On Model Theory for Intuitionistic Bounded Arithmetic with Applications to Independence Results

Samuel R. Buss*

Abstract

IPV^+ is IPV (which is essentially IS^1_2) with polynomial-induction on Σ^{b+}_1-formulas disjoined with arbitrary formulas in which the induction variable does not occur. This paper proves that IPV^+ is sound and complete with respect to Kripke structures in which every world is a model of CPV (essentially S^1_2). Thus IPV is sound with respect to such structures. In this setting, this is a strengthening of the usual completeness and soundness theorems for first-order intuitionistic theories. Using Kripke structures a conservation result is proved for PV_1 over IPV.

Cook-Urquhart and Krajíček-Pudlák have proved independence results stating that it is consistent with IPV and PV that extended Frege systems are super. As an application of Kripke models for IPV, we give a proof of a strengthening of Cook and Urquhart's theorem using the model-theoretic construction of Krajíček and Pudlák.

1 Introduction

An equational theory PV of polynomial time functions was introduced by Cook [4]; a classical first-order theory S^1_2 for polynomial time computation was developed in Buss [1]; and intuitionistic theories IS^1_2 and IPV for polynomial time computation have been discussed by Buss [2] and by Cook and Urquhart [5]. This paper discusses (a) model theory for the intuitionistic

*Supported in part by NSF Grant DMS-8902480.

fragments IPV and IPV^+ of Bounded Arithmetic (IPV is essentially IS^1_2 enlarged to the language of PV) and (b) the relationship between two recent independence results for IPV and CPV. The theories IPV and CPV have the same axioms but are intuitionistic and classical, respectively. Our model theory for IPV and IPV^+ is a strengthening of the usual Kripke semantics for intuitionistic first-order logic: we consider Kripke structures in which each "world" is a classical model of CPV. The use of these so-called CPV-normal Kripke structures is in contrast to the usual Kripke semantics which instead require each world to intuitionistically satisfy (or "force") the axioms; the worlds of a CPV-normal Kripke structure must classically satisfy the axioms. The main new results of this paper establish the completeness and soundness of IPV^+ with respect to CPV-normal Kripke structures.

The outline of this paper is as follows: in section 2, the definitions of PV_1, IPV and CPV are reviewed and the theory IPV^+ is introduced; in section 3, we develop model theory for IPV and IPV^+ and prove the soundness of these theories with respect to CPV-normal Kripke structures; in section 4 we apply the usual intuitionistic completeness theorem to prove a conservation result of PV_1 over IPV. Section 5 contains the completeness theorem for IPV^+ with respect to CPV-normal Kripke models. In section 6, we apply the soundness theorem to prove a strengthening of Cook and Urquhart's independence result for IPV and show that this strengthened result implies Krajíček and Pudlák's independence result.

2 The Feasible Theories

Cook [4] defined an equational theory PV for polynomial time computation. Buss [1] introduced a first-order theory S^1_2 with proof-theoretic strength corresponding to polynomial time computation and in which precisely the polynomial time functions could be Σ^b_1-defined. There is a very close connection between S^1_2 and PV: let $S^1_2(PV)$ (also called CPV) be the theory defined conservatively over S^1_2 by adding function symbols for polynomial time functions and adding defining equations (universal axioms) for the new function symbols; then $S^1_2(PV)$ is conservative over PV [1].

Buss [2] defined an intuitionistic theory IS^1_2 for polynomial time computation and Cook and Urquhart [5] gave similarly feasible, intuitionistic proof systems PV^ω and IPV^ω for feasible, higher-type functionals.

This paper will deal exclusively with the following theories, which are defined in more detail in the next paragraphs: (1) PV_1 is PV conservatively extended to *first-order* classical logic—PV_1 is defined by Krajíček-Pudlák-Takeuti [12] and should not be confused Cook's *propositional* expansion $PV1$ of PV [4], (2) IPV is an intuitionistic theory in the language of PV and is

essentially equivalent to IS^1_2, (3) CPV is $S^1_2(PV)$, and (4) the intuitionistic theory IPV^+ is an extension of IPV and is defined below. We now review the definitions of these four theories—it should be noted that our definitions are based on Bounded Arithmetic and not all of them are the historical definitions.

Recall that S^1_2 is a classical theory of arithmetic with language 0, S, $+$, $\cdot$, $\lfloor \frac{1}{2}x \rfloor$, $|x|$, $\#$ and $\leq$ where $|x| = \lceil \log_2(x+1) \rceil$ is the length of the binary representation of x and $x\#y = 2^{|x|\cdot|y|}$. A *bounded quantifier* is of the form $(Qx \leq t)$ where t is a term not involving x; a *sharply bounded quantifier* is one of the form $(Qx \leq |t|)$. A *bounded formula* is a first-order formula in which every quantifier is bounded. The bounded formulas are classified in a syntactic hierarchy Σ^b_i, Π^b_i by counting alternations of bounded quantifiers, ignoring sharply bounded quantifiers. There is a close connection between this hierarchy of bounded formulas and the polynomial time hierarchy; namely, a set of integers is in the class Σ^p_i of the polynomial time hierarchy if and only if it is definable by a Σ^b_i-formula. The theory S^1_2 is axiomatized by some purely universal formulas defining basic properties of the non-logical symbols and by PIND (polynomial induction) on Σ^b_1-formulas:

$$A(0) \wedge (\forall x)(A(\lfloor \tfrac{1}{2}x \rfloor) \supset A(x)) \supset (\forall x)A(x)$$

for A any Σ^b_1-formula. A function f is Σ^b_1-definable in S^1_2 if and only if it is provably total in S^1_2 with a Σ^b_1-formula defining the graph of f. In [1] it is shown that a function is Σ^b_1-definable in S^1_2 if and only if it is polynomial time computable. Let $S^1_2(PV)$ denote the conservative extension of S^1_2 obtained by adjoining a new function symbol for each polynomial time (Σ^b_1-defined) function. These new function symbols may be used freely in terms in induction axioms. Another name for the theory $S^1_2(PV)$ is CPV and we shall use the latter name for most of this paper. We use $\Sigma^b_1(PV)$ and $\Pi^b_1(PV)$ to denote hierarchy of classes of bounded formulas in the language of CPV.

PV is the equational theory consisting of all (intuitionistic) sequents of atomic formulas provable in $S^1_2(PV)$, i.e., PV is the theory containing exactly those formulas of the form

$$(r_1 = s_1 \wedge \cdots \wedge r_k = s_k) \supset t_1 = t_2$$

which are consequences of $S^1_2(PV)$. PV_1 is the classical, first-order thoery axiomatized by formulas in PV and is conservative over PV. Equivalently, PV_1 is the theory axiomatized by the $\Delta^b_1(PV)$-consequences of $S^1_2(PV)$ (where $\Delta^b_1(PV)$ means provably equivalent to a $\Sigma^b_1(PV)$- and to a $\Pi^b_1(PV)$-formula).

