

For the second claim, let x > 0. We have y ≤ P(0,y) < P(x,y), and x ≤ P(0,x) < P(x,0) ≤ P(x,y).

The third claim follows from the first two claims.

To see that P is one-one, let P(x,y) = P(x',y'). If (x,y) <* (x',y') then P(x,y) < P(x',y'). If (x',y') <* (x,y) then P(x',y') < P(x,y). Hence (x,y) = (x',y').

To see that P is onto, let x be the least element of C that is not a value of P. By the first claim, if P(y,z) < x then (y,z) <* (0,x). It is easy to see that the strict sup of the (y,z) with P(y,z) < x exists. Then the value of P at this strict sup must be x. Hence x is a value of P. This is a contradiction. QED

DEFINITION 5.8.5. We inductively define $P(x_1,...,x_{k+1}) = P(P(x_1,x_2),x_3,...,x_{k+1})$, for $k \geq 1$. Also define $P(x) = x$. This is our mechanism for coding sequences of points of standard finite length as points.

LEMMA 5.8.6. In each arity $k \geq 1$, P is a bijection. For all $k \geq 1$, $(\forall x_1,...,x_k)(x_1,...,x_k \leq P(x_1,...,x_k))$. For all $k,n \geq 1$, $(\forall x_1,...,x_k)(x_1,...,x_k \leq c_n \rightarrow P(x_1,...,x_k) < c_{n+1})$.

Proof: The first claim is proved by external induction on the arity, using that $P:C \rightarrow C$ and $P:C^2 \rightarrow C$ are bijections.

The second claim is proved by external induction on $k \geq 1$, using Lemma 5.8.5.

For the third claim, let $k,n \geq 1$ and $x_1,...,x_k \leq c_n$. By Lemma 5.7.30 v), let $m > n$ be such that $P(x_1,...,x_k) < c_m$. By Lemma 5.7.30 ix), $P(x_1,...,x_k) < c_{n+1}$. QED

LEMMA 5.8.7. Let $k \geq 1$ and $R \subseteq C^k$. Then R is an internal relation if and only if $\{P(x_1,...,x_k): R(x_1,...,x_k)\}$ is an internal set.

Proof: Let k,R be as given. In the interest of caution, rewrite this set as

$$A = \{y: (\exists x_1,...,x_k)(y = P(x_1,...,x_k) \wedge R(x_1,...,x_k))\}.$$

Suppose R is an internal relation; i.e., $R \in Y_k$. Then R is bounded. Hence by Lemma 5.8.1, A is bounded. By Lemma 5.7.30 vii), A is an internal set; i.e., $A \in Y_1$.

Now suppose A is an internal set. Then A is bounded. Hence by Lemma 5.8.6, R is bounded.

We claim that for all $x_1,...,x_k \in C$,

$$R(x_1,...,x_k) \leftrightarrow P(x_1,...,x_k) \in A.$$

To see this, suppose $R(x_1,...,x_k)$. Then $P(x_1,...,x_k) \in A$. Suppose $P(x_1,...,x_k) \in A$. Let $x_1',...,x_k'$ be such that $P(x_1,...,x_k) = P(x_1',...,x_k') \wedge R(x_1',...,x_k')$. Since P is one-one, we have $x_1 = x_1',...,x_k = x_k'$, and $R(x_1,...,x_k)$. Hence R is an internal relation, by Lemma 5.7.30 vii). QED

LEMMA 5.8.8. Any definable subset of C that contains 0 and is closed under +1, contains all $x < \omega$.

Proof: Let $B \subseteq C$ be definable, contain 0, and be closed under +1. Let $x < \omega$, $x \notin B$. By Lemma 5.7.30 viii), let x be least such that $x < \omega$, $x \notin B$. Then $x > 0$. By Lemma 5.7.30 iii), we have $x-1 < x$, and hence $x-1 \in B$. Therefore $x \in B$, which is a contradiction. QED

Lemma 5.8.8 supports proof by internal induction on $x < \omega$.

DEFINITION 5.8.6. An internal finite sequence is an internal function whose domain is some [1,x], $x < \omega$.

We can use P to code internal finite sequences (from C) of indefinite length, as a single element of C.

LEMMA 5.8.9. Let $f:[1,x] \rightarrow C$, $x < \omega$, be internal. There exists a unique internal $g:[1,x] \rightarrow C$ such that for all $1 \leq u < x$,
i) $g(1) = f(1)$;
ii) $g(u+1) = P(g(u),f(u+1))$.
For this g, we have $g(x) \geq \max(f)$.

Proof: Let f,x be as given. We prove by internal induction on $z \leq x$, that there is an internal $g:[1,z] \rightarrow C$ such that for all $1 \leq u < z$, clauses i) and ii) hold. Internal induction below ω is supported by Lemma 5.8.8. The uniqueness of g can also be obtained using internal induction.

Clearly max(f) exists by induction. Also by induction, for all $1 \leq u \leq v \leq x$, $g(v) \geq f(u)$. Hence $g(x) \geq \max(f)$. QED

We use Lemma 5.8.9 to code finite sequences. Let $f:[1,x] \rightarrow C$, $x < \omega$.

DEFINITION 5.8.7. Define $\#(f) = P(x,g(x))+1$, where g is given by Lemma 5.8.9. For empty f, define $\#(f) = 0$.

LEMMA 5.8.10. For all internal finite sequences f,f', if $\#(f) = \#(f')$ then $f = f'$.

Proof: Let f,f' be internal finite sequences. Let $f:[1,x) \rightarrow C$, $f':[1,y) \rightarrow C$. Suppose $\#(f) = \#(f')$. If $x = 0 \vee y = 0$ then $\#(f) = \#(f') = 0$, and hence $x = y = 0$. So we assume that $x,y > 0$.

Let g,g' be given by Lemma 5.8.9, for f,f', respectively. Then #(f) = #(f') = P(x,g(x))+1 = P(y,g'(y))+1. Hence P(x,g(x)) = P(y,g'(y)), x = y, g(x) = g'(y). Hence g(x) = g'(x).

We now prove that f = f'. The case x = 1 is immediate, so we assume x > 1.

We first prove by reverse induction that for all 1 < x' ≤ x, f(x') = f'(x') ∧ g(x') = g'(x'). The basis case is x' = x. By Lemma 5.8.9, we have g(x) = P(g(x-1),f(x)), g'(x) = P(g'(x-1),f'(x)). Hence f(x) = f'(x) ∧ g(x) = g'(x).

Suppose 2 < x' ≤ x, f(x') = f'(x'), g(x') = g'(x'). By Lemma 5.8.9, g(x') = P(g(x'-1),f(x')), g'(x') = P(g'(x'-1),f'(x')). Then g(x'-1) = g'(x'-1). By Lemma 5.8.9, g(x'-1) = P(g(x'-2),f(x'-1)), g'(x'-1) = P(g'(x'-2),f'(x'-1)). Hence f(x'-1) = f'(x'-1). This establishes the induction step.

So we have shown that for all 1 < x' ≤ x, f(x') = f'(x') ∧ g(x') = g'(x'). Hence f(2) = f'(2), g(2) = g'(2). By Lemma 5.8.9, g(1) = g'(1) = f(1) = f'(1). Hence f = f'. QED

LEMMA 5.8.11. (∀x)(∃y > x,ω)(∀z,w ≤ x)(P(z,w) < y).

Proof: Let x ∈ C. By Lemma 5.7.30 v), ω < c_1, and we can let x ≤ c_n. By Lemma 5.8.6, for all k ≥ 1 and $z_1,...,z_k \leq c_n$, $P(z_1,...,z_k) < c_{n+1}$ and ω < c_{n+1}. QED

LEMMA 5.8.12. (∀x)(∃y > x,ω)(∀z,w < y)(P(z,w) < y).

Proof: Let x be given. Let u = max(x,ω). Informally, we want to construct u < P(u,u) < P(P(u),P(u)) < ... and take the sup. We can obviously prove by internal induction (Lemma 5.8.8) that for all n < ω, there exists unique internal f_n:[1,n] → C such that $f_n(1)$ = u, and for all 1 ≤ m < n, $f_n(m+1) = P(f_n(m),f_n(m))$. By internal induction, these f_n are comparable, and so we can form their union F as an M^ definable function F with domain {n: 0 < n < ω}.

By Lemma 5.8.1, F is an internal function. Also by internal induction, for all 0 < n < ω,

$$F(0) = u, F(n+1) = P(F(n),F(n)).$$

By Lemma 5.7.30 viii), let the strict sup of the values of F be y. We claim that

$$(\forall z,w < y)(P(z,w) < y).$$

Let z,w < y. Let z,w ≤ F(n). Then

$$P(z,w) \leq P(F(n),F(n)) = F(n+1) < y.$$

QED

According to Lemma 5.8.12, for x ∈ C, we let P*(x) be the least y > x,ω such that for all z,w < y, P(z,w) < y.

LEMMA 5.8.13. Let f be an internal finite sequence, rng(f) ⊆ [0,x]. Then max(f) < #(f) < P*(x).

Proof: Let f be as given. If f is empty then #(f) = 0 and we are done. We can assume that f:[1,n] → [0,x], where 1 ≤ n < ω. Then ω < P*(x). Let g be given by Lemma 5.8.9. By internal induction, for all 1 ≤ i ≤ n, g(i) < P*(x). Hence P(n,g(n)) < P(ω,g(n)) < P*(x). Therefore #(f) = P(n,g(n))+1 ≤ P(ω,g(n)) < P*(x). By Lemma 5.8.9, max(f) ≤ g(n) < #(f) < P*(x). QED

We will need a notation for reverse finite sequence coding.

DEFINITION 5.8.8. Let y ∈ C and 1 ≤ i,n < ω. We define y[i:n] to be the i-th term in the finite sequence of length n coded by y, if this exists; undefined otherwise. I.e., y[i:n] is f(i),

where i ≤ n and f is such that
f:[1,n] → C, #(f) = y,
provided f exists;
undefined otherwise.

By Lemma 5.8.10, the choice of f here, if it exists, is unique.

LEMMA 5.8.14. x[i:n] forms an M^ definable partial function from C × $[0,\omega)^2$ into C without parameters. Let f:[1,n] → C be internal, 1 ≤ n < ω. The maximum value max(f) of f exists. There exists a unique x such that for all i ≤ n, f(i) = x[i:n]. max(f) < x < P*(max(f)).

Proof: The first claim is obvious from the internal definition of x[i:n] above.

Now let f:[1,n] → C. For the second claim, an easy induction, using Lemma 5.7.30 i)-iii), shows that for all 1 ≤ i ≤ n, the maximum value of f on [0,i] exists.

By definition, #(f) = P(n,u)+1, for some u. Obviously u is unique, and we set x = #(f). Since rng(f) ⊆ [0,max(f)], we have max(f) < x = #(f) < P*(max(f) by Lemma 5.8.13. QED

M^, with its internal well foundedness (Lemma 5.7.30 viii)) and bounded comprehension (Lemma 5.7.30 vii)), is a relatively familiar context in which to work, compared with the earlier contexts in this chapter.

In order to construct the constructible hierarchy, we will use the usual language of set theory, L(∈,=).

DEFINITION 5.8.9. We take L(∈,=) to be based on ∈,=, variables v_n, n ≥ 1, and ¬,∧,∀.

By the internal induction in Lemma 5.8.8, and Lemma 5.7.30 iii), we take internal arithmetic for granted, formulated on [0,ω).

In particular, we have access to the internal set GN of all Gödel numbers of formulas of L(∈,=).

DEFINITION 5.8.10. Let R be an internal binary relation. We let R# = P*(y), where y is least such that (∀x ∈ fld(R))(x < y).

The idea is that R# is large enough to accommodate all of the internal finite sequence codes that we need, in the sense of Lemma 5.8.14.

We wish to formally define the notion SAT(R,n,x,m).

DEFINITION 5.8.11. The intended meaning of SAT(R,n,x,m) is that

i) R is a binary relation;
ii) n ∈ GN, x < R#;
iii) the subscript of every free variable in the formula φ of L(∈,=) with Gödel number n is ≤ m < ω;
iv) (fld(R),R) satisfies φ at the partial assignment x[1:m],x[2:m],...,x[m:m].

Note that we allow R to be empty.

In order for clause iv) to hold, we require that x[1:m],x[2:m],...,x[m:m] ∈ fld(R).

Note that if m = 0 then the partial assignment in clause iv) is empty.

In order to make this definition over M^, we first need the following.

LEMMA 5.8.15. Let R be an internal binary relation. There exists a unique internal ternary relation $SAT_R \subseteq GN \times [0,R\#) \times [0,\omega)$ satisfying the usual Tarski satisfaction conditions.

Proof: Let R be as given. Note that in M^, the code of every finite length sequence form fld(R) is < R#, by Lemma 5.8.14. The uniqueness of $SAT_R(n,x,m)$ is proved by internal induction on n. For existence, prove by internal induction on r < ω that there is a ternary relation $T_r \subseteq GN|r \times [0,R\#) \times [0,\omega)$, that satisfies the usual Tarski satisfaction conditions for all n ∈ GN|r. Here GN|r is the set of all n ∈ GN which is at most r. Also prove by internal induction on r < ω that each T_r is unique, and the T_r's are compatible, in the sense that they agree on their common domain. Furthermore, each $T_r \subseteq [0,R\#]^3$. By Lemma 5.7.30, we can take SAT_R to be the union of the T_r's. Finally, an internal induction shows that SAT_R is unique. QED

DEFINITION 5.8.12. We now define SAT(R,n,x,m) if and only if R is a binary relation, and $SAT_R(n,x,m)$ holds, where $SAT_R(n,x,m)$ is given by Lemma 5.8.15.

DEFINITION 5.8.13. Let R be an internal binary relation. We say that n,x,m is a code over R if and only if

i) n ∈ GN;
ii) 1 ≤ m < ω;
iii) x < R# is greater than all elements of fld(R).

We remark that condition iii) is convenient because x does not interfere with the elements of fld(R).

DEFINITION 5.8.14. If n,x,m is a code over R then we write H(R,n,x,m) for

$$\{y: (\exists z)(z[1:m] = y \wedge z[2:m] = x[2:m] \wedge \ldots \wedge z[m:m] = x[m:m] \wedge SAT(R,n,z,m))\}.$$

Note that in the above definition, we use x[2:m],...,x[m:m] but not x[1:m]. This means that we can easily modify x without changing H(R,n,x,m). We will exploit this freedom below.

We think of H(R,n,x,m) as the internal subset of fld(R) that is coded by the code n,x,m. Informally, the H(R,n,x,m), where n,x,m is a code over R, code exactly the "subsets of fld(R) that are first order definable over R". The case R = ∅ is handled appropriately with this notation.

DEFINITION 5.8.15. We say that n,x,m is a minimal code over R if and only if n,x,m is a code over R such that

i) for all codes n′,x′,m′ over R, if H(R,n′,x′,m′) = H(R,n,x,m) then P(n,x,m) ≤ P(n′,x′,m′);
ii) for all y ∈ fld(R), H(R,n,x,m) ≠ {z: R(z,y)}.

Thus the minimal codes over R code exactly the R definable subsets of fld(R) that are not already of the form {z: R(z,y)}, y ∈ fld(R). Also, by minimality, no two distinct minimal codes over R code the same subset of fld(R).

Minimal codes are preferred codes used in order to ensure the propagation of extensionality as we construct the constructible hierarchy.

LEMMA 5.8.16. Let $\varphi(v_1,...,v_m)$, m ≥ 1, be a formula of L(∈,=) with Gödel number n. Let R be an internal binary relation. Then SAT(R,n,x,m) holds if and only if φ(x[1:m],...,x[m:m]) holds in (fld(R),R). H(R,n,x,m) = {y: φ(y,x[2:m],...,x[m:m]) holds in (fld(R),R)}.

Proof: Left to the reader. Note that φ,m,n are standard. QED

LEMMA 5.8.17. Let $\varphi(v_1,...,v_m)$, m ≥ 1, be a formula of L(∈,=). Let R be an internal binary relation, and $z_1,...,z_{m-1}$ ∈ fld(R). Then {y: $\varphi(y,z_1,...,z_{m-1})$ holds in (fld(R),R)} is either of the form {y: R(y,x)}, x ∈ fld(R), or of the form H(R,n′,x',m′), for some unique minimal code n′,x',m′ over R, but not both.

Proof: Use Lemma 5.8.16. Note that φ,m,n are standard. Assume that

{y: $\varphi(y,z_1,...,z_{m-1})$ holds in (fld(R),R)}
is not of the form {y: R(y,x)}, x ∈ fld(R).

Let $f:[1,m] \to C$, where $f(2) = z_1,...,f(m) = z_{m-1}$, and where f(1) is the least point greater than all elements of fld(R). Let x = #f. Then x < R# = P*(f(1)), is greater than all elements of fld(R), and

$$H(R,n,x,m) = \{y: \varphi(y,z_1,...,z_{m-1}) \text{ holds in } (fld(R),R)\}.$$

So we can minimize over the relevant n,x,m in order to obtain the required minimal code n′,x,m′ over R. By the definition of minimal codes over R, the or is exclusive. QED

We are now ready to construct the binary relation FODO(R), for internal R, obtained by "adjoining" all sets first order definable over (fld(R),R) to R.

DEFINITION 5.8.16. We say that a binary relation R is adequate if and only if

$$R(0,1) \wedge (\forall x)(\neg R(x,0)).$$

In particular, for adequate R, we have $0,1 \in fld(R)$.

For internal adequate binary relations R, we construct FODO(R) as follows.

DEFINITION 5.8.17. We define FODO(R)(u,v) if and only if either R(u,v), or

i) there exists a minimal code n,x,m over R such that v = P(n,x,m);
ii) $u \in H(R,n,x,m)$.

The reason that we need the adequacy of R is that $\emptyset = \{x: R(x,0)\}$, and so there is no minimal code n,x,m over R with $H(R,n,x,m) = \emptyset$. It will be convenient to have the sets with minimal codes over R be nonempty.

DEFINITION 5.8.18. Let R be an internal binary relation. We say that R is extensional if and only if for all $x,y \in fld(R)$, $(\forall z)(R(z,x) \leftrightarrow R(z,y)) \to x = y$.

DEFINITION 5.8.19. We say that a binary relation R is sharply extended by a binary relation S if and only if

i) $(\forall x \in fld(S)\backslash fld(R))(\forall y \in fld(R))(y < x)$;
ii) $(\forall x,y \in fld(R))(R(x,y) \leftrightarrow S(x,y))$.

iii) $S(x,y) \wedge y \in fld(R) \rightarrow x \in fld(R)$.
iv) fld(R) is a proper subset of fld(S).

LEMMA 5.8.18. Let R be an internal adequate binary relation. Then FODO(R) is an internal adequate binary relation. In addition, R extensional $\rightarrow$ FODO(R) extensional. FODO(R) sharply extends R. $(\forall x,y)(R(x,y) \rightarrow x < y) \rightarrow (\forall x,y)(FODO(R)(x,y) \rightarrow x < y)$.

Proof: Let R be as given. Note that FODO(R) is bounded by R#. By Lemma 5.6.30 vii), FODO(R) is internal. We claim that

$$1)\ v \in fld(R) \rightarrow FODO(R)(u,v) \leftrightarrow R(u,v).$$

$$2)\ FODO(R)(u,v) \rightarrow u \in fld(R).$$

For 1), let $v \in fld(R)$. If $R(u,v)$ then $FODO(R)(u,v)$. Suppose $FODO(R)(u,v)$. Assume $\neg R(u,v)$. Let $v = P(n,x,m)$, where n,x,m is a minimal code over R. Then x is greater than all elements of fld(R). Hence $x > v$, which is impossible.

For 2), let $FODO(R)(u,v)$. If $R(u,v)$ then obviously $u \in fld(R)$. So we can let $v = P(n,x,m)$, n,x,m a minimal code over R. Then $u \in H(R,n,x,m) \subseteq fld(R)$.

FODO(R) is adequate since $R \subseteq FODO(R)$ and by 1), $FODO(R)(u,0) \rightarrow R(u,0)$, which is impossible.

Assume R is extensional. We claim that FODO(R) is extensional. Suppose

$$3)\ (\forall x)(FODO(R)(x,y) \leftrightarrow FODO(R)(x,z)).$$

case 1. $y,z \in fld(R)$. Since R is extensional, $y = z$.

case 2. $y,z \notin fld(R)$. Let $y = P(n,x,m)$, $z = P(n',x',m')$, where n,x,m and n',x',m' are minimal codes over R. By 2),3), $H(R,n,x,m) = H(R,n',x',m')$. Hence $P(n,x,m) \leq P(n',x',m') \leq P(n,x,m)$. So $P(n,x,m) = P(n',x',m') = y = z$.

case 3. $y \in fld(R)$, $z \notin fld(R)$. Let $z = P(n,x,m)$, n,x,m a minimal code over R, $H(R,n,x,m) \neq \{z: R(z,y)\}$, $H(R,n,x,m)$, and $\{z: R(z,y)\} \subseteq dom(R)$. This contradicts 3).

case 4. $y \notin fld(R)$, $z \in fld(R)$. This leads to a contradiction as in case 3.

We have thus derived $y = z$ from 3), and FODO(R) is extensional.

We claim that FODO(R) sharply extends R. For i) of the definition of sharply extended, let $x \in fld(FODO(R))\backslash fld(R)$, $y \in fld(R)$. Then $x = P(n,u,m)$, where n,u,m is a minimal code over R. Hence u is greater than all elements of fld(R), and so $x > y$.

For ii), use 1).

For iii), use 2).

For iv), note that $\{x \in fld(R): \neg R(x,x)\}$ cannot be of the form $\{y: R(y,x)\}$, $x \in fld(R)$. Let n,x,m be a minimal code over R such that $H(R,n,x,m) = \{x \in fld(R): \neg R(x,x)\}$. THen $P(n,x,m) \in fld(FODO(R))\backslash fld(R)$.

Hence by Lemma 5.8.17, $fld(R) = H(R,n,x,m)$, for some minimal code n,x,m over R. Hence $fld(R) = \{y: FODO(R)(y,x)\}$. Therefore $fld(R) \neq fld(FODO(R))$.

For the last claim, assume $(\forall x,y)(R(x,y) \rightarrow x < y)$. Let FODO(R)(x,y). By construction, either R(x,y) or

$$x \in fld(R) \wedge y \text{ is some } P(n,z,m),$$
$$\text{where } z \text{ is greater than all elements of } fld(R).$$

In either case, $x < y$. QED

LEMMA 5.8.19. Let R be an internal adequate binary relation. Every set definable in (fld(R),R) is of the form $\{x: FODO(R)(x,y)\}$, where $y \in fld(FODO(R))$.

Proof: By the construction of FODO(R), and Lemmas 5.8.17, 5.8.18. QED

Here we have interpreted Lemma 5.8.19 as a scheme of assertions about M^, where we take “definable” in the external sense. However, we also want to interpret Lemma 5.8.19 in a stronger, internal sense - using SAT_R from Lemma 5.8.15. This stronger form of Lemma 5.8.19 can also be proved with the help of internal inductions.

We now wish to transfinitely iterate the FODO operation.

The base of the transfinite iteration will be the adequate relation

$$R_0(x,y) \leftrightarrow$$
$$x = 0 \wedge y = 1.$$

In order to accomplish this, we must be a bit careful. Firstly, we must note that, conceptually, we are manipulating internal relations, and these internal relations are not points; they are elements of Y_2. Furthermore, these internal relations are not even coded as points. In contrast, recall that internal finite sequences f of points are coded as points using f#.

Secondly, note that the operation that sends appropriate R to FODO(R) is even further removed from being an object. It is merely a description of a relationship between objects (not even between points), given in a first order way, without parameters, over M^.

Our strategy is to properly define what we mean by a transfinite iteration of the operation up through a point, *as an object*. The objects for this purpose are the elements of the Y_k, $k \geq 1$. These are components of M^.

DEFINITION 5.8.20. Let T be a k+1-ary relation, $k \geq 1$. For $x \in C$, we write T_x for the cross section $\{(y_1,\ldots,y_k): T(x,y_1,\ldots,y_k)\}$.

Note that T_x is a k-ary relation.

LEMMA 5.8.20. Let $x \in C$. There is a unique internal ternary relation T such that
i) $T_0 = R_0$;
ii) For all $y < x$, $T_{y+1} = \text{FODO}(T_y)$;
iii) For all limits $y \leq x$, $T_y = \cup_{z<y} T_z$;
iv) For all $y \leq x$, T_y is adequate;
v) For all $y > x$, $T_y = \emptyset$.

Proof: Define $\Gamma(T,x)$ if and only if $x \in C \wedge T$ is an internal ternary relation obeying i)-v).

We first claim that for all x,T,T',

$$\Gamma(T,x) \wedge \Gamma(T',x) \rightarrow T = T'.$$

Suppose this is false. Choose x to be least such that

$$(\exists T,T')(\Gamma(T,x) \wedge \Gamma(T',x) \wedge T \neq T'.$$

Clearly $x \neq 0$, since $T_0 = T'_0 = R_0$. Hence $x > 0$.

Let $x = z+1$. Let

$$\Gamma(T,z+1),\ \Gamma(T',z+1), T_{z+1} \neq T'_{z+1}.$$
$$\text{FODO}(T_z) \neq \text{FODO}(T'_z).$$
$$T_z \neq T'_z.$$

This contradicts the choice of x.

Finally, let x be a limit. We claim that

$$(\forall z < x)(T_z = T'_z).$$

To see this, let $z < x$. Let T^* be the restriction of T to triples whose first argument is $\leq z$, and $T^{*\prime}$ be the restriction of T^* to triples whose first argument is $\leq z$. Then $\Gamma(T^*,z)$, $\Gamma(T^{*\prime},z)$. Hence $T^* = T^{*\prime}$. This is a contradiction.

The first claim has been established. In fact, it is now clear that the T's such that $(\exists x)(\Gamma(T,x))$ are comparable in that any two agree on their common domain.

To prove existence, let $u > 0$, and suppose

$$(\forall x < u)(\exists T)(\Gamma(T,x)).$$

We now show

$$(\exists T)(\Gamma(T,u)).$$

The case $u = 0$ is obvious, by defining

$$T(a,b,c) \leftrightarrow a = 0 \wedge R_0(b,c).$$

Assume u is a successor, $u = v+1$. Let $\Gamma(T,v)$. Define

$$T'(a,b,c) \leftrightarrow$$
$$T(a,b,c) \vee (a = v+1 \wedge \text{FODO}(T_v)(b,c)).$$

To see that T′ is internal, it suffices to show that T′ is bounded. This follows from the boundedness of T and $\text{FODO}(T_v)$.

Note that by Lemma 5.8.18, $FODO(T_v) = T'_{v+1}$ is adequate. Also,

$$x \leq v \rightarrow T'_x = T_x.$$
$$T'_{v+1} = FODO(T_v) = FODO(T'_v).$$
$$\Gamma(T',v+1),\ \Gamma(T',u).$$

Assume u is a limit. Define

$$T^*(a,b,c) \leftrightarrow$$
$$a < u \wedge (\exists T)(\Gamma(T,a) \wedge T(a,b,c)).$$

To see that T* is internal, it suffices to show that T* is bounded. We have $(\forall a < u)(\exists! T)(\Gamma(T,a))$, by the first claim (uniqueness).

Let $a < u < c_n$, $n \geq 1$. By Lemma 5.7.30 ix), we have

$$(\exists w)(\exists T)(\Gamma(T,a) \wedge T \text{ lies entirely below } w).$$
$$(\exists w < c_{n+1})(\exists T)(\Gamma(T,a) \wedge T \text{ lies entirely below } w).$$
$$(\exists T)(\Gamma(T,a) \wedge T \text{ lies entirely below } c_{n+1}).$$
$$T^* \text{ lies entirely below } c_{n+1}.$$
$$T^* \text{ is internal.}$$

Let a < u. Let

$$\Gamma(T,0),\ \Gamma(T,a),\ \Gamma(T',a+1).$$

From the definition of T* and the uniqueness/comparability (first claim),

$$T^*_0 = T_0,\ T^*_a = T_a = T'_a,\ T^*_{a+1} = T'_{a+1}.$$
$$T_0 = R_0,\ T^*_{a+1} = FODO(T'_a) = FODO(T^*_a).$$
$$\text{All of these relations are adequate.}$$

Now let z < u be a limit. Let $\Gamma(z,T'')$. Then

$$T''_z = T^*_z.$$
$$T''_z = \cup_{a<z} T''_a = \cup_{a<z} T^*_a.$$

Hence T* obeys i)-v) for $\Gamma(T^*,u)$, except clause iii) holds only for y < u. To fix this, define

$$T^{**}(a,b,c) \leftrightarrow$$
$$T^*(a,b,c) \vee (a = u \wedge (\exists a < u)(T^*(a,b,c))).$$

It is easy to see that T^{**}_u is adequate. Then $\Gamma(T^{**},u)$. QED

DEFINITION 5.8.21. For each $x \in C$, we let $L(x) = T_x$, where T is the ternary relation given by Lemma 5.8.20. I.e., where $\Gamma(T,x)$ as defined in the proof of Lemma 5.8.20. Thus each $L(x) \in Y_2$.

DEFINITION 5.8.22. For each $x \in C$, we define $L[x] = fld(L(x))$. Note that $L[0] = \{0,1\}$, and that $L[x] \subseteq C$.

DEFINITION 5.8.23. We define $L[\infty]$ as the union of the L[x].

We caution the reader that $L[\infty] \subseteq C$ is not internal, because it is not bounded. It is, however, M^ definable without any parameters.

DEFINITION 5.8.24. We define $L(\infty)$ be the union of the L(x).

Thus $L(\infty)(x,y)$ if and only if there exists $z \in C$ such that $L(z)(x,y)$. Obviously $L(\infty) \subseteq C^2$.

The various L[x] correspond to the initial segments of the constructible hierarchy. The various L(x) correspond to the epsilon relations on the initial segments of the constructible hierarchy. $L[\infty]$ corresponds to the class of constructible sets. $L(\infty)$ corresponds to the epsilon relation on the class of constructible sets.

Clearly $L(\infty)$ is the version of the epsilon relation on the constructible sets in M^, and is a binary relation. Its field is $L[\infty]$.

We caution the reader that L[x] may not be an initial segment of points, and may not be a subset of [0,x). It may have elements that are greater than x.

LEMMA 5.8.21. $L(0) = R_0$. For all $x \in C$, $L(x+1) = FODO(L(x))$. For all limits $x \in C$, L(x) is the union of the L(y), $y < x$. For all $x < y$, L(x) is sharply extended by L(y). Each L(x) is extensional. Each L(x) has $L(x)(y,z) \rightarrow y < z$.

Proof: $L(0) = T$, where $\Gamma(T,0)$. Hence $L(0) = R_0$. $L(x+1) = T_{x+1}$, where $\Gamma(T,x+1)$. Hence $L(x+1) = FODO(T_x)$. Let T′ be the restriction of T to triples whose first argument is $\leq x$. Then $\Gamma(T',x)$, $T'_x = T_x$, $L(x+1) = FODO(T'_x) = FODO(L(x))$.

Let x be a limit. $L(x) = T_x$, where $\Gamma(T,x)$. Now $T_x = \cup_{y<x}T_y$. By using restrictions as in the previous paragraph, we see that for all $y < x$, $T_y = L(y)$. Hence $L(x) = T_x = \cup_{y<x}T_y$.

For the fourth claim, fix x. We prove by transfinite induction on y that

$$x < y \rightarrow L(x) \text{ is sharply extended by } L(y).$$

This is obvious for y = x.

Suppose y > x, and L(x) is sharply extended by L(y). By Lemma 5.8.18, L(y) is sharply extended by L(y+1). Since L(x) is sharply extended by L(y), clearly L(x) is sharply extended by L(y+1).

Suppose y > x, where y is a limit, and L(x) is sharply extended by every L(z), x ≤ z < y. We claim that L(x) is sharply extended by L(y). To see this, first let u ∈ fld(L(y))\fld(L(x)), v ∈ fld(L(x)). Let u ∈ fld(L(z))\fld(L(x)), x < z < y. Since L(z) is sharply extended by L(x), we have u < v.

Next let u,v ∈ fld(L(x)). If L(x)(u,v) then obviously L(y)(u,v). If L(y)(u,v) then let x < z < y, L(z)(u,v). Since L(x) is sharply extended by L(z), we have L(x)(u,v).

Now let L(y)(u,v), v ∈ fld(L(x)). Let u ∈ L(z), where x < z < y. Since L(z) is sharply extended by L(y), L(z)(u,v). Since L(x) is sharply extended by L(z), we have u ∈ L(x).

Finally, fld(L(x)) is a proper subset of fld(L(y)) since fld(L(x)) is a proper subset of fld(L(x+1)) ⊆ fld(L(y)), by Lemma 5.8.18.