Since $S^1_2(PV)$ has a function symbol for each polynomial time function symbol, the use of sharply bounded quantifiers is not necessary; in particular, every $\Sigma^b_1(PV)$-formula is equivalent to a formula of the form

$$(\exists x \leq t)(r = s).$$

Hence $CPV = S^1_2(PV)$ may be axiomatized by PIND on formulas in this latter form.

IS^1_2 is an intuitionistic theory of arithmetic. A *hereditarily* Σ^b_1-formula, or $H\Sigma^b_1$-formula, is defined to be a formula in which every subformula is a Σ^b_1-formula. IS^1_2 is axiomatized like S^1_2 except with PIND restricted to $H\Sigma^b_1$-formulas. Any function definable in IS^1_2 is polynomial time computable and, conversely, every polynomial time computable function is $H\Sigma^b_1$-definable in IS^1_2. Let $IPV = IS^1_2(PV)$ be the conservative extension of IS^1_2 obtained by adjoining every polynomial time function with a $H\Sigma^b_1$-defining equation. Note IPV and CPV have the same language.

An alternative definition of IPV is that it is the intuitionistic theory axiomatized by PV plus PIND for formulas of the form $(\exists x \leq t)(r = s)$. In this way, IPV and CPV can be taken to have precisely the same axioms; the former is intuitionistic and the latter is classical. The theories IPV and IS^1_2 have the law of the excluded middle for atomic formulas, that is to say, the law of the excluded middle holds for polynomial time computable predicates. This restricted law of excluded middle also applies to the theory IPV^+ defined next.

Definition IPV^+ is the intuitionistic theory which includes PV and has the PIND axioms for formulas $\psi(b, \vec{c})$ of the form

$$\varphi(\vec{c}) \vee (\exists x \leq t(b, \vec{c}))[r(x, b, \vec{c}) = s(x, b, \vec{c})]$$

where r, s and t are terms and $\varphi(\vec{c})$ is an *arbitrary* formula in which the variable b does not occur. The induction axiom is with respect to the variable b and is:

$$\psi(0, \vec{c}) \wedge (\forall z)(\psi(\lfloor \tfrac{1}{2} z \rfloor, \vec{c}) \supset \psi(z, \vec{c})) \supset (\forall z)\psi(z, \vec{c}).$$

Note that $IPV^+ \supseteq IPV$ since φ can be taken to be $0 = 1$, for instance.

In [3] a theory IS^{1+}_2 was defined by allowing PIND on $H\Sigma^{b*}_1$-formulas where $H\Sigma^{b*}_1$-formulas are $H\Sigma^b_1$-formulas disjoined with an arbitrary formula in which the induction variable does not occur. It is readily checked that IPV^+ is equivalent to the theory IS^{1+}_2 extended to the language of PV_1 by introducing symbols for all polynomial functions via $H\Sigma^b_1$-definitions.

We use $\vdash_c$ and $\vdash_i$ for classical and intuitionistic provability, respectively; thus we shall (redundantly) write $CPV \vdash_c \varphi$ and $IPV \vdash_i \varphi$ and $IPV^+ \vdash_i \varphi$. Whenever we write $\Gamma \vdash_i \varphi$ or $\Gamma \vdash_c \varphi$, we require that Γ be a set of *sentences*;[†] however, φ may be a formula and may also involve constant symbols not occuring in any formula in Γ.

[†]By convention, a first-order theory is identified with the set of sentences provable in that theory.

Definition A *positive* formula is one in which no negation signs ($\neg$) and no implication symbols ($\supset$) appear. If θ is a positive formula and φ is an arbitrary formula, then θ^φ is the formula obtained from θ by replacing every atomic subformula χ of θ by $(\chi \vee \varphi)$. We do not allow free variables in φ to become bound in θ^φ: this can be done either by using the conventions of the sequent calculus which has distinct sets of free and bound variables or by renaming bound variables in θ to be distinct from the free variables in φ.

Theorem 1 *Let θ be a positive formula. If $CPV \vdash_c \neg\theta$ then $IPV \vdash_i \neg\theta$.*

Theorem 2 *Let θ be a positive formula and φ be an arbitrary formula. If $CPV \vdash_c \neg\theta$ then $IPV^+ \vdash_i \theta^\varphi \supset \varphi$.*

These theorems follow readily from the corresponding facts for S^1_2 and IS^{1+}_2 which are proved in Buss [3]. Theorem 2 can be obtained as a corollary to Theorem 1 via Lemma 3.5.3(a) of [15].

3 Kripke structures for intuitionistic logic

A *classical model* for PV_1 or CPV is defined as usual for classical first-order logic using Tarskian semantics. The corresponding semantic notion for intuitionistic first-order logic is that of a Kripke model. We briefly define Kripke models for IPV and IPV^+, a slightly more general definition of Kripke models can be found in the textbook by Troelstra and van Dalen [15]. (Kripke models for IPV are slightly simpler than in the general case since IPV has the law of the excluded middle for atomic formulas.)

A Kripke model $\mathcal{K}$ for the language of IPV is an ordered pair $(\{\mathcal{M}_i\}_{i\in\mathcal{I}}, \preccurlyeq)$ where $\{\mathcal{M}_i\}_{i\in\mathcal{I}}$ is a set of (not necessarily distinct) classical structures for the language of IPV indexed by elements of the set $\mathcal{I}$ and where $\preccurlyeq$ is a reflexive and transitive binary relation on $\{\mathcal{M}_i\}_{i\in\mathcal{I}}$.[‡] Furthermore, whenever $\mathcal{M}_i \preccurlyeq \mathcal{M}_j$ then $\mathcal{M}_i$ is a substructure of $\mathcal{M}_j$ in that $\mathcal{M}_i$ is obtainable from $\mathcal{M}_j$ by restricting functions and predicates to the domain $|\mathcal{M}_i|$ of $\mathcal{M}_i$. The $\mathcal{M}_i$'s are called *worlds*.

If φ is a formula and if $\vec{c} \in |\mathcal{M}_i|$ then we define $\mathcal{M}_i \models \varphi(\vec{c})$, $\mathcal{M}_i$ *classically satisfies* $\varphi(\vec{c})$, as usual, ignoring the rest of the worlds in the Kripke structure. To define the intuitionistic semantics, $\mathcal{M}_i \Vdash \varphi(\vec{c})$, $\mathcal{M}_i$ *forces* $\varphi(\vec{c})$, is defined inductively on the complexity of φ as follows:[§]

[‡]Strictly speaking, $\preccurlyeq$ should be a relation on $\mathcal{I}$ since the $\mathcal{M}_i$'s may not be distinct. However, we follow standard usage and write $\preccurlyeq$ as a relation on worlds.

[§]A more proper notation would be $(\mathcal{K}, \mathcal{M}_i) \Vdash \varphi(\vec{c})$ or even $(\mathcal{K}, i) \Vdash \varphi(\vec{c})$ but we use the simpler notation $\mathcal{M}_i \Vdash \varphi(\vec{c})$ when $\mathcal{K}$ is specified by the context.

(1) If φ is atomic, $\mathcal{M}_i \Vdash \varphi$ if and only if $\mathcal{M}_i \models \varphi$.

(2) If φ is $\psi \wedge \chi$ then $\mathcal{M}_i \Vdash \varphi$ if and only if $\mathcal{M}_i \Vdash \psi$ and $\mathcal{M}_i \Vdash \chi$.

(3) If φ is $\psi \vee \chi$ then $\mathcal{M}_i \Vdash \varphi$ if and only if $\mathcal{M}_i \Vdash \psi$ or $\mathcal{M}_i \Vdash \chi$.

(4) If φ is $\psi \supset \chi$ then $\mathcal{M}_i \Vdash \varphi$ if and only if for all $\mathcal{M}_j \succcurlyeq \mathcal{M}_i$, if $\mathcal{M}_j \Vdash \psi$ then $\mathcal{M}_j \Vdash \chi$.

(5) If φ is $\neg\psi$ then $\mathcal{M}_i \Vdash \varphi$ if and only if for all $\mathcal{M}_j \succcurlyeq \mathcal{M}_i$, $\mathcal{M}_j \nVdash \psi$. Alternatively one may define $\neg\psi$ to mean $\psi \supset \perp$ where $\perp$ is always false (not forced).

(6) If φ is $(\exists x)\psi(x)$ then $\mathcal{M}_i \Vdash \varphi$ if and only if there is some $b \in |\mathcal{M}_i|$ such that $\mathcal{M}_i \Vdash \psi(b)$.

(7) If φ is $(\forall x)\psi(x)$ then $\mathcal{M}_i \Vdash \varphi$ if and only if for all $\mathcal{M}_j \succcurlyeq \mathcal{M}_i$ and all $b \in |\mathcal{M}_j|$, $\mathcal{M}_j \Vdash \varphi(b)$.

An immediate consequence of the definition of forcing is that if $\mathcal{M}_i \Vdash \varphi$ and $\mathcal{M}_i \preccurlyeq \mathcal{M}_j$ then $\mathcal{M}_j \Vdash \varphi$; this is proved by induction on the complexity of φ. Also, the law of the excluded middle for *atomic* formulas will be forced at every world $\mathcal{M}_i$ because we required $\mathcal{M}_i$ to be a substructure of $\mathcal{M}_j$ whenever $\mathcal{M}_i \preccurlyeq \mathcal{M}_j$[¶]. In other words, both truth and falsity of atomic formulas are preserved in "reachable" worlds. Consequently, the law of the excluded middle for quantifier-free formulas is also forced at each world. Hence, if φ is quantifier-free, then $\mathcal{M}_i \Vdash \varphi$ if and only if $\mathcal{M}_i \models \varphi$.

A formula $\varphi(\vec{x})$ is *valid* in $\mathcal{K}$, denoted $\mathcal{K} \Vdash \varphi(\vec{x})$, if and only if for all worlds $\mathcal{M}_i$ and all $\vec{c} \in |\mathcal{M}_i|$, $\mathcal{M}_i \Vdash \varphi(\vec{c})$. A set of formulas Γ is valid in $\mathcal{K}$, $\mathcal{K} \Vdash \Gamma$, if and only if every formula in Γ is valid in $\mathcal{K}$. $\Gamma \Vdash \varphi$, φ is a *Kripke consequence* of Γ, if and only if for every Kripke structure $\mathcal{K}$, if $\mathcal{K} \Vdash \Gamma$ then $\mathcal{K} \Vdash \varphi$. A Kripke model for IPV is one in which the axioms of IPV are valid. Likewise, a Kripke model for IPV^+ is one in which the axioms of IPV^+ are valid.

The usual strong soundness and completeness theorems for intuitionistic logic state that for any set of sentences Γ and any sentence φ, $\Gamma \Vdash \varphi$ if and only if $\Gamma \vdash_i \varphi$ (see Troelstra and van Dalen [15] for a proof). Hence validity in Kripke models corresponds precisely to intuitionistic provability. A countable Kripke model is one in which there are countably many worlds each with a countable domain. The usual strong completeness theorem further states that if Γ is a countable set of formulas and $\Gamma \nvdash_i \psi$ then there is a countable Kripke structure in which Γ is valid but ψ is not.

[¶]This differs from the usual definition of Kripke models for intuitionistic logic.

The usual strong soundness and completeness theorems give a semantics for the theory IPV in that for any formula φ, $IPV \vdash_i \varphi$ if and only if for all $\mathcal{K}$, if $\mathcal{K} \Vdash IPV$ then $\mathcal{K} \Vdash \varphi$. It is, however, a little difficult to interpret directly what it means for $\mathcal{K} \Vdash IPV$ to hold; and we feel that it is more natural to consider CPV-normal Kripke structures instead:

Definition A Kripke model $\mathcal{K} = (\{\mathcal{M}_i\}_{i\in\mathcal{I}}, \preccurlyeq)$ is *CPV-normal* if and only if for all $i \in \mathcal{I}$, the world $\mathcal{M}_i$ is a classical model of CPV.

Theorem 3 *(Soundness of IPV and IPV$^+$ for CPV-normal Kripke models.)*

(a) *If $\mathcal{K}$ is a CPV-normal Kripke structure then $K \Vdash IPV$. Hence for all φ, if $IPV \vdash_i \varphi$ then $\mathcal{K} \Vdash \varphi$.*

(b) *If $\mathcal{K}$ is a CPV-normal Kripke structure then $K \Vdash IPV^+$. Hence for all φ, if $IPV^+ \vdash_i \varphi$ then $\mathcal{K} \Vdash \varphi$.*

The converse to Theorem 3(b) is proved in section 5 below.

Proof It will clearly suffice to prove only (b) since $IPV^+ \supseteq IPV$. Suppose $\mathcal{K}$ is a CPV-normal Kripke structure. Since every world $\mathcal{M}_i$ is a classical model of CPV and hence of PV_1, it follows immediately from the definition for forcing and from the fact that PV_1 is axiomatized by universal formulas that $\mathcal{K} \Vdash PV_1$. So it will suffice to show that the PIND axioms of IPV^+ are valid in $\mathcal{K}$. Let $\mathcal{M}_i$ be a world and consider a formula $\varphi(b, \vec{c})$ of the form $\psi(\vec{c}) \vee \chi(b, \vec{c})$ where $\chi(b, \vec{c})$ is a formula of the form

$$(\exists x \leq t(b, \vec{c}))(r(x, b, \vec{c}) = s(x, b, \vec{c}))$$

and where b is a variable, $\vec{c} \in |\mathcal{M}_i|$ and $\psi(\vec{c})$ is an arbitrary formula not involving b. We must show that

$$\mathcal{M}_i \Vdash \varphi(0, \vec{c}) \wedge (\forall z)(\varphi(\lfloor \tfrac{1}{2} z \rfloor, \vec{c}) \supset \varphi(z, \vec{c})) \supset (\forall x)\varphi(x, \vec{c}).$$