For the fifth claim, we argue by transfinite induction on x. L(0) = R_0 is extensional. Suppose L(x) is extensional. By Lemma 5.8.18, L(x+1) = FODO(L(x)) is extensional. Suppose x is a limit, where for all y < x, L(y) is extensional. Let a,b ∈ fld(L(x)), (∀z)(L(x)(z,a) ↔ L(x)(z,b)). Let a,b ∈ fld(L(y)), y < x. Since L(x) is a sharp extension of L(y), we have (∀z)(L(y)(z,a) ↔ L(y)(z,b)). Since L(y) is extensional, a = b.

For the sixth claim, we argue by transfinite induction on x. Obviously L(0)(y,z) → y < z since L(0) = R_0. Suppose

$$(\forall y,z)(L(x)(y,z) \rightarrow y < z).$$

By Lemma 5.8.18,

$$(\forall y,z)(L(x+1)(y,z) \rightarrow y < z).$$

Let x be a limit, where

$$(\forall y < x)(\forall u,v)(L(y)(u,v) \rightarrow u < v).$$

Let L(x)(u,v). Let L(y)(u,v), y < x. Then u < v. QED

DEFINITION 5.8.25. Let x ∈ L[∞]. We write lrk(x) for the least y such that x ∈ L[y+1]. This is the L rank of x. Note that lrk is a function from C into C that is M^ definable without parameters.

LEMMA 5.8.22. Let x,y ∈ C. L(∞)(x,y) → (lrk(x) < lrk(y) ∧ x < y). L(∞)(x,y) ↔ L(lrk(y)+1)(x,y). L[∞] ∩ [0,x) ⊆ L[x].

Proof: Let L(∞)(x,y). Let L(z)(x,y). By Lemma 5.8.21, x < y. Also, let y ∈ L[u+1]\L[u]. Then lrk(y) = u, u+1 ≤ z. By Lemma 5.8.21, z = u+1 ∨ L(u+1) is sharply extended by L(z). Therefore x ∈ L(u+1), L(u+1)(x,y), x ∈ L(u). Hence lrk(x) < lrk(y) = u. This also establishes the second claim.

We prove the final claim by transfinite induction on x. We have L[∞] ∩ [0,0) ⊆ L[0], vacuously.

Suppose L[∞] ∩ [0,x) ⊆ L[x]. We want L[∞] ∩ [0,x] ⊆ L[x+1]. It suffices to prove x ∈ L[∞] → x ∈ L[x+1]. Assume x ∈ L[∞]\L[x+1]. Let x ∈ L[y]. Then y > x+1. Since L[y] sharply extends L[x+1], x is greater than all elements of L[x+1]. Since L[x+1] sharply extends L[x], there is an element of L[x+1] that is greater than all elements of L[x], and L[x] ⊇ [0,x). Hence there is an element of L[x+1] that is ≥ x. This is a contradiction.

Suppose x is a limit, where for all y < x,

$$L[\infty] \cap [0,y) \subseteq L[y].$$

We claim that

$$L[\infty] \cap [0,x) \subseteq L[x].$$

To see this, let z ∈ L[∞], z < x. Let z < y < x. Then z ∈ L[y], z ∈ L[x]. QED

DEFINITION 2.8.26. A Δ_0 formula of L(∈,=) is a formula of L(∈,=) in which all quantifiers are ∈ bounded; i.e.,

$$(\exists x \in y)$$

$(\forall x \in y)$

where x,y are distinct variables.

LEMMA 5.8.23. Let $\varphi(x_1,...,x_k)$ be a Δ_0 formula of $L(\in,=)$. Let $y_1,...,y_k,z,w$ be such that $y_1,...,y_k \in L[z],L[w]$. Then $\varphi(y_1,...,y_k)$ holds in $(L[z],L(z))$ if and only if $\varphi(y_1,...,y_k)$ holds in $(L[w],L(w))$ if and only if $\varphi(y_1,...,y_k)$ holds in $(L[\infty],L(\infty))$.

Proof: Here k,φ are standard. The first claim is by external induction on the number of occurrences of variables in φ. Use Lemma 5.8.21 (sharp extensions). QED

LEMMA 5.8.24. Extensionality, pairing, and union hold in $(L[\infty],L(\infty))$.

Proof: For extensionality, let $x,y \in L[u]$, where $(\forall z)(z \in x \leftrightarrow z \in y)$ holds in $(L[\infty],L(\infty))$. By Lemma 5.8.23, $(\forall z)(z \in x \leftrightarrow z \in y)$ holds in $(L[u],L(u))$. By Lemma 5.8.21, $x = y$. Since u is arbitrary, extensionality holds in $(L[\infty],L(\infty))$.

For pairing, let $x,y \in L[u]$. By Lemma 5.8.19, let $z \in L[u+1]$ be such that $(\forall w)(w \in z \leftrightarrow (w = x \vee w = y))$ holds in $L[u+1]$. By Lemma 5.8.21 (sharp extensions), $(\forall w)(w \in z \leftrightarrow (w = x \vee w = y))$ holds in $(L[\infty],L(\infty))$. Since u is arbitrarily, pairing holds in $(L[\infty],L(\infty))$.

For union, let $x \in L[u]$. By Lemma 5.8.19, let y in $L[u+1]$ be such that
$(\forall z)(z \in y \leftrightarrow (\exists w)(z \in w \wedge w \in x))$ holds in $(L[u+1],L(u+1))$. By Lemmas 5.8.21 (sharp extensions) and 5.8.23, $(\forall z)(z \in y \leftrightarrow (\exists w)(z \in w \wedge w \in x))$ holds in $(L[\infty],L(\infty))$. Since u is arbitrary, union holds in $(L[\infty],L(\infty))$. QED

LEMMA 5.8.25. Infinity holds in $(L[\omega+1],L(\omega+1))$. Infinity holds in $(L[\infty],L(\infty))$.

Proof: Infinity has the form

$$(\exists x)(\emptyset \in x \wedge (\forall y \in x)(y \cup \{y\} \in x))$$

which makes perfectly good sense in the presence of extensionality, union, and pairing. It is clear that 0 serves as the $\emptyset$ in $(L[\infty],L(\infty))$.

We say that a set is epsilon connected if and only if any two elements are either equal, or one is an element of the other.

Prove by internal induction on $n < \omega$ that "the epsilon connected transitive sets are linearly ordered by epsilon, and there is a largest epsilon connected transitive set" holds in $(L[n],L(n))$. For each $n < \omega$, let $h(n)$ be the witness to this statement in $(L[n+1],L(n+1))$. Prove by internal induction on $n < \omega$ that $h(0) = \emptyset$, and "$h(n+1) = h(n) \cup \{h(n)\}$" holds in $(L[n+2],L(n+2))$. Prove that for all $u \in L(\omega)$, $(\exists n < \omega)(u = h(n))$ if and only if "u is epsilon connected and transitive" holds in $(L[\omega],L(\omega))$. By Lemma 5.8.19, let $x \in L(\omega+1)$, where $(\forall y)(L(\omega+1)(y,x) \leftrightarrow (\exists n < \omega)(y = h(n))$. Then in $(L[\omega+1],L(\omega+1))$, x is a witness for Infinity.

To see that Infinity holds in $(L[\infty],L(\infty))$, apply Lemma 5.8.21, with parameters x,0. QED

LEMMA 5.8.26. Every $L(x)$ is internally well founded. $L(\infty)$ is internally well founded. Foundation holds in every $(L[x],L(x))$. Foundation holds in $(L[\infty],L(\infty))$.

Proof: The first claim follows from the internal well foundedness of < by Lemma 5.8.21. The internal well foundedness of < is by Lemma 5.7.30 viii). The remaining claims follow easily from the first claim, using Lemma 5.8.23. QED

LEMMA 5.8.27. Let $n \geq 1$ and $\varphi_1,\ldots,\varphi_n$ be formulas of $L(\in,=)$ that begin with, respectively, existential quantifiers $(\exists y_1),\ldots,(\exists y_n)$. For all z there exists $w > z$ such that the following holds. Let $1 \leq i \leq n$. Let the free variables of φ_i be assigned elements of $L[z]$. If φ_i holds in $(L[\infty],L(\infty))$ then $(\exists y_i \in L[w])(\varphi_i(y_i))$ holds in $(L[\infty],L(\infty))$.

Proof: By Lemma 5.8.1, we can choose internal witness functions $f_1,\ldots,f_k$, whose domains are Cartesian powers of $L[z]$. By applying the lrk function to the values of the f's, we see that the set A of values of lrk(z), z a value of the f's, must be internal - again using Lemma 5.8.1. Take w to be the strict sup of A. QED

LEMMA 5.8.28. Let $\varphi(v_1,\ldots,v_k)$ be a formula of $L(\in,=)$. For all z there exists $w > z$ such that the following holds. Let $y_1,\ldots,y_k \in L[w]$. Then $\varphi(y_1,\ldots,y_k)$ holds in $(L[\infty],L(\infty))$ if and only if $\varphi(y_1,\ldots,y_k)$ holds in $(L[w],L(w))$.

Proof: Without loss of generality, we can assume that $\varphi(v_1,...,v_k)$ is in prenex normal form. Let $\varphi_1,...,\varphi_n$ be a listing of all direct subformulas of φ, and duals of subformulas of φ, which begin with an existential quantifier.

Informally, we define, internally, an infinite sequence $z < w_1 < w_2 < ...$ as follows. w_1 is the least $w > z$ given by Lemma 5.8.27 for $\varphi_1,...,\varphi_n$. Suppose w_j has been defined, $j \geq 1$. w_{j+1} is the least $w > w_j$ given by Lemma 5.8.27 with z set to w_j.

We convert this to a construction within M^ as follows. First prove that for all $n < \omega$, there is a unique finite sequence $f:[1,n] \to C$, where $f(1) = w_1$ and each $f(i+1)$ is obtained from $f(i)$ according to the previous paragraph. This yields a function $g:[1,\omega) \to C$ by taking the union of these f's. Now apply Lemma 5.8.1 to show that g is internal. In particular, g is bounded, and so we let w be the strict sup of the values of g.

An external induction argument shows that for all $y_1,...,y_k \in L[w]$ and $1 \leq i \leq n$,

$$\varphi_i(y_1,...,y_k) \text{ holds in } (L[\infty],L(\infty)) \leftrightarrow \varphi_i(y_1,...,y_k) \text{ holds in } (L[w],L(w)).$$

The induction is on the number of quantifiers present in φ_i. Since φ is among the $\varphi_1,...,\varphi_n$, we are done. QED

DEFINITION 2.8.27. Collection is the scheme

$$(\forall x \in y)(\exists z)(\varphi) \to (\exists w)(\forall x \in y)(\exists z \in w)(\varphi)$$

where φ is a formula of $L(\in,=)$, x,y,z,w are distinct variables, and w is not free in φ.

LEMMA 5.8.29. Every instance of Separation holds in $(L[\infty],L(\infty))$. Every instance of Collection holds in $(L[\infty],L(\infty))$.

Proof: Consider $(\exists x)(\forall y)(y \in x \leftrightarrow (y \in z \wedge \varphi))$, where x,y,z are distinct variables and x is not free in φ. Let $z \in L[\infty]$. Let u be such that z and all parameters in φ lie in L[u].

By Lemma 5.8.28, let $v > u$ be such that for all $y \in L[v]$,

$$\varphi(y) \text{ holds in } (L[\infty],L(\infty)) \leftrightarrow \varphi(y) \text{ holds in } (L[v],L(v)).$$

Let b ∈ L[v+1], where

$$(\forall y)(L(\infty)(y,b) \leftrightarrow ((y \in z \wedge \varphi(y)) \text{ holds in } (L[v],L(v)))).$$

Then

$$(\forall y)(y \in b \leftrightarrow (y \in z \wedge \varphi))$$

holds in (L[∞],L(∞)).

Now consider

$$(\forall x \in y)(\exists z)(\varphi) \rightarrow (\exists w)(\forall x \in y)(\exists z \in w)(\varphi),$$

where x,y,z,w are distinct variables and w is not free in φ. Let y ∈ L[∞]. Let u be such that y and all parameters in φ lie in L[u]. Assume (∀x ∈ y)(∃z)(φ) holds in (L[∞],L(∞)).

By Lemma 5.8.22, L(∞)(x,y) → x < y. For each x such that L(∞)(x,y), we can consider the < least u such that (∃z ∈ L[u])(φ holds in (L[∞],L(∞))). This gives us an M^ definable function to which we can apply Lemma 5.8.1, and then take its strict sup, v, using Lemma 5.7.30 viii). By Lemma 5.8.19, set w ∈ L[v+1], where (∀v)(L(∞)(v,w) ↔ v ∈ L[u]). QED

DEFINITION 5.8.28. Let ZF\P be all axioms of ZF less Power Set, using Collection.

LEMMA 5.8.30. Every axiom of ZF\P with Collection holds in (L[∞],L(∞)).

Proof: From Lemmas 5.8.24, 5.8.25, 5.8.26, 5.8.29, 5.8.30. QED

Note that we have shown that all axioms of ZFC hold in (L[∞],L(∞)), with the exceptions of Power Set and Choice. In fact, we have verified Collection, which implies Replacement (in the presence of separation).

We now show that the power set axiom holds in (L[∞],L(∞)) using indiscernibility.

LEMMA 5.8.31. For all $n \geq 2$, $L[c_n] \subseteq [0,c_{n+1})$.

Proof: Let $n \geq 2$. Now $L[c_n]$ is internal, and in particular, bounded. By Lemma 5.7.30 v), let $m > n$ be such that $L[c_n] \subseteq [0,c_m)$. We can view this as a true statement about c_n,c_m. By Lemma 5.7.30 ix), the statement is true of c_n,c_{n+1}. I.e., $L[c_n] \subseteq [0,c_{n+1})$. QED

DEFINITION 5.8.29. It is very convenient to define $x \subseteq^* y$ if and only if

$$x \in L[\infty] \wedge (\forall z \in L[\infty])(L(\infty)(z,x) \rightarrow L(\infty)(z,y)).$$

Also, $x \subseteq^{**} y$ if and only if

$$x \in L[\infty] \wedge (\forall z \in L[\infty])(L(\infty)(z,x) \rightarrow z \in L[y]).$$

LEMMA 5.8.32. Let $x \subseteq^{**} c_2$. Then $x < c_3$.

Proof: Suppose

$$1)\ (\exists x \geq c_3)(x \subseteq^{**} c_2).$$

By Lemma 5.7.30 ix), for every $n \geq 3$,

$$2)\ (\exists x \geq c_n)(x \subseteq^{**} c_2).$$

For each $n \geq 3$, let $J(n)$ be the $<$ least $x \geq c_n$ such that $x \subseteq^{**} c_2$.

Note that the $J(n)$, $n \geq 3$, are uniformly defined from c_2,c_n without parameters.

Fix $n \geq 3$. By Lemma 5.7.30 v), let $m > n$, and $J(n) < c_m$. By Lemma 5.7.30 ix), $J(n) < c_{n+1}$.

We have established that for all $n \geq 3$,

$$c_n \leq J(n) < c_{n+1} \wedge$$
$$\text{"}J(n) \subseteq L[c_2]\text{" holds in } (L[\infty],L(\infty)).$$

In particular, for all $n \geq 3$, $J(n) < J(n+1)$.

Let $y \in L[c_2]$. By Lemma 5.8.32, $y < c_3$. By Lemma 5.7.30 ix),

$$L(\infty)(y,J(4)) \leftrightarrow L(\infty)(y,J(5)).$$

This is because J(4),J(5) are defined the same way from c_2,c_4 and from c_2,c_5, respectively, without parameters. I.e.,

3) $(\forall y \in L[c_2])(L(\infty)(y,J(4)) \leftrightarrow L(\infty)(y,J(5)))$.

By the construction of J, we have

4) $J(4) \subseteq^{**} c_2$.
$J(5) \subseteq^{**} c_2$.
$(\forall y \in L[\infty])(L(\infty)(z,J(4)) \rightarrow y \in L[c_2])$.
$(\forall y \in L[\infty])(L(\infty)(z,J(5)) \rightarrow y \in L[c_2])$.

By 3),4), and extensionality in $(L[\infty],L(\infty))$, we have $J(4) = J(5)$. This contradicts $J(4) < J(5)$.

We have thus refuted 1). Hence

$$(\forall x)(x \subseteq^{**} c_2 \rightarrow x < c_3).$$

QED

LEMMA 5.8.33. Let $n \geq 2$ and $x \subseteq^{**} c_n$. Then $x < c_{n+1}$.

Proof: By Lemmas 5.8.32 and 5.7.30 ix). QED

LEMMA 5.8.34. Power Set holds in $(L[\infty],L(\infty))$.

Proof: Let $x \in L[\infty]$. By Lemma 5.7.30 v), let $x \in L[c_n]$, $n \geq 2$. Let $y \subseteq^* x$. Then $y \subseteq^{**} c_n$. By Lemma 5.8.33, $y < c_{n+1}$.

By Lemma 5.7.30 v), let $y \in L[c_m]$, $m \geq n+2$. By Lemma 5.7.30 ix), $y \in L[c_{n+2}]$. We have thus shown that for all y,

1) $y \subseteq^* x \rightarrow y \in L[c_{n+2}]$.

Clearly $\{y \in L[c_{n+2}]: y \subseteq^* x\}$ is definable in $(L[c_{n+2}],L(c_{n+2}))$. Hence by Lemma 5.8.19, there exists $z \in L[c_{n+2}+1]$ such that

2) $(\forall y)(y \subseteq^* x \leftrightarrow (L(c_{n+2}+1)(y,z)))$.

It follows that in $(L[\infty],L(\infty))$, z is the power set of x, using Lemma 5.8.21 (sharp extensions). Since $x \in L[\infty]$ is arbitrary, power set holds in $(L[\infty],L(\infty))$. QED

LEMMA 5.8.35. ZF holds in $(L[\infty],L(\infty))$. All sentences in $TR(\Pi^0_1,L)$ hold in $(L[\infty],L(\infty))$.

Proof: The first claim follows from Lemmas 5.8.30 and 5.8.34. For the second claim, from the proof of Lemma 5.8.25, we see that the finite von Neumann ordinals of (L[∞],L(∞)) are in order preserving one-one correspondence with {x: x < ω}. Therefore the 0,1,+,-,•,↑,log of (L[∞],L(∞)) is isomorphic to the 0,1,+,-,•,↑,log of M^, by M^ induction, given the one-one correspondence and the operations are all internal to M^. The second claim now follows from Lemma 5.7.30 iii). QED

LEMMA 5.8.36. There exists a countable model M^+ of ZF + TR(Π^0_1,L), with distinguished elements $d_1,d_2,\ldots$, such that
i) The d's are strictly increasing ordinals in the sense of M^+, without an upper bound;
ii) Let r ≥ 1, and $i_1,\ldots,i_{2r} \geq 1$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and min. Let R be a 2r-ary relation M^+ definable without parameters. Let $\alpha_1,\ldots,\alpha_r \leq \min(d_{i\_1},\ldots,d_{i\_r})$. Then $R(d_{i\_1},\ldots,d_{i\_r},\alpha_1,\ldots,\alpha_r) \leftrightarrow R(d_{i\_r+1},\ldots,d_{i\_2r},\alpha_1,\ldots,\alpha_r)$.

Proof: Take M^+ to be (L[∞],L(∞)). By Lemma 5.8.35, we have ZF + TR(Π^0_1,L) in M^+.

For all n ≥ 1, take d_n to be the minimum ordinal of (L[∞],L(∞)) lying outside $L[c_{2n}]$. In fact, $d_n \in L[c_{2n}+1]$ is the set of all ordinals in $L[c_{2n}]$, in the sense of (L[∞],L(∞)).

Note that $d_n \geq c_{2n}$ by Lemma 5.8.22. Also, since d_n is defined without parameters from c_{2n}, we have $d_n < c_{2n+1}$. I.e., for all n, $c_{2n} \leq d_n < c_{2n+1}$. Hence claim i) holds.

Let R be a 2r-ary relation M^+ definable without parameters. Then R is a 2r-ary relation on L[∞] that is M^ definable without parameters. Let $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and min. Let the min be j. Let $\alpha_1,\ldots,\alpha_r \leq d_j$, where the α's are ordinals in the sense of M^+. In particular, $\alpha_1,\ldots,\alpha_r$ are ordinals of (L[∞],L(∞)). It follows that $\alpha_1,\ldots,\alpha_r < c_{2j+1}$.

We claim that

$$1)\ R(d_{i\_1},\ldots,d_{i\_r},\alpha_1,\ldots,\alpha_r) \leftrightarrow R(d_{i\_r+1},\ldots,d_{i\_2r},\alpha_1,\ldots,\alpha_r)$$

holds in M^+. To see this, replace each d_{i_p} by its definition in M^ from c_{2i_p}. Then 1) can be viewed as an assertion in M^ involving the parameters

2) $c_{2i\_1},\ldots,c_{2i\_r}$ on the left.
$c_{2i\_r+1},\ldots c_{2i\_2r}$ on the right.
$\alpha_1,\ldots,\alpha_r \leq c_{2j+1}$.
$j = \min(i_1,\ldots,i_{2r})$.

We can treat c_{2j} as an additional parameter. So we have the parameters

3) $c_{2i\_1},\ldots,c_{2i\_r}$ on the left, without c_{2j}.
$c_{2i\_r+1},\ldots c_{2i\_2r}$ on the right, without c_{2j}.
$\alpha_1,\ldots,\alpha_r,c_{2j} \leq c_{2j+1}$.
$j = \min(i_1,\ldots,i_{2r})$.

The 2j must occupy the same positions in $i_1,\ldots,i_r$ as they do in $i_{r+1},\ldots,i_{2r}$. Therefore, in 3), the remaining c's on the left have the same order type as the remaining c's on the right. But they do not necessarily have the same min. So we can insert a dummy variable at the end for c_{2j+1}. Thus we have

4) $c_{2i\_1},\ldots,c_{2i\_r},c_{2j+1}$ on the left, without c_{2j}.
$c_{2i\_r+1},\ldots c_{2i\_2r},c_{2j+1}$ on the right, without c_{2j}.
$\alpha_1,\ldots,\alpha_r,c_{2j} \leq c_{2j+1}$.
$j = \min(i_1,\ldots,i_{2r})$.

We now see that the equivalence holds because of Lemma 5.7.30 ix). QED

LEMMA 5.8.37. There exists a countable model M^+ of ZFC + V = L + TR(Π^0_1,L), with distinguished elements $d_1,d_2,\ldots$, such that
i) The d’s are strictly increasing ordinals in the sense of M^+, without an upper bound;
ii) Let $r \geq 1$, and $i_1,\ldots,i_{2r} \geq 1$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and min. Let R be a 2r-ary relation M^+ definable without parameters. Let $\alpha_1,\ldots,\alpha_r \leq \min(d_{i\_1},\ldots,d_{i\_r})$. Then $R(d_{i\_1},\ldots,d_{i\_r},\alpha_1,\ldots,\alpha_r) \leftrightarrow R(d_{i\_r+1},\ldots,d_{i\_2r},\alpha_1,\ldots,\alpha_r)$.

Proof: We could have proved the stronger form of Lemma 5.8.36, with ZFC + V = L instead of ZF. However, this would require a bit more than the usual hand waving with regards to internalized constructibility. So we have choose to wait until we have Lemma 5.8.36, with its honest to goodness model of ZF.

Start with the structure given by Lemma 5.8.36. Take the usual inner model of L. Ordinals are preserved. So we take the same d's, and i) is immediate. We still have $TR(\Pi^0_1,L)$, and since this inner model is definable without parameters, we preserve ii). QED

5.9. ZFC + V = L + $\{(\exists\kappa)(\kappa$ is strongly k-Mahlo$)\}_k$ + $TR(\Pi^0_1,L)$, and 1-Con(SMAH).

We fix a countable model M^+ and $d_1,d_2,\ldots$, as given by Lemma 5.8.37. We will show that M^+ satisfies, for each $k \geq 1$, that "there exists a strongly k-Mahlo cardinal".

In section 4.1, we presented a basic discussion of n-Mahlo cardinals and strongly n-Mahlo cardinals. The formal systems MAH, SMAH, MAH^+, and $SMAH^+$, were introduced in section 4.1 just before Theorem 4.1.7.

Recall the partition relation given by Lemma 4.1.2. Note that Lemma 4.1.2 states this partition relation with an infinite homogenous set. A closely related partition relation was studied in [Sc74], for both infinite and finite homogenous sets. In [Sc74] it is shown that this closely related partition relation with finite homogenous sets produces strongly Mahlo cardinals of finite order, where the order corresponds to the arity of the partition relation.

We give a self contained treatment of the emergence of strongly Mahlo cardinals of finite order from this related partition relation for finite homogenous sets. We have been inspired by [HKS87], which also contains a treatment of essentially the same partition relation, and answers some questions left open in [Sc74]. Our main combinatorial result, in the spirit of [Sc74], is Theorem 5.9.5. This is a theorem of ZFC, and so we use it within M^+.

We then show that this partition relation for finite homogenous sets holds in M^+. As a consequence, M^+ has strongly Mahlo cardinals of every finite order.

DEFINITION 5.9.1. We write $S \subseteq On$ to indicate that S is a set of ordinals.

The only proper class considered in this section is On, which is the class of all ordinals. Hence S must be bounded in On.

DEFINITION 5.9.2. We write sup(S) for the least ordinal that is at least as large as every element of S.

DEFINITION 5.9.3. We write $[S]^k$ for the set of all k element subsets of S. We say that $f:[S]^k \rightarrow On$ is regressive if and only if for all $A \in [S\backslash\{0\}]^k$, $f(A) < \min(A)$.

DEFINITION 5.9.4. We say that E is min homogeneous for f if and only if $E \subseteq S$ and for all $A,B \in [E]^k$, if min(A) = min(B) then f(A) = f(B).

DEFINITION 5.9.5. We write R(S,k,r) if and only if $S \subseteq On$, $k,r \geq 1$, and for all regressive $f:[S]^k \rightarrow On$, there exists min homogenous $E \in [S]^r$ for f.

DEFINITION 5.9.6. We say that $S \subseteq On$ is closed if and only if the sup of every nonempty subset of S lies in S. Thus $\emptyset$ is closed. Note that every nonempty closed S has $\sup(S) \in S$.

DEFINITION 5.9.7. Let $f:[S]^k \rightarrow On$. When we write $f(\alpha_1,\ldots,\alpha_k)$, we mean $f(\{\alpha_1,\ldots,\alpha_k\})$, and it is assumed that $\alpha_1 < \ldots < \alpha_k$.

LEMMA 5.9.1. The following is provable in ZFC. Suppose R(S,k,r), where $S \subseteq On\backslash\omega$. Let $n \geq 1$ and $f_1,\ldots,f_n$ each be regressive functions from $[S]^k$ into On. There exists $E \in [S]^r$ which is min homogenous for $f_1,\ldots,f_n$.

Proof: Let $S,k,r,n,f_1,\ldots,f_n$ be as given. Let $H:(\sup(S)+1)^{1+n} \rightarrow \sup(S)+1$ be such that

i) For all $\omega \leq \alpha \leq \sup(S)$ and $\beta_1,\ldots,\beta_n \leq \alpha$, $H(\alpha,\beta_1,\ldots,\beta_n) < \alpha$;
ii) For all $\omega \leq \alpha \leq \sup(S)$ and $\beta_1,\ldots,\beta_n,\gamma_1,\ldots,\gamma_n \leq \alpha$, $H(\alpha,\beta_1,\ldots,\beta_n) = H(\alpha,\gamma_1,\ldots,\gamma_n) \rightarrow (\beta_1 = \gamma_1 \wedge \ldots \wedge \beta_n = \gamma_n)$.

We can find such an H because for all $\alpha \geq \omega$, $|\alpha^n| = |\alpha|$.

Let $g:[S]^k \rightarrow On$ be defined as follows. $g(x_1,\ldots,x_k) = H(x_1,f_1(x_1,\ldots,x_k),\ldots,f_n(x_1,\ldots,x_k))$.

To see that g is regressive, let $x_1 < \ldots < x_k$ be from S. Then $\omega \leq x_1,\ldots,x_k$, and so

$$f_1(x_1,\ldots,x_k),\ldots,f_n(x_1,\ldots,x_k) < x_1.$$
$$g(x_1,\ldots,x_k) =$$

$$H(x_1,f_1(x_1,\ldots,x_k),\ldots,f_n(x_1,\ldots,x_k)) < x_1.$$

By R(S,k,r), let $E \in [S]^r$ be min homogenous for g. To see that E is min homogenous for $f_1,\ldots,f_n$, let $V_1,V_2 \subseteq E$ be k element sets with the same minimum, say $\alpha \in E$. Then $\omega \leq \alpha$ and $g(V_1) = g(V_2)$. Hence

$$H(\alpha,f_1(V_1),\ldots,f_n(V_1)) = H(\alpha,f_1(V_2),\ldots,f_n(V_2)).$$

By ii), each $f_i(V_1) = f_i(V_2)$. QED

LEMMA 5.9.2. The following is provable in ZFC. Let S be a closed set of infinite ordinals, none of which are strongly inaccessible cardinals. Then ¬R(S,3,5).

Proof: Let S be as given, and assume R(S,3,5). Then $|S| \geq 5$. We assume that this S has been chosen so that $\max(S) = \alpha$ is least possible. Then

i. S is a closed set of infinite ordinals with $\max(S) = \alpha$.
ii. S contains no strongly inaccessible cardinals.
iii. R(S,3,5).
iv. If S' is a closed set of infinite ordinals containing no strongly inaccessible cardinals, $\max(S') < \alpha$, then ¬R(S',3,5).

In particular,

v. For all $\delta < \alpha$, $\neg R(S \cap \delta+1,3,5)$.

We will obtain a contradiction. Note that α is infinite, but not a strongly inaccessible cardinal. By i) and $|S| \geq 5$, we see that $\alpha > \omega$.

case 1. α is a limit ordinal, but not a regular cardinal. Let $cf(\alpha) = \beta < \alpha$, and let $\{\alpha_\gamma: \gamma < \beta\}$ be a strictly increasing transfinite sequence of ordinals that forms an unbounded subset of α, where $\alpha_0 > \beta$. Note that β is a regular cardinal.

For $\delta < \alpha$, we write $\tau[\delta]$ for the least γ such that $\delta \leq \alpha_\gamma$.

For each $\gamma < \beta$, let $f_\gamma:[S \cap \alpha_\gamma+1]^3 \to On$ be regressive, where there is no min homogenous $E \in [S \cap \alpha_\gamma+1]^5$ for f_γ.

Let $g:[S]^3 \to On$ be defined as follows. $g(x,y,z) = f_{\tau[z]}(x,y,z)$ if $z < \alpha$; 0 otherwise. Note that in the first case, $z < \alpha$, we have $z \leq \alpha_{\tau[z]} < \alpha$, and $x,y,z \in S \cap \alpha_{\tau[z]}+1$. Hence in the first case, $f_{\tau[z]}(x,y,z)$ is defined.

Let $h:[S]^3 \rightarrow On$ be defined by $h(x,y,z) = \tau[y]$ if $\tau[y] < x$; 0 otherwise.

Let $h':[S]^3 \rightarrow On$ be defined by $h'(x,y,z) = \tau[z]$ if $\tau[z] < x$; 0 otherwise.

Let $J:[S]^3 \rightarrow On$ be defined by $J(x,y,z) = 1$ if $z < \alpha$; 0 otherwise.

Let $K:[S]^3 \rightarrow On$ be defined by $K(x,y,z) = 1$ if $y < \beta$; 0 otherwise.

Let $T:[S]^3 \rightarrow On$ be defined by $T(x,y,z) = 1$ if $z < \beta$; 0 otherwise.

Obviously g,h,h',J,K,T are regressive. By R(S,3,5) and Lemma 5.9.1, let $E \in [S]^5$ be min homogenous for g,h,h',J,K,T.

Write $E = \{x,y,z,w,u\}_<$. Suppose $u = \alpha$. Then $J(x,y,u) = J(x,y,w) = 0$, and so $w = u = \alpha$, which is impossible. Hence $u < \alpha$.

Now suppose $y < \beta$. Then $K(x,y,z) = K(x,z,u) = 1$, and so $z < \beta$. Hence $T(x,y,z) = T(x,y,u) = 1$. Therefore $u < \beta$. Hence $\tau[b] = 0$ for all $b \in E$.

We now claim that E is min homogenous for f_0. To see this, let $V_1,V_2 \subseteq E$ be 3 element sets with the same min. Since $\tau[\max(V_1)] = \tau[\max(V_2)] = 0$, we see that $g(V_1) = g(V_2) = f_0(V_1) = f_0(V_2)$. This establishes the claim.

Since $y < \beta$, we have $E \subseteq S \cap \alpha_0+1$ (using $\alpha_0 > \beta$). This min homogeneity contradicts the choice of f_0. Hence $y < \beta$ has been refuted.