To prove this, suppose that $\mathcal{M}_i \preccurlyeq \mathcal{M}_j$ and that

$$\mathcal{M}_j \Vdash \varphi(0, \vec{c}) \wedge (\forall z)(\varphi(\lfloor \tfrac{1}{2} z \rfloor, \vec{c}) \supset \varphi(z, \vec{c}));$$

we must show $\mathcal{M}_j \Vdash (\forall x)\varphi(x, \vec{c})$. If $\mathcal{M}_j \Vdash \psi(\vec{c})$ then this is clear, so suppose $\mathcal{M}_j \nVdash \psi(\vec{c})$. Note that for any $b \in |\mathcal{M}_j|$, $\mathcal{M}_j \Vdash \chi(b, \vec{c})$ if and only if $\mathcal{M}_j \vDash \chi(b, \vec{c})$. Hence, since $\mathcal{M}_j \Vdash \varphi(0, \vec{c})$ and $\mathcal{M}_j \nVdash \psi(\vec{c})$, $\mathcal{M}_j \vDash \chi(0, \vec{c})$. And similarly, by reflexivity of $\preccurlyeq$, for each $b \in |\mathcal{M}_j|$, if $\mathcal{M}_j \vDash \chi(\lfloor \frac{1}{2} b \rfloor, \vec{c})$ then $\mathcal{M}_j \vDash \chi(b, \vec{c})$. In other words, $\mathcal{M}_j \vDash (\forall z)(\chi(\lfloor \frac{1}{2} z \rfloor, \vec{c}) \supset \chi(z, \vec{c}))$. But now since $\mathcal{M}_j \vDash CPV$ and CPV has PIND for $\chi(b, \vec{c})$, $\mathcal{M}_j \vDash (\forall z)\chi(z, \vec{c})$.

We have established that either $\mathcal{M}_j \Vdash \chi(b, \vec{c})$ for every $b \in |\mathcal{M}_j|$ or $\mathcal{M}_j \Vdash \psi(\vec{c})$. The same reasoning applies to any world $\mathcal{M}_k \succcurlyeq \mathcal{M}_i$ and in particular, for any $\mathcal{M}_k \succcurlyeq \mathcal{M}_j$, either $\mathcal{M}_k \Vdash \chi(b, \vec{c})$ for every $b \in |\mathcal{M}_k|$ or $\mathcal{M}_k \Vdash \psi(\vec{c})$. Hence by the definition of forcing, $\mathcal{M}_j \Vdash (\forall z)\varphi(z, \vec{c})$.

We have shown that if $\mathcal{K}$ is a CPV-normal Kripke model then every axiom of IPV^+ is valid in $\mathcal{K}$. It now follows by the usual soundness theorem for intuitionistic logic that every intuitionistic consequence of IPV^+ is valid in $\mathcal{K}$. Q.E.D. Theorem 3

4 A conservation theorem

The usual Gödel-Kolmogorov "negative translations" don't seem to apply to IPV since we don't know whether the negative translations of the PIND axioms of IPV are consequences of IPV. However, the usual completeness theorem for Kripke models of IPV does allow us to prove the following substitute:

Theorem 4 *Let φ be a quantifier-free formula.*

(a) *If ψ is a sentence of the form $\neg(\exists x)(\forall y)\neg(\forall z)\varphi$ and $PV_1 \vdash_c \psi$ then $IPV \vdash_i \psi$.*

(b) *If ψ is a sentence of the form*

$$\neg(\exists x_1)(\forall y_1)\neg\neg(\exists x_2)(\forall y_2)\neg\neg \cdots \neg\neg(\exists x_r)(\forall y_r)\varphi$$

and $PV_1 \vdash_c \psi$ then $IPV \vdash_i \psi$.

This theorem is a statement about how strong IPV is; although IPV has stronger axioms than PV_1, it uses intuitionistic logic instead of classical logic so it makes sense to establish a conservation result for PV_1 over IPV. Of course, at least some of the negation signs in ψ are required for Theorem 4 to be true; for example, PV_1 proves $(\forall x)(\exists y)(\forall z)(|z| = x \supset |y| = x)$ but IPV cannot prove this since otherwise, by the polynomial time realizability of IPV-provable formulas, y would be polynomial time computable in terms of x, which is false since y must be greater than or equal to 2^{x-1}.

Proof Let's prove (1) first. Suppose $IPV \nvdash_i \neg(\exists x)(\forall y)\neg(\forall z)\varphi$; we must show $PV_1 \nvdash_c (\forall x)(\exists y)(\forall z)\varphi$. By the usual completeness theorem for Kripke models for IPV, there is a Kripke model $\mathcal{K} = (\{\mathcal{M}_i\}_{i\in\mathcal{I}}, \preccurlyeq)$ of IPV such that $\mathcal{K} \nVdash \neg(\exists x)(\forall y)\neg(\forall z)\varphi$ and such that each $\mathcal{M}_i$ is countable. Hence there is a world, say $\mathcal{M}_0$ such that $\mathcal{M}_0 \Vdash (\exists x)(\forall y)\neg(\forall z)\varphi$. Our stategy is to find a chain of worlds $\mathcal{M}_0 \preccurlyeq \mathcal{M}_1 \preccurlyeq \mathcal{M}_2 \preccurlyeq \cdots$ such that their union is a model

of PV_1 and of $(\exists x)(\forall y)(\exists z)\neg\varphi$. First of all note that each $\mathcal{M}_i \vDash PV_1$ since IPV includes the (purely universal) axioms of PV_1. Hence $\bigcup_{i=0,1,2,\cdots} \mathcal{M}_i$ is a model of PV_1, again because PV_1 has universal axioms. Let $x_0 \in |\mathcal{M}_0|$ be such that $\mathcal{M}_0 \Vdash (\forall y)\neg(\forall z)\varphi(x_0, y, z)$. It will suffice to find the $\mathcal{M}_i$'s so that $\left(\bigcup_{i\in\mathbb{N}} \mathcal{M}_i\right) \vDash (\forall y)(\exists z)\neg\varphi(x_0, y, z)$. Suppose we have already picked worlds $\mathcal{M}_0, \ldots, \mathcal{M}_{k-1}$ and that $y_k \in |\mathcal{M}_{k-1}|$; we pick $\mathcal{M}_k \succcurlyeq \mathcal{M}_{k-1}$ so that for some $z_k \in |\mathcal{M}_k|$, $\mathcal{M}_k \Vdash \neg\varphi(x_0, y_k, z_k)$, or equivalently, $\mathcal{M}_k \vDash \neg\varphi(x_0, y_k, z_k)$. Such an $\mathcal{M}_k$ and z_k must exist since $\mathcal{M}_0 \Vdash (\forall y)\neg(\forall z)\varphi(x_0, y_k, z_k)$ and $\mathcal{M}_0 \preccurlyeq \mathcal{M}_{k-1}$ and thus $\mathcal{M}_{k-1} \nVdash (\forall z)\varphi(x_0, y_k, z)$. Since each $\mathcal{M}_i$ is countable, we may choose the y_k's in the right order so that $y_1, y_2, \ldots$ enumerates every element in the union of the $\mathcal{M}_i$'s. Thus for every y in the union $\bigcup_{i\in\mathbb{N}} \mathcal{M}_i$ there is a z such that $\neg\varphi(x_0, y, z)$ holds. That gives a model of PV_1 in which ψ is false, proving (1).

The proof of (2) is similar but with more complicated bookkeeping. Let $\mathcal{K}$ be a Kripke model of IPV such that ψ is not valid in $\mathcal{K}$. Here if $\mathcal{M}_0, \ldots \mathcal{M}_{k-1}$ have already been chosen and if $x_{k,1}, \ldots, x_{k,i-1}$ and $y_{k,1}, \ldots, y_{k,i-1}$ are in $\mathcal{M}_{k-1}$ so that

$$\mathcal{M}_{k-1} \Vdash \neg\neg(\exists x_i)(\forall y_i)\cdots\neg\neg(\exists x_r)(\forall y_r)$$
$$\varphi(x_{k,1}, \ldots, x_{k,i-1}, x_i, \ldots, x_r, y_{k,1}, \ldots, y_{k,i-1}, y_i, \ldots, y_r)$$

then we may pick $\mathcal{M}_k \succcurlyeq \mathcal{M}_{k-1}$ and $x_{k,i} \in |\mathcal{M}_k|$ so that

$$\mathcal{M}_k \Vdash (\forall y_i)\cdots\neg\neg(\exists x_r)(\forall y_r)$$
$$\varphi(x_{k,1}, \ldots, x_{k,i}, x_{i+1}, \ldots, x_r, y_{k,1}, \ldots, y_{k,i-1}, y_i, \ldots, y_r)$$

By appropriately diagonalizing through the countably many choices for i and $\vec{x}$ and $\vec{y}$ we may ensure that $\bigcup_{k\in\mathbb{N}} \mathcal{M}_k$ is a model of $PV_1 \cup \{\neg\psi\}$. We omit the details. □

5 A completeness theorem for IPV^+

We next establish the main theorem of this paper.

Theorem 5 *(Completeness Theorem for IPV^+ with respect to CPV-normal Kripke models)*

Let φ be any sentence. If $IPV^+ \nvdash_i \varphi$ then there is a CPV-normal Kripke model $\mathcal{K}$ such that $\mathcal{K} \Vdash IPV^+$ and $\mathcal{K} \nVdash \varphi$.

Note that the conclusion "$\mathcal{K} \Vdash IPV^+$" is superfluous as this is already a consequence of Theorem 3. The proof of this theorem will proceed along the lines of the proof of the usual strong completeness theorem for intuitionistic

logic as exposited in section 2.6 of Troelstra and van Dalen [15]. The new ingredient and the most difficult part in our proof is Lemma 7 below which is needed to ensure that the Kripke model is CPV-normal.

Although we shall not prove it here, Theorem 5 can be strengthened to require $\mathcal{K}$ to be countable.

Definition Let C be a set of constant symbols. A C-formula or C-sentence is a formula or sentence in the language of PV_1 plus constant symbols in C. All sets of constants are presumed to be countable.

Definition A set of C-sentences Γ is *C-saturated* provided the following hold:

(1) Γ is intuitionistically consistent,

(2) For all C-sentences φ and ψ, if $\Gamma \vdash_i \varphi \vee \psi$ then $\Gamma \vdash_i \varphi$ or $\Gamma \vdash_i \psi$.

(3) For all C-sentences $(\exists x)\varphi(x)$, if $\Gamma \vdash_i (\exists x)\varphi(x)$ then for some $c \in C$, $\Gamma \vdash_i \varphi(c)$.

The next, well-known lemma shows that C-saturated sets can be readily constructed.

Lemma 6 *Let Γ be a set of sentences and φ be a sentence such that $\Gamma \nvdash_i \varphi$. If C is a set of constant symbols containing all constants in Γ plus countably infinitely many new constant symbols, then there is a C-saturated set Γ^* containing Γ such that $\Gamma^* \nvdash_i \varphi$.*

The proof of Lemma 6 is quite simple, merely enumerate with repetitions all C-sentences which either begin with an existential quantifier or are a disjunction and then form Γ^* by adding new sentences to Γ so that (2) and (3) of the definition of C-saturated are satisfied. This can be done so that φ is still not an intuitionistic consequence. (For a full proof, refer to lemma 2.6.3 of [15].) In the proof of the usual completeness theorem for Kripke models and intuitionistic logic, the C-saturated sets of sentences constructed with Lemma 6 specify worlds in a canonical Kripke model. However, Lemma 6 is not adequate for the proof of Theorem 5 and Lemma 7 below is needed instead.

A C-saturated set Γ defines a world with domain C in which an atomic formula φ is forced if and only $\Gamma \vdash_i \varphi$. For the proof of Theorem 5, we shall only consider sets Γ which contain IPV^+ and hence imply the law of the excluded middle for atomic formulas; the C-saturation of Γ thus implies that for any atomic C-sentence φ, either $\Gamma \vdash_i \varphi$ or $\Gamma \vdash_i \neg\varphi$. Thus Γ specifies a classical structure $\mathcal{M}_\Gamma$ defined as follows:

Definition Suppose $\Gamma \supset IPV$, Γ is a C-saturated set, and for all distinct $c, c' \in C$, $\Gamma \vdash_i c \neq c'$. Then $\mathcal{M}_\Gamma$ is the classical structure in the language of PV plus constant symbols in C such that the domain of $\mathcal{M}_\Gamma$ is C itself (so $c^{\mathcal{M}_\Gamma} = c$) and such that for every atomic C-sentence φ, $\mathcal{M}_\Gamma \models \varphi$ if and only if $\Gamma \vdash_i \varphi$.

It is straightforward to check that $\mathcal{M}_\Gamma$ is a classical structure: the only thing to check is that the equality axioms hold (it suffices to do this for atomic formulas). Note the equality relation $=^{\mathcal{M}_\Gamma}$ in $\mathcal{M}_\Gamma$ is true equality in that $\mathcal{M} \Vdash c = c'$ if and only if $c = c'$ because of the restriction that $\Gamma \vdash_i c \neq c'$ if c and c' are distinct. This restriction is not very onerous as we will be able to make it hold by eliminating duplicate constant symbols.[‖]

In order to prove Theorem 5 we must construct sets Γ so that the structures $\mathcal{M}_\Gamma$ are classical models of CPV; Lemma 7 is the crucial tool for this:

Lemma 7 *Suppose Γ is a set of C-sentences, φ is a C-sentence and $\Gamma \supseteq IPV^+$. Further suppose $\Gamma \nvdash_i \varphi$ and $\Gamma \vdash_i c \neq c'$ for distinct $c, c' \in C$. Then there is a set Γ^* of sentences and a set C^* of constants such that*

(a) $\Gamma^* \supset \Gamma$

(b) Γ^* *is C^*-saturated*

(c) $\Gamma^* \nvdash_i \varphi$

(d) $\Gamma^* \vdash_i c \neq c'$ *for all distinct $c, c' \in C^*$*

(e) $\mathcal{M}_{\Gamma^*} \models CPV$.