We have thus shown that $\beta \leq y,z,w,u < \alpha$. Hence $\tau[z],\tau[w],\tau[u] < y$. Since $h'(y,z,w) = h'(y,z,u)$, we have $\tau[w] = \tau[u]$. Since $h(y,z,w) = h(y,w,u)$, we have $\tau[z] = \tau[w]$.

We claim that E is min homogenous for $f_{\tau[u]}$. To see this, let $V_1,V_2 \subseteq E$ be 3 element sets with the same min. Then $\tau[\max(V_1)] = \tau[\max(V_2)] = \tau[u]$. Hence $g(V_1) = g(V_2) = f_{\tau[u]}(V_1) = f_{\tau[u]}(V_2)$. This establishes the claim. This min homogeneity contradicts the choice of $f_{\tau[u]}$.

case 2. α is a regular cardinal or a successor ordinal. In an abuse of notation, we reuse several letters from case 1.

Since $\alpha > \omega$ is not strongly inaccessible, let $\beta < \alpha$, $2^\beta \geq \alpha$. Let $K:\alpha \to \wp(\beta)$ be one-one, where $\wp(\beta)$ is the power set of β. Obviously $\beta \geq \omega$.

Let $f:[S \cap \beta+1]^3 \to On$ be regressive, where there is no min homogenous $E \in [S \cap \beta+1]^5$ for f.

Let $f':[S]^3 \to On$ extend f with the default value 0.

Let $g:[S]^3 \to On$ be defined by $g(x,y,z) = \min(K(y) \Delta K(z))$ if this min is < x; 0 otherwise. Since K is one-one, we are not taking min of the empty set, and so g is well defined.

Let $h:[S]^3 \to On$ be defined by $h(x,y,z) = 1$ if $y \leq \beta$; 0 otherwise.

Let $h':[S]^3 \to On$ be defined by $h'(x,y,z) = 1$ if $z \leq \beta$; 0 otherwise.

Obviously f',g,h,h' are regressive. By R(S,3,5) and Lemma 5.9.1, let $E \in [S]^5$ be min homogenous for f',g,h,h'. Write $E = \{x,y,z,w,u\}_<$. If $y \leq \beta$ then $h(x,y,z) = 1$, and hence $h(x,w,u) = 1$. Therefore $w \leq \beta$. Also $h'(x,y,w) = 1$. Hence $h'(x,y,u) = 1$, and so $u \leq \beta$. Since E is min homogenous for f', clearly E is min homogenous for f (using $u \leq \beta$). This contradicts the choice of f.

So we have established that $y > \beta$. Note that

$$g(y,z,w) = \min(K(z) \Delta K(w))$$
$$g(y,z,u) = \min(K(z) \Delta K(u))$$
$$g(y,w,u) = \min(K(w) \Delta K(u))$$

since K is one-one, and these min's are $< \beta < y$. Therefore

$$g(y,z,w) = g(y,z,u) = g(y,w,u).$$
$$\min(K(z) \Delta K(w)) = \min(K(z) \Delta K(u)) = \min(K(w) \Delta K(u)).$$

This is a contradiction. Hence the Lemma is proved. QED

LEMMA 5.9.3. The following is provable in ZFC. Let $k \geq 0$ and S be a closed set of infinite ordinals, none of which are strongly k-Mahlo cardinals. Then $\neg R(S,k+3,k+5)$.

Proof: We proceed by induction on $k \geq 0$. The case $k = 0$ is from Lemma 5.9.2. Suppose this is true for a fixed $k \geq 0$. We want to prove this for k+1.

Assume this is false for k+1, $k \geq 0$. As in Lemma 5.9.2, we minimize max(S). Thus we start with the following assumptions, and derive a contradiction:

i. S is a closed set of infinite ordinals with $\max(S) = \alpha$,
ii. S contains no strongly (k+1)-Mahlo cardinals.
iii. R(S,k+4,k+6).
iv. If S' is a closed set of infinite ordinals containing no strongly (k+1)-Mahlo cardinals, $\max(S') < \alpha$, then $\neg R(S',k+4,k+6)$.
v. If S' is a closed set of infinite ordinals containing no strongly k-Mahlo cardinals, then $\neg R(S',k+3,k+5)$.

In particular,

vi. For all $\beta < \alpha$, $\neg R(S \cap \beta+1,k+4,k+6)$.

We will obtain a contradiction. Note that α is infinite but not a strongly (k+1)-Mahlo cardinal. By iii), $|S| \geq k+6$, and $\alpha > \omega$.

We first prove that α is a limit ordinal. Suppose $\alpha = \beta+1$. Then $S \cap \beta+1 = S \cap \alpha = S\backslash\{\alpha\}$, and so by vi), $\neg R(S\backslash\{\alpha\},k+4,k+6)$.

Let $G:[S\backslash\{\alpha\}]^{k+4} \to On$ be regressive, where there is no min homogenous $E \in [S\backslash\{\alpha\}]^{k+6}$ for G.

Let $G^*:[S]^{k+4} \to On$ extend G with default value 0.

Let $H:[S]^{k+4} \to On$ be defined by $H(x_1,...,x_{k+4}) = 1$ if $x_{k+4} = \alpha$; 0 otherwise.

Obviously G^*,H are regressive. By R(S,k+4,k+6) and Lemma 5.9.1, let $E \in [S]^{k+6}$ be min homogenous for G^*,H. Write $E = \{u_1,...,u_{k+6}\}_<$.

Suppose $u_{k+6} = \alpha$. Then $H(u_1,...,u_{k+3},u_{k+6}) = 1 = H(u_1,...,u_{k+4})$. Hence $u_{k+4} = u_{k+6} = \alpha$. This is impossible. Hence $u_{k+6} < \alpha$, $\{u_1,...,u_{k+6}\} \subseteq S\backslash\{\alpha\}$. Obviously $\{u_1,...,u_{k+6}\}$ is min homogenous for G. This is a contradiction.

Thus we have shown that α is a limit ordinal $> \omega$.

Since α is not strongly (k+1)-Mahlo, let A be a closed and unbounded subset of $[\omega,\alpha]$, where $\omega \in A$, and no element of A is a strongly k-Mahlo cardinal.

By assumptions vi,v, for each $\beta < \alpha$, let

i) $f_\beta:[S \cap \beta+1]^{k+4} \to On$ be regressive, where there is no min homogenous $E \in [S \cap \beta+1]^{k+6}$ for f_β.
ii) $g_\beta:[A \cap \beta+1]^{k+3} \to On$ be regressive, where there is no min homogenous $E \in [A]^{k+5}$ for g_β.

For all $x \in [\omega,\alpha)$, let $\beta[x]$ be the greatest $\beta \in A$ such that $\beta \leq x$. Let $\gamma[x]$ be the least $\gamma \in A$ such that $x < \gamma$.

Let $f':[S]^{k+4} \to On$ be defined by $f'(x_1,\ldots,x_{k+4}) = f_{\gamma[x\_k+4]}(x_1,\ldots,x_{k+4})$ if $x_{k+4} < \alpha$; 0 otherwise.

Let $g':[S]^{k+4} \to On$ be defined by $g'(x_1,\ldots,x_{k+4}) = g_{\beta[x\_k+4]}(\beta[x_1],\ldots,\beta[x_{k+3}])$ if $x_{k+4} \in [\omega,\alpha) \wedge \beta[x_1] < \ldots < \beta[x_{k+4}]$; 0 otherwise.

Let $h:[S]^{k+4} \to On$ be defined by $h(x_1,\ldots,x_{k+4}) = 1$ if $x_{k+4} = \alpha$; 0 otherwise.

For $1 \leq i \leq k+3$, let $J_i:[S]^{k+4} \to On$ be defined by

$$J_i(x_1,\ldots,x_{k+4}) = 1 \text{ if } \beta[x_i] < \beta[x_{i+1}]; \ 0 \text{ otherwise.}$$

Obviously $f',g',h,J_1,\ldots,J_{k+3}$ are regressive. By R(S,k+4,k+6) and Lemma 5.9.1, let $E \in [S]^{k+6}$ be min homogenous for $f',g',h,J_1,\ldots,J_{k+3}$. Write $E = \{u_1,\ldots,u_{k+6}\}_<$. Obviously, u_1 is infinite, and so $\beta[u_1]$ is defined.

Suppose $u_{k+6} = \alpha$. Then $h(u_1,\ldots,u_{k+3},u_{k+6}) = h(u_1,\ldots,u_{k+3},u_{k+5}) = 1$, and so $u_{k+5} = \alpha$. This is impossible. Hence $u_{k+6} < \alpha$.

Suppose $\beta[u_i] = \beta[u_{i+1}] < \beta[u_{i+2}]$, for some $1 \leq i \leq k+2$. Then $J_i(u_1,\ldots,u_{k+4}) = 0 \wedge J_i(u_1,\ldots,u_i,u_{i+2},\ldots,u_{k+5}) = 1$. This is a contradiction.

Suppose $\beta[u_i] < \beta[u_{i+1}] = \beta[u_{i+2}]$, for some $2 \leq i \leq k+2$. Then $J_i(u_1,\ldots,u_{k+4}) = 1 \wedge J_i(u_1,\ldots,u_{i-1},u_{i+1},\ldots,u_{k+5}) = 0$. This is also a contradiction.

We claim that

$$1)\ \beta[u_2] = \ldots = \beta[u_{k+4}] \vee \beta[u_1] < \ldots < \beta[u_{k+4}].$$

To see this, suppose $\neg(\beta[u_i] < \beta[u_{i+1}])$, $1 \leq i \leq k+3$. Then $\beta[u_i] = \beta[u_{i+1}]$. Hence $\beta[u_1] = \ldots = \beta[u_i] = \beta[u_{i+1}] = \ldots = \beta[u_{k+4}]$.

Under the first disjunct of 1), $J_{k+3}(u_1,\ldots,u_{k+4}) = 0 = J_{k+3}(u_1,\ldots,u_{k+2},u_{k+4},u_{k+5}) = J_{k+3}(u_1,\ldots,u_{k+2},u_{k+5},u_{k+6})$. Hence $\beta[u_{k+4}] = \beta[u_{k+5}] = \beta[u_{k+6}]$.

Under the second disjunct of 1), $J_{k+3}(u_1,\ldots,u_{k+4}) = 1 = J_{k+3}(u_1,\ldots,u_{k+2},u_{k+4},u_{k+5}) = J_{k+3}(u_1,\ldots,u_{k+2},u_{k+5},u_{k+6})$. Hence $\beta[u_{k+4}] < \beta[u_{k+5}] < \beta[u_{k+6}]$.

We have thus shown that

$$2)\ \beta[u_2] = \ldots = \beta[u_{k+6}] \vee \beta[u_1] < \ldots < \beta[u_{k+6}].$$

case 1. $\beta[u_2] = \ldots = \beta[u_{k+6}]$. We claim that E is min homogenous for $f_{\gamma[u\_k+6]}$. To see this, let $V_1,V_2 \subseteq E$ be k+4 element sets with the same min. Then $\beta[\max(V_1)] = \beta[\max(V_2)] = \beta[u_{k+6}]$, $\gamma[\max(V_1)] = \gamma[\max(V_2)] = \gamma[u_{k+6}]$, $f'(V_1) = f'(V_2)$, and $u_{k+6} < \alpha$. Hence $f_{\gamma[u\_k+6]}(V_1) = f_{\gamma[u\_k+6]}(V_2)$. This establishes the claim. This contradicts the choice of $f_{\gamma[u\_k+6]}$.

case 2. $\beta[u_1] < \ldots < \beta[u_{k+6}]$. We claim that $\beta[u_1],\beta[u_2],\ldots,\beta[u_{k+5}]\}$ is min homogenous for $g_{\beta[u\_k+6]}$. To see this, let $V_1,V_2 \subseteq \{\beta[u_1],\beta[u_2],\ldots,\beta[u_{k+5}]\}$ be k+3 element subsets with the same min. Then $g'(V_1 \cup \{\beta[u_{k+6}]\}) = g'(V_2 \cup \{\beta[u_{k+6}]\}) = g_{\beta[u\_k+6]}(V_1) = g_{\beta[u\_k+6]}(V_2)$, using $u_{k+6} < \alpha$. This establishes the claim. Note that $\{\beta[u_1],\beta[u_2],\ldots,\beta[u_{k+5}]\} \subseteq A \cap \beta[u_{k+6}]+1$, $u_{k+6} < \alpha$, $\beta[u_{k+6}] < \alpha$. But this contradicts the choice of $g_{\beta[u\_k+6]}$.

We have derived the required contradiction, and the Lemma has been proved. QED

LEMMA 5.9.4. The following is provable in ZFC. For all integers $k \geq 0$ and ordinals α, if $R(\alpha+1\backslash\omega,k+3,k+5)$ then there is a strongly k-Mahlo cardinal $\leq \alpha$.

Proof: Let $k \geq 0$ and $R(\alpha+1\backslash\omega,k+3,k+5)$. Note that $S = \alpha+1\backslash\omega$ is a closed set of infinite ordinals. By Lemma 5.9.3, if none of them are strongly k-Mahlo cardinals, then $\neg R(S,k+3,k+5)$. Hence $\alpha+1\backslash\omega$ contains a strongly k-Mahlo cardinal. Therefore there is a strongly k-Mahlo cardinal $\leq \alpha$. QED

We will not need the following result, which is of independent interest.

THEOREM 5.9.5. The following is provable in ZFC. Let $k < \omega$ and α be an ordinal. Then $R(\alpha\backslash\omega,k+3,k+5)$ if and only if there is a strongly k-Mahlo cardinal $\leq \alpha$.

Proof: Let $R(\alpha\backslash\omega,k+3,k+5)$. It is immediate that $R(\alpha+1\backslash\omega,k+3,k+5)$. By Lemma 5.9.4, there is a strongly k-Mahlo cardinal $\leq \alpha$.

Now let $\kappa \leq \alpha$ be strongly k-Mahlo. It follows easily from [Sc74] that $R(\kappa,k+3,k+5)$. Hence $R(\alpha,k+3,k+5)$. QED

We now return to the model M^+ of ZFC + V = L + $TR(\Pi^0_1,L)$ given by Lemma 5.8.37.

LEMMA 5.9.6. Let $k,r \geq 1$ be standard integers. Then $R(d_{r+2}+1\backslash\omega,k,r)$ holds in M^+.

Proof: Let k be as given. We argue in M^+. By Lemma 5.8.37, M^+ satisfies ZFC + V = L.

Suppose $R(d_{r+2}+1\backslash\omega,k,r)$ fails in M^+. We can choose $f:[d_{r+2}+1\backslash\omega]^k \to On$ to be least in the constructible hierarchy such that f is regressive and there is no $E \in [d_{r+2}+1\backslash\omega]^r$ that is min homogenous for f. Note that f is M^+ definable from d_{r+2}.

We claim that $\{d_2,\ldots,d_{r+1}\}$ is min homogenous for f. To see this, let $2 \leq i_1 < \ldots < i_k \leq r+1$, and $2 \leq j_1 < \ldots < j_k \leq r+1$, where $i_1 = j_1$. By Lemma 5.8.37 ii), for all $\alpha \leq d_{i\_1}$,

$$f(d_{i\_1},\ldots,d_{i\_k}) = \alpha \leftrightarrow f(d_{j\_1},\ldots,d_{j\_k}) = \alpha.$$

Since f is regressive, choose $\alpha = f(d_{i\_1},\ldots,d_{i\_k}) < d_{i\_1}$. By Lemma 5.8.37 ii),

$$f(d_{i\_1},\ldots,d_{i\_k}) = \alpha \leftrightarrow f(d_{j\_1},\ldots,d_{j\_k}) = \alpha.$$
$$f(d_{j\_1},\ldots,d_{j\_k}) = \alpha = f(d_{i\_1},\ldots,d_{i\_k}).$$

Note that by Lemma 5.8.37, $d_2 > \omega$. Hence $\{d_2,\ldots,d_{r+1}\} \subseteq d_{r+2}+1\backslash\omega$ is min homogenous for f. But this contradicts the choice of f. QED

LEMMA 5.9.7. Let k ≥ 0 be a standard integer. Then "there exists a strongly k-Mahlo cardinal" holds in M^+. As a consequence, ZFC + V = L + {there exists a strongly k-Mahlo cardinal}$_k$ + TR(Π^0_1,L) is consistent.

Proof: Immediate from Lemmas 5.8.37, 5.9.4, and 5.9.6. QED

LEMMA 5.9.8. ZFC proves that Proposition C implies 1-Con(SMAH).

Proof: We argue in ZFC + Proposition C. Now the entire reversal from section 5.1 through Lemma 5.9.7 was conducted within ZFC. So M^+ is available, and we know that SMAH holds in M^+. Let SMAH prove φ, where φ is a Σ^0_1 sentence of L. Since SMAH holds in M^+, so does φ. If φ is false then ¬φ ∈ TR(Π^0_1,L), in which case ¬φ holds in M^+. This contradicts that φ holds in M^+. Hence φ is true. (Here the outermost ¬ in ¬φ is pushed inside). QED

THEOREM 5.9.9. None of Propositions A,B,C are provable in SMAH, provided MAH is consistent. They are provable in MAH^+. These claims are provable in RCA_0.

Proof: Suppose Proposition C is provable in SMAH. By Lemma 5.9.8, SMAH proves the consistency of SMAH. By Gödel's second incompleteness theorem, SMAH is inconsistent. By the last claim of Theorem 4.1.7, it follows that MAH is inconsistent. Both Propositions A,B each imply Proposition C over RCA_0 (see Lemma 4.2.1).

The second claim is by Theorem 4.2.26. These claims are provable in RCA_0 since RCA_0 can recognize proofs, and prove the Gödel second incompleteness theorem. QED

We now provide more refined information.

Recall the formal system ACA' from Definition 1.4.1.

LEMMA 5.9.10. The derivation of 1-Con(SMAH) from Proposition C, in sections 5.1-5.9, can be formalized in ACA'. I.e., ACA' proves that each of Propositions A,B,C implies 1-Con(SMAH).

Proof: Most of the development lies within RCA_0. But since we are stuck using ACA' already in section 5.2, we will use the stronger fragment ACA_0 of ACA' instead of RCA_0 for the discussion. We regard Proposition C, which is readily formalized in ACA_0 (or even RCA_0), as the hypothesis, which we take as implicit in the section by section analysis below.

section 5.1. All within ACA_0.

section 5.2. All within ACA_0 except Lemma 5.2.5. Lemma 5.2.5 is a sharp form of the usual Ramsey theorem on N. This is provable in ACA'. In fact, it is provably equivalent to ACA' over RCA_0. Hence Lemma 5.2.12 is provable in ACA'.

section 5.3. All within ACA_0, from Lemma 5.2.12. In the proof of Lemma 5.3.3, we apply the compactness theorem to a set T of sentences that is Π^0_1. T has bounded quantifier complexity, and the proof that every finite subset of T has a model, and the proof that every finite subset of T has a model can be formulated and proved in ACA_0. The application of compactness to obtain a model M of T can be formalized in ACA_0. In fact, we obtain a model M of T with a satisfaction relation, within ACA_0. In the proof, we then adjust M by taking an initial segment. This construction can also be formalized in ACA_0. However, we lose the satisfaction relation within ACA_0, and cannot recover it even within ACA'. Nevertheless, we retain a satisfaction relation for all formulas whose quantifiers are bounded in the adjusted M, since this restricted satisfaction relation is obtained from the satisfaction relation for the original unadjusted M in ACA_0. The statement of Lemma 5.3.18 has bounded quantifier complexity, and so is formalizable in th language of ACA_0. We conclude that Lemma 5.3.18, with bounded satisfaction relation, is provable in ACA_0 from Lemma 5.2.12. This bounded satisfaction relation incorporates the constants from M.

section 5.4. All within ACA_0, from Lemma 5.3.18. The quantifiers in E formulas of L(E) are required to be bounded in the structure M. Hence the E formulas of L(E) are covered by the bounded satisfaction relation for M. Since only E formulas of L(E) are considered, Lemma 5.4.17 is provable in ACA_0 from Lemma 5.3.18.

section 5.5. All within ACA', from Lemma 5.4.17. Lemma 5.5.1 involves arbitrary formulas of L(E), and so it needs ACA' to formulate, using partial satisfaction relations for M. The induction hypothesis as stated in the proof of Lemma 5.5.1 is Σ^1_1 (or Π^1_1), and therefore the induction, as it stands, is not formalizable in ACA'. However, this can be fixed. We fix n, the number of quantifiers, and form the satisfaction relation for n quantifier formulas, for M, in

ACA'. We then prove the displayed equivalence by all 0 ≤ n' ≤ n by induction on n'. This modification reduces the induction to an arithmetical induction, well within ACA'. Note that we can use Lemma 5.5.1 to construct the full satisfaction relation for M from the bounded satisfaction relation for M, within ACA_0. Also, the construction of the sets X_k can easily be formalized in ACA'. In the proof of Lemma 5.5.4, second order quantification in formulas of the language L*(E) are removed. This removal allows us to construct the satisfaction relation for M* from the satisfaction relation for M, within ACA_0. This allows us to argue freely within ACA_0 throughout the rest of section 5.5. We conclude that Lemma 5.5.8, with satisfaction relation, is provable in ACA' from Lemma 5.4.17.

section 5.6. The formalization in ACA_0 is straightforward through the development of internal arithmetic in Lemma 5.6.12, via the internal structure M(I). The substructure M|rng(h) is defined arithmetically, with an arithmetic isomorphism from M(I) onto M|rng(h). The satisfaction relation for M|rng(h) is constructed from the satisfaction relation for M(I) via the isomorphism, within ACA_0. Hence the statement and proof that M|rng(h) satisfies PA(L) + TR(Π^0_1,L) lie within ACA_0. It immediately follows, in ACA_0, that M(I) satisfies PA(L) + TR(Π^0_1,L). It is clear that the use of h and M|rng(h) is an unnecessary convenience that causes no difficulties within ACA_0. The conversion to linearly ordered set theory is by explicit definition, and so Lemma 5.6.20, with satisfaction relation, is provable in ACA_0 from Lemma 5.5.8.

section 5.7. The development through Lemma 5.7.28 is internal to M#, and so cause no difficulties within ACA_0. In the subsequent construction of M^, we use equivalence classes under a definable equivalence relation as points. Instead of using the actual equivalence classes, we can instead use the equivalence relation as the equality relation. The sets Y_k become families of relations that respect the equality relation. The construction is by explicit definition, and so we obtain a version of the M^ of Lemma 5.7.30 using this equality relation, with a satisfaction relation. We can then factor out by the equality relation, using a set of representatives of the equivalence classes. Specifically, taking the numerically least element of each equivalence class as the representative of that equivalence class. All of this can easily be done in ACA_0. Hence Lemma 5.7.30, with satisfaction relation, is provable in ACA_0 from Lemma 5.6.20.

section 5.8. All within ACA_0 from Lemma 5.7.30. This is an inner model construction that is totally definable. Hence Lemma 5.8.37, with satisfaction relation, is provable in ACA_0 from Lemma 5.7.30.

section 5.9. Using the satisfaction relation for M^+, we see that M^+ satisfies ZFC + V = L + SMAH + Π^0_1(L), within ACA_0. Again using the satisfaction relation for M^+, we have 1-Con(SMAH), within ACA_0.

From these considerations, we see that ACA' + Proposition C proves 1-Con(SMAH). Since B → A → C in RCA_0, we have that ACA' + Proposition A, and ACA' + Proposition B, also prove 1-Con(SMAH). QED

We conjecture that RCA_0 proves that Propositions A,B,C each imply 1-Con(SMAH).

DEFINITION 5.9.8. The system EFA = exponential function arithmetic is in the language 0,<,S,+,-,•,↑,log, and consists of the axioms for successor, defining equations for <,+,-,•,↑,log and induction for all Δ_0 formulas in 0,<,S,+,-,•,↑,log.

EFA is essentially the same as the system $I\Sigma_0$(exp). See [HP93].

Also recall the following result from Chapter 4.

THEOREM 4.4.11. Propositions A,B,C are provable in ACA' + 1-Con(MAH).

Thus we have

THEOREM 5.9.11. ACA' proves the equivalence of each of Propositions A,B,C and 1-Con(MAH), 1-Con(SMAH).

Proof: We have only to remark that EFA proves 1-Con(MAH) → 1-Con(SMAH). This is from Lemma 4.1.7. QED

THEOREM 5.9.12. None of Propositions A,B,C are provable in any set of consequences of SMAH that is consistent with ACA'. The preceding claim is provable in RCA_0. For finite sets of consequences, the first claim is provable in EFA.

Proof: Suppose Proposition C is provable in T, where

SMAH proves T.
T + ACA’ is consistent.
T proves Proposition C.

Let T* be finitely axiomatized, where

SMAH proves T*.
T* + ACA' is consistent.
T* proves Proposition C.

By Theorem 5.9.11, T* proves 1-Con(SMAH). In particular, T* proves Con(T* + ACA'), using that T* + ACA' is finite, and SMAH proves T* + ACA'. By Gödel’s second incompleteness theorem, T* + ACA' is inconsistent. This is a contradiction. The argument is obviously formalizable in RCA_0. If T is already finite, then there is no need for RCA_0, and we can use EFA = $I\Sigma_0$(exp) instead. QED

CHAPTER 6. FURTHER RESULTS

6.1. Propositions D-H.

Our treatment of Propositions A,B,C culminated with Theorems 5.9.9, 5.9.11, and 5.9.12 at the end of Chapter 5.

In this section, we consider five Propositions D-H that have the same metamathematical properties as Propositions A,B,C. We will also consider some variants of Propositions D-H that do not share these properties, or whose status is left open.

Recall the main theorems of Chapter 5 (in section 5.9), which are Theorems 5.9.9, 5.9.11, and 5.9.12. Examination of the proofs of these three Theorems reveal that Theorem 5.9.11 with 1-Con(SMAH) is the key. If ACA’ proves the equivalence of a statement with 1-Con(SMAH) then all of the other properties provided by these three Theorems quickly follow.

Accordingly, we establish these same three Theorems for Propositions D-H by showing that they are also each equivalent to 1-Con(SMAH) over ACA'.

We begin with Proposition D (see below), which is a sharpening of Proposition B. Proposition D immediately implies Propositions A-C over RCA_0.

Note that Propositions A-C are based on ELG. Examination of the proof of Proposition B in Chapter 4 shows that we can separately weaken the conditions on f,g in different ways. Also, we can place an inclusion condition on the starting set A_1. As usual, we use | | for the sup norm, or max. This results in Proposition D below.

DEFINITION 6.1.1. We say that f is linearly bounded if and only if f ∈ MF, and there exists d such that for all x ∈ dom(f),

$$f(x) \leq d|x|.$$

We let LB be the set of all linearly bounded f.

DEFINITION 6.1.2. We say that g is expansive if and only if g ∈ MF, and there exists c > 1 such that for all but finitely many x ∈ dom(f),

$$c|x| \leq g(x)$$

We let EXPN be the set of all expansive g.

Recall the definitions of MF, SD (Definition 1.1.2), and ELG, EVSD (Definitions 2.1, 2.2).

PROPOSITION D. Let f ∈ LB ∩ EVSD, g ∈ EXPN, E ⊆ N be infinite, and n ≥ 1. There exist infinite $A_1 \subseteq \ldots \subseteq A_n \subseteq N$ such that
i) for all $1 \leq i < n$, $fA_i \subseteq A_{i+1} \cup. gA_{i+1}$;
ii) $A_1 \cap fA_n = \emptyset$;
iii) $A_1 \subseteq E$.

Note that ELG ⊆ LB ∩ EVSD ∩ EXPAN, and so Proposition D immediately implies Proposition B.

Proposition D is the strongest Proposition that we prove in this book (from large cardinals).

Recall that Propositions A-C are official statements of BRT. More accurately, Proposition B is really an infinite collection of statements of BRT.

Proposition D not a statement (or statements) of BRT for two reasons.

a. There is no common set of functions used for f,g (asymmetry).
b. The set E is used as data, rather than just f,g.

Features a,b both suggest very natural expansions of BRT. Feature a suggests "mixed BRT", where one uses several classes of functions instead of just one. One can go further and use several classes of sets as well.

Feature b in Proposition D suggests another very natural expansion of BRT. In BRT, we consider statements of the form

given functions there are sets such that
a given Boolean relation holds between the sets
and their images under the functions.

We can expand BRT with

given functions and sets there are sets such that
a given Boolean relation holds between the sets
and their images under the functions.

We will not pursue such expansions of BRT in this book.

We remark that feature b can be removed (in some contexts such as here) by introducing a new function h and asserting that $A_1 \subseteq hN$ (obviously $hN = rng(h)$).

We now prove Proposition D in $SMAH^+$ by adapting the proof of Proposition B in $SMAH^+$ given in section 4.2.

We fix f,g,E as given by Proposition D. Analogously to section 4.2, we let f be p-ary, g be q-ary. We fix an integer $b \geq 1$ such that for all $x \in N^p$ and $y \in N^q$,

i. if $|x|,|y| > b$ then

$$|x| < f(x) \leq b|x|.$$
$$(1 + 1/b)|y| \leq g(y).$$

ii. if $|x| \leq b$ then $f(x) \leq b^2$.

Note how our inequalities are weaker than those used in section 4.2.

We also fix $n \geq 1$ and a strongly p^{n-1}-Mahlo cardinal κ.

The first place in section 4.2 that needs to be modified is at Lemma 4.2.2. Here we must use the given infinite set $E \subseteq N$.

LEMMA 4.2.2'. There exist infinite sets $E \supseteq E_0 \supseteq E_1 \supseteq \ldots$ indexed by N, such that for all $i \geq 0$, $\varphi \in AF(L)$, $lth(\varphi) \leq i$, and increasing partial $h_1,h_2:V(L) \to N$ adequate for φ with $rng(h_1),rng(h_2) \subseteq E_i$, we have $Sat(M,\varphi,h_1) \leftrightarrow Sat(M,\varphi,h_2)$.

Proof: See the proof of Lemma 4.2.2. QED

Lemma 4.2.3 do not involve our inequalities i,ii, and therefore require no modification.

We need to sharpen Lemma 4.2.4 for later purposes, since we do not have an upper bound for g. We use the # notation that was introduced much later just before Lemma 4.2.16.

LEMMA 4.2.4'. Let $\varphi \in AS(L^*)$. $Sat(M^*,\varphi)$ if and only if $\varphi \in T$. $<^*$ is a linear ordering on N^*. Let $n \geq 0$, $t \in CT(L^*)$, $\#(t) \leq n$. Then $t < c_{n+1} \in T$.

Proof: For the first claim, see the proof of Lemma 4.2.4. For the last claim, let $i = lth(t < c_{n+1})$. The unique increasing bijection $h:V(L) \to E_i$ has $Val(M,t',h) < h(v_{n+1})$, where t' is the result of replacing each c_i by v_i, using the indiscernibility of E_i. Argue as before. QED

Lemmas 4.2.5 - 4.2.8 do not involve our inequalities i,ii, and therefore require no modification.

We sharpen Lemma 4.2.9 for later purposes, since we do not have an upper bound for g.

LEMMA 4.2.9'. These definitions of $<^{**}$, $+^{**}$, f^{**}, g^{**} are well defined. Let $t \in CT(L^{**})$, $\#(t) \leq \alpha$. Then $t <^{**} c_{\alpha+1}{}^{**}$.

Proof: Use Lemma 4.2.4' and the proof of Lemma 4.2.9. QED

Lemmas 4.2.10' - 4.2.14' do not involve our inequalities i,ii.

We need to weaken Lemma 4.2.15, in light of our inequalities i,ii.

LEMMA 4.2.15′. Let $x_1,...,x_p,y_1,...,y_q \in N^{**}$, where $|x_1,...,x_p|,|y_1,...,y_q| >^{**} b\hat{}$. Then

$$|x_1,...,x_p| <^{**} f^{**}(x_1,...,x_p) \leq^{**} b|x_1,...,x_p|.$$
$$(1 + 1/b)|y_1,...,y_q| \leq^{**} g^{**}(y_1,...,y_q).$$

If $|x_1,...,x_p| \leq^{**} b\hat{}$ then $f(x_1,...,x_p) \leq^{**} b^2\hat{}$.

Proof: See the proof of Lemma 4.2.15. QED

We aim for a modification of the crucial well foundedness given by Lemma 4.2.19. This was stated using all elements of N**. In other words, for all terms in CT(L**). We cannot establish such a well foundedness result in the present setting for all terms in CT(L**). We have weakened the inequalities for f**,g** too much.

However, we can establish this well foundedness result for the restricted class of terms, CT(L**\g) consisting of all closed terms of L** in which g does not appear.

LEMMA 4.2.16′. Let $t \in CT(L^{**})$. $\#(t) = -1 \leftrightarrow Val(M^{**},t)$ is standard. Suppose $\#(t) = c_\alpha$. Then $c_\alpha^{**} \leq Val(M^{**},t) <^{**} c_{\alpha+1}^{**}$. Let $s \in CT(L^{**}\backslash g)$. Suppose $\#(s) = c_\alpha$. There exists a positive integer d such that $c_\alpha^{**} \leq^{**} Val(M^{**},s) <^{**} dc_\alpha^{**} <^{**} c_{\alpha+1}^{**}$.