Proof Γ^* and $\mathcal{M}_{\Gamma^*}$ are constructed by a technique similar to Henkin's proof of Gödel's completeness theorem. We pick C^+ to be C plus countably infinitely many new constant symbols and enumerate the C^+ formulas as $\alpha_1, \alpha_2, \alpha_3, \ldots$ with each C^+-formula appearing infinitely many times in the enumeration. We shall form classically consistent sets of sentences $\Pi_0, \Pi_1, \Pi_2, \ldots$ so that $\Pi_0 \supseteq CPV$ and so that, for all k, $\Pi_k \supseteq \Pi_{k-1}$ and either $\alpha_k \in \Pi_k$ or $\neg\alpha_k \in \Pi_k$. Furthermore, if $\alpha_k = (\exists x)\beta(x)$ and $\alpha_k \in \Pi_{k-1}$ then for some constant symbol c, $\Pi_k \vdash_c \beta(c)$. Thus, as usual in a Henkin-style model construction, the union of the Π_k's will specify a classical model $\mathcal{M}$ of CPV with domain formed of equivalence classes of constants in C^+. This $\mathcal{M}$ will become $\mathcal{M}_{\Gamma^*}$ after elimination of duplicate constant names.

[‖]If we did not adopt this restiction, then the domain of $\mathcal{M}_\Gamma$ would have to be equivalence classes of constants in C instead of just the set C. But this would cause some inconveniences later on in the definition of the canonical CPV-normal Kripke structure.

While defining the sets Π_k we also define sets Π'_k, Γ_k, C_k and C'_k so that $\Pi_{k-1} \subseteq \Pi'_k \subseteq \Pi_k$ and

$$\Gamma = \Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \cdots$$

and such that C_0 is C, $C_k \supseteq C'_k \supseteq C_{k-1}$, and $C^+ = \bigcup_k C_k$. Γ^* will be the union of the Γ_i's after elimination of duplicate constant names.

Definition Let D be a set of constants and Λ be a set of D-sentences. Then $Th^{+\varphi}[\Lambda, D]$ is the set

$$\{\theta : \theta \text{ is a positive } D\text{-sentence and } \Lambda \vdash_i \theta^{\varphi}\}$$

For us, the formula φ is fixed, so we also denote this set by $Th^+[\Lambda, D]$. If Δ is a classical theory then the $[\Lambda, D]$-*closure* of Δ is the classical theory axiomatized by $\Delta \cup Th^+[\Lambda, D]$.

Definition We define Γ_0 to be Γ, C_0 to be C and Π_0 to be the $[\Gamma, C]$-closure of CPV. For $k > 0$, Π_k, Π'_k, Γ_k, C_k and C'_k are inductively defined by:

(1) Suppose $\alpha_k \in \Pi_k$ and α_k is of the form $(\exists x)\beta_k(x)$. Then C'_k is C_{k-1} plus an additional new constant symbol $c \in C^+ \setminus C_{k-1}$. And Π'_k is the $[\Gamma_{k-1}, C'_k]$-closure of $\Pi_{k-1} \cup \{\beta_k(c)\}$.

(2) If Case (1) does not apply then C'_k is C_{k-1} plus the constant symbols in α_k and:

   (a) Let Π'_k be $\Pi_{k-1} \cup \{\alpha_k\} \cup Th^+[\Gamma_{k-1}, C'_k]$ if this theory is classically consistent,

   (b) Otherwise, let Π'_k be $\Pi_{k-1} \cup \{\neg\alpha_k\} \cup Th^+[\Gamma_{k-1}, C'_k]$

(3) If α_k is of the form $(\exists x)\beta_k(x)$ and $\Gamma_{k-1} \vdash_i \alpha_k$ then C_k is $C'_k \cup \{d\}$ where d is a new constant symbol from $C^+ \setminus C'_k$, Γ_k is $\Gamma_{k-1} \cup \{\beta_k(d)\}$ and Π_k is the $[\Gamma_k, C_k]$-closure of Π'_k.

(4) If α_k is of the form $\beta_k \vee \gamma_k$ and $\Gamma_{k-1} \vdash_i \alpha_k$ then C_k is C'_k and:

   (a) If the $[\Gamma_{k-1} \cup \{\beta_k\}, C_k]$-closure of Π'_k is classically consistent then Π_k defined to be equal to this theory and Γ_k is $\Gamma_{k-1} \cup \{\beta_k\}$.

   (b) Otherwise, Γ_k is $\Gamma_{k-1} \cup \{\gamma_k\}$ and Π_k is the $[\Gamma_k, C_k]$-closure of Π'_k.

Define $\Pi_\omega = \bigcup_k \Pi_k$ and $\Gamma_k = \bigcup_k \Gamma_k$. Note $C^+ = \bigcup_k C_k$.

The point of cases (1) and (2) above is to make Π_ω a complete theory with witnesses for existential consequences. The point of cases (3) and (4) is to force Γ_ω to be C^+-saturated. The requirement that Π_k contain $Th^+[\Gamma_k, C_k]$ and Π'_k contain $Th^+[\Gamma_{k-1}, C'_k]$ serves to maintain the condition that $\Gamma_k \nvdash_i \varphi$.

Claim: For $k = 0, 1, 2$,

(1) Π_k is classically consistent for all k.

(2) $\Gamma_k \nvdash_i \varphi$ (so Γ_k is intuitionistically consistent).

Note that if $\Gamma_k \vdash_i \varphi$, then $\Gamma_k \vdash_i (0 = 1)^\varphi$ and hence $\Pi_k \vdash_c 0 = 1$ and Π_k is inconsistent. So to prove the claim, it suffices to show Π_k is consistent which we do by induction on k. The base case is $k = 0$. Suppose for a contradiction that Π_0 is inconsistent. Then $CPV \vdash_c \neg\theta_1 \vee \neg\theta_2 \vee \cdots \vee \neg\theta_s$ for positive C-sentences θ_j such that $\Gamma \vdash_i \theta_j^\varphi$. By taking the conjunction of the θ_j's there is a single positive C-sentence θ such that $CPV \vdash_c \neg\theta$ and $\Gamma \vdash_i \theta^\varphi$. But, by Theorem 2, $IPV^+ \vdash_i \theta^\varphi \supset \varphi$ and thus, since $\Gamma \supseteq IPV^+$, $\Gamma \vdash_i \varphi$; which is a contradiction.

For the induction step, we first assume Π_{k-1} is consistent and show that Π'_k is consistent. Referring to Case (1) of the definition of Π'_k, suppose $\alpha_k = (\exists x)\beta_k(x)$ and that Π'_k is inconsistent. This means that there is a positive C'_k-sentence $\theta(c)$ such that $\Pi_{k-1} \vdash_c \beta_k(c) \supset \neg\theta(c)$ and $\Gamma_{k-1} \vdash_i \theta(c)^\varphi$. Then, since c was a new constant symbol, $\Pi_{k-1} \vdash_c (\exists x)\beta_k(x) \supset (\exists x)\neg\theta(x)$ and so $\Pi_{k-1} \vdash_c \neg(\forall x)\theta(x)$; also, $\Gamma_{k-1} \vdash_i [(\forall x)\theta(x)]^\varphi$. But $(\forall x)\theta(x)$ is a positive C_{k-1}-sentence and Π_{k-1} contains $Th^+[\Gamma_{k-1}, C_{k-1}]$, so Π_{k-1} contains $(\forall x)\theta(x)$ which contradicts our assumption that Π_{k-1} is consistent. Now suppose Case (2) of the definition applies. Let $\alpha_k = \alpha_k(\vec{e})$ where $\vec{e}$ denotes all the constant symbols in α_k that are not in C_{k-1} (so $C'_k = C_{k-1} \cup \{\vec{e}\}$). Let Π_k^a and Π_k^b be the $[\Gamma_{k-1}, C'_k]$-closures of $\Pi_{k-1} \cup \{\alpha_k\}$ and $\Pi_{k-1} \cup \{\neg\alpha_k\}$, respectively. We need to show that at least one of these theories is classically consistent, so suppose that both are inconsistent. Then there are positive C'_k-sentences $\theta_a(\vec{e})$ and $\theta_b(\vec{e})$ such that $\Gamma_{k-1} \vdash_i \theta_a(\vec{e})^\varphi$, $\Gamma_{k-1} \vdash_i \theta_b(\vec{e})^\varphi$, $\Pi_{k-1} \vdash_c \alpha_k(\vec{e}) \supset \neg\theta_a(\vec{e})$ and $\Pi_{k-1} \vdash_c \neg\alpha_k(\vec{e}) \supset \neg\theta_b(\vec{e})$ Then $\Pi_{k-1} \vdash_c \neg(\exists\vec{x})(\theta_a(\vec{x}) \wedge \theta_b(\vec{x}))$ and $\Gamma_{k-1} \vdash_i [(\forall\vec{x})(\theta_a(\vec{x}) \wedge \theta_b(\vec{x}))]^\varphi$. Since Π_{k-1} contains $Th^+[\Gamma_{k-1}, C_{k-1}]$, $(\forall\vec{x})(\theta_a(\vec{x}) \wedge \theta_b(\vec{x}))$ is in Π_{k-1}, contradicting the consistency of Π_{k-1}.

To finish the induction step and prove the claim, we assume Π'_k is consistent and show that Π_k is consistent. First suppose Case (3) of the definition of Γ_k and Π_k applies and that Π_k is inconsistent. Then there is a positive C_k-sentence $\theta(d)$ such that $\Pi'_k \vdash_c \neg\theta(d)$ and $\Gamma_{k-1} \vdash_i \beta_k(d) \supset (\theta(d))^\varphi$. Since d is a new constant symbol, $\Pi_{k-1} \vdash_c (\forall x)\neg\theta(x)$ and likewise, since $\Gamma_{k-1} \vdash_i (\exists x)\beta_k(x)$, $\Gamma_{k-1} \vdash_i (\exists x)\theta(x)^\varphi$. Hence $(\exists x)\theta(x)$ is in Π'_k which contradicts the consistency of Π'_k. Second, suppose Case (4) of the definition applies. Let Π_k^c and Π_k^d be the $[\Gamma_{k-1} \cup \{\beta_k\}, C_k]$-closure and $[\Gamma_{k-1} \cup \{\gamma_k\}, C_k]$-closure of Π'_k, respectively. Suppose, for sake of a contradiction, that both Π_k^c and Π_k^d are inconsistent. Then there are positive C_k-sentences θ_c and θ_d such that $\Gamma_{k-1} \vdash_i \beta_k \supset (\theta_c)^\varphi$ and $\Gamma_{k-1} \vdash_i \gamma_k \supset (\theta_d)^\varphi$ and such that $\Pi'_k \vdash_c \neg\theta_c$

and $\Pi'_k \vdash_c \neg\theta_d$. Since $\Gamma_{k-1} \vdash_i \alpha_k$, $\Gamma_{k-1} \vdash_i (\theta_c \vee \theta_d)^\varphi$ and hence $\theta_a \vee \theta_b$ is in Π'_k. But this contradicts the consistency of Π'_k and completes the proof of the claim.

We are now ready to complete the proof of Lemma 7. Recall $\Gamma_\omega = \bigcup_k \Gamma_k$ and $\Pi_\omega = \bigcup_k \Pi_k$. By choice of constant symbols, $C^+ = \bigcup_k C_k$. First note that if χ is an atomic C^+-formula then $\Pi_\omega \vdash_c \chi$ if and only if $\Gamma_\omega \vdash_i \chi$. This is readily by proved by noting that $\Gamma_\omega \vdash_i \chi \vee \neg\chi$ since χ is atomic and hence $\Gamma_\omega \vdash_i \chi$ or $\Gamma_\omega \vdash_i \neg\chi$. Now if $\Gamma_\omega \vdash_i \chi$ then $\Gamma_\omega \vdash_i \chi^\varphi$ and hence $\Pi_\omega \vdash_c \chi$ since Π_ω contains $Th^+[\Gamma_\omega, C^+]$. Likewise, if $\Gamma_\omega \vdash_i \neg\chi$ then $\Pi_\omega \vdash_c \neg\chi$ since $\neg\chi$ is equivalent to an atomic formula.

Clearly Π_ω is a consistent, complete theory and since the α_k's enumerate all C^+-formulas, whenever $\Pi_\omega \vdash_c (\exists x)\beta(x)$ then $\Pi_\omega \vdash_c \beta(c)$ for some $c \in C^+$. Hence, the Henkin construction gives us a model $\mathcal{M}$ with domain a set of equivalence classes of C^+ and $\mathcal{M} \vDash CPV$ since $\mathcal{M} \vDash \Pi_\omega$ and $\Pi_\omega \supset CPV$. The equivalence classes of C^+ which form the domain of $\mathcal{M}$ are defined by $[c] = \{c' : \Pi_\omega \vdash_c c = c'\}$. The equivalence class $[c]$ is also equal to $\{c' : \Gamma_\omega \vdash_i c = c'\}$ since $c = c'$ is an atomic formula. In order to eliminate duplicate constant symbols we let C^* be a set of set of constant symbols so that $C \subset C^* \subset C^+$ and C^* contains exactly one constant symbol from each equivalence class. Such a C^* exists since no equivalence class can contain more than one constant symbol from C because $\Gamma_\omega \supset \Gamma$ and $\Gamma \vdash_i c \neq c'$ for distinct $c, c' \in C$. Now let Γ^* be the set of C^*-sentences which are intuitionistic consequences of Γ_ω. Let $\mathcal{M}_{C^*}$ be $\mathcal{M}$ restricted to the language of PV plus the constant symbols in C^*; obviously $\mathcal{M}_{\Gamma^*}$ is isomorphic to $\mathcal{M}_{C^*}$ by the mapping $c \mapsto [c]$. It remains to check that Γ^* satisfies conditions (a)-(e) of Lemma 7. (a) $\Gamma^* \supset \Gamma$ is immediate from our construction since $\Gamma_\omega \supset \Gamma$ and $C^* \supseteq C$. (b) To show Γ^* is C^*-saturated, suppose $\Gamma^* \vdash_i (\exists x)\psi(x)$ for ψ a C^*-formula. Then $\Gamma_\ell \vdash_i (\exists x)\psi(x)$ for some ℓ; and because the α_k's enumerate at C^+-sentences with infinitely many repetitions, $(\exists x)\psi(x)$ is α_k for some $k \geq \ell$. Hence $\Gamma_k \vdash_i \psi(d)$ for some $d \in C^+$. Also, $\Gamma_\omega \vdash_i c = d$ for some $c \in C^*$ so $\Gamma_\omega \vdash_i \psi(c)$ and thus $\Gamma^* \vdash_i \psi(c)$ by the definition of Γ^*. Similar reasoning shows that if $\Gamma^* \vdash_i \psi \vee \chi$ then $\Gamma^* \vdash_i \psi$ or $\Gamma^* \vdash_i \chi$ where ψ and χ are arbitrary C^*-sentences. (c) $\Gamma^* \nvdash_i \varphi$ by (2) of the Claim. (d) $\Gamma^* \vdash_i c \neq c'$ for all distinct $c, c' \in C^*$ since $\Pi_\omega \vdash_c c \neq c'$ (by definition of C^*). (e) $\mathcal{M}_{\Gamma^*} \vDash CPV$ since $\mathcal{M}_{\Gamma^*}$ is isomorphic to $\mathcal{M}_{C^*}$ and $\mathcal{M}$ is a model of $\Pi_\omega \supset \Pi_0 = CPV$.
Q.E.D. Lemma 7