Proof: For the equivalence in the first claim, see the proof of Lemma 4.2.16. For the remaining claims, use induction on s,t, Lemmas 4.2.4′, 4.2.9′, 4.2.15′, and the proof of Lemma 4.2.16. QED

Lemmas 4.2.17, 4.2.18 do not involve our inequalities i,ii, and therefore require no modification.

DEFINITION 6.1.3. It is convenient to write VCT(L**\g) for the set of values of terms in CT(L**\g).

DEFINITION 6.1.4. Let s be a rational number. We write $<_s^{**\prime}$ for the relation on VCT(L**\g) given by $x <_s^{**} y \leftrightarrow sx <^{**} y$.

LEMMA 4.2.19'. Let s be a rational number > 1. There exists $k \geq 1$ such that for all $x_1 <_s**' x_2 <_s**' \ldots <_s**' x_k$, we have $2x_1 <**' x_k$.

Proof: See the proof of Lemma 4.2.19. QED

Lemma 4.2.20 has to be weakened as follows.

LEMMA 4.2.20'. Let s be a rational number > 1. The relation $<_s**'$ on VCT(L**\g) is transitive, irreflexive, and well founded.

Proof: We adapt the proof of Lemma 4.2.20 with the following modification. In the fourth paragraph, $d \in N\backslash\{0\}$ is fixed such that Val(M**,t) <** dc_α**, using Lemma 4.2.16. Here we use Lemma 4.2.16' under the assumption that t ∈ VCT(L**\g). QED

DEFINITION 6.1.5. Let s = 1 + 1/2b for using Lemma 4.2.20'.

LEMMA 4.2.21'. There is a unique set W such that W = {x ∈ VCT(L**\g) ∩ nst(M**): x ∉ g**W}. For all $\alpha < \kappa$, c_α** ∉ rng(f**),rng(g**). In particular, each c_α** ∈ W.

Proof: Note that g**:NST(M**)^q → NST(M**), but g**:(VCT(L**\g) ∩ nst(M**))^q → VCT(L**\g) ∩ nst(M**) may be false. So we regard g** as a partial function from (VCTM(L**\g) ∩ nst(M**))^q into VCT(L**\g) ∩ nst(M*). Note that g** is strictly dominating from nst(M**) into nst(M**), in the sense of $<_s$**, by 4.2.15'. Since $<_s$** is well founded on VCT(L**\g) ∩ nst(M**), we can apply the Complementation Theorem for Well Founded Relations, proved in section 1.3 to obtain the first claim.

For the second claim, write c_α** = f**$(x_1,\ldots,x_p)$. By Lemma 4.2.15', each x_i <** c_α**. By Lemma 4.2.18, f**$(x_1,\ldots,x_p)$ <** c_α**. This is a contradiction. The same argument applies to g**.

The third claim follows immediately from the second claim. QED

Lemma 4.2.22 - Theorem 4.2.26, Corollary 4.2.27, go through using the present W ⊆ VCT(L**\g) ∩ nst(M**), instead of the W ⊆ nst(M**) in section 4.2. We have shown the following.

THEOREM 6.1.1. Proposition D is provable in $SMAH^+$. For fixed arity of f and fixed $n \geq 1$, Proposition D is provable in SMAH.

We now adapt section 4.4 to Proposition D. We redefine the p,q,b-structures, p,q,b;r-structures, p,q,b;n,r-special structures, p,q,b;r-types, p,q,b;n,r-special types, to take into account the weaker inequalities now placed on f,g. Specifically, clauses 4,5 in the definition of p,q,b-structure should now read

4′. f* obeys the above two inequalities for membership in LB(p,b) ∩ EVSD(p,b) given above right after we introduced Proposition D, internally in M*.
5′. g* obeys the above two inequalities for membership in EXPN(q,b), given above right after we introduced Proposition D, internally in M*.

These modified notions are written with ′.

The entire development of section 4.4 goes through without modification until we arrive at Theorem 4.4.11.

THEOREM 4.4.11′. Proposition D is provable in ACA′ + 1-Con(MAH).

Proof: We argue in ACA′ + 1-Con(MAH). Let $p,q,b,n \geq 1$, and $f \in LB(p,b) \cap EVSD(p,b)$, $g \in EXPN(q,b)$. Let r be given by Lemma 4.4.10′. By Ramsey's theorem for 2r-tuples in ACA′, we can find a p,q,b;r-structure′ M = $(N,0,1,<,+,f,g,c_0,c_1,...)$, where $c_0,c_1,... \in E$. Let τ be its p,q,b;r-type′. By Lemma 4.4.10′, τ is a p,q,b,n,r-special′ type. By Lemma 4.4.2, M is a p,q,b;r;n-special' structure. Let $D_1 \subseteq ... \subseteq D_n \subseteq N$, where $D_1 \subseteq \{c_0,c_1,...\} \subseteq E$, and each $fD_i \subseteq D_{i+1} \cup. gD_{i+1}$, and $D_1 \cap fD_n = \emptyset$. This is Proposition D, thus concluding the proof. QED

THEOREM 6.1.2. ACA′ proves the equivalence of Proposition D and 1-Con(MAH), 1-Con(SMAH).

Proof: This is immediate from Theorems 4.4.11′, 5.9.11, and that Proposition D immediately implies Proposition B. QED

Recall that Proposition D is the strongest Proposition that we prove in this book (using large cardinals).

There are some natural variants of Proposition D, some of which are provable in RCA_0, and some of which are refutable.

PROPOSITION D[1]. Let $f,g \in EVSD$, $E \subseteq N$ be infinite, and $n \geq 1$. There exist infinite $A_1 \subseteq \ldots \subseteq A_n \subseteq N$ such that
i) for all $1 \leq i < n$, $fA_i \subseteq A_{i+1} \cup. gA_{i+1}$;
ii) $A_1 \cap fA_n = \emptyset$;
iii) $A_1 \subseteq E$.

Proposition D[1] is refutable in RCA_0. In fact, in section 6.3, we refute the following in RCA_0.

PROPOSITION α. For all $f,g \in SD \cap BAF$ there exist $A,B,C \in INF$ such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

Note Proposition α follows immediately from Proposition D[1], even without E. This is because from the former, we get

$$A \cup. fA \subseteq B \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC$$
$$B \subseteq C$$
$$A \cup. fA \subseteq C \cup. gB.$$

Therefore Proposition D[1] is refutable in RCA_0 even if we remove E.

However, we can use EVSD if we drop the inclusions on the A's.

PROPOSITION D[2]. Let $f,g \in EVSD$, $E \subseteq N$ be infinite, and $n \geq 1$. There exist infinite sets $A_1,\ldots,A_n \subseteq N$ such that
i) for all $1 \leq i < n$, $fA_i \subseteq A_{i+1} \cup. gA_{i+1}$;
ii) for all $1 \leq i \leq n$, $A_1 \cap fA_n = \emptyset$;
iii) $A_1 \subseteq E$.

The weakness in Proposition D[2] stems from the fact that we drop the tower condition, and use the same subscript twice on the right sides, and have no tower.

THEOREM 6.1.3. Proposition D[2] is provable in RCA_0.

Proof: Let f,g,E,n be as given. Let $t \gg n \geq 1$. By a straightforward combinatorial argument, for all $t \geq 1$, we can find an infinite $E' \subseteq E$ such that

a. f,g are strictly dominating on the elements of their respective domains whose sup norm is at least $\min(E')$.

b. the values of all terms in f,g and elements of E′, using at most t applications of functions, and at least one application of a function, lie outside E′.

We now inductively define $A_1,...,A_n$. Set $A_1 = E'$. Suppose $A_1,...,A_i$ have been defined for $1 \leq i < n$, where each A_j is an infinite subset of $[\min(E'),\infty)$. Set A_{i+1} to be the unique subset of fA_i such that $fA_i \subseteq A_{i+1} \cup. gA_{i+1}$. This unique A_{i+1} exists by i) above and Lemma 3.3.3. Also A_{i+1} is infinite since fA_i is infinite (using a) above).

It is clear by the construction of the A′s, that all elements of the fA_i and gA_i meet the criterion in b) above for t = n+1, so that their values lie outside $E' = A_1$. This establishes Proposition D[2] in RCA_0. QED

Continuing with our use of EVSD, it is natural to consider the following.

PROPOSITION D[3]. Let $f,g \in$ EVSD and $n \geq 1$. There exist infinite sets $A_1,...,A_n \subseteq N$ such that
i) for all $1 \leq i < j,k \leq n$, $fA_i \subseteq A_j \cup. gA_k$;
ii) $A_1 \cap fA_n = \emptyset$.

However, Proposition α is an obvious consequence of Proposition D[3] even for the case n = 3. So Proposition D[3] is refutable in RCA_0.

PROPOSITION D[4]. Let $f,g \in$ EVSD, $E \subseteq N$ be infinite, and $n \geq 1$. There exist infinite sets $A_1,...,A_n \subseteq N$ such that
i) for all $1 \leq i < j,k \leq n$, $fA_i \subseteq A_j \cup. gA_k$;
ii) $A_1 \subseteq E$.

THEOREM 6.1.4. Proposition D[4] is provable in RCA_0.

Proof: Let f,g,E be as given. Let m be such that f,g are strictly dominating on $[m,\infty)$. Let B be unique such that $B \subseteq [m,\infty) \subseteq B \cup. gB$. Set $A_1 = E \cap [m,\infty)$, $A_2 = ... = A_n = B$. QED

PROPOSITION D[5]. Let $f,g \in$ EVSD (ELG, ELG $\cap$ SD $\cap$ BAF), $E \subseteq N$ be infinite, and $n \geq 1$. There exist $A_1,...,A_n \subseteq N$ such that
i) for all $1 \leq i < j,k \leq n$, $fA_i \subseteq A_j \cup. gA_k$;
ii) for all $1 \leq i \leq n$, $A_i \cap E$ is infinite.

We do not know the status of Proposition D[5], other than it follows immediately from Proposition D.

We now present the remaining Propositions E,F that have the same metamathematical properties as Propositions A,B,C,D. These two propositions use ELG ∩ SD ∩ BAF.

DEFINITION 6.1.6. The powers of 2 are the integers 1,2,4,8,... . For E ⊆ N, we write $2^{(E)}$ for $\{2^n: n \in E\}$.

PROPOSITION E. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A ⊆ B ⊆ C ⊆ N, each containing infinitely many powers of 2, such that

$$fA \subseteq B \cup. gB$$
$$fB \subseteq C \cup. gC.$$

PROPOSITION F. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A ⊆ B ⊆ C ⊆ N, each containing infinitely many powers of 2, such that

$$fA \subseteq C \cup. gB$$
$$fB \subseteq C \cup. gC.$$

PROPOSITION G. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A,B,C ⊆ N, whose intersection contains infinitely many powers of 2, such that

$$fA \subseteq C \cup. gB$$
$$fB \subseteq C \cup. gC.$$

PROPOSITION H. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A,B,C ⊆ N, where A ∩ B contains infinitely many powers of 2, such that

$$fA \subseteq C \cup. gB$$
$$fB \subseteq C \cup. gC.$$

Note that Propositions E-H are statements in BRT, where the BRT setting consists of "subsets of N with infinitely many powers of 2", and ELG ∩ SD ∩ BAF. Propositions E,F,G immediately follow from Proposition D, using $E = 2^{(N)}$.

LEMMA 6.1.5. The following is provable in RCA_0. D → E → F → G → H.

Proof: For D → E, let $E = 2^{(N)}$. For E → F, use the derivation

$$fA \subseteq B \cup. gB$$
$$fB \subseteq C \cup gC$$
$$B \subseteq C$$
$$C \cap gB = \emptyset$$
$$fA \subseteq C \cup. gB.$$

$F \rightarrow G \rightarrow H$ is immediate. QED

We also consider two additional variants.

PROPOSITION E[1]. For all $f,g \in ELG \cap SD \cap BAF$ there exist $A,B,C \subseteq N$, whose intersection contains infinitely many powers of 2, such that

$$fA \subseteq B \cup. gB$$
$$fB \subseteq C \cup. gC.$$

PROPOSITION G[1]. For all $f,g \in ELG \cap SD \cap BAF$ there exist $A,B,C \subseteq N$, each containing infinitely many powers of 2, such that

$$fA \subseteq C \cup. gB$$
$$fB \subseteq C \cup. gC.$$

THEOREM 6.1.6. Proposition E[1] is provable in RCA_0.

Proof: Let f,g,E be as given. We follow the proof of Lemma 3.12.7. In the proof of Theorem 3.2.5, we can arrange that $A \subseteq E$. So in the proof of Lemma 3.12.7, we can assume that $A \subseteq E$. We also have $A \subseteq B$, $A \subseteq C$. QED

We do not know the status of Proposition G[1], even if we use ELG instead of $ELG \cap SD \cap BAF$. Obviously, this follows from Proposition D with $E = 2^{(N)}$.

Until Theorem 6.1.10, we work in RCA_0 and assume Proposition H.

LEMMA 6.1.7. For all $f,g \in ELG \cap SD \cap BAF$ there exist infinite $A,B,C \subseteq N$ such that

$$fA \subseteq C \cup. gB$$
$$fB \subseteq C \cup. gC$$
$$A \subseteq B,2^{(N)}.$$

Proof: Let f,g be as given. Let A,B,C be given by Proposition G. Replace A by $A \cap B \cap 2^{(N)}$, which is infinite. QED

LEMMA 6.1.8. The function $f:N \rightarrow N$ given by $f(n) = 1$ if n is a power of 2; 0 otherwise, lies in BAF.

Proof: Note that n is a power of 2 if and only if $n = 2^{\log(n)}$. QED

LEMMA 5.1.7'. Let $f,g \in ELG \cap SD \cap BAF$. There exist $f',g' \in ELG \cap SD \cap BAF$ such that the following holds. Let $S \subseteq N$.

i) $g'S = g(S^*) \cup 12S+2 \cup (f(S^*) \cap 2^{(N+2)})$.
ii) $f'S = f(S^*) \cup g'S \cup 12f(S^*)+2 \cup 2S^*+1 \cup 3S^*+1$.

Proof: Let $f,g \in ELG \cap SD \cap BAF$, where $f:N^p \to N$ and $g:N^q \to N$. We define $g':N^{q+p} \to N$ as follows. Let $x_1,\ldots,x_q,y_1,\ldots,y_p \in N$.

case 1. $x_1,\ldots,x_q > y_1,\ldots,y_p$. Set $g'(x_1,\ldots,x_q,y_1,\ldots,y_p) = g(x_1,\ldots,x_q)$.

case 2. $y_1,\ldots,y_p > x_1,\ldots,x_q$ and $f(y_1,\ldots,y_p) \in 2^{(N+2)}$. Set $g'(x_1,\ldots,x_q,y_1,\ldots,y_p) = f(y_1,\ldots,y_p)$.

case 3. Otherwise. Set $g'(x_1,\ldots,x_q,y_1,\ldots,y_p) = 12|x_1,\ldots,x_q,y_1,\ldots,y_p|+2$.

We define $f':N^{5p+q+p} \to N$ as follows. Let $x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p \in N$.

case a. $|y_1,\ldots,y_q,z_1,\ldots,z_p| = |x_1,\ldots,x_p| = |x_{p+1},\ldots,x_{2p}| = |x_{2p+1},\ldots,x_{3p}| = |x_{3p+1},\ldots,x_{4p}| = |x_{4p+1},\ldots,x_{5p}|$. Set $f'(x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p) = g'(y_1,\ldots,y_q,z_1,\ldots,z_p)$.

case b. $|y_1,\ldots,y_q,z_1,\ldots,z_p| = |x_1,\ldots,x_p| = |x_{p+1},\ldots,x_{2p}| = |x_{2p+1},\ldots,x_{3p}| = |x_{3p+1},\ldots,x_{4p}| < \min(x_{4p+1},\ldots,x_{5p})$. Set $f'(x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p) = f(x_{4p+1},\ldots,x_{5p})$.

case c. $|y_1,\ldots,y_{q+1},z_1,\ldots,z_p| = |x_1,\ldots,x_p| = |x_{p+1},\ldots,x_{2p}| = |x_{2p+1},\ldots,x_{3p}| = |x_{4p+1},\ldots,x_{5p}| < \min(x_{3p+1},\ldots,x_{4p}|$. Set $f'(x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p) = 12f(x_{3p+1},\ldots,x_{4p})+2$.

case d. $|y_1,\ldots,y_q,z_1,\ldots,z_p| = |x_1,\ldots,x_p| = |x_{p+1},\ldots,x_{2p}| = |x_{3p+1},\ldots,x_{4p}| = |x_{4p+1},\ldots,x_{5p}| < \min(x_{2p+1},\ldots,x_{3p})$. Set $f'(x_1,\ldots,x_{3p},y_1,\ldots,y_q,z_1,\ldots,z_p| = 2|x_{2p+1},\ldots,x_{3p}|+1$.

case e. $|y_1,\ldots,y_q,z_1,\ldots,z_p| = |x_1,\ldots,x_p| = |x_{2p+1},\ldots,x_{3p}| = |x_{3p+1},\ldots,x_{4p}| = |x_{4p+1},\ldots,x_{5p}| < \min(x_{2p+1},\ldots,x_{3p}|$. Set $f'(x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p) = 3|x_{p+1},\ldots,x_{2p}|+1$.

case f. Otherwise. Set $f'(x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p) = 2|x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p|+1$.

Note that in case 1, $|x_1,\ldots,x_q,y_1,\ldots,y_p| = |x_1,\ldots,x_q|$, and in case 2, $|x_1,\ldots,x_q,y_1,\ldots,y_p| = |y_1,\ldots,y_p|$. Also note that in cases a)-e),

$$|x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p| = |y_1,\ldots,y_q,z_1,\ldots,z_p|$$
$$|x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p| = |x_{4p+1},\ldots,x_{5p}|$$

$$|x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p| = |x_{3p+1},\ldots,x_{4p}|$$
$$|x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p| = |x_{2p+1},\ldots,x_{3p}|$$
$$|x_1,\ldots,x_{5p},y_1,\ldots,y_q,z_1,\ldots,z_p| = |x_{p+1},\ldots,x_{2p}|$$

respectively. Hence f',g' ∈ ELG ∩ SD ∩ BAF.

Let S ⊆ N. From S, case 1 produces exactly g(S*). Case 2 produces exactly f(S*) ∩ $2^{(N+2)}$. Case 3 produces exactly 12S+2. This establishes i).

Case a) produces exactly g'S. Case b) produces exactly f(S*). Case c) produces exactly 12f(S*)+2. Case d) produces exactly 2S*+1. Case e produces exactly 3S*+1.

Case f) produces exactly 2S*+1 since 2min(S)+1 is not produced. This is because 2min(S)+1 is produced from case f) if and only if all of the arguments are min(S), which can only happen under case a). This establishes ii). QED

LEMMA 6.1.9. 12E+2, 6E, 2E+1 ∪ 3E+1, $2^{(N+2)}$ are pairwise disjoint, with the sole exception of 2E+1 ∪ 3E+1 and $2^{(N+2)}$.

Proof: Obviously, 12E+2, 6E, 2E+1 ∪ 3E+1 are pairwise disjoint by divisibility considerations. Also 12n+2 = 2m → 6n+1 = 2^{m-1}, which is impossible for m ≥ 3. QED

LEMMA 5.1.8'. Let f,g ∈ ELG ∩ SD ∩ BAF and rng(g) ⊆ 6N. There exist infinite A ⊆ B ⊆ C ⊆ N\{0} such that

i) fA ∩ 6N ⊆ B ∪ gB;
ii) fB ∩ 6N ⊆ C ∪ gC;
iii) fA ∩ 2N+1 ⊆ B;
iv) fA ∩ 3N+1\$2^{(N+2)}$ ⊆ B;
v) fB ∩ 2N+1 ⊆ C;
vi) fB ∩ 3N+1\$2^{(N+2)}$ ⊆ C;
vii) C ∩ gC = ∅;
viii) A ∩ fB = ∅.

Proof: Let f,g be as given. Let f',g' be given by Lemma 5.1.7'. Let A,B,C ⊆ N be given by Lemma 6.1.7 for f',g'. Then A,B,C are infinite, and

f'A ⊆ C ∪. g'B
f'B ⊆ C ∪. g'C
A ⊆ B,$2^{(N)}$.

Since we can shrink A to any infinite subset, we will assume that A ⊆ $2^{(N+2)}$.

Let n ∈ B. Then 12n+2 ∈ g'B ∩ f'B, and so 12n+2 ∈ C ∪ g'C. Now 12n+2 ∉ C by C ∩ g'B = ∅. Hence 12n+2 ∈ g'C. Therefore 12n+2 ∈ 12C+2. Hence n ∈ C. So we have established that A ⊆ B ⊆ C.

We now verify all of the required conditions i)-viii) above using the three sets A*,B*,C*.

Firstly note that A* ⊆ B* ⊆ C* ⊆ N\{0}. To see this, first observe that min(A) ≥ min(B) ≥ min(C). Now let n ∈ A*. Then n ∈ B ∧ n > min(A) ≥ min(B). Hence n ∈ B*. Thus A* ⊆ B*. The same argument establishes B* ⊆ C*.

We now claim that A* ∩ f(B*) = ∅. Let n ∈ A*, n ∈ f(B*). Then n ∈ f(B*) ∩ $2^{(N+2)}$, n ∈ g'B, n ∈ C. This is a contradiction.

Next we claim that C* ∩ g(C*) = ∅. This follows from C ⊆ C*, g(C*) ⊆ g'C, and C ∩ g'C = ∅.

Now we claim that f(A*) ∩ 6N ⊆ B* ∪ g(B*). To see this, let n ∈ f(A*) ∩ 6N. Then n ∈ f'A, n ∈ C ∪ g'B.

case 1. n ∈ C. Now 12n+2 ∈ g'C and 12n+2 ∈ 12f(A*)+2 ⊆ f'A. Since C ∩ g'C = ∅, we have 12n+2 ∉ C. Also 12n+2 ∈ C ∪ g'B. Hence 12n+2 ∈ g'B. Therefore 12n+2 ∈ 12B+2, and so n ∈ B. Since n ∈ f(A*) and f is strictly dominating, we have n > min(A) ≥ min(B). Hence n ∈ B*.

case 2. n ∈ g'B. Since n ∈ 6N, n ∈ g(B*). This establishes the claim.

Next we claim that f(B*) ∩ 6N ⊆ C* ∪ g(C*). To see this, let n ∈ f(B*) ∩ 6N. Then n ∈ f'B. Hence n ∈ C ∪ g'C.

case 1'. n ∈ C. Since n ∈ f(B*) and f is strictly dominating, we have n > min(B) ≥ min(C). Hence n ∈ C*.

case 2'. n ∈ g'C. Since n ∈ 6N, we have n ∈ g(C*). This establishes the claim.

Now we claim that f(A*) ∩ 2N+1, f(A*) ∩ 3N+1\$2^{(N+2)}$ ⊆ B*. To see this, let n ∈ f(A*), n ∈ 2N+1 ∪ 3N+1, n ∉ $2^{(N+2)}$. Note that n ∉ rng(g'). Also, n ∈ f'A, n ∈ C ∪ g'B. Hence n ∈ C, 12n+2 ∈ g'C, 12n+2 ∉ C. Now 12n+2 ∈ 12f(A*)+2 ⊆ f'A ⊆ C ∪ g'B, 12n+2 ∈ g'B, n ∈ B. Since f is strictly dominating, n > min(A) ≥ min(B), and so n ∈ B*.

Finally we claim that $f(B^*) \cap 2N+1, f(B^*) \cap 3n+1\backslash 2^{(N+2)} \subseteq C^*$. To see this, let $n \in f(B^*)$, $n \in 2N+1 \cup 3N+1$, $n \notin 2^{(N+2)}$. Note that $n \notin rng(g')$. Also, $n \in f'B$, $n \in C \cup g'C$. Hence $n \in C$, $12n+2 \in g'C$, $12n+2 \notin C$. Now $12n+2 \in 12f(B^*)+2 \subseteq f'B \subseteq C \cup g'C$. Hence $12n+2 \in g'C$, $n \in C$. Since f is strictly dominating, $n > \min(B) \geq \min(C)$, and so $n \in C^*$. QED

The proof of 1-Con(SMAH) from Proposition C given in Chapter 5 is strictly modular, in that we can start with Lemma 5.1.8 instead of Proposition C.

Here we repeat the proof in Chapter 5 using Lemma 5.1.8' instead of Lemma 5.1.8. However, Lemma 5.1.8' is slightly weaker than Lemma 5.1.8, because of the weakened clauses iv) and vi), where we use $3N+1\backslash 2^{(N+2)}$ instead of 3N+1.

So we need to identify the few places at which we use 3N+1 and make sure that we can get away with $3N+1\backslash 2^{(N+2)}$ instead.

By examination of the proofs, we obtain the following series of slightly weakened Lemmas from the end of sections 5.1 - 5.5. Finally, we show that we obtain Lemma 5.6.20 without modification.

LEMMA 5.2.12'. Let $r \geq 3$ and $g \in ELG \cap SD \cap BAF$, where $rng(g) \subseteq 48N$. There exists $(D_1,\ldots,D_r)$ such that
i) $D_1 \subseteq \ldots \subseteq D_r \subseteq N\backslash\{0\}$;
ii) $|D_1| = r$ and D_r is finite;
iii) for all $x < y$ from D_1, $x\uparrow < y$;
iv) for all $1 \leq i \leq r-1$, $48\alpha(r,D_i;1,r) \subseteq D_{i+1} \cup gD_{i+1}$;
v) for all $1 \leq i \leq r-1$, $2\alpha(r,D_i;1,r)+1, 3\alpha(r,D_i;1,r)+1\backslash 2^{(N+2)} \subseteq D_{i+1}$;
vi) $D_r \cap gD_r = \emptyset$;
vii) $D_1 \cap \alpha(r,D_2;2,r) = \emptyset$;
viii) Let $1 \leq i \leq \beta(2r)$, $x_1,\ldots,x_{2r} \in D_1$, $y_1,\ldots,y_r \in \alpha(r,D_2)$, where $(x_1,\ldots,x_r)$ and $(x_{r+1},\ldots,x_{2r})$ have the same order type and min, and $y_1,\ldots,y_r \leq \min(x_1,\ldots,x_r)$. Then
$t[i,2r](x_1,\ldots,x_r,y_1,\ldots,y_r) \in D_3 \leftrightarrow$
$t[i,2r](x_{r+1},\ldots,x_{2r},y_1,\ldots,y_r) \in D_3$.

LEMMA 5.3.18'. There exists a countable structure $M = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,\ldots)$ such that the following holds.
i) $(A,<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies $TR(\Pi^0{}_1,L)$;
ii) $E \subseteq A\backslash\{0\}$;
iii) The c_n, $n \geq 1$, form a strictly increasing sequence of nonstandard elements in $E\backslash\alpha(E;2,<\infty)$ with no upper bound in A;

iv) Let $r,n \geq 1$, $t(v_1,\ldots,v_r)$ be a term of L, and $x_1,\ldots,x_r \leq c_n$. Then $t(x_1,\ldots,x_r) < c_{n+1}$;
v) $2\alpha(E;1,<\infty)+1,\ 3\alpha(E;1,<\infty)+1\backslash 2^{(A+2)} \subseteq E$;
vi) Let $r \geq 1$, $a,b \in N$, and $\varphi(v_1,\ldots,v_r)$ be a quantifier free formula of L. There exist $d,e,f,g \in N\backslash\{0\}$ such that for all $x_1 \in \alpha(E;1,<\infty)$, $(\exists x_2,\ldots,x_r \in E)(x_2,\ldots,x_r \leq ax_1+b \wedge \varphi(x_1,\ldots,x_r)) \leftrightarrow dx_1+e \notin E \leftrightarrow fx_1+g \in E$;
vii) Let $r \geq 1$, $p \geq 2$, and $\varphi(v_1,\ldots,v_{2r})$ be a quantifier free formula of L. There exist $a,b,d,e \in N\backslash\{0\}$ such that the following holds. Let $n \geq 1$ and $x_1,\ldots.,x_r \in \alpha(E;1,<\infty) \cap [0,c_n]$. Then
$(\exists y_1,\ldots,y_r \in E)(y_1,\ldots,y_r \leq \uparrow p(|x_1,\ldots,x_r|) \wedge \varphi(x_1,\ldots,x_r,y_1,\ldots,y_r)) \leftrightarrow$
$a\text{CODE}(c_{n+1};x_1,\ldots,x_r)+b \notin E \leftrightarrow$
$d\text{CODE}(c_{n+1};x_1,\ldots,x_r)+e \in E$. Here CODE is as defined just before Lemma 5.3.11;
viii) Let $k,n,m \geq 1$, and $x_1,\ldots,x_k \leq c_n < c_m$, where $x_1,\ldots,x_k \in \alpha(E;1,<\infty)$. Then $\text{CODE}(c_m;x_1,\ldots,x_k) \in E$;
ix) Let $r \geq 1$ and $t(v_1,\ldots,v_{2r})$ be a term of L. Let $i_1,\ldots,i_{2r} \geq 1$ and $y_1,\ldots,y_r \in E$, where $(i_1,\ldots,i_r)$ and $(i_{r+1},\ldots,i_{2r})$ have the same order type and min, and $y_1,\ldots,y_r \leq \min(c_{i\_1},\ldots,c_{i\_r})$. Then
$t(c_{i\_1},\ldots,c_{i\_r},y_1,\ldots,y_r) \in E \leftrightarrow$
$t(c_{i\_r+1},\ldots,c_{i\_2r},y_1,\ldots,y_r) \in E$.

Lemma 5.4.12 uses $2\alpha(E;1,<\infty)+1,\ 3\alpha(E;1,<\infty)+1 \subseteq E$. However, we only have $3\alpha(E;1,<\infty)+1\backslash 2^{(A+2)} \subseteq E$. So it suffices to augment the displayed derivation in Lemma 5.4.12 with the second derivation

$$t(x_1,\ldots,x_k) < c_{n+1}.$$
$$2c_{n+1}+t(x_1,\ldots,x_k)+3, 3c_{n+1}+t(x_1,\ldots,x_k)+2 \in \alpha(E;1,<\infty).$$
$$3(2c_{n+1}+t(x_1,\ldots,x_k)+2)+1,\ 2(3c_{n+1}+t(x_1,\ldots,x_k)+3)+1 \in E.$$
$$6c_{n+1}+3t(x_1,\ldots,x_k)+7,\ 6c_{n+1}+2t(x_1,\ldots,x_k)+7 \in E.$$
$$(6c_{n+1}+3t(x_1,\ldots,x_k)+7)-(6c_{n+1}+2t(x_1,\ldots,x_k)+7) =$$
$$t(x_1,\ldots,x_k) \in E-E.$$

provided we verify that

$$3(2c_{n+1}+t(x_1,\ldots,x_k))+1 \notin 2^{(A+2)} \vee 3(2c_{n+1}+t(x_1,\ldots,x_k)+2)+1 \notin 2^{(A+2)}.$$

This is evident, since any two powers of 2 that are ≥ 4 cannot differ by 6.

LEMMA 5.4.17'. There exists a countable structure $M = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,\ldots)$, and terms $t_1,t_2,\ldots$ of L,

where for all i, t_i has variables among $v_1,...,v_{i+8}$, such that the following holds.
i) $(A,<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies $TR(\Pi^0{}_1,L)$;
ii) $E \subseteq A\backslash\{0\}$;
iii) The c_n, $n \geq 1$, form a strictly increasing sequence of nonstandard elements in $E\backslash\alpha(E;2,<\infty)$ with no upper bound in A;
iv) Let $r,n \geq 1$ and $t(v_1,...,v_r)$ be a term of L, and $x_1,...,x_r \leq c_n$. Then $t(x_1,...,x_r) < c_{n+1}$;
v) $2\alpha(E;1,<\infty)+1$, $3\alpha(E;1,<\infty)+1\backslash 2^{(A+2)} \subseteq E$;
vi) Let $k,n \geq 1$ and R be a c_n-definable k-ary relation. There exists $y_1,...,y_8 \in E \cap [0,c_{n+1}]$ such that $R = \{(x_1,...,x_k) \in E^k \cap [0,c_n]^k: t_k(x_1,...,x_k,y_1,...,y_8) \in E\}$;
vii) Let $r \geq 1$ and $\varphi(v_1,...,v_{2r})$ be a formula of L(E). Let $1 \leq i_1,...,i_{2r} < n$, where $(i_1,...,i_r)$ and $(i_{r+1},...,i_{2r})$ have the same order type and the same min. Let $y_1,...,y_r \in E$, $y_1,...,y_r \leq \min(c_{i\_1},...,c_{i\_r})$. Then $\varphi(c_{i\_1},...,c_{i\_r},y_1,...,y_r)^{c\_n} \leftrightarrow \varphi(c_{i\_r+1},...,c_{i\_2r},y_1,...,y_r)^{c\_n}$.

LEMMA 5.5.8'. There exists a countable structure $M^* = (A,<,0,1,+,-,\bullet,\uparrow,\log,E,c_1,c_2,...,X_1,X_2,...)$, where for all $i \geq 1$, X_i is the set of all i-ary relations on A that are c_n-definable for some $n \geq 1$; and terms $t_1,t_2,...$ of L, where for all i, t_i has variables among $x_1,...,x_{i+8}$, such that the following holds.
i) $(A,<,0,1,+,-,\bullet,\uparrow,\log)$ satisfies $TR(\Pi^0{}_1,L)$;
ii) $E \subseteq A\backslash\{0\}$;
iii) The c_n, $n \geq 1$, form a strictly increasing sequence of nonstandard elements of $E\backslash\alpha(E;2,<\infty)$ with no upper bound in A;
iv) For all $r,n \geq 1$, $\uparrow r(c_n) < c_{n+1}$;
v) $2\alpha(E;1,<\infty)+1$, $3\alpha(E;1,<\infty)+1\backslash 2^{(A+2)} \subseteq E$;
vi) Let $k,n \geq 1$ and R be a c_n-definable k-ary relation. There exists $y_1,...,y_8 \in E \cap [0,c_{n+1}]$ such that $R = \{(x_1,...,x_k) \in E^k \cap [0,c_n]^k: t_k(x_1,...,x_k,y_1,...,y_8) \in E\}$;
vii) Let $k \geq 1$, $m \geq 0$, and φ be an E formula of L*(E) in which R is not free, where all first order variables free in φ are among $x_1,...,x_{k+m+1}$. Then $x_{k+1},...,x_{k+m+1} \in E \rightarrow (\exists R)(\forall x_1,...,x_k \in E)(R(x_1,...,x_k) \leftrightarrow (x_1,...,x_k \leq x_{k+m+1} \wedge \varphi))$;
viii) Let $r \geq 1$, and $\varphi(x_1,...,x_{2r})$ be an E formula of L*(E) with no free second order variables. Let $1 \leq i_1,...,i_{2r}$, where $(i_1,...,i_r)$ and $(i_{r+1},...,i_{2r})$ have the same order type and the same min. Let $x_1,...,x_r \in E$, $x_1,...,x_r \leq \min(c_{i\_1},...,c_{i\_r})$. Then $\varphi(c_{i\_1},...,c_{i\_r},x_1,...,x_r) \leftrightarrow \varphi(c_{i\_r+1},...,c_{i\_2r},x_1,...,x_r)$.

Lemma 5.6.2 involves reproving a weak form of Lemma 5.4.12 using a related construction. Here $3\alpha(E;1,<\infty)+1 \subseteq E$ can also be replaced by $3\alpha(E;1,<\infty)+1\backslash 2^{(A+2)}$, also by the same method.

In the remainder of section 5.6, we do not use $3\alpha(E;1,<\infty)+1\backslash 2^{(A+2)} \subseteq E$. Hence we obtain Lemma 5.6.20. We have proved the following.

THEOREM 6.1.10. ACA' proves that each of Propositions A-H are equivalent to Con(SMAH).

Proof: We have completed the proof that ACA' proves Proposition H implies 1-Con(SMAH). The result follows by Lemmas 5.9.11 and 6.1.5. QED

6.2. Effectivity.

We begin with a straightforward effectivity result concerning Propositions A-H. Specifically, we show that Propositions A-H hold in the arithmetic sets. Later we will show that Propositions C,E-H hold in the recursive sets.

We don’t know if any or all of Propositions A,B,D hold in the recursive sets. We conjecture that

i. None of Propositions A,B,D hold in the recursive sets.
ii. This fact can be proved in ACA’.

DEFINITION 6.2.1. Let ACA^+ be the formal system consisting of ACA_0 and “for all $x \subseteq \omega$, the ω-th Turing jump of x exists”.

See [Si99,09], p. 404, where ACA^+ is written as ACA_0^+. ACA^+ is a proper extension of ACA’ that allows us to handle ω models of ACA_0.

Note that the countable ω models of ACA_0, ACA', ACA are the same as the countable families of subsets of N that are closed under relative arithmeticity, as induction is automatic in ω models. (Here ACA is ACA_0 with induction for all formulas, and is a proper extension of ACA').

THEOREM 6.2.1. Let X be any of Propositions A-H. The following are provably equivalent in ACA^+.
i. X is true.
ii. X is true in the arithmetic sets.
iii. X is true in every countable ω model of ACA_0.
iv. X is true in some countable ω model of ACA_0.

v. 1-Con(MAH).
vi. 1-Con(SMAH).

Proof: Let X be as given. We argue in ACA^+. By Theorems 5.9.11, 6.1.2, and 6.1.10, X is equivalent to 1-Con(MAH), 1-Con(SMAH). Hence i,v,vi are equivalent. It suffices to prove vi → iii → ii → iv → vi.

Since ACA' proves X is equivalent to 1-Con(SMAH), we see that in any ω model of ACA_0, X is equivalent to 1-Con(SMAH).

For vi → iii, suppose 1-Con(SMAH). Then 1-Con(SMAH) is true in any ω model of ACA_0. Hence X is true in every ω model of ACA_0, and therefore iii,ii,iv.

iii → ii → iv is trivial.

For iv → vi, suppose X is true in some countable ω model of ACA_0. Then 1-Con(SMAH) is true in some ω model of ACA_0. Hence 1-Con(SMAH). QED

We are now going to show that Propositions C,E-H hold in the recursive subsets of N. Propositions C,E-H, when stated in the recursive sets, become Π^0_4 statements.

We shall see that Propositions C,E-H hold in the smaller family of infinite sets with primitive recursive enumeration functions.

We also show that all of these variants of C,E-H are provably equivalent to 1-Con(SMAH) in ACA'.

We conjecture that a more careful argument will show that Propositions C,E-H hold in the yet smaller family of infinite superexponentially Presburger sets. In light of the primitive recursive decision procedure for superexponential Presburger arithmetic, Propositions C,E-H, when stated in the superexponentially Presburger sets, become Π^0_2 statements. This topic will be discussed at the end of this section.

Recall TM(0,1,+,-,•,↑,log), ETM(0,1,+,-,•,↑,log), BAF, EBAF, from Definitions 5.1.1 - 5.1.7. According to Theorem 5.1.4, BAF = EBAF.

DEFINITION 6.2.2. Sometimes we will omit some items among 0,1,+,-,•,↑,log when using this notation. E.g., terms in TM(0,1,+,-) use only 0,1,+,-, and not •,↑,log. E.g., terms and formulas in ETM(0,1,+) use only 0,1,+. In ETM(___) we always use <,= as the relations for the quantifier free formulas.

We will develop explicit infinite sets of indiscernibles for functions in BAF, in the appropriate sense, using iterated base 2 exponentials. It is particularly convenient to use the following definition for our purposes.

DEFINITION 6.2.3. Let $f:N^k \to N$. An SOI for f is a set $A \subseteq N$ such that for all $x,y \in A^k$,

if $x,y \in A^k$ are order equivalent
(i.e., have the same order type)
then f(x) and f(y) have the same sign
(i.e., either > 0 or = 0).

We first define the set of functions $\Gamma(\mathfrak{R})$. For this purpose, we take +′,
-′,↑′ to be the ordinary addition, subtraction, and base 2 exponentiation functions from $\mathfrak{R}^2$ into $\mathfrak{R}$ (↑' maps $\mathfrak{R}$ into $\mathfrak{R}$).

It will be important to recall that, according to section 5, we use +,-,•,↑,log for functions from and into N, where -,log are modified so that they are N valued. We call this N arithmetic.

On the other hand, +',-',↑' take arguments and values from $\mathfrak{R}$, and we call this Z arithmetic.

In this section, we will not use real numbers after we have proved Lemma 6.2.6.

DEFINITION 6.2.4. $\Gamma(\mathfrak{R})$ is the set of all functions from $\mathfrak{R}$ into $\mathfrak{R}$ that are given by terms in 0,1,+′,-′,↑′ in only the variable x.

DEFINITION 6.2.5. By positive, we will always mean > 0. By negative, we will always mean < 0.

LEMMA 6.2.2. Every function in $\Gamma(\mathfrak{R})$ is eventually positive, eventually negative, or eventually zero.

Proof: $\Gamma(\mathfrak{R})$ is a small fragment of what are called the exp-log functions. Thus the statement is a special case of a well known theorem of Hardy from [Ha10]. QED

LEMMA 6.2.3. Let $f:N \to N$ be given by a term in TM(0,1,+,-,↑). There exists $f^* \in \Gamma(\mathfrak{R})$ such that for sufficiently large $x \in N$, $f(x) = f^*(x)$. f is eventually positive or eventually zero.

Proof: By induction on $t \in$ TM(0,1,+,-,↑). Suppose that we have defined r* with the required property, for all terms r in TM(0,1,+,-,↑) with less symbols that t has.

case 1. t is 0,1,v. Set t* = t.

case 2. t is s↑. Set t* = s*↑.

case 3. t is r-s. By the induction hypothesis, for sufficiently large $x \in N$, $t(x) = r^*(x)-s^*(x)$. By Lemma 6.2.2, $r^*(x)-'s^*(x)$ is either eventually ≥ 0 or eventually $<$ 0. In the former case, set $t^* = r^*-'s^*$. In the latter case, set $t^* = 0$.

The final claim follows from the first claim and Lemma 6.2.2. QED

LEMMA 6.2.4. Let $f:N \to N$ be given by a term in ETM(0,1,+,-,↑). There exists $f^* \in \Gamma(\mathfrak{R})$ such that for sufficiently large $x \in N$, $f(x) = f^*(x)$. f is eventually positive or eventually zero.

Proof: We first claim the following. Let $\varphi(v)$ be a quantifier free formula in 0,1,+,-,↑,<. Then either $\varphi(x)$ is true for all sufficiently large $x \in N$, or $\varphi(x)$ is false for all sufficiently large $x \in N$. The claim is proved by induction on φ.

The atomic cases are $s(x) < t(x)$, $s(x) = t(x)$. In either case, apply Lemma 6.2.3 to $s(x)-t(x)$ and $t(x)-s(x)$. Then

$s(x)-t(x)$ is eventually positive or eventually zero.
$t(x)-s(x)$ is eventually positive or eventually zero.

If $s(x)-t(x)$ is eventually positive then $s(x) < t(x)$ and $s(x) = t(x)$ are eventually false. If $t(x)-s(x)$ is eventually positive then $s(x) < t(x)$ is eventually true and $s(x) = t(x)$ is eventually false.

Suppose $s(x)-t(x)$ is not eventually positive and $t(x)-s(x)$ is not eventually positive. Then $s(x)-t(x)$ and $t(x)-s(x)$ are both eventually zero. Hence $s(x) = t(x)$ eventually holds. This establishes the claim.

Now write f as an extended term t from ETM(0,1,+,-,↑), according to Definition 5.1.5. We can assume that t has at most the variable v and does not use •,log. Apply the claim to each of the finitely many cases in t. Then only one case applies for all sufficiently large x ∈ N. Let this be the j-th case, 1 ≤ j ≤ n+1. Then t = t_j holds eventually. Apply Lemma 6.2.3 to t_j. QED

The structure (N,+) has been extensively studied, and its first order theory is called Presburger arithmetic. It has a well known decision procedure, conducted well within PRA. This is proved using quantifier elimination in an expanded language. See [Pr29], [En72].

The structure (N,+,↑) has also been studied, and its first order theory is called (base 2) exponential Presburger arithmetic. It also has a decision procedure, conducted well within PRA. Again this is proved using quantifier elimination in an expanded language. See [Se80], [Se83], [CP85]. Appendix B provides a self contained exposition of this result by F. Point.

DEFINITION 6.2.6. Recall from Definition 5.3.6 that ↑p is 0↑...↑, and ↑p(n) = n↑...↑, where there are p ↑'s, p ≥ 0. ↑0 = 0. For E ⊆ N, define

↑E = {↑p: p ∈ E}, for E ⊆ N.
mesh(E) = min(E ∪ {x-y > 0: x,y ∈ E}).

THEOREM 6.2.5. The first order theory of the structure (N,+,↑) is primitive recursive. Suppose the sentence $(\forall n_1,\ldots,n_k)(\exists m)(\varphi(n,m))$ holds in (N,+,↑). There exists p ≥ 1 such that $(\forall n_1,\ldots,n_k)(\exists m \leq \uparrow p(|n_1,\ldots,n_k|))(\varphi(n,m))$ holds in (N,+,↑).

Proof: This result first appeared in [Se80] and [Se83]. It is implicit in [CP86]. For a clearer, self contained exposition, see Theorem 3.3 in Appendix B by F. Point. QED

Recall the definition of an SOI for $f:N^k \to N$. It is convenient to use the following weaker notion.

DEFINITION 6.2.7. Let $f:N^k \to N$. A restricted SOI for f is a set A ⊆ N such that for all $x,y \in A^k$,

if $x,y \in A^k$ are each strictly increasing
then f(x) and f(y) have the same sign

(either > or =).

LEMMA 6.2.6. Let $f:N^k \to N$ be given by a term in TM(0,1,+,-,↑). If mesh(A) is sufficiently large then ↑A is a restricted infinite SOI for f.

Proof: We prove by induction on $k \geq 1$ that this is true for all such $f:N^k \to N$. For $k = 1$, let $f:N \to N$ be as given. By Lemma 6.2.4, let t be such that f has constant sign on $[t,\infty)$. Then for $\text{mesh}(A) \geq t$, ↑A is a restricted infinite SOI for f.

Now fix $k \geq 1$, and let $f:N^{k+1} \to N$ be as given. By Lemma 6.2.4,

$$(\forall x \in N^k)(\exists t \in N)$$
$$(f(x,m) \text{ has constant sign for } m \geq t).$$

By Lemma 6.2.5, let $p \in N$ be such that

$$(\forall x \in N^k)$$
$$(f(x,m) \text{ has constant sign for } m \geq {\uparrow}p(|x|)).$$

1) $(\forall x \in N^k)$(the eventual sign of f(x,_) is the sign of $f(x,{\uparrow}p(|x|))$).

We now apply the induction hypothesis to the k-ary function $f(x,{\uparrow}p(|x|))$ to obtain the following.

2) $(\forall A \subseteq N)(\text{mesh}(A) \text{ sufficiently large} \to$
$(\forall x,y \in ({\uparrow}A)^k)(x,y \text{ strictly increasing} \to$
$f(x,{\uparrow}p(|x|), g(y,{\uparrow}p(|y|) \text{ have the same sign})).$

By 1),2),

3) $(\forall A \subseteq N)(\text{mesh}(A) \text{ sufficiently large} \to$
$(\forall x,y \in ({\uparrow}A)^k)(x,y \text{ strictly increasing} \to$
$f(x,x'), f(y,y') \text{ have the same sign}$
$\text{provided } x' \geq {\uparrow}p(|x|, y' \geq {\uparrow}p(|y|))).$

We now claim that

$$(\forall A \subseteq N)(\text{mesh}(A) \text{ sufficiently large} \to$$
$$A \text{ is a restricted SOI for } f).$$

To see this, let mesh(A) be sufficiently large, and $x,y \in ({\uparrow}A)^{k+1}$ be strictly increasing. Then

4) $x_1 < ... < x_k$, and $x_{k+1} > \uparrow p(|x_1,...,x_k|)$.
$y_1 < ... < y_k$, and $y_{k+1} > \uparrow p(|y_1,...,y_k|)$.

This is because we can write

$$|x_1,...,x_k| = \uparrow u,\ x_{k+1} = \uparrow v,\ u,v \in A,$$
where v-u is sufficiently large.
$$v-u > p.$$
$$\uparrow p(|x_1,...,x_k|) = \uparrow p(\uparrow u) = \uparrow(p+u)$$
$$< \uparrow v = \uparrow p(|x_1,...,x_k|).$$

By 3),4),

$$f(x_1,...,x_k,x_{k+1}),\ f(y_1,...,y_k,y_{k+1})$$
have the same sign.

This verifies the claim. QED

LEMMA 6.2.7. Let $f:N^k \rightarrow N$ be given by a term in ETM(0,1,+,-,↑). There are finitely many functions $g_1,...,g_n$ whose domains are various $N^{k'}$, $k' < k$, and whose range is a subset of N, given by terms in TM(0,1,+,-,↑), such that any common restricted infinite SOI for $g_1,...,g_n$ is an infinite SOI for f.

Proof: Let f be as given. Enumerate the order types of k-tuples from N, by $\alpha_1,...,\alpha_n$. Pick the unique representatives $\beta_1,...,\beta_n$ which are k-tuples whose range is an interval $[1,p]$, $1 \leq p \leq n$. Set $g_i(x_1...,x_k) = f(x[\beta_i[1]],...,x[\beta_i[k]])$. Each g_i handles the order type α_i in the definition of SOI. QED

LEMMA 6.2.8. Let $f:N^k \rightarrow N$ be given by a term in ETM(0,1,+,-,↑). If mesh(A) is sufficiently large, then ↑A is an infinite SOI for f.

Proof: Let f be as given, and let $g_1,...,g_n$ be as given by Lemma 6.2.7. By Lemma 6.2.6, for all $1 \leq i \leq n$, if mesh(A) is sufficiently large then ↑A is a restricted SOI for g_i. Hence if mesh(A) is sufficiently large then ↑A is a common restricted SOI for $g_1,...,g_n$. Now apply Lemma 6.2.7. QED

We now wish to establish Lemma 6.2.8 for ETM(0,1,+,-,•,↑,log). We do this by showing that • and log can be eliminated in these terms, when restricting to $\uparrow([r,\infty))$, provided r is sufficiently large.

DEFINITION 6.2.8. Let $n,k \geq 1$. The n,k-terms are the terms $v_1,\ldots,v_n$, and v_i+j, where $1 \leq i \leq n$, $1 \leq j \leq k$.

DEFINITION 6.2.9. An n,k-ordering consists of an ordering of the n,k-terms. I.e., a listing

$$\alpha_1 \text{ rel } \alpha_2 \text{ rel } \ldots \text{ rel } \alpha_{n(k+1)}$$

where each rel is either < or =, and $\alpha_1,\ldots,\alpha_{n(k+1)}$ is an enumeration without repetition of the n,k-terms.

An n,k-ordering may or may not hold, given an assignment of elements of N to the variables $v_1,\ldots,v_n$.

Example 1. $v_1 < v_1+1 < v_1+2 < v_2 = v_3 < v_2+1 = v_3+1 < v_2+2 = v_3+2$ is a 3,2-ordering which holds for some $v_1,v_2,v_3 \in N$. E.g., $v_1 = 0$, $v_2 = v_3 = 3$.

Example 2. $v_1 < v_2 < v_3 < v_1+1 < v_2+1 < v_3+1 < v_1+2 < v_2+2 < v_3+2$ is a 3,2-ordering which does not hold for any $v_1,v_2,v_3 \in N$. From $v_3 < v_1+1$, we obtain $v_3 \leq v_1$, contradicting $v_1 < v_3$.

We can obviously view every n,k-ordering as a conjunction of comparisons between all pairs of the n-terms. Only some of these conjunctions of comparisons hold for some choice of $v_1,\ldots,v_n \in N$.

DEFINITION 6.2.10. Let X be an n,k-ordering. We write $\alpha <_X \beta$, $\alpha =_X \beta$, for n,k-terms α,β, according to the relevant position of α,β in X. Here $<_X$ and $=_X$ are transitive. Define $\alpha >_X \beta \leftrightarrow \alpha <_X \beta$, $\alpha \geq_X \beta \leftrightarrow \beta \leq_X \alpha$.

DEFINITION 6.2.11. The signed X sums are of the form

$$\beta_1\uparrow \pm \beta_2\uparrow \pm \ldots \pm \beta_m\uparrow.$$
$$0.$$

where

i. $m \geq 1$.
ii. $\beta_1,\ldots,\beta_m$ are n,k-terms.
iii. $\beta_1 >_X \beta_2 >_X \ldots >_X \beta_m$ holds in the n,k-ordering X.
iv. There is no consecutive pair $+ \beta_i\uparrow,- \beta_{i+1}\uparrow$ for which $\beta_i =_X \beta_{i+1}+1$. For this purpose, $\beta_1\uparrow$ is considered to be $+ \beta_1\uparrow$.
v. There is no consecutive pair $- \beta_i\uparrow,+ \beta_{i+1}\uparrow$ for which $\beta_i =_X \beta_{i+1}+1$ in X.

We evaluate signed X sums at elements of N only, and we always associate to the left

$$(\ldots(\beta_1\uparrow \pm \beta_2\uparrow) \pm \ldots \pm \beta_m\uparrow).$$

where each ± is + or -, both interpreted in the usual way using N arithmetic; i.e., - indicates cutoff subtraction. Also note that the first summand, $\beta_1\uparrow$, is not signed, which has the same effect as + $\beta_1\uparrow$.

It is clear that the evaluation of a signed X sum is the same as the evaluation in Z arithmetic, since cutoff subtraction never gets triggered.

Conditions iv,v in Definition 6.2.10 rule out the possibility of an obvious simplification in signed X sums, corresponding to the ordinary algebraic laws $2^{p+1}-2^p = 2^p$, and $-2^{p+1}+2^p = -2^p$.

DEFINITION 6.2.12. Let X be an n,k-ordering. For X sums λ, we write lth(λ) for the number of summands in λ, and #(λ) for the largest j such that some v_i+j is a summand. We take lth(0) = #(0) = 0. Also, if λ has no v_i+j (i.e., λ consists entirely of variables), then #(λ) = 0. Obviously #(λ) ≤ k.

LEMMA 6.2.9. Let n ≥ 3 and X be an n,n^2-ordering. Let t = $y_1\uparrow \pm y_2\uparrow \pm \ldots \pm y_m\uparrow$ be parenthesized in any way, where $\{y_1,\ldots,y_m\} \subseteq \{v_1,\ldots,v_n\}$, and the y's are distinct, m ≥ 1. There exists a signed X sum t*, with lth(t*) ≤ m and #(t*) ≤ m^2, which agrees with t at all $v_1,\ldots,v_n \in N$ for which X is true. Here t (and of course t*) are evaluated using N arithmetic.

Proof: Fix n,X as given. We prove the claim by induction on 1 ≤ m ≤ n.

The basis case m = 1 is trivial. Now fix 1 ≤ m ≤ n, and assume that the claim is true for all 1 ≤ m' < m. We now prove the claim for m.

Let t = $y_1\uparrow \pm y_2\uparrow \pm \ldots \pm y_m\uparrow$ be parenthesized in any way, where $\{y_1,\ldots,y_m\} \subseteq \{v_1,\ldots,v_n\}$, and the y's are distinct.

First suppose t is (r)+(s), lth(r)+lth(s) = m. By the induction hypothesis, let r*,s* be signed X sums, lth(r*),lth(s*) < m, #(r*),#(s*) ≤ $(m-1)^2$, where r agrees with r* provided X holds, and s agrees with s* provided X holds. Then t agrees with (r*)+(s*) provided X holds. Write t = (r*)+(s*) as

$$1)\ t = (\beta_1\uparrow \pm \ldots \pm \beta_p\uparrow) + (\gamma_1\uparrow \pm \ldots \pm \gamma_q\uparrow)$$

with N arithmetic for t, and Z arithmetic for the two summands on the right, provided X holds.

Since we are using Z arithmetic on the right, we can rearrange the terms on the right. Place γ_1 and the $\pm\gamma$'s in their appropriate positions amongst the β's, in X, resulting in

$$2)\ t = \delta_1\uparrow \pm \ldots \pm \delta_{p+q}\uparrow$$

with N arithmetic on the left and Z arithmetic on the right, provided X holds.

so that we have $\delta_1 \geq_X \ldots \geq_X \delta_{p+q}$. Note that conditions iii-v in Definition 6.2.11, may fail for the right side of 3).

We continue to work in Z arithmetic. We iterate a process, which, at each stage, shortens the right side of 2). Recall that $p+q \leq m$. So the process will continue for at most m steps. The process runs as follows. Choose any i such that the consecutive pair $\pm \delta_i\uparrow, \pm \delta_{i+1}\uparrow$ violates any of conditions iii-v. Remove or replace $\pm \delta_i\uparrow \pm \delta_{i+1}\uparrow$ as follows.

case 1. $\delta_i = \delta_{i+1}$ in X.

Replace $+ \delta_i\uparrow + \delta_{i+1}\uparrow$ by $(\delta_i+1)\uparrow$.
Replace $- \delta_i\uparrow - \delta_{i+1}\uparrow$ by $- (\delta_i+1)\uparrow$.
Remove $+ \delta_i\uparrow - \delta_{i+1}\uparrow$.
Remove $- \delta_i\uparrow + \delta_{i+1}\uparrow$.

case 2. $\delta_i = \delta_{i+1}+1$ in X.

Replace $+ \delta_i\uparrow - \delta_{i+1}\uparrow$ by $+ \delta_{i+1}\uparrow$.
Replace $- \delta_i\uparrow + \delta_{i+1}\uparrow$ by $- \delta_{i+1}\uparrow$.

If at some stage, there are no terms left, then the result is 0.

These replacements are of course valid in Z arithmetic. So it is clear that this process results in a signed X term t* such that

$$3)\ t = t^*$$

with N arithmetic on the left and Z arithmetic on the right,
provided X holds.

Note that every step in the process raises the constants used by at most 1. In addition, lth(t*) ≤ lth(r*)+lth(s*) ≤ m. Hence #(t*) ≤ $(m-1)^2+m \leq m^2$. Also, t* is of form 3), where the δ's must obey the conditions iii-v in the definition of signed X sum. So t* is the desired signed X sum.

Finally, suppose t is (r)-(s), lth(r)+lth(s) = m. By the induction hypothesis, let r*,s* be signed X sums, lth(r*),lth(s*) < m, #(r*),#(s*) ≤ $(m-1)^2$, where r agrees with r* provided X holds, and s agrees with s* provided X holds. Then

$$4)\ t = (\beta_1\uparrow \pm \ldots \pm \beta_p\uparrow) - (\gamma_1\uparrow \pm \ldots \pm \gamma_q\uparrow)$$

with N arithmetic on the left and Z arithmetic for the two summands on the right,
provided X holds.

We can obviously assume that p,q ≥ 1. The - on the right is in N arithmetic. We will convert to Z arithmetic by comparing

$$\beta_1\uparrow \pm \ldots \pm \beta_p\uparrow$$
$$\gamma_1\uparrow \pm \ldots \pm \gamma_q\uparrow$$

simply on the basis of X, and not dependent on the values of variables. Recall that the β's are strictly decreasing in X, and the γ's are strictly decreasing in X.

Let i ∈ [0,min(p,q)] be greatest such that the first i terms of $\beta_1\uparrow \pm \ldots \pm \beta_p\uparrow$ and the first i terms of $\gamma_1\uparrow \pm \ldots \pm \gamma_q\uparrow$ are equal according to X (with the same signs).

If $\pm\ \beta_{i+1} <_X \pm\ \gamma_{i+1}$ then for all $x_1,\ldots,x_n$ obeying X,

$$\beta_1\uparrow \pm \ldots \pm \beta_p\uparrow < \gamma_1\uparrow \pm \ldots \pm \gamma_q\uparrow$$

with Z arithmetic.

If $\pm\ \beta_{i+1} >_X \pm\ \gamma_{i+1}$ then for all $x_1,\ldots,x_n$ obeying X,

$$\beta_1\uparrow \pm \ldots \pm \beta_p\uparrow > \gamma_1\uparrow \pm \ldots \pm \gamma_q\uparrow$$

with Z arithmetic.

It might be the case that $i+1 > \min(p,q)$. In this event, use 0 for the nonexistent term.

In the former case, use the signed X sum 0. In the latter case, rewrite 4) as

$$5)\ t = \beta_1\uparrow \pm \ldots \pm \beta_p\uparrow - \gamma_1\uparrow \pm \ldots \pm \gamma_q\uparrow$$

with N arithmetic on left and Z arithmetic on right, provided X holds.

where the second group of ± are reversed from what they were in 4). Now treat 5) as we treated 1), obtaining the form 2) with decreasing terms. QED

LEMMA 6.2.10. Let $t = y_1\uparrow \pm y_2\uparrow \pm \ldots \pm y_m\uparrow$ be parenthesized in any way, where the y's are distinct variables from $\{v_1,\ldots,v_n\}$.
i. t is equivalent to a term in ETM(0,1,+,-,↑).
ii. log(t) is equivalent to a term in ETM(0,1,+,-).
iii. $\pm y_1\uparrow \pm y_2\uparrow \pm \ldots \pm y_m\uparrow$, interpreted in Z arithmetic, is equivalent, in absolute value, to a term in ETM(0,1,+,-,↑).

Proof: Let t be as given. By Lemma 6.2.9, we obtain a system of signed X sums equivalent to t, under X, for the various n,n2-orderings. This provides the appropriate definition by cases of t. This establishes i).

For ii), note that under each of these n,n2-orderings X, t is equivalent to a signed X sum, which takes one of the form

$$0.$$
$$\beta\uparrow.$$
$$(\ldots(\beta_1\uparrow + \beta_2\uparrow \ldots).$$
$$(\ldots(\beta_1\uparrow - \beta_2\uparrow \ldots).$$

where in the last two cases, the number of β's is 2 or greater. Note that we have, respectively,

$$\log(t) = 0.$$
$$\log(t) = \beta.$$
$$\log(t) = \beta_1.$$
$$\log(t) = \beta_1-1.$$

which gives rise to a definition of log(t) by cases. The cases are given by the various n,n^2-orderings. This provides the appropriate definition by cases of log(t). This establishes ii).

For iii), let any n,n-ordering X be given. If the greatest y's under X appear with +, then we use $\pm y_1\uparrow \pm y_2\uparrow \pm \ldots \pm y_n\uparrow$. Otherwise, we reverse the ±. Then we rewrite in descending y's under X, and left associate, obtaining an equivalent expression in N arithmetic. No given the appropriate definition by cases, where the cases are given by the X's. QED

LEMMA 6.2.11. Let $s = y_1\uparrow \pm y_2\uparrow \pm \ldots \pm y_p\uparrow$ and $t = z_1\uparrow \pm z_2\uparrow \pm \ldots \pm z_q\uparrow$ be parenthesized in any way, where $\{y_1,\ldots,y_p,z_1,\ldots,z_q\} \subseteq \{x_1,\ldots,x_n\}$, and $y_1,\ldots,y_p,z_1,\ldots,z_q$ are distinct variables. Then $s\bullet t$ is equivalent to a term $r \in \mathrm{ETM}(0,1,+,-,\uparrow)$ whose variables are among $y_1,\ldots,y_p,z_1,\ldots,z_q$.

Proof: Let $s,t,y_1,\ldots,y_p,z_1,\ldots,z_q,n$ be as given.

According Lemma 6.2.9, under each such n,n^2-ordering X, we can write s,t as signed X sums

$$s = (\alpha_1\uparrow \pm \ldots \pm \alpha_b\uparrow).$$
$$t = (\beta_1\uparrow \pm \ldots \pm \beta_c\uparrow).$$

where the left sides use N arithmetic and the right sides use Z arithmetic.

We now have

$$(s)\bullet(t) = \gamma_1\uparrow \pm \ldots \pm \gamma_{bc}\uparrow.$$

where the left side uses N arithmetic and the right side uses Z arithmetic. Here each $\gamma\uparrow$ takes the form

$$\alpha_i\uparrow\bullet\beta_j\uparrow = (\alpha_i+\beta_j)\uparrow.$$

and hence each γ takes the form $\alpha_i+\beta_j$. We can now treat the various γ_i as new variables, and get an appropriate definition by cases for $\gamma_1\uparrow \pm \ldots \pm \gamma_{bc}\uparrow$ using Lemma 6.2.10 iii). We can then substitute the sums $\alpha_i+\beta_j$ for the new variables, and get the desired definition by cases for $(s)\bullet(t)$. QED

DEFINITION 6.2.13. Let $p \geq 0$. We define $\mathrm{TM}(0,1,+,-,\bullet,\uparrow,\log{:}p)$ as the terms in $\mathrm{TM}(0,1,+,-,\bullet,\uparrow,\log)$ where every occurrence of every variable is followed by (at least) p $\uparrow$'s.

DEFINITION 6.2.14. We define ETM(0,1,+,-,•,↑,log:p) as the terms in ETM(0,1,+,•,↑,log) where every occurrence of every variable is followed by (at least) p ↑'s. This applies to occurrences in both the terms and the quantifier free formulas.

As usual, we can omit some of the symbols 0,1,+,-,•,↑,log, for the above definition.

LEMMA 6.2.12. Let $p \geq 1$ and $t \in$ TM(0,1,+,-,↑:p). Then t is equivalent to a term of the form s_1↑ ± ... ± s_k↑, parenthesized in some way, where each $s_i \in$ TM(0,1,+,-,↑:p-1).

Proof: Let $p \geq 1$. We define * by recursion on terms $t \in$ TM(0,1,+,-,↑;p). The basis cases are t = 0,1,↑p(x_n). Define 0* = ↑p(x_1)-↑p(x_1). 1* = 0↑. ↑p(x_n)* = ↑p(x_n). t↑* = t*↑. (s+t)* = s*+t*. (s-t)* = s*-t*. QED

LEMMA 6.2.13. Let $t \in$ ETM(0,1,+,-,•,↑,log:p), $p \geq 1$, with at most one occurrence of log and • combined. Then t is equivalent to a term t* ∈ ETM(0,1,+,-,↑:p-1).

Proof: By Lemma 6.2.12, this holds if there are no occurrences of log and •. We can assume that either there is a unique occurrence of • and no occurrence of log, or there is a unique occurrence of log and no occurrence of •. Thus we have a split into the following two cases.

case 1. log(u) is a subterm of t. Then $u \in$ TM(0,1,+,-,↑:p). By Lemma 6.2.12, write

$$u = t_1↑ ± ... ± t_k↑$$

parenthesized in some way, where $t_1,\ldots,t_k \in$ TM(0,1,+,-,↑:p-1). Introduce distinct variables $y_1,\ldots,y_k$ for $t_1,\ldots,t_k$. By Lemma 6.2.10, log(y_1↑ ± ... ± y_k↑) is equivalent to some term $\alpha(y_1,\ldots,y_k) \in$ ETM(0,1,+,-) . By substitution, log(u) = log(t_1↑ ± ... ± t_k↑) is equivalent to a term $\alpha(t_1,\ldots,t_k) \in$ ETM(0,1,+,-,↑;p-1). Replace log(u) in t by $\alpha(t_1,\ldots,t_k)$, and expand to a term t* in ETM(0,1,+,-,↑). In this expansion, we use the same cases that we use for $\alpha(t_1,\ldots,t_k)$, moving these cases out in front. Therefore t* ∈ ETM(0,1,+,-,↑:p-1).

case 2. r•s is a subterm of t. Then r,s ∈ TM(0,1,+,-,↑:p). By Lemma 6.2.12, write

$$r = r_1\uparrow \pm \ldots \pm r_p\uparrow$$
$$s = s_1\uparrow \pm \ldots \pm s_q\uparrow$$

parenthesized in some way, where $r_1,\ldots,r_p,s_1,\ldots,s_q \in$ TM(0,1,+,-,↑;p-1). Introduce distinct variables $y_1,\ldots,y_p,z_1,\ldots,z_q$ for $r_1,\ldots,r_p,s_1,\ldots,s_q$. By Lemma 6.2.11, $(y_1\uparrow \pm \ldots \pm y_p)\bullet(z_1\uparrow \pm \ldots \pm z_q\uparrow)$ is equivalent to some term $\beta(y_1,\ldots,y_p,z_1,\ldots,z_q) \in$ ETM(0,1,+,-,↑) = ETM(0,1,+,-,↑:0). By substitution, $r\bullet s = (r_1\uparrow \pm \ldots \pm r_p\uparrow)\bullet(s_1\uparrow \pm \ldots \pm s_q\uparrow)$ is equivalent to the term $\beta(s_1,\ldots,s_p,t_1,\ldots,t_q) \in$ ETM(0,1,+,-,↑:p-1). Replace r•s in t by $\beta(s_1,\ldots,s_p,t_1,\ldots,t_q)$, and expand to a term t* in ETM(0,1,+,-,↑). In this expansion, we use the same cases that we use for $\alpha(t_1,\ldots,t_k)$, moving these cases out in front. Therefore t* ∈ ETM(0,1,+,-,↑:p-1).

QED

LEMMA 6.2.14. Let t ∈ ETM(0,1,+,-,•,↑,log:p), p ≥ n ≥ 1, with at most n occurrences of log and • combined. Then t is equivalent to a term t* ∈ ETM(0,1,+,-,↑:p-n).

Proof: We argue by induction on n ≥ 1, that the statement is true for all p ≥ n ≥ 1. The case n = 1 is Lemma 6.2.13. Suppose this is true for a fixed n ≥ 1. Let t ∈ ETM(0,1,+,-,•,↑,log:p), p ≥ n+1 ≥ 1, with exactly n+1 occurrences of log and • combined.

It is clear that there is an occurrence of log(u) where u has no log or •, or there is an occurrence of u•v, where u,v have no occurrence of log or •. I.e., there is a subterm s ∈ TM(0,1,+,-,•,↑,log) of t with exactly one occurrence of log and • combined. It is obvious that s ∈ TM(0,1,+,-,•,↑,log:p).

By Lemma 6.2.13, s is equivalent to a term r ∈ ETM(0,1,+,-,↑:p-1). Replace s in t by r, and expand the result to a term t′ by bring the cases inside r outside. Note that the cases inside r contain no occurrences of log and •. Then t′ ∈ ETM(0,1,+,-,•,↑,log:p-1) has at most n occurrences of log and • combined. Now apply the induction hypothesis to t′ to obtain the required t* ∈ ETM(0,1,+,-,↑:(p-1)-n)) = ETM(0,1,+,-,↑:p-(n+1)). QED

LEMMA 6.2.15. Let t ∈ ETM(0,1,+,-,•,↑,log:p), p ≥ 1, with at most p occurrences of log and • combined. Then t is equivalent to a term t* ∈ ETM(0,1,+,-,↑).

Proof: Immediate from Lemma 6.2.14. QED

LEMMA 6.2.16. Let $f:N^k \to N$ be given by a term in ETM(0,1,+,−,•,↑,log). If mesh(A) is sufficiently large, then ↑A is an infinite SOI for f.

Proof: Let f be given by t ∈ ETM(0,1,+,−,•,↑,log) with at most p occurrences of log and • combined, p ≥ 1.

Let t′ be the result of replacing every occurrence of every variable v in t by ↑p(v). Then t′ ∈ ETM(0,1,+,−,•,↑,log:p). By Lemma 6.2.15, let t′ be equivalent to t′* ∈ ETM(0,1,+,-,↑).

According to Lemma 6.2.8,

if mesh(A) is sufficiently large,
then ↑A is an infinite SOI for t′*,
and hence for t′.

Obviously,

if mesh(A) ≥ p and ↑A is an infinite SOI for t′,
then ↑(A+p) is an infinite SOI for t.

Therefore,

if mesh(A) is sufficiently large,
then ↑A is an infinite SOI for t.

QED

We can usefully sharpen the indiscernibility given by Lemma 6.2.16.

Recall Definition 5.2.2 of #(φ) in Definition

LEMMA 6.2.17. Fix r ≥ 1. If mesh(A) is sufficiently large, then ↑A is an infinite set of indiscernibles for all quantifier free formulas φ of (N,0,1,+,−,•,↑,log) with #(φ) ≤ r.

Proof: Let r ≥ 1. For each such $\varphi(v_1,...,v_r)$, define

$$f_\varphi(x_1,...,x_r) = 1 \text{ if } \varphi(x_1,...,x_r);\ 0 \text{ otherwise.}$$

Then f_φ ∈ BAF. Now apply Lemma 6.2.16 to each f_φ. The Lemma follows easily. QED

We now provide a required link between Lemma 6.2.16 and Chapter 4 in order to show that Propositions C,E-H hold in the recursive subsets of N - and in fact, in the subsets of N that have primitive recursive enumerations.

Let us now look at the proof given in Chapter 4 of Proposition B in ACA′ + 1-Con(MAH), with an eye towards showing that Propositions C,E-H hold in the sets with primitive recursive enumeration functions. This is Theorem 4.4.11.

Our strategy is to first rework much of sections 4.3 and 4.4 primitive recursively.

Before getting into full details, we now illustrate the power of Lemma 6.2.17 for this purpose. Note that in the proof of Theorem 4.4.11, we took the following step, which must now be avoided:

...By Ramsey's theorem for 2r-tuples in ACA′, we can find a p,q,b;r-structure $M = (N,0,1,<,+,f,g,c_0,c_1,...)$. ...

The notion of p,q,b;r-structure was defined just before Lemma 4.4.2. Note that in this context of N, the atomic indiscernibility clause 7′ is the only substantial clause.

We avoid this use of Ramsey's theorem for f,g ∈ BAF, as follows.

LEMMA 6.2.18. Let p,q,b,r ≥ 1, f ∈ ELG(p,b), g ∈ ELG(q,b), f,g ∈ SD ∩ BAF. Then $(N,0,1,<,+,f,g,(\uparrow A)_1,(\uparrow A)_2,...)$ is a p,q,b;r-structure, provided mesh(A) is sufficiently large. Here $(\uparrow A)_1,(\uparrow A)_2,...$ is the strictly increasing enumeration of the set ↑A.

Proof: Lemma 6.2.17 takes care of clause 7′. So this is immediate. QED

Lemma 6.2.18 takes care of one crucial step in the proof of Theorem 4.4.11. We still have to show that the D1 ⊆ ... ⊆ Dn ⊆ N there can be taken to be recursive, or even have primitive recursive enumeration functions.

Let us now proceed systemically. Our first aim is to obtain a new form of Theorem 4.3.8, and use it in an adaptation of section 4.4.

Recall the definition of a special SOI for $f:N^p \to N$ in Definition 4.3.6. We repeat this definition, by rearranging its components.

DEFINITION 6.2.15. Let $f:N^p \to N$ and $A \subseteq N$. We say that A is a special SOI for f if and only if the following holds.

a. The truth value of any statement

$$f(x_1,\ldots,x_p) < f(y_1,\ldots,y_p)$$

where $x_1,\ldots,x_p,y_1,\ldots,y_p \in A$, depends only on the order type of the 2p-tuple $(x_1,\ldots,x_p,y_1,\ldots,y_p)$.

b. Let $x_1,\ldots,x_p,y_1,\ldots,y_p \in A$. Suppose $(x_1,\ldots,x_p)$ and $(y_1,\ldots,y_p)$ have the same order type. Suppose also that for all $1 \leq i \leq p$, $x_i = y_i \vee y_i > \max(x_1,\ldots,x_p)$. Then i) $f(x_1,\ldots,x_p) \leq f(y_1,\ldots,y_p)$; ii) if $f(x_1,\ldots,x_p) < f(y_1,\ldots,y_p)$ then $f(y_1,\ldots,y_p)$ is greater than all $f(z_1,\ldots,z_p)$, $|z_1,\ldots,z_p| \leq |x_1,\ldots,x_p|$.

The conditions on $x,y \in A^p$ in b) play an important role. We say that x,y are specially related if and only if the conditions on $x,y \in A^p$ in b) hold.

Recall the key indiscernible stretching Lemma 4.3.5. Since ACA′ was being used freely, we did not consider any effectivity issues with regard to Lemma 4.3.5. We will refine Lemma 4.3.5 below. First we need a Lemma.

LEMMA 6.2.19. For all $p \geq 1$ there is a primitive recursive function $f:N^2 \to N$ such that the following holds. Let $x_0,\ldots,x_n \in N^p$, $c \in N$, where $n = f(c,|x_1|)$ and each $|x_{i+1}| \leq |x_i|+c$. Then there exists $1 \leq i < j \leq n$ such that x_i,x_{i+1} are specially related.

Proof: Fix $p \geq 1$. The statement

$$\begin{gathered}1)\ (\forall c,x_0)(\exists n)(\forall x_1,\ldots,x_n \in N^p) \\ ((\forall i \leq n-1)(|x_{i+1}| \leq |x_i|+c) \to \\ (\exists i < j)(x_i,x_{i+1} \text{ obey b}))\end{gathered}$$

is provable in the formal system WKL_0 (see [Si99]), as follows. Assume false, and fix c,x_0. Then apply WKL_0 to produce an infinite counterexample $x_0,x_1,\ldots \in N^p$. Then choose an infinite subsequence so that the p-tuples have the same order type and the first terms are all = or all <.

Iterate this construction for p steps, arriving at an infinite counterexample $y_0,y_1,\ldots$ where for all $1 \le i \le p$, the i-th coordinates are all = or all <. For j large enough, y_0,y_j are specially related. This is a contradiction.

It is obvious that 1) is in Π^0_2 form, and so we can apply our Theorem that every Π^0_2 sentence provable in WKL_0 has a primitive recursive bounding function. See [Si99,09], p. 37, p. 381. QED

LEMMA 4.3.5'. The following is provable in ACA'. Let $q \ge 3p \ge 1$, and $f:[0,q]^p \to N$. Assume $[0,q]$ is a special SOI for f. There exists primitive recursive $g:N^p \to N$ such that N is a special SOI for g, where $g|[0,q]^p$ is isomorphic to f in the following sense. For all $x,y \in [0,q]^p$, $f(x) \le f(y) \leftrightarrow g(x) \le g(y)$.

Proof: Let p,q,f be as given. The proof of Lemma 4.3.5 begins by putting the following recursive relation $\le^*$ on N^p. $x \le^* y$ if and only if there exists $\alpha,\beta \in [0,q]^p$ such that

i. (x,y) and (α,β) have the same order type.
ii. $f(\alpha) \le f(\beta)$.

In the proof of Lemma 4.3.5, it is shown that $\le^*$ is reflexive, connected, transitive, and its order type, modulo $=^*$, is finite or ω.

Then we defined $g:N^p \to N$ by

$g(x)$ is the position in $\le^*$ of x counting from 0.

We proved that g is as required here, except for "primitive recursive". We did not address any issues of effectivity for g in the proof of Lemma 4.3.5.

Thus it suffices to prove that g is primitive recursive.

We say that a finite or infinite sequence $x_0,x_1,\ldots \in N^p$ is complete if and only if each $x_i <^* x_{i+1}$, and every $y \in N^p$ is equivalent ($=^*$) to some x_i. By the proof of Lemma 4.3.5, there is a complete sequence.

Suppose $x_0,\ldots,x_n$ is a finite complete sequence. We claim that g is elementary recursive. Let $x \in N^p$. Return i such that $x =^* x_i$.

So we will assume that complete sequences are infinite. We fix a complete sequence $x_0,x_1,\ldots$. Obviously, all complete sequences are equivalent (=*), term by term.

We claim that for all $x \in N^p$ there exists $y \in N^p$ such that

1) $|y| \leq |x|+2^p+p$.
y is an immediate successor of x in <*.

To see this, let $x = (x_1,\ldots,x_p)$, and let $y = (y_1,\ldots,y_p)$ be an immediate successor of x in <* with least possible |y|. Assume $|y| > |x| + 2^p + p$.

Let y_i be a greatest coordinate of y. We claim that the greatest coordinate of y bigger than y_i is y_i-1. To see this, suppose otherwise, and let y' be the result of decrementing the y_i's in y by 1. Then x,y' and x,y have the same order type, and so x <* y'. Also y',y obeys the hypotheses of clause b), and so y' ≤* y. Hence y' is another immediate successor of x in <* of lower |y'|. This contradicts the choice of y.

Now the same argument will *not* show that the greatest coordinate of y bigger than y_i-1 is y_i-2. However, this argument does show that the greatest coordinate of y bigger than y_i-1 is at least y_i-3. This is because we can drop the y_i,y_i-1 in y by 2 each. We repeat this argument p times, thereby obtaining $\min(y) > |x|+p$. Then we can push all of the coordinates of y down by p, obtaining another immediate successor of x in <* of lower | |. This is a contradiction.

Next we claim that for all $x \in N^p$, not minimal in <*, there exists $y \in N^p$ such that

2) $|y| \leq |x|+2^p+p$.
y is an immediate predecessor of x in <*.

To see this, let $x = (x_1,\ldots,x_p)$, and let $y = (y_1,\ldots,y_p)$ be an immediate predecessor of x in <* with least possible |y|. Assume $|y| > |x| + 2^p + p$.

Let y_i be a greatest coordinate of y. If we raise the y_i in y by 1 then we obtain z with y ≤* z <* x. Hence y =* z.

We now claim that the greatest coordinate of y bigger than y_i is y_i-1. To see this, suppose otherwise, and let y' be the result of decrementing the y_i's in y by 1. Then y' <* x. Since y =* z, we have y =* y'. Hence y' is another immediate predecessor of x in <* of lower |y'|. This contradicts the choice of y.

Now the same argument will *not* show that the greatest coordinate of y bigger than y_i-1 is y_i-2. However, we now show that the greatest coordinate of y bigger than y_i-1 is at least y_i-3. This is because if otherwise, we can first raise the yi,y_i-1 in y by 2 each, with =*. Then we drop the y_i,y_i-1 in y by 2, also with =*, contradicting the choice of y.

We repeat this argument p times, thereby obtaining min(y) > |x|+p. Then we can push all of the coordinates of y first up by p, and then down by p, obtaining another immediate predecessor of x in <* of lower | |. This is a contradiction.

We now claim the following. Let x <* y <* z. There exists w such that

$$3)\ |w| \leq |x|+|z|+p.\quad x <^* w <^* z.$$

To see this, choose y such that x <* y <* z, where |y| is minimal. Assume |y| > |x|+|z|+p. We can move a nonempty tail of the coordinates of y that are > |x|+|z|, down by 1, obtaining y', with x <* y' <* z. This contradicts the choice of y.

Note that 3) gives us a bounded search algorithm for testing whether z is an immediate successor of x in <*.

From 1),2), we have

$$4)\ (\forall i \geq 1)(|x_i-1|,|x_i+1| \leq |x_i|+2^p+p).$$

We say that a complete sequence is minimal if and only if each x_i has minimum $|x_i|$ among the x =* x_i.

We can now build a minimal complete sequence algorithmically. Let x_1 be any <* minimal element of N^p. Suppose x_i has been defined. Search among the y with |y| ≤ $|x_i|+2^p+p$ for an immediate successor y of x_i in <*. By 1), there is such a y. By the previous paragraph, we can test whether y is an immediate successor of x_i in <*.

This construction provides a complete sequence $x_0,x_1,\ldots$ and an algorithm for producing x_i from i. It is easy to see that the running time of this algorithm is bounded by an iterated exponential. I.e., $x_0,x_1,...$ is elementary recursive.

However, we still have to show that the function

$$g(x) = \text{the unique } n \text{ such that } x = x_n$$

is primitive recursive. For this, we use Lemma 6.2.19. Let $x \in N^p$. Let $x = x_n$. We need to give an upper bound on n, primitive recursively in x.

Consider the sequence

$$x = x_n,x_{n-1},...,x_0 \in N^p.$$

Let $f:N^2 \to N$ be the primitive recursive function given by Lemma 6.2.19. If $n \geq f(2^p+p,|x|)$ then by Lemma 6.2.19,

there exists $1 \leq i \leq n$ such that x_{i+1},x_i are specially related.

But then, $x_{i+1} \leq^* x_i$, which is a contradiction. Hence we have the primitive recursive upper bound

$$n \leq f(2^p+p,|x|).$$

We can now compute g(x) primitive recursively, by computing $x_0,x_1,...$ elementary recursively, out to $f(2p+p,|x|)+1$ terms and testing for $x =^* x_i$. QED

The following adds to Lemma 4.3.7.

LEMMA 4.3.7'. The following is provable in ACA'. Every true $\nu(p,q,\psi)$ is primitive recursively true.

Proof: Let $\nu(p,q,\psi)$ be true. As in the proof of Lemma 4.3.7, there exists $f:[0,q]^p \to N$ in the sense of Lemma 4.3.5'. Now apply Lemma 4.3.4' and 4.3.6. QED

The following adds to Lemma 4.3.8.

THEOREM 4.3.8'. The following is provable in ACA'. Every true $\lambda(k,n,m,R_1,...,R_{n-1})$ is primitive recursively true.

Proof: Use Lemma 4.3.7' and the proof of Theorem 4.3.8. QED

Recall these definitions made in section 4.4:

p,q,b-structure. (Definition 4.4.2)
p,q,b;r-structure. (Definition 4.4.4)
p,q,b;r,n-special structure. (Definition 4.4.5)
p,q,b;r-type. (Definition 4.4.7)
p,q,b;r,n-special type. (Definition 4.4.7)

We need modified forms of the last four of these notions. For this purpose, let M* be a p,q,b;r-structure. Recall that M*<r> is the set of all values of closed terms of length ≤ r in M*. By the almost strict dominance of +*,f*,g* in M*, we see that M*<r> has order type ω.

DEFINITION 6.2.16. We say that M* is a p,q,b;r-structure/prim if and only if

i. M* is a p,q,b;r-structure.
ii. Every element of M* is the value of a closed term.
iii. The <* relation on closed terms is primitive recursive.

DEFINITION 6.2.17. A p,q,b;r-type/prim is the type of some p,q,b;r-structure/prim.

DEFINITION 6.2.18. We say that h:N → M* is primitive recursive if and only if there is a primitive recursive function h' from N into closed terms such that the value in M* of each h'(n) is h(n).

DEFINITION 6.2.19. A p,q,b;r,n-special structure/prim is a p,q,b;r,n-structure/prim in which witnessing D's can be found whose enumeration functions are primitive recursive.

DEFINITION 6.2.20. A p,q,b;r,n-special type/prim is the p,q,b;r-type of some p,q,b;r,n-special structure/prim.

The following adds to Lemma 4.4.4.

LEMMA 4.4.4'. The following is provable in RCA_0. Let M* be a p,q,b;r-structure. Then M*<r> is of order type ω. There is an increasing primitive recursive bijection f:N → M*<r>. Every p,q,b;r-type is a p,q,b;r-type/prim.

Proof: Let M* be a p,q,b;r-structure, M* = (N*,0*,1*,<*,+*,f*,g*,c_0*,...). Let α be a closed term of length at most r, representing an element of M*<r>, in which some c_i appears. The value of α must lie in [c_i*,c_{i+1}*), where i is greatest such that c_i appears in α.

There are only finitely many such α for each i. Also, if no c_i appears in α then the value of α lies in $[0,c_1)$, and there are only finitely many of these α, as well. Hence the order type of M*<r> is ω. Furthermore, there are obvious double exponential bounds on the sizes of these finite sets. We can use the p,q,b;r-type of M* and the restricted indiscernibility of the c*'s to obtain the increasing primitive recursive bijection f:N → M*<r>.

Let τ be the p,q,b;r-type of the p,q,b;r-structure M. We can build another p,q,b;r-structure on the basis of τ using the appropriate equivalence relation on terms of bounded length, so that the equivalence classes are finite. This construction is very effective in τ, and results in a p,q,b;r-structure/prim. QED

The following adds to Lemma 4.4.7.

LEMMA 4.4.7'. The following is provable in RCA_0. Every p,q,b;r,n-special type is a p,q,b;r,n-special type/prim.

Proof: Let τ be a p,q,b;r,n-special type. By Lemma 4.4.4', τ is a p,q,b;r-type/prim. From the proofs of Lemmas 4.4.5 and 4.4.6, we see that RCA_0 proves that the witnesses to τ being a p,q,b;r,n-special type are the same as the witnesses to some $\lambda(k,n,p+q+2,R_1,...,R_{n-1})$ explicitly produced from p,q,b,r,n,τ. Since τ is a p,q,b;r,n-special type, $\lambda(k,n,p+q+2,R_1,...,R_{n-1})$ it true. By Theorem 4.3.7', $\lambda(k,n,p+q+2,R_1,...,R_{n-1})$ is primitively recursively true. Hence τ is a p,q,b;r,n-special type/prim. QED

The following adds to Lemma 4.4.10.

LEMMA 4.4.10'. The following is provable in ACA' + 1-Con(MAH). $(\forall p,q,b,n \geq 1)(\exists r)(\forall \tau)(\tau$ is a p,q,b;r-type → τ is a p,q,b;r,n-special type/prim).

Proof: By Lemma 4.4.7' and 4.4.10. QED

THEOREM 6.2.20. Propositions C,E-H are primitive recursively true. I.e., there exist infinite A,B,C whose enumeration functions are primitive recursive. This is provable in ACA' + 1-Con(MAH).

Proof: We argue in ACA' + 1-Con(MAH). Let p,q,b,n ≥ 1, and f ∈ ELG(p,b), g ∈ ELG(q,b), where f,g ∈ SD ∩ BAF. Let r be given by Lemma 4.4.10'. By Lemma 6.2.18, we can find a p,q,b;r-structure $M = (N,0,1,<,+,f,g,c_0,c_1,...)$, where the c’s form a primitive recursive sequence of powers of 2. By Lemma 4.4.10’, **τ** is a p,q,b,n,r-special type/prim. Let M* = (N*,0*,1*,<*,+*,f*,g*,c_0*,c_1*,...) be a p,q,b;n,r-special structure/prim with p,q,b;r-type **τ**. Let $D_1^* \subseteq \ldots \subseteq D_n^* \subseteq$ M*<r> be infinite, where $D_1^* \subseteq \{c_0^*,c_1^*,\ldots\}$, each $f^*D_i^* \subseteq D_{i+1}^*$ ∪. $g^*D_{i+1}^*$, and $D_1^* \cap f^*D_n^* = \emptyset$, and where the enumeration functions of the D*’s are primitive recursive. Since M,M* have the same p,q,b;r-type, M*<r> and M<r> are isomorphic by a primitive recursive bijection. This isomorphism sends $D_1^*,\ldots,D_n^*$ to infinite $D_1 \subseteq \ldots \subseteq D_n \subseteq$ M<r> with primitive recursive enumeration functions, where $D_1 \subseteq \{c_0,c_1,\ldots\} \subseteq N\uparrow$, and each $fD_i \subseteq D_{i+1}$ ∪. gD_{i+1}, and $D_1 \cap fD_n = \emptyset$. QED

Note that Theorem 6.2.20 provides us with explicitly Π^0_3 forms of Propositions C,E-H as stated in Appendix A.

COROLLARY 6.2.21. Theorems 5.9.11 and 5.9.12 apply to Propositions C[prim], E[prim], F[prim], G[prim], H[prim].

Proof: By Theorem 6.2.20 and the fact that Propositions C[prim], E[prim], F[prim] immediately imply Propositions C,F,G. QED

Recall the tameness of the structure (N,+,↑) used in Lemma 6.2.5.

DEFINITION 6.2.21. The superexponential is the function f:N → N given by f(n) = 2^2^...^2, where there are n 2's. Here f(0) = 1, f(1) = 2.

We claim the same kind of tameness holds for (N,+,↑). This follows from the fact that the superexponential f satisfies the Semenov conditions discussed in section 4 of Appendix B.

The nontrivial fact that we need to verify is that for all m ≥ 1, the residues of the values of f mod m are ultimately periodic.

Thus it follows from [Se83] that (N,+f) has a natural expansion with elimination of quantifiers, and (N,+,f) is primitive recursively decidable. We make the following definitions.

LEMMA 6.2.22. If m is odd then the residues of f(0),f(1),... mod m are ultimately periodic.

Proof: Let 2^k be congruent to 1 mod m. Let $r > s \geq 1$ be such that $g(r) \equiv g(s)$ mod k. Then $g(r+1) \equiv g(s+1)$ mod m. To see this, we have to check that

$$2^{f(r)} - 2^{f(s)} \equiv 0 \bmod m.$$

Obviously,

$$2^{f(r)} - 2^{f(s)} = 2^{f(s)}(2^{f(r)-f(s)} - 1).$$

Since $k|f(r)-f(s)$, we see that $2^{f(r)-f(s)} = (2^k)^{(f(r)-f(s))/k}$. Since $2^k \equiv 1$ mod m, we see that $2^{f(r)-f(s)} \equiv 1$ mod m.

Hence we have periodicity for f(n), $n \geq r$, with period r-s. QED

LEMMA 6.2.23. If $n \geq 1$ then the residues of g(0),g(1),... mod n are ultimately periodic.

Proof: Write $n = 2^r m$, where $m \geq 1$ is odd. Then the residues of f(n),f(n+1),... mod n are just the residues of $f(n)/2^r, f(n+1)/2^r, \ldots$ mod m, multiplied by 2^r. Since the later residues are ultimately periodic, the former residues are ultimately periodic. QED

THEOREM 6.2.24. Let f be the superexponential. The first order theory of the structure (N,+,f) is primitive recursive.

Proof: By Lemma 6.2.23, f obeys the Semenov conditions from section 4 of Appendix B. QED

DEFINITION 6.2.22. The Presburger sets are the sets definable in (N,+). The exponentially Presburger sets are the sets definable in $(N,+,\uparrow)$. The superexponentially Presburger sets are the sets definable in (N,+,f), where f is the superexponential.

As stated earlier, we conjecture that a more careful argument will show that Propositions C,E-H hold in the superexponentially Presburger sets.

In light of the primitive recursive decision procedure for superexponential Presburger arithmetic in Theorem 6.2.24, Propositions C,E-H, when stated in the superexponentially Presburger sets, become Π^0_2 statements. We conjecture that these Π^0_2 statements are provably equivalent to 1-Con(SMAH) in ACA'.

6.3. A Refutation.

In Proposition A, can we replace ELG by the simpler and more basic SD? We refute this in a strong way. In particular, we refute Proposition C with ELG removed.

PROPOSITION α. For all f,g ∈ SD ∩ BAF there exist A,B,C ∈ INF such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

We will even refute the following weaker Proposition.

PROPOSITION β. Let f,g ∈ SD ∩ BAF. There exist A,B,C ⊆ N, |A| ≥ 4, such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

We assume Proposition β, and derive a contradiction.

We begin with a modification of Lemmas 5.1.6 and 5.1.7. Basically, these go through without any change in the proof, but we provide some additional details.

LEMMA 5.1.6'. Let f,g ∈ SD ∩ BAF. There exist f',g' ∈ SD ∩ BAF such that the following holds.
i) g'S = g(S*) ∪ 6S+2;
ii) f'S = f(S*) ∪ g'S ∪ 6f(S*)+2 ∪ 2S*+1 ∪ 3S*+1.

Proof: In the proof of Lemma 5.1.6, f',g' are constructed explicitly from f,g. It is obvious that if f,g ∈ SD ∩ BAF, then f',g' ∈ SD ∩ BAF. The verification goes through without change. QED

LEMMA 5.1.7'. Let f,g ∈ SD ∩ BAF and rng(g) ⊆ 6N. There exist A ⊆ B ⊆ C ⊆ N\{0}, |A| ≥ 3, such that
i) fA ∩ 6N ⊆ B ∪ gB;
ii) fB ∩ 6N ⊆ C ∪ gC;
iii) fA ∩ 2N+1 ⊆ B;
iv) fA ∩ 3N+1 ⊆ B;
v) fB ∩ 2N+1 ⊆ C;
vi) fB ∩ 3N+1 ⊆ C;
vii) C ∩ gC = ∅;
viii) A ∩ fB = ∅;

Proof: In the proof Lemma 5.1.6, f',g' are constructed explicitly from f,g. Then A,B,C are used from Proposition C, and it is verified that $A \subseteq B \subseteq C$, $A^* \subseteq B^* \subseteq C^* \subseteq N\backslash\{0\}$, and A^*,B^*,C^* obey i) - viii). Suppose $f,g \in SD \cap BAF$, $rng(g) \subseteq 6N$. Then $f',g' \in SD \cap BAF$, and we take A,B,C from Proposition β, $|A| \geq 4$. The same argument shows that $A \subseteq B \subseteq C$, $A^* \subseteq B^* \subseteq C^* \subseteq N\backslash\{0\}$, and A^*,B^*,C^* obey i) - viii). Obviously $|A^*| \geq 3$. QED

LEMMA 6.3.1. Suppose $n > m \wedge x > c \wedge 48n\uparrow-24m = 48x\uparrow-24c$. Then $n = x \wedge m = c$.

Proof: Let n,m,x,c be as given. Then

$$48n\uparrow-48x\uparrow = 24m-24c.$$
$$2(n\uparrow-x\uparrow) = m-c.$$
$$n \neq x \rightarrow \max(n,x)\uparrow \leq |2(n\uparrow-x\uparrow)| = |m-c| < \max(n,x).$$
$$n = x,\ m = c.$$

QED

Define $f:N^5 \rightarrow N$ as follows. Let $a,b,c,d,e \in N$.

case 1. $a = b = c \wedge |a,b,c,d,e| = e$. Define $f(a,b,c,d,e) = e+1$.

case 2. $a = b > c \wedge |a,b,c,d,e| = e$. Define $f(a,b,c,d,e) = e+2$.

case 3. $a = b < c \wedge |a,b,c,d,e| = e$. Define $f(a,b,c,d,e) = 48e\uparrow+12$.

case 4. $a < b = c \wedge |a,b,c,d,e| = e$. Define $f(a,b,c,d,e) = 48e\uparrow-24d$.

case 5. $a < b \wedge a = c \wedge |a,b,c,d,e| = e$. Define $f(a,b,c,d,e) = 48e\uparrow-24(d+1)$.

case 6. $a > b = c \wedge |a,b,c,d,e| = e$. Define $f(a,b,c,d,e) = 48e\uparrow-24(d+2)$.

case 7. otherwise. Define $f(a,b,c,d,e) = |a,b,c,d,e|+1$.

Define $g:N^5 \rightarrow 6N$ as follows. Let $n,t,m,r,s \in N$.

case 1. $n = t > m > r$, $s = 48n\uparrow-24m$. Define $g(n,t,m,r,s) = 48n\uparrow-24r$.

case 2. $n > t = m > r$, $s = 48n\uparrow-24m$. Define $g(n,t,m,r,s) = 48n\uparrow+12$.

case 3. otherwise. Define $g(n,t,m,r,s) = 48|n,t,m,r,s|+6$.

Note the modest use of t in the definition of g.

LEMMA 6.3.2. $f,g \in SD \cap BAF$. For all $S \subseteq N$, $S^*+1 \cup S^*+2 \cup \{48n\uparrow+12: n \in S^*\} \cup \{48n\uparrow-24(m+j): n,m \in S^* \wedge m \leq n \wedge j \leq 2\} \subseteq fS$. The outputs of cases 1-3 in the definition of g are pairwise disjoint.

Proof: Let $S \subseteq N$. At arguments from S, case 1 in the definition of f produces $S+1$; case 2 produces S^*+2, case 3 produces $48n\uparrow+12$, $n \in S^*$; case 4 produces the $48n\uparrow-24m$, $n,m \in S^*$, $m \leq n$; case 5 produces the $48n\uparrow-24(m+1)$, $n,m \in S^*$, $m \leq n$, and case 6 produces the $48n\uparrow-24(m+2)$, $n,m \in S^*$, $m \leq n$. (In cases 4-6, additional integers can be produced). Since $e > 0 \rightarrow 48e\uparrow-24(e+2) > e$, we see that $f \in SD \cap BAF$.

Note that if $n > m > r$ then $48n\uparrow-24r > 24n\uparrow > n$, and $48n\uparrow-24r > 48n\uparrow-24m$. Also, if $n > m > r$ then $48n\uparrow+12 > 48n\uparrow-24m,n$. Hence $g \in SD \cap BAF$.

The three cases in the definition of g yield integers congruent to 24,12,6 modulo 48, respectively. QED

We now apply Lemma 5.1.7' to f,g. Fix A,B,C according to Lemma 5.1.7'.

LEMMA 6.3.3. Let $n \in C$. There is at most one $m \in C$ such that $m < n \wedge 48n\uparrow-24m \in C$.

Proof: Let $m,m' \in C$, $m < m' < n$, $48n\uparrow-24m, 48n\uparrow-24m' \in C$. Then $g(n,n,m',m,48n\uparrow-24m') = 48n\uparrow-24m$. Hence $48n\uparrow-24m \in C \cap gC$, which contradicts Lemma 5.1.7' vii). QED

LEMMA 6.3.4. Let $n \in A^*$. Then $(\forall m \in C^*)(m < n \rightarrow 48n\uparrow-24m \notin C)$.

Proof: Let $n \in A^*$, $m \in C^*$, $m < n$, $48n\uparrow-24m \in C$. Then $g(n,m,m,\min(C),48n\uparrow-24m) = 48n\uparrow+12 \in gC$. By Lemma 5.1.7' vii), $48n\uparrow+12 \notin C$. By Lemma 6.3.2, $48n\uparrow+12 \in fA \cap 6N$. By Lemma 5.1.7' i), we have $48n\uparrow+12 \in B \cup gB$. Hence $48n\uparrow+12 \in gB$. Let $48n\uparrow+12 = g(a,t,b,c,d)$, $a,t,b,c,d \in B$. Then case 2 applies and $g(a,t,b,c,d) = 48a\uparrow+12$, $d = 48a\uparrow-24b$, $a > b > c$. Obviously $a = n$ and $b \in B^*$.

Thus we have b < n, and 48n↑-24b ∈ B, b,n ∈ B. Note that m < n, 48n↑-24m ∈ C, m,n ∈ C. By Lemma 6.3.3, m = b < a = n. Hence m ∈ B*, m < n, 48n↑-24m ∈ B.

By Lemma 6.3.2, m+1,m+2 ∈ fB. By Lemma 5.1.7' viii), we have m+1,m+2 ∉ A. In particular, m+1,m+2 ≠ n. Since m < n, we have m+2 < n. Let i ∈ {1,2} be such that m+i is odd, m+i < n. By Lemma 5.1.7' v), m+i ∈ C.

By Lemma 6.3.3, 48n↑-24(m+i) ∉ C. Note that n,m ∈ B*, m < n, and so by Lemma 6.3.2, 48n↑-24(m+i) ∈ fB. By Lemma 5.1.7' ii), 48n↑-24(m+i) ∈ C ∪ gC, 48n↑-24(m+i) ∈ gC. Let 48n↑-24(m+i) = g(x,t,b,c,d), x,t,b,c,d ∈ C. Then case 1 applies and g(x,t,b,c,d) = 48x↑-24c, d = 48x↑-24b, x > b > c. By Lemma 6.3.1, x = n ∧ m+i = c < b. Hence b < n, 48n↑-24b = d ∈ C, b,n ∈ C. By Lemma 6.3.3, b = m. This contradicts b > m+i. QED

THEOREM 6.3.5. Proposition α is refutable in RCA_0. In fact, Proposition β is refutable in RCA_0.

Proof: Let s,n ∈ A*, s < n. This is supported by |A| ≥ 3. Hence s ∈ C*. By Lemma 6.3.4, 48n↑-24s ∉ C. By Lemma 6.3.2, 48n↑-24s ∈ fA. By Lemma 5.1.7' i), we have 48n↑-24s ∈ B ∪ gB, 48n↑-24s ∈ gB. Let 48n↑-24s = g(a,t,b,c,d), a,t,b,c,d ∈ B. Then case 1 applies, and g(a,t,b,c,d) = 48a↑-24c, a > b > c, d = 48a↑-24b. By Lemma 6.3.1, a = n ∧ c = s. Now b < n ∧ 48n↑-24b ∈ B. Clearly b ∈ B* ⊆ C*. This contradicts Lemma 6.3.4. QED

APPENDIX A

PRINCIPAL CLASSES OF FUNCTIONS AND SETS

N is the set of all nonnegative integers. |x| is max(x).

MF is the set of all functions whose domain is a subset of some N^k and whose range is a subset of N.

SD is the set of all f ∈ MF such that for all x ∈ dom(f), f(x) > |x|.

EVSD is the set of all $f \in MF$ such that for all but finitely many $x \in dom(f)$, $f(x) > |x|$.

ELG is the set of all $f \in MF$ such that there exist $c,d > 1$ obeying the following condition. For all but finitely many $x \in dom(f)$, $c|x| \leq f(x) \leq d|x|$.

LB is the set of all $f \in MF$ such that there exists d obeying the following condition. For all $x \in dom(f)$, $|x| \leq d|x|$.

EXPN is the set of all $f \in MF$ such that there exists $c > 1$ obeying the following condition. For all but finitely many $x \in dom(f)$, $c|x| \leq f(x)$.

BAF is the set of all $f \in MF$ which can be written using $0,1,+,-,\bullet,\uparrow,\log$, where $x-y = \max(x-y,0)$, $x\uparrow = 2^x$, $\log(x) = \text{floor}(\log(x))$ if $x > 0$; 0 otherwise. Closure under definition by cases, using $<,=$, is derived in section 5.1.

INF is the set of all infinite subsets of N.

PRINCIPAL FORMAL SYSTEMS

The systems RCA_0, WKL_0, ACA_0 , ATR_0, Π^1_1-CA_0 of Reverse Mathematics (see section 0.4).

The systems ACA', ACA^+ (Definitions 1.4.1, 6.2.1).

The systems ZFC, MAH, SMAH, MAH^+, $SMAH^+$. MAH = ZFC + $\{$there exists an n-Mahlo cardinal$\}_n$. SMAH = ZFC + $\{$there exists a strongly n-Mahlo cardinal$\}_n$. MAH^+ = ZFC + $(\forall n < \omega)(\exists \kappa)(\kappa$ is an n-Mahlo cardinal). $SMAH^+$ = ZFC + $(\forall n < \omega)(\exists \kappa)(\kappa$ is a strongly n-Mahlo cardinal). (Definitions 4.1.1, 4.1.2).

INDEPENDENT PROPOSITIONS

PROPOSITION A. For all $f,g \in ELG$ there exist $A,B,C \in INF$ such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

PROPOSITION B. Let $f,g \in ELG$ and $n \geq 1$. There exist infinite $A_1 \subseteq \ldots \subseteq A_n \subseteq N$ such that
i) for all $1 \leq i < n$, $fA_i \subseteq A_{i+1} \cup. gA_{i+1}$;

ii) $A_1 \cap fA_n = \emptyset$.

PROPOSITION C. For all $f,g \in ELG \cap SD \cap BAF$, there exist $A,B,C \in INF$ such that

$$A \cup. fA \subseteq C \cup. gB$$
$$A \cup. fB \subseteq C \cup. gC.$$

$\cup.$ is disjoint union. Its presence indicates that its left and right sides are disjoint sets.

Trivial implications: $B \rightarrow A \rightarrow C$.

Proposition A is the Principal Exotic Case, which arises in Chapter 3 (see section 3.13). Proposition B is proved in Chapter 4 in ACA' + 1-Con(SMAH). Proposition C is shown in Chapter 5 to imply 1-Con(SMAH) in ACA'.

In section 6.1, we treat the following five Propositions.

PROPOSITION D. Let $f \in LB \cap EVSD$, $g \in EXPN$, $E \subseteq N$ be infinite, and $n \geq 1$. There exist infinite $A_1 \subseteq ... \subseteq A_n \subseteq N$ such that
i) for all $1 \leq i < n$, $fA_i \subseteq A_{i+1} \cup. gA_{i+1}$;
ii) $A_1 \cap fA_n = \emptyset$;
iii) $A_1 \subseteq E$.

PROPOSITION E. For all $f,g \in ELG \cap SD \cap BAF$ there exist $A \subseteq B \subseteq C \subseteq N$, each containing infinitely many powers of 2, such that

$$fA \subseteq B \cup. gB$$
$$fB \subseteq C \cup. gC$$

PROPOSITION F. For all $f,g \in ELG \cap SD \cap BAF$ there exist $A \subseteq B \subseteq C \subseteq N$, each containing infinitely many powers of 2, such that

$$fA \subseteq C \cup. gB$$
$$fB \subseteq C \cup. gC$$

PROPOSITIOIN G. For all $f,g \in ELG \cap SD \cap BAF$ there exist $A,B,C \subseteq N$, whose intersection contains infinitely many powers of 2, such that

$$fA \subseteq C \cup. gB$$
$$fB \subseteq C \cup. gC$$

PROPOSITIOIN H. For all $f,g \in ELG \cap SD \cap BAF$ there exist $A,B,C \subseteq N$, where $A \cap B$ contains infinitely many powers of 2, such that

$$fA \subseteq C \cup. gB$$

fB ⊆ C ∪. gC

Each of these seven Propositions are shown in ACA' to be equivalent to 1-Con(SMAH).

Trivial implications: D → B → A → C, and D → E → F → G → H.

In section 6.2, we treat the following arithmetic forms.

PROPOSITION C[prim]. For all f,g ∈ ELG ∩ SD ∩ BAF, there exist A,B,C ∈ INF with primitive recursive enumeration functions, such that

A ∪. fA ⊆ C ∪. gB
A ∪. fB ⊆ C ∪. gC.

PROPOSITION E[prim]. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A ⊆ B ⊆ C ⊆ N with primitive recursive enumeration functions, each containing infinitely many powers of 2, such that

fA ⊆ B ∪. gB
fB ⊆ C ∪. gC

PROPOSITION F[prim]. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A ⊆ B ⊆ C ⊆ N with primitive enumeration functions, each containing infinitely many powers of 2, such that

fA ⊆ C ∪. gB
fB ⊆ C ∪. gC

PROPOSITION G[prim]. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A,B,C ⊆ N with primitive recursive enumeration functions, whose intersection contains infinitely many powers of 2, such that

fA ⊆ C ∪. gB
fB ⊆ C ∪. gC

PROPOSITION H[prim]. For all f,g ∈ ELG ∩ SD ∩ BAF there exist A,B,C ⊆ N with primitive enumeration functions, where A ∩ B contains infinitely many powers of 2, such that

fA ⊆ C ∪. gB
fB ⊆ C ∪. gC

APPENDIX B - FRANCOISE POINT.

REFERENCES

[Al16] P. Aleksandrov, Sur la puissance des ensembles mesurables, Bulletin Comptes Rendus Hebdomadaires des Seances de l'Académie des Sciences, Paris, B. 162 (1916), 323-325, 1916.

[Ar59,62] V.I. Arnold, On the representation of continuous functions of three variables by the superpositions of continuous functions of two variables. Matem. Sbornik, 1959, 48:1, 3-74 and 1962, 56:3, 392.

[Ara98] T. Arai, Some results on cut-elimination, provable well-orderings, induction and reflection, Ann. Pure Appl. Logic 95 (1998), no. 1-3, 93-184.

[Art27] E. Artin, Uber die Zerlegung definiter Funktionen in Quadrate. Hamb. Abh. 5, 100-115 (1927); Collected Papers 273-288.

[As04] M. Aschenbrenner, Ideal membership in polynomial rings over the integers, Journal of the AMS, 17 (2004), 407-441.

[Av03] J. Avigad, Number theory and elementary arithmetic, Philosophia Mathematica, 11:257-284, 2003

[AH77] K. Appel and W. Haken, Every planar map is four-colorable. I. Discharging, Illinois Journal of Mathematics 21 (1977), 429-490

[AH77] K. Appel, W. Haken and J. Koch, Every planar map is four-colorable. II. Reducibility, Illinois Journal of Mathematics 21 (1977), 491-567.

[AH89] K. Appel and W. Haken, Every planar map is four colorable, A.M.S. Contemporary Math. 98 (1989).

[AK65] J. Ax and S. Kochen, Diophantine problems over local fields I. Amer. J. Math. 87, 1965, 605-630.

[AK65a] J. Ax and S. Kochen, Diophantine problems over local fields II. Amer. J. Math. 87, 1965, 631-648.

[AK66] J. Ax and S. Kochen, Diophantine problems over local fields III. Ann. Math. 83, 1966, 437-456.

[Ba75] J. Baumgartner, Ineffability properties of cardinals I. In: Hajnal-Rado-Sós, editors, Infinite and Finite Sets. Colloquia Mathematica Societatis Janos Bolyai vol. 10. Amsterdam, North-Holland 1975.

[Be73] C. Berge, Graphs and Hypergraphs, North-Holland Mathematical Library, 1973, English translation, originally published in French, 1970.

[Bek06] L. Beklemishev, The Worm principles. In: Z Chatzidakis, P. Koepke, W. Pohlers, editors, Logic Colloquium '02, Lecture Notes in Logic 27, ASL Publications.

[Bi11] L. Bieberbach, (1911), "Über die Bewegungsgruppen der Euklidischen Räume", Mathematische Annalen 70 (3): 297–336, doi:10.1007/BF01564500, ISSN 0025-5831

[Bi12] L. Bieberbach, (1912), "Über die Bewegungsgruppen der Euklidischen Räume (Zweite Abhandlung.) Die Gruppen mit einem endlichen Fundamentalbereich", Mathematische Annalen 72 (3): 400–412, doi:10.1007/BF01456724, ISSN 0025-5831

[Bo07] A. Bovykin, Unprovability of sharp versions of Friedman's sine-principle (2007), Proceedings of the American Mathematical Society, 135, 2967-2973.

[Br76] F. Browder (editor), Mathematical Developments Arising from Hilbert Problems, Proceedings of Symposia in Pure Mathematics XXVIII (1976), American Mathematical Society.

[Bu87] W. Buchholz, An independence result for Π^1_1-CA + BI, Annals of Pure and Applied Logic 33 (1987) 131-155.

[Bu91] W. Buchholz, Notation systems for infinitary derivations, Arch. Math. Logic 30 (1991), no 5-6, 177-196.

[BFPS81] W. Buchholz, S. Feferman, W. Pohlers, W. Sieg, Iterated Inductive Definitions and Subsystems of Anlysis: Recent Proof-Theoretical Studiees, Lecture Notes in Mathematics 897, Springer-Verlag, 1981.

[BG06] E. Boros and V. Gurvidh, Perfect graphs, kernels and cooperative games, Discrete Mathematics, 306 (2006) 2336-2354.

[BK96] H. Becker and A. Kechris, The Descriptive Set Theory of Polish Group Actions, London Math. Soc. Lecture Note Series, 232, Cambridge University Press, 1996.

[BGG01] E. Borger, E. Gradel, and Y. Gurevich, The Classical Decision Problem, Universitext, Springer, 2001.

[BM90] M.R. Burke, M. Magidor, Shelah's pcf Theory and its Applications, Annals of Pure and Applied Logic, vol. 50, no. 3, 1990, pp. 207-254.

[BW87] W. Buchholz and S. Wainer, Provably computable functions and the fast growing hierarchy. In: Logic and Combinatorics, Amer. Math. Soc., Contemporary Mathematics, Volume 65, 1987, pp. 179-198.

[Ci83] E.A. Cichon, A short proof of two recently discovered results using recursion theoretic methods, Proceedings of the AMS 87, 1983, pp. 704-706.

[Co63,64] P.J. Cohen, The independence of the continuum hypothesis. Proc. Nat. Acad. Sci. U.S.A. 50 (1963), 1143-1148; 51, 105-110.

[Co69] P.J. Cohen, Decision procedures for real and p-adic fields. Comm. Pure Appl. Math. XXII, 1969, 131-151.

[CDW10] L. Carlucci, P. Dehornoy, and A. Weiermann, Unprovability results involving braids, Proceedings of the London Mathematical Society, Proc. London Math. Soc. (2011) 102(1): 159-192.

[CFS10] D. Conlon, J. Fox, B. Sudakov, Higher Ramsey Numbers, J. Amer. Math. Soc., 23 (2010), 247-266.

[CGHJ05] Peter Cholak, Mariagnese Giusto, Jeffry Hirst, and Carl Jockusch, Free sets and reverse mathematics, in: Reverse Mathematics, ed. S. Simpson, Lecture Notes in Logic, Association for Symbolic Logic, 1905. http://www.nd.edu/~cholak/papers/preincollection.html

[CJS01], P. Cholak, C. Jockusch, T. Slaman, On the strength of Ramsey's theorem for pairs. Journal of Symbolic Logic, 66, No.1, 1-55 (2001).

[CLW11] L. Carlucci, G. Lee, A. Weiermann, Sharp thresholds for hypergraph regressive Ramsey numbers, Journal of Combinatorial Theory, Series A 118 (2011), pp. 558-585.

[CM07] M. Carl and B.Z. Moroz, On a Diophantine representation of the predicate of provability, Max-Planck Institute Preprint Series, 2007, 21 pages.

[CP86] G. Cherlin and F. Point, Humboldt University, Seminarberichte Number 86, Proceedings of the Fourth Easter Conference on Model Theory, Gross Koris, March 31 - April 5, 1986.

[CT06] A.M. Castravet and J. Tevelev, Hilbert's 14'th problem and Cox rings. Compositio Math. 142 (2006), 1479 - 1498.

[Da73] M. Davis, Hilbert's tenth problem is unsolvable, Amer. Math. Mon. Vol. 80, 1973, p. 233-269.

[Day61] D. Daykin, Hilbert's 17th problem. Ph.D. Thesis, unpublished (1961).

[De84] K. Devlin, Constructibility. Perspectives in Mathematical Logic. Berlin, Springer-Verlag 1984.

[Deh94] P. Dehornoy, Braid groups and left distributive operations, Trans. Amer. Math. Soc. 345 (1994), 115-150.

[Deh00] P. Dehornoy, Braids and Self Distributivity, Progress in Mathematics, volume 192; xvi + 624 pages, Birkhauser (2000).

[De01] M. Dehn, "Über den Rauminhalt", Mathematische Annalen 55 (1901), no. 3, p. 465–478.

[Dr98] L. van den Dries, Tame Topology and o-minimal Structures, London Mathematical Society Lecture Note Series, 248, Cambridge University Press, 1998.

[DG82] C. Dimitracopoulos and H. Gaifman, Fragments of Peano's Arithmetic and the MRDP theorem, in Logic and Algorithmic, Monogr. Enseign. Math. University of Geneva, 1982, pp. 187-206.

[DGL92] C. Delzell, L. Gonzalez-Vega, and H. Lombardi, A new rational and continuous solution for the Hilbert's 17th problem, Extracta Mathematicae 7(1) (1992), 59-64.

[DJ97] R. Dougherty and T. Jech, Left-Distributive Embedding Algebras, Electronic Research Announcements of the American Mathematical Society, Vol. 3, 28-37 (April 9, 1997).

[DJ97a] R. Dougherty and T. Jech, Finite left-distributive algebras and embedding algebras, Advances in Mathematics 130 (1997), 201–241.

[DLR95] D. Duffus, H. Lefmann, V. Rödl, Shift graphs and lower bounds on Ramsey numbers rk(l;r), Discrete Mathematics, Volume 137, Issue 1-3, p. 177-187, January 1995.

[DM94] L. van den Dries and C. Miller, On the real exponential field with restricted analytic functions, Israel J. Math. 85 (1994), 19–56.

[DM96] L. van den Dries and C. Miller, Geometric categories and o-minimal structures, Duke Math. J. 84 (1996), 497–540.

[DMM94] L. van den Dries, A. Macintyre, and D. Marker, The elementary theory of restricted analytic fields with exponentiation, Ann. of Math. 140 (1994), 183–205.

[DMR76] M. Davis, Y. Matiyasevich, and J. Robinson, Hilbert's Tenth Problem. Diophantine Equations: Positive Aspects of a Negative Solution, in: Mathematical developments arising from Hilbert Problems, Proceedings of Symposia in Pure Mathematics, Volume XXVIII, Part 2, 1976, 323-378.

[DP77] D.H.J. de Jongh and R. Parikh, Well-partial orderings and hierarchies, Nederl. Akad. Wetensch. Proc. Ser. A 80, Indag. Math. 39 (1977), no. 3, 195-207.

[DPR61] M. Davis, H. Putnam, J. Robinson, The decision problem for exponential Diophantine equations, Annals of Mathematics, Vol. 74, 1961, p. 425-436.

[DS96] G. Debs and J. Saint Raymond, Compact covering and game determinacy, Topology and Its Applications, vol 68 (1996), pp. 153-185.

[DS99] G. Debs and J. Saint Raymond, Cofinal $\boldsymbol{\Sigma}^1_1$ and $\boldsymbol{\Pi}^1_1$ subsets of N^N, Fundamenta Mathematicae, vol. 159 (1999), pp. 161-193.

[DS01] G. Debs and J. Saint Raymond, Compact covering mappings and cofinal families of compact subsets of a Borel set, Fundamenta Mathematicae, vol. 167 (2001), pp. 213-249.

[DS04] G. Debs and J. Saint Raymond, Compact covering mappings between Borel sets and the size of constructible reals, Transactions of the American Mathematical Society, vol. 356 (2004), pp. 73-117.

[DS07] G. Debs and J. Saint Raymond, Borel Lifting of Borel Sets: Some Decidable and Undecidable Statements, Memoirs of the AMS, vol. 187, No. 876, May 2007.

[Ec92] J. Ecalle, Introduction aux fonctions analysables et preuve constructive de la conjecture de Dulac. (French) Introduction to analyzable functions and constructive proof of the Dulac conjecture (Actualités Mathématiques. Current Mathematical Topics Hermann, Paris.) 1992.

[Eg98] L. Egidi, A quantifier elimination for the theory of p-adic numbers, Computational Complexity, 7 (1998), 205 - 263, Birkhauser Verlag, Basel 1998.

[El88] N. Elkies, On $A^4 + B^4 + C^4 = D^4$, Mathematics of Computation 51 (184), 1988, 825–835.

[En72] H.B. Enderton, A Mathematical Introduction to Logic, Academic Press, 1972, XIII+295.

[EHMR84] P. Erdos, A. Hajnal, A. Mate, R. Rado, Combinatorial Set Theory: Partition Relations for Cardinals, Studies in Logic and the Foundations of Mathematics, vol. 106, North-Holland, 1984.

[EM81] P. Erdos and G. Mills, Some bounds for the Ramsey-Paris-Harrington numbers, Journal of Combinatorial Theory, Series A Vol. 30, No. 1, January 1981, p. 53-70.

[EMS87] F. van Engelen, A.W. Miller, J. Steel, Rigid Borel sets and better quasiorder theory, in: Logic and Combinatorics, Contemporary Mathematics, Vol. 65, American Mathematical Society, 229-261.

[Fe60] S. Feferman, Arithmetization of metamathematics in a general setting, Fundamenta Mathematicae 49 (1960), 35-92.

[Fe64] Systems of predicative analysis, Journal of Symbolic Logic, vol. 29 (1964), pp. 1-30.

[Fe70] S. Feferman, Formal theories for transfinite iterations of generalized inductive definitions and some subsystems of analysis, in Intuitionism and Proof Theory, (Proc. Conf., Buffalo, 1968), pp. 303-326, North-Holland, Amsterdam, 1970.

[Fe82] S. Feferman, Inductively presented systems and the formalization of meta-mathematics, in Logic Colloquium '80, pp. 95-128, North-Holland, Amsterdam, 1982.

[Fe05] S. Feferman, Predicativity. The Oxford Handbook of the Philosophy of Mathematics and Logic (S. Shapiro ed.), Oxford University Press, Oxford (2005) 590-624.

[FeR79] J. Ferrante and C. Rackoff, 1979. The Computational Complexity of Logical Theories. Lecture Notes in Mathematics 718. Springer-Verlag.

[Fr67] H. Friedman, Subsystems of set theory and analysis, Ph.D., MIT, 1967.

[Fr69] H. Friedman, Bar induction and Π^1_1-CA, Journal of Symbolic Logic 34 (1969), 353-362.

[Fr70] H. Friedman, Iterated inductive definitions and Σ^1_2-AC, in: Intuitionism and Proof Theory, ed. A. Kino, j. Myhill, R.E. Vesley, Studies in Logic and the Foundations of Mathematics, North-Holland, 1970, pp. 435-442.

[Fr71] H. Friedman, Higher set theory and mathematical practice, Annals of Math. Logic, Vol. 2, No. 3, (1971), pp. 325-357.

[Fr71a] H. Friedman, A more explicit set theory, in: Axiomatic Set Theory, Proceedings of Symposia in Pure Mathematics, Vol. XIII, Part 1, AMS, 1971, 49-65.

[Fr73] H. Friedman, Countable Models of Set Theories, Lecture Notes in Mathematics, Vol. 337, Springer-Verlag, (1973), pp. 539-573.

[Fr74] H. Friedman, Some systems of second order arithmetic and their use, Proceedings of the International Congress of Mathematicians (Vancouver, B. C., 1974), Vol. 1, 1975, pp. 235–242.

[Fr75-76] H. Friedman, The Analysis Of Mathematical Texts, And Their Calibration In Terms Of Intrinsic Strength I-IV, 1975. The Logical Strength Of Mathematical Statements I, 1976. http://www.math.ohio-state.edu/%7Efriedman/manuscripts.html, Preprints, Drafts, and Abstracts, 1.

[Fr76] H. Friedman, Abstracts: Systems of second order arithmetic with restricted induction, I and II, J. Symbolic Logic 41 (1976), 557–559.

[Fr78] H. Friedman, On rates of growth and sizes of proofs, unpublished notes, Ohio State University, February, 1978.

[Fr79] H. Friedman, On the incompleteness of axiomatic set theory (abstract), unpublished notes, Ohio State University, March, 1978.

[Fr80] H. Friedman, A Consistent Fubini-Tonelli Theorem for Nonmeasureable Functions, Illinois J. Math., Vol. 24, No. 3, (1980), pp. 390-395.

[Fr80a] H. Friedman, Translatability and relative consistency II, unpublished notes, Ohio State University, September, 1980.

[Fr81] H. Friedman, On the Necessary Use of Abstract Set Theory, Advances in Math., Vol. 41, No. 3, September 1981, pp. 209-280.

[Fr81a] H. Friedman, Independence results in finite graph theory I-VII. Unpublished manuscripts, Ohio State University, 76 pages, February-March 1981.

[Fr82] H. Friedman, Beyond Kruskal's theorem, Unpublished manuscripts, Ohio State University, 48 pages, June-July 1982.

[Fr83] H. Friedman, Unary Borel Functions and Second Order Arithmetic, Advances in Math., Vol. 50, No. 2, November 1983, pp. 155-159.

[Fr84] H. Friedman, Notes on Kruskal's Theorem, Unpublished handwritten notes, Ohio State University, 163 pages, 1984.

[Fr86] H. Friedman, Necessary Uses of Abstract Theory in Finite Mathematics, Advances in Math., Vol. 60, No. 1, 1986, 92-122.

[Fr92] H. Friedman, The Incompleteness Phenomena, Proceedings of the AMS Centennial Celebration, AMS Centennial Publications, Volume II, Mathematics into the Twenty-first Century, 1992, pp. 49-84.

[Fr98] H. Friedman, Finite Functions and the Necessary Use of Large Cardinals, Annals of Math., Vol. 148, No. 3, 1998, pp. 803-893.

[Fr99] H. Friedman, #39:Large Cardinals/Synthesis, FOM posting, http://www.cs.nyu.edu/pipermail/fom/1999-April/003027.html

[Fr99a] H. Friedman, #53:Free sets/Reverse Math, FOM posting, http://www.cs.nyu.edu/pipermail/fom/1999-July/003306.html
http://www.cs.nyu.edu/pipermail/fom/1999-July/003307.html

[Fr99b] H. Friedman, Adjacent Ramsey Theory, #23, http://www.math.ohio-state.edu/%7Efriedman/manuscripts.html October, 1999.

[Fr99c] H. Friedman, #61:Finitist proofs of conservation, FOM posting, http://www.cs.nyu.edu/pipermail/fom/1999-September/003405.html September, 1999.

[Fr00] H. Friedman, #92:Thin Set Theorem, FOM posting, http://www.cs.nyu.edu/pipermail/fom/2000-June/004183.html

[Fr01] H. Friedman, Subtle Cardinals and Linear Orderings, Annals of Pure and Applied Logic 107 (2001), 1-34.

[Fr01a] H. Friedman, Boolean relation theory notes, October 6, 2001, 20 pages, http://www.math.ohio-state.edu/%7Efriedman/.

[Fr01b] H. Friedman, Lecture notes on baby Boolean relation theory, October 3, 2001, 11 pages, http://www.math.ohio-state.edu/%7Efriedman/.

[Fr01c] H. Friedman, Long Finite Sequences, Journal of Combinatorial Theory, Series A 95, 102-144 (2001).

[Fr02] H. Friedman, Internal finite tree embeddings, Reflections on the Foundations of Mathematics: Essays in honor of Solomon Feferman, ed. Sieg, Sommer, Talcott, Lecture Notes in Logic, volume 15, 62-93, 2002, ASL.

[Fr02a] H. Friedman, Equational Boolean relation theory, September 3, 2002, 25 pages, http://www.math.ohio-state.edu/%7Efriedman/.

[Fr02b] H. Friedman, Demonstrably necessary uses of abstraction, Hans Rademacher Lectures, University of Pennsylvania, September 17-20, 2002, 53 pages, http://www.math.ohio-state.edu/%7Efriedman/.

[Fr03a] H. Friedman, Primitive Independence Results, Journal of Mathematical Logic, Volume 3, Number 1, May 2003, 67-83.

[Fr03b] H. Friedman, Three quantifier sentences, Fundamenta Mathematicae, 177 (2003), 213-240.

[Fr04] H. Friedman, Working with Nonstandard Models, in: Nonstandard Models of Arithmetic and Set Theory, American Mathematical Society, ed. Enayat and Kossak, 71-86, 2004.

[Fr04a] H. Friedman, Adventures in the foundations of mathematics, VIGRE Lectures, Ohio State University, April 28-May 7, 2003, 64 pages, http://www.math.ohio-state.edu/%7Efriedman/.

[Fr04b] H. Friedman, Unprovable theorems, April 15, 2004, 11 pages, http://www.math.ohio-state.edu/%7Efriedman/.

[Fr05] H. Friedman, Selection for Borel relations, in: Logic Colloquium '01, Lecture Notes in Logic, LNL 20, Association for Symbolic Logic, ed. Matthias Baaz, Sy David Friedman, J. Krajicek, 151-169, 2005.

[Fr05a] H. Friedman, Metamathematics of comparability, in: Reverse Mathematics 2001, Lecture Notes in Logic, LNL 21, Association for Symbolic Logic, edited by S.G. Simpson, 201-218, 2005.

[Fr05b] H. Friedman, Maximal nonfinitely generated subalgebras, in: Reverse Mathematics 2001, Lecture Notes in Logic, LNL 21, Association for Symbolic Logic, edited by S.G. Simpson, 189-200, 2005.

[Fr06] Concept Calculus, October 25, 2006, 42 pages, abstract. http://www.math.ohio-state.edu/%7Efriedman/manuscripts.html, Preprints, Drafts, and Abstracts, No. 53, 2006.

[Fr07] H. Friedman, The Nineteenth Annual Tarski Lectures, Interpretations of Set Theory in Discrete Mathematics and Informal Thinking, UC Berkeley, April, 2007. Lecture 1: Interpretations, According to Tarski. Lecture 2: Interpreting Set Theory in Discrete Mathematics: Boolean Relation Theory. Lecture 3: Interpreting Set Theory in Ordinary Thinking: Concept Calculus. http://www.math.ohio-state.edu/%7Efriedman/manuscripts.html Preprints, Drafts, and Abstracts, No. 60, 2007.

[Fr07a] H. Friedman, New Borel independence results, unpublished, http://www.math.ohio-state.edu/%7Efriedman/manuscripts.html Preprints, Drafts, and Abstracts, No. 57, 2007.

[Fr07b] H. Friedman, Formal statements of Gödel's second incompleteness theorem, unpublished, http://www.math.osu.edu/~friedman/manuscripts.html, Preprints, Drafts, and Abstracts, No. 56, 2007.

[Fr08] H. Friedman, PA Incompleteness. Draft, January 23, 2008. Revised version to appear.

[Fr09] H. Friedman, The Inevitably of Logical Strength: strict reverse mathematics, in: Logic Colloquium '06, ASL, p. 135-183, 2009.

[Fr09a] H. Friedman, Strict Reverse Mathematics, Reverse Mathematics Workshop, University of Chicago, November 7, 2009, 19 pages. http://www.math.ohio-state.edu/%7Efriedman/manuscripts.html Lecture Notes, 47.

[Fr09-10] H. Friedman, FOM postings #340-433, FOM Archives, http://www.cs.nyu.edu/pipermail/fom/ May 13, 2009 - June 2, 2010,

[Fr10] H. Friedman, Forty years on his shoulders, in: Kurt Gödel and the Foundations of Mathematics: Horizons of Truth, Cambridge University Press, 2010.

[Fr10a] H. Friedman, Adjacent Ramsey Theory, http://www.math.ohio-state.edu/%7Efriedman/manuscripts.html Preprints, Drafts, and Abstracts, No. 66, 2010, 17 pages.

[Fr11] H. Friedman, Concept Calculus: Much Better Than, in: Infinity, New Research Frontiers, ed. Michael Heller, and W. Hugh Woodin, Cambridge University Press, 2011, 311 pages.

[Fr∞] H. Friedman, Gödel Incompleteness Restated, in preparation.

[FH90] H. Friedman and J. Hirst, Weak comparability of well orderings and reverse mathematics, Annals of Pure and Applied Logic, vol. 7 (1990), pp. 11-29.

[FH91] H. Friedman and J. Hirst, Reverse mathematics of homeomorphic embeddings, Annals of Pure and Applied Logic, vol. 54 (1991), pp. 229-253.

[FFMS00] H. Friedman, S. Feferman, P. Maddy, J. Steel, Does mathematics need new axioms?, The Bulletin of Symbolic Logic, volume 6, Number 4, December 2000, 401-446.

[FMS82] H. Friedman, K. McAloon, S. Simpson, A finite combinatorial principle which is equivalent to the 1-consiteny of predicative analysis, in: Patras Logic Symposion, Studies in Logic and the Foundations of Mathematics, North-Holland, 1982.

[FMW∞] H. Friedman, A. Montalban, and A. Weiermann, Logical analysis of forms of Kruskal's Theorem, in preparation.

[FOM] Archives of the FOM e-mail list, from September 1997 to present, http://www.cs.nyu.edu/pipermail/fom/

[FR74] M. Fischer and M. Rabin, Super exponential complexity of Presburger arithmetic. SIAM-AMS Proceedings 7, 27 - 41.

[FRS87] H. Friedman, N. Robertson, P. Seymour, The metamathematics of the graph minor theorem, in: Logic and Combinatorics, Contemporary Mathematics, Vol. 65, American Mathematical Society, 229-261.

[FS00] H. Friedman and S. Simpson, Issues and problems in reverse mathematics, 127-144, in: Computability Theory and Its Applications, ed. Cholak, Lempp, Lerman, Shore, American Mathematical Society, 2000.

[FSS83] H. Friedman, S. Simpson, and R. Smith, Countable algebra and set existence axioms, Annals of Pure and Applied Logic 25 (1983), 141-181. Addendum: Annals of Pure and Applied Logic 27 (1985), 319-320.

[FSh95] H. Friedman and M. Sheard, Elementary descent recursion and proof theory, Annals of Pure and Applied Logic 71 (1995), pp. 1-45.

[FSt89] H. Friedman and L. Stanley, A Borel Reducibility Theory for Classes of Countable Structures, J. of Symbolic Logic, Vol. 54, No. 3, September 1989, pp. 894-914.

[FVxx] H. Friedman and A. Visser, Interpretations Between Theories, book in preparation.

[FWa] H. Friedman and A. Weiermann, Embeddings between unstructured and structured trees, in preparation.

[FWb] H. Friedman and A. Weiermann, Kruskal's Theorem and ATR_0, in preparation.

[Gi87] J.Y. Girard, Proof Theory and Logical Complexity, Bibliopolis, 1987, 500 pages.

[Go29] K. Gödel, On the completeness of the calculus of logic. In [Go86-03], Vol. I, 61-101.

[Go31] K. Gödel, On formally undecidable propositions of Principia mathematica and related systems I. In: [Go86-03], Vol. I, 145-195.

[Go38] K. Gödel, The consistency of the axiom of choice and of the generalized continuum hypothesis. In: [Go86-03], Vol. II, 26-27.

[Go86-03] Collected Works. Vol. I-V. Oxford: Oxford University Press (S. Feferman et al., editors).

[Goo44] R.L. Goodstein, On the restricted ordinal theorem, Journal of Symbolic Logic 9, 1944, pp. 33-41.

[Gor89] L. Gordeev, Generalizations of the one-dimensional version of the Kruskal-Friedman theorems, Journal of Symbolic Logic, Vol. 54, No. 1, March 1989, 100-121.

[Gor90] L. Gordeev, Generalizations of the Kruskal-Friedman Theorems, Journal of Symbolic Logic, Vol. 55, No. 1, March 1990.

[Gor93] L. Gordeev, Strong well-quasi-ordering tree theorem, Preprint (1993), talk at Fourteenth British Combinatorial Conference (Keele, 1993).

http://www-ls.informatik.uni-tuebingen.de/gordeew/publikationen/QuasiOrdering.pdf

[Gow01] W.T. Gowers, A new proof of Szemeredi's theorem, Geometric and Functional Analysis, Volume 11, No. 3, 2001, pp. 465-588.

[Gr62] O. A. Gross, Preferential arrangements, Amer. Math. Monthly 69 (1962), 4–8.

[Gu94] R.K. Guy, Unsolved Problems in Number Theory, 2nd ed. New York: Springer-Verlag, pp. 139-144 and 192-193, 1994.

[GD82] H. Gaifman, C. Dimitracopoulos, Fragments of Peano Arithmetic and the MRDP theorem. In: Logic and algorithmic (Zurich, 1980) (Monograph. Enseign. Math., 30), Geneve, Univ. Geneve, 1982 p. 187-206.

[GLP98] J. Ghoshal, R.C. Laskar, D. Pillone, Topics on Domination in Directed Graphs, in: [HSS98].

[GRS80,90] R.L. Graham, B.L. Rothschild, J.H. Spencer, Ramsey Theory, John Wiley & Sons, 1980. Second edition, 1990.

[GS53] D. Gale and F. Stewart, Infinite games with perfect information, in: H.W. Kuhn and A.W. Tucker (eds.) Contributions to the Theory of Games, vol. 2, Annals of Mathematical Studies #28, Princeton University Press, 1953, 245-266.

[Ha10] G.H. Hardy, Orders of Infinity, Cambridge University Press, 1910, Cambridge Tracts in Mathematics, vol. 12.

[Ha12] G.H. Hardy, Properties of logarithmico-exponential functions, Proc. London Math. Soc. 10 (1912), 54–90.

[Has94] R. Hasegawa, Well-ordering of algebras and Kruskal's theorem, Logic, Language, and Csomputation, 133-172, Lecture Notes in Computer Science, 792, Berlin, 1994.

[Hau16] F. Hausdorff, Die Mächtigkeit der Borelschen Mengen, Mathematische Annalen, 77 (1916), 430-437, 1916.

[He26] G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math. Ann. 95 (1926), 736–788.

[Hei86] G. Heinzmann, ed., Poincaré, Russell, Zermelo et Peano. Textes de la discussion (1906-1912) sur les fondements des mathématiques: des antinomies à la prédicativité, Albert Blanchard (Paris), 1986.

[Hi11890] D. Hilbert, Uber die Theorie der algebraischen Formen, Math. Ann., 36, (1890), 473-534.

[Hi00] D. Hilbert, "Mathematical Problems", Bulletin of the American Mathematical Society, vol. 8, no. 10 (1902), pp. 437-479. Earlier publications (in the original German) appeared in *Göttinger Nachrichten*, 1900, pp. 253-297, and *Archiv der Mathematik und Physik*, 3dser., vol. 1 (1901), pp. 44-63, 213-237.

[Hig52] G. Higman, Ordering by divisibility in abstract algebras, Proceedings of the London Mathematical Society, vol. 2 (1952), pp. 326-336.

[Hir94] J. Hirst, Reverse mathematics and ordinal exponentiation, Annals of Pure and Applied Logic 66 (1994), 1-18.

[Hir98], Reverse mathematics and ordinal multiplication, Mathematical Logic Quarterly, 44, (1998) 459-464.

[HB34,39] D. Hilbert and P. Bernays, Grundlagen der Mathematik, Vol. I. Berlin, 1934, xii + 471 pp.; Vol. II, Berlin 1939, xii + 498 pp. Second edition, Grundlehren der mathematischen Wiβenschaften, Springer-Verlag, 1968-1970, volume I, XV + 475 pages, volume II, XIV + 561 pages.

[HHS98] T.W. Haynes, S.T. Hedetniemi, P.J. Slater, Fundamentals of Domination in Graphs, Marcel Dekker, 1998.

[HK96] G. Hjorth and A. Kechris, Borel equivalence relations and classifications of countable models, Ann. Pure and Appl. Logic 82 (1996), 221-272.

[HK97], G. Hjorth and A. Kechris, New dichotomies for Borel equivalence relations, Bull. Symb. Logic 3(3) (1997), 329-346.

[HK01] G. Hjorth and A. Kechris, Recent developments in the theory of Borel reducibility, Fund. Math. 170(1) (2001), 21-52 (volume dedicated to the memory of J. Los).

[HKL98] G. Hjorth, A. Kechris, and A. Louveau, Borel equivalence relations induced by actions of the symmetric group, Ann. Pure and Appl. Logic 92 (1998), 63-112.

[HKS87] A. Hajnal, A. Kanamori, S. Shelah, Regressive Partition Relations for Infinite Cardinals, Transactions of the American Mathematical Society, Volume 299, Number 1, January 1987, 145-154.

[HMSS855] L.A. Harrington, M.D. Morley, A. Scedrov, S.G. Simpson (eds.), Harvey Friedman's Research on the Foundations of Mathematics, Studies in Logic and the Foundations of Mathematics, vol. 117, North-Holland, 1985.

[HP93] P. Hajek, P. Pudlak, Metamathematics of First-Order Arithmetic, Perspectives in Mathematical Logic, Springer, 1993.

[Il91] Yu.S. Il'yashenko, Finiteness theorems for limit cycles. (Translations of Mathematical Monographs, 94. American Mathematical Society, Providence, RI. 1991.

[Ja80] G. Jäger, Theories for iterated jumps, unpublished notes, Oxford, 1980.

[Je78,06] T. Jech, Set Theory, Academic Press, 1978, 621 p. Third Edition, Springer, 2006, 772 p.

[Jen72] R. Jensen, The fine structure of the constructible hierarchy. AML 4 (1972), 229-308.

[Jer73] R. Jerosolow, Redundancies in the Hilbert-Bernays Derivability Conditions for Gödel's Second Incompleteness Theorem, J. Symbolic Logic Volume 38, Issue 3 (1973), 359-367.

[Ka89] A. Kanamori, Regressive Partitions and Borel Diagonalization, The Journal of Symbolic Logic 54(1989), 540-552.

[Ka91] A. Kanamori, Regressive Partitions, Borel Diagonalization, and n-subtle cardinals, Annals of Pure and Applied Logic 52(1991), 65-77.

[Ka94] A. Kanamori, The Higher Infinite, Perspectives in Mathematical Logic, Springer, 1994.

[Ke95] A. Kechris, Classical Descriptive Set Theory, Graduate Texts in Mathematics, 156, Springer-Verlag, 1994.

[Kre60] G. Kreisel, Sums of squares. Summaries of Talks Presented at the Summer Institute in Symbolic Logic in 1957 at Cornell Univ., Institute Defense Analyses, Princeton (1960), 313–320.

[Kre68] G. Kreisel, Survey of Proof Theory, The Journal of Symbolic logic, Vol. 33, No 3 (Sept., 1968), pp. 321-388.

[Kri89a] I. Kriz, Proving a witness lemma in better-quasiordering thery: the method of extensions, Mathematical Proceedings of the Cambridge Philosophical Society 106 (1989), 253-262.

[Kri89b] I. Kriz, Well quasiordering finite trees with gap condition, Annals of Mathematics 130 (1989), 215-226.

[Kri95] I. Kriz, The structure of infinite Friedman trees, Advance in Mathematics, 115 (1995), 141-199.

[Kr60] J.B. Kruskal, Well-quasi-ordering, the tree theorem, and Vazsonyi's conjecture, Transactions of the American Mathematical Society, vol. 95 (1960), pp. 210-225.

[KM87] A. Kanamori and K. McAloon, On Gödel Incompleteness and Finite Combinatorics, Annals of Pure and Applied Logic 33(1987), 23-41.

[KP82] L. Kirby and J. Paris, Accessible independence results for Peano arithmetic, Bulletin of the London Mathematical Society, 14, 1982, pp. 285-293.

[KW10] P. Koellner, W.H. Woodin, Large Cardinals from Determinacy, in: Handbook of Set Theory, eds. M. Foreman, A. Kanamori, M. Magidor, 2010.

[La71] R. Laver, On Fraïssé's order type conjecture, Annals of Mathematics 93 (1971), 89-111.

[La92] R. Laver, The left distributive law and the freeness of an algebra of elementary embeddings, Adv. Math. 91 (1992), 209-231.

[Lar04] P. Larson, The Stationary Tower, University Lecture Series, vol. 32, AMS, Providence, RI, 2004.

[Lz95] R. Laver, On the algebra of elementary embeddings of a rank into itself, Adv. Math. 110 (1995), 334-346.

[LL66] H. Lauchli and J. Leonard, On the elementary theory of linear orderings, Fundamenta Matematicae, vol. 59 (1966), pp. 109–116.

[LM87] M. Loebl and J. Matoušek, On undecidability of the weakened Kruskal theorem. Logic and combinatorics (Arcata, Calif., 1985), 275-280, Contemp. Math., 65, Amer. Math. Soc., Providence, RI, 1987.

[LN92] M. Loebl, J. Nesetril, An unprovable Ramsey-type theorem,. Proceedings of the AMS, Vol. 116, Issue 3, 819-824, 1992.

[Ma96] Dave Marker, Model Theory and Exponentiation, Notices of the AMS, July 1996, volume 43, number 7, 753-759.

[Ma02] Dave Marker, Model Theory: An Introduction, Graduate Texts in Mathematics, Springer, 342 p, 2002.

[Mac11] A. Macintyre, The Impact of Gödel's Incompleteness Theorems on Mathematics. In: Horizons of Truth, Cambridge University Press, 2011.

[Mah11] P. Mahlo, Über lineare transfinite Mengen. BKSG 63 (1911), 187-225.

[Mah12] P. Mahlo, Zur Theorie und Anwendung der ρ_0-Zahlen. BKSG 64 (1912), 108-112.

[Mah13] Zur Theorie und Anwendung der ρ_0-Zahlen II. BKSG 65 (1913), 268-282.

[Mar96], A. Marcone, On the logical strength of Nash-Williams' theorem on transfinite sequences, in: Logic: From Foundations to Applications, Keele 1993, ed. W. Hodges, M. Hyland, C. Steinhorn, J. Truss, Oxford Science Publications, Oxford University Press, 1996, pp. 327-351.

[Mart69] D. Martin, Measurable cardinals and analytic games, Fund. Math. 66 (1969/1970), 287-291.

[Mart74] D.A. Martin, Σ^0_4-determinacy, circulated handwritten notes dated March 20, 1974.

[Mart75] D.A. Martin, Borel Determinacy, Annals of Mathematics, 102, 1975, 363-371.

[Mat70] Y. Matiyasevich, (1970). "Диофантовость перечислимых множеств [Enumerable sets are Diophantine]" (in Russian). Doklady Akademii Nauk SSSR 191: 279–282. English translation in Soviet Mathematics 11 (2), pp. 354-357.

[Mat93] Y. Matiyasevich, Hilbert's Tenth Problem, Foundations of Computing Series, MIT Press, 264 + i-vii, 1993.

[Math01] A. Matthias, Journal of Symbolic Logic 66 (2001) 487-496.

[Mc10] C. McLarty, What Does It Take to Prove Fermat's Last Theorem? Grothendieck and the Logic of Number Theory. Bulletin of Symbolic Logic 16 (3), 2010, 359-377.

[Mi94] C. Miller, Exponentiation is hard to avoid, Proc. Amer. Math. Soc. 122 (1994), 257–259.

[Min73] G. Mints, Quantifier-free and one-quantifier systems, Journal of Mathematical Sciences, Volume 1, Number 1, January, 1973, 71-84.

[Mo06] A. Montalban, Indecomposable linear orderings and hyperarithmetic analysis, J. Math. Log., vol. 6 (2006), no. 1, pp. 89–120.

[Mo∞] A. Montalban, On the Π^1_1 separation principle, Mathematical Logic Quarterly, to appear.

[MR10] B. Mazur, and K. Rubin, Ranks of twists of elliptic curves and Hilbert's Tenth Problem, Inventiones Mathematicae, 2010.

[MS∞] A. Montalban and R. Shore, The limits of determinacy in second order arithmetic, to appear.

[MSt89] D. Martin and J. Steel, A proof of Projective Determinacy, JAMS 85 (1988), 6582-6586, 1989.

[MT07] M.O. MedSalem, and K. Tanaka, Δ^0_3-determinacy, comprehension and induction, Journal of Symbolic Logic 72, 452-462.

[MT08] M.O. MedSalem and K. Tanaka, Weak determinacy and iterations of inductive definitions, in Computational Prospects of Infinity, Part II: Presented Talks, C. Chong, Q. Feng, T. Slaman, H. Woodin, and Y. Yang, Y. eds., LNS, Institute for Mathematical Sciences, National University of Singapore, World Scientific, Singapore, 333-353.

[MW96] A. Macintyre and A. Wilkie. On the decidability of the real exponential field. In P. Odifreddi, editor, Kreiseliana - About and Around Georg Kreisel, pages 441--467. A K Peters, 1996.

[Na59] M. Nagata, On the 14th problem of Hilbert, Am. J. Math., 81 (1959), p. 766.

[Ne95] I. Neeman, Optimal proofs of determinacy, Bulletin of Symbolic Logic, Vol. 1, No. 3 (Sep., 1995), pp. 327-339.

[Ne09] I. Neeman, The strength of Jullien's indecomposability theorem, J. of Mathematical Logic, vol. 8 (2008, published June 2009), pp. 93–119.

[Ne∞1] I. Neeman, Determinacy in L($\Re$), to appear in Handbook of Set Theory, M. Foreman and A. Kanamori (Editors).

[Ne∞2] I. Neeman, Necessary use of Σ^1_1 induction in a reversal, to appear.

[NMT07] T. Nemoto, M.O. MedSalem, and K. Tanaka, Infinite games in the Cantor space and subsystems of second order arithmetic, Mathematical Logic Quarterly 53, 226-236.

[NW63] C.St.J.A. Nash-Williams, On well-quasi-ordering finite trees, Proceedings of the Cambridge Philosophical Society, vol. 59 (1963), pp. 833-835.

[NW65] C.St.J.A. Nash-Williams, On well-quasi-ordering infinite trees, Proceedings of the Cambridge Philosophical Society, vol. 61 (1965), pp. 697-720.

[NW68] C.St.J.A. Nash-Williams, On better-quasi-ordering transfinite sequences, Proc. Cambridge Philosophical Society, vol. 64 (1968), 273-290.

[Pa70] C. Parsons, On a number-theoretic choice schema and its relation to induction, in: *Intuitionism and Proof Theory: Proceedings of the Summer Conference at Bu®alo N.Y. 1968*, A. Kino, J. Myhill, and R. E. Vesley, eds., North-Holland, Amsterdam, pp. 459-473.

[Po06] H. Poincaré, Les mathématiques et la logique, Revue de métaphysique et de morale 14, 294-317, 1906. Reprinted in Heinzmann (1986), 11-53.

[Pr29] M. Presburger, Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, Comptes rendus du I", Congrès des Mathématiciens des pays Slaves, Marszawa, pp. 92-101.

[PH77] J. Paris and L. Harrington, A mathematical incompleteness in Peano arithmetic, in; Handbook of Mathematical Logic, ed. J. Barwise, North-Holland, 1977, pp. 1133-1142.

[PS86] A. Pillay and C. Steinhorn, Definable sets in ordered structures I, Trans. Amer. Math. Soc. 295 (1986), 565–592.

[Ra30] R.P. Ramsey, On a problem of formal logic, Proc. London Math. Soc. 30, 1930, pp. 264-286.

[Rab68] M. Rabin, Decidability of second order theories and automata on infinite trees, Tans. Am. Math. Soc., 141, 1-35.

[Rab77] M. Rabin, Decidable theories, Handbook fo Mathematical Logic, ed. Jon Barwise, 1977, Elsevier, p. 595 - 829.

[Ri46] M. Richardson, On weakly ordered systems, Bull. Amer. Math. Soc., 52 (1946).

[Ri53] M. Richardson, Solutions of Irreflexive Relations, The Annals of Mathematics, Second Series, Vol. 58, No. 3 (Nov., 1953), pp. 573-390.

[Ro52] R.M. Robinson, An essentially undecidable axiom system, Proceedings of the 1950 International Congress of Mathematicians, Cambridge MA, 1952, pp. 729-730.

[Rob55] A. Robinson, On ordered fields and definite forms. Math. Ann. 130 (1955), 257–271.

[Rob56] A. Robinson, Further remarks on ordered fields and definite forms. Math. Ann. 130 (1956), 405–409.

[Robs78a] J.C. Robson, Polynomials satisfied by matrices, Journal of Algebra, vol. 55 (1978), pp. 509-520.

[Robs78b] J.C. Robson, Well quasi-ordered sets and ideals in free semigroups and algebras, Journal of Algebra, vol. 55 (1978), pp. 521-535.

[Ros84] H.E. Rose, Subrecursion: Functions and hierarchies, Oxford Logic Guides 9, 1984.

[Ross36] J.B. Rosser, Extensions of some theorems of Gödel and Church, Journal of Symbolic Logic, vol. 1, 1936, pp. 87-91.

[Ru08,67[B. Russell, Mathematical logic as based on the theory of types, Amer. J. of Mathematics 30, 222-262, 1908. Reprinted in van Heijenoort (1967),150-182.

[RS04] N. Robertson and P. Seymour, Graph Minors. XX. Wagner's conjecture, Journal of Combinatorial Theory, Series B 92 (2): 325–357, 2004.

[RW93] M. Rathjen and A. Weiermann, Proof-theoretic investigations on Kruskal's theorem, Ann. Pure Appl. Logic 60 (1993) 49–88.

[Sc74] J. Schmerl, A partition property characterizing cardinals hyperinaccessible of finite type, Transactions of the American Mathematical Society, 188 (1974), 281-291.

[Sch65] K. Schütte, Predicative well-orderings, in: Formal systems and recursive functions, ed. Crossley and Dummett, North-Holland, 1965, pp. 176-184.

[Sch77] K. Schütte, Proof Theory, A Series of Comprehensive Studies in Mathematics, 225, Springer Verlag, 1977.

[Se80] A. Semenov, On certain extensions of the arithmetic of addition of natural numbers, Math USSR Izv., 1980, 15 (2), 401-418.

[Se83] A. Semenov, Logical theories of one place functions on the set of natural numbers (in russian), Izv. Acad. Nauka. SSSR ser. mat. 47 pp. 623-658, English translation in Mat. USSR-Izv. 22, 1984, pp.587-61.

[Sh95] S. Shelah, Cardinal Arithmetic, Oxford University Press, 1995.

[Sho93] R. Shore, On the strength of Fraïssé's conjecture, in: Logical Methods, ed. J.N. Crossley, J.B. Remmel, R.A. SHore, M.E. Sweedler, Birkhäuser, 782-813

[Si82] S. Simpson, Σ^1_1 and Π^1_1 transfinite induction, Logic Colloquium ’80 (Prague, 1980), Stud. Logic Foundations Math., vol. 108, North-Holland, Amsterdam, 1982, pp. 239–253.

[Si85] S. Simpson, Nonprovability of certain combinatorial properties of finite trees, Harvey Friedman's research on the foundations of mathematics (L. Harrington, M. Morley, A. Scedrov, and S. Simpson, editors), Studies in Logic and the Foundations of Mathematics, vol. 117, North-Holland, 1985, pp. 87-117.

[Si85a] S. Simpson, BQO theory and Fraïssé's conjecture, in: R. Mansfield, G. Weitkamp, Recursive Aspects of Descriptive Set Theory, Oxford Logic Guides, Oxford University Press, 1985.

[Si88] S. Simpson, Ordinal numbers and the Hilbert basis theorem, Journal of Symbolic Logic, 53 (1988), 961-974.

[Si99,09] S. Simpson, Subsystems of Second Order Arithmetic, Springer Verlag, 1999. Second edition, ASL, 2009.

[Si02] S. Simpson, Predicativity: The outer limits, in: Reflections on the Foundations of Mathematics: Essays in honor of Solomon Feferman, ed. Sieg, Sommer, Talcott, Lecture Notes in Logic, volume 15, 130-136, 2002, ASL.

[Sie91] W. Sieg, Herbrand analyses. Archive for Mathematical Logic 30(5-6), 1991, 409-441.

[Sm00] S. Smale, "Mathematical problems for the next century". Mathematics: frontiers and perspectives (Providence, RI: American Mathematics Society): 271–294, 2000.

[Smo84] C. Smorynski, Nonstandard models and related developments, p. 179-229, in: Harvey Friedman's Research on the Foundations of Mathematics, ed. L. Harrington, M.D. Morley, A. Scedrov, S.G. Simpson, Studies in Logic and The Foundations of Mathematics, volume 117, North-Holland, 1985.

[So71] R. Solovay, Real-valued measurable cardinals, in: Axiomatic Set Theory, Proceedings of Symposia in Pure Mathematics, Volume XIII, Part 1, 1971, 397-428.

[Soc92] G. Socıas, Length of polynomial ascending chains and primitive recursiveness, Math. Scand. 71 (1992), 181-205.

[St76] J. Steel, Determinateness and Subsysiems of Analysis, Ph.D. thesis, University of California at Berkeley, 1976.

[St09] J. Steel, The derived model theorem, in: Logic Colloquium '06, ASL, p. 135-183, 2009.

[Sta85] L. Stanley, Borel diagonalization and abstract set theory, in: [HMSS85], 11-86.

[SS85] K. Schütte and S. Simpson, Eine in der reinen Zahlentheorie unbeweisbarer Satz über endliche Folgen von natürlichen Zahlen, Archiv für Mathematische Logik and Grundlagenforschung, vol. 25 (1985), pp. 75-89.

[Ta51] A. Tarski, A Decision Method for Elementary Algebra and Geometry. Univ. of California Press, 1951.

[Tai61] W.W. Tait, Nested Recursion, Math. Ann., 143, 1961, 236-250.

[Tak75] G. Takeuti, Proof Theory, Studies in Logic and the Foundations of Mathematics, volume 81, North-Holland, 1975.

[Tak90] Some relations among systems for bounded arithmetic, in: *Mathematical Logic, Proceedings of the Heyting 1988 Summer School*, P. P. Petkov, ed., Plenum Press, New York, pp. 139{154.

[Tan89] K. Tanaka, The Galvin-Prikry theorem and set existence axioms, Annals of Pure and Applied Logic, 42:81-104, 1989.

[Tan90] K. Tanaka, Weak axioms of determinacy and subsystems of analysis I: Δ^0_2 games, Zeitschr. f.

math. Logik und Grundlagen d. Math. 36, 1990, 481-491.

[Tan91] K. Tanaka, Weak axioms of determinacy and subsystems of analysis II (Σ^0_2 games), Annals of Pure and Applied Logic 52, 1991, 181-193.

[Th∞] S. Thomas, The Friedman embedding theorem, to appear.

[To87] S. Todorcevic, Partitioning pairs of countable ordinals, Acta Mathematica, vol. 159 (1987), pp. 261-294.

[TG99] A. Tarski and S. Givant, Tarski's System of Geometry, The Bulletin of Symbolic Logic, Vol. 5, No. 2 (Jun., 1999), pp. 175-214.

[TMR53] Alfred Tarski, A. Mostowski, and R.M. Robinson, 1953. Undecidable Theories. North Holland.

[Vi90] A. Visser, Interpretability logic, in: Mathematical Logic, Proceedings of the 1988 Heyting Conference, p. 307-359, 1990 Plenum Press.

[Vi92] A. Visser, An Inside View of Exp; or, The Closed Fragment of the Provability Logic of $I\Delta_0 + \Omega_1$ with a Propositional Constant for Exp, J. Symbolic Logic, Volume 57, Issue 1 (1992), 131-165.

[Vi09] A. Visser, Can we make the Second Incompleteness Theorem coordinate free?, Journal of Logic and Computation, 2009.

[VH67] J. van Heijenoort, From Frege to Gödel. A Source Book in Mathematical Logic 1879-1931, Harvard Univ. Press (Cambridge), 1967.

[VM44] J. Von Neumann and O. Morgenstern, Theory of Games and Economic Behavior, Princeton University Press, Princeton, (1944).

[VV05] F. van Vugt, Independence of Variations to Kruskal's Theorem in ACA_0, 2005, http://florisvanvugt.free.fr/thesis.pdf

[We03] A. Weiermann, An application of graphical enumeration to PA. J. Symbolic Logic 68 (2003), no. 1, 5-16.

[We04] A. Weiermann, A classification of rapidly growing

Ramsey functions. Proc. Amer. Math. Soc. 132 (2004), no. 2, 553--561.

[We09] A. Weiermann, Phase transitions for Gödel incompleteness. Ann. Pure Appl. Logic 157(2009), no. 2-3, 281-296.

[Wel09] P. Welch, Weak systems of determinacy and arithmetical quasi-inductive definitions, 2009, preprints.

[Wei32] R. Weitzenbock, Uber die Invarianten von Linearen Gruppen, Acta. Math, 58 (1932), 230-250.

[Wey18,87] H. Weyl, The Continuum. A critical Examination of the Foundations of Analysis. English translation of Weyl 1918 in German), by S. Pollard and T. Bole (Thomas Jefferson Press, University Press of America, Latham, distributors).

[Wi77] A.J. Wilkie, Some results and problems on weak systems of arithmetic. Logic Colloquium '77 (Proc. Conf., Wrocaw, 1977), pp. 285--296.

[Wi96] A.J. Wilkie, Some model completeness results for expansions of the ordered field of reals by Pfaffian functions and exponentiation, J. Amer. Math. Soc. 9 (1996), 1051-1094.

[Wi99] A.J. Wilkie, A theorem of the complement and some new o-minimal structures, Sel. Math. 5 (1999), pp.397–421.

[Wil09] R. Wilson, Four Colors Suffice: How the Map Problem Was Solved, Princeton University Press 2004.

[Wo88] H. Woodin, Supercompact cardinals, sets of reals, and weakly homogeneous trees, PNAS, vol. 85 (1988), no. 18, pp. 6587-6591.

[WGB10] M. Walicki, C. Grabmayer, M. Bezem, Expressive Power of Digraph Solvability, Logic Group Preprint Series, Utrecht, no. 286, October, 2010.

[Ze08,67] E. Zermelo, Investigations in the foundations of set theory, in: [VH67].

*This research was partially supported by NSF Grants DMS-9970459 and DMS-0245349.

INDEX