We are now ready to define the CPV-normal Kripke model $\mathcal{K}$ for the proof of the completeness theorem. Recall that a CPV-normal Kripke model is an ordered pair $(\{\mathcal{M}_i\}_{i\in\mathcal{I}}, \preccurlyeq)$ where $\mathcal{I}$ is an index set, each $\mathcal{M}_i \vDash CPV$

and $\preccurlyeq$ is the reachability relation. The index set $\mathcal{I}$ will be the set of sets Γ of sentences such that

(a) Γ is C-saturated (where C is the set of constant symbols appearing in sentences in Γ,

(b) $\Gamma \supseteq \mathit{IPV}^+$,

(c) $\Gamma \vdash_i c \neq c'$ for distinct $c, c' \in C$ and

(d) $\mathcal{M}_\Gamma \models \mathit{CPV}$.

As an additional technical condition we require the set C of constant symbols be a coinfinite subset of some fixed countable set of constant symbols: this makes $\mathcal{I}$ a set rather than a proper class. Note that $\mathcal{I}$ is non-empty by Lemma 7. The worlds of $\mathcal{K}$ are the structures $\mathcal{M}_\Gamma$ such that $\Gamma \in \mathcal{I}$. By the Soundness Theorem proved above, $\mathcal{K} \Vdash \mathit{IPV}^+$. The reachability relation $\preccurlyeq$ is defined by $\mathcal{M}_{\Gamma_1} \preccurlyeq \mathcal{M}_{\Gamma_2}$ if and only if $\Gamma_1 \subseteq \Gamma_2$. It is easy to check from the definitions that, if $\Gamma_1 \subseteq \Gamma_2$ then $\mathcal{M}_{\Gamma_1}$ is a substructure of $\mathcal{M}_{\Gamma_2}$. Hence $\mathcal{K}$ is a CPV-normal Kripke model.

We are now ready to finish the proof of Theorem 3. Suppose $\mathit{IPV}^+ \nvdash_i \varphi$ for φ an arbitrary sentence. By Lemma 7 there is a $\Gamma \in \mathcal{I}$ such that $\Gamma \nvdash_i \varphi$. It will suffice to prove that $\mathcal{M}_\Gamma \nVdash \varphi$ since then $\mathcal{K} \nVdash \varphi$. This follows from the next lemma which also implies that for any sentence θ, $\mathit{IPV}^+ \vdash_i \theta$ if and only if $\mathcal{K} \Vdash \theta$; in other words, $\mathcal{K}$ is a CPV-normal, canonical Kripke model for IPV^+.

Lemma 8 *For any C-saturated $\Gamma \in \mathcal{I}$ and C-sentence ψ,*

$$\mathcal{M}_\Gamma \Vdash \psi \quad \Leftrightarrow \quad \Gamma \vdash_i \psi.$$

Proof (This is exactly like lemma 2.6.5 of Troelstra and van Dalen [15].) The lemma is proved by induction on the complexity of ψ:

Case (1): ψ is atomic. By definition of $\Vdash$ and $\mathcal{K}$.

Case (2): ψ is $\chi \wedge \gamma$.

$$\begin{aligned} \mathcal{M}_\Gamma \Vdash \chi \wedge \gamma &\Leftrightarrow \mathcal{M}_\Gamma \Vdash \chi \text{ and } \mathcal{M}_\Gamma \Vdash \gamma \\ &\Leftrightarrow \Gamma \vdash_i \chi \text{ and } \Gamma \vdash_i \gamma \qquad \text{by ind. hyp.} \\ &\Leftrightarrow \Gamma \vdash_i \chi \wedge \gamma \end{aligned}$$

Case (3): ψ is $\chi \vee \gamma$. Then

$$\begin{aligned} \mathcal{M}_\Gamma \Vdash \chi \vee \gamma &\Leftrightarrow \mathcal{M}_\Gamma \Vdash \chi \text{ or } \mathcal{M}_\Gamma \Vdash \gamma \\ &\Leftrightarrow \Gamma \vdash_i \chi \text{ or } \Gamma \vdash_i \gamma \qquad \text{by ind. hyp.} \\ &\Leftrightarrow \Gamma \vdash_i \chi \vee \gamma \qquad \text{by } C\text{-saturation of } \Gamma \end{aligned}$$

Case (4): ψ is $(\exists x)\chi(x)$. Then

$$\begin{aligned}\mathcal{M}_\Gamma \Vdash (\exists x)\chi(x) &\Leftrightarrow \exists c \in C,\ \mathcal{M}_\Gamma \Vdash \chi(c) \\ &\Leftrightarrow \exists c \in C,\ \Gamma \vdash_i \chi(c) && \text{by ind. hyp.} \\ &\Leftrightarrow \Gamma \vdash_i (\exists x)\chi(x) && \text{by } C\text{-saturation of } \Gamma\end{aligned}$$

Case (5): ψ is $\chi \supset \gamma$. ($\Leftarrow$) First suppose $\Gamma \vdash_i \chi \supset \gamma$. We must show that if $\mathcal{M}_\Gamma \preccurlyeq \mathcal{M}_{\Gamma_2}$ and $\mathcal{M}_{\Gamma_2} \Vdash \chi$ then $\mathcal{M}_{\Gamma_2} \Vdash \gamma$. Since $\Gamma_2 \supseteq \Gamma$, $\Gamma_2 \vdash_i \chi \supset \gamma$. Hence, if $\mathcal{M}_{\Gamma_2} \Vdash \chi$ then, by the induction hypothesis $\Gamma_2 \vdash_i \chi$, so $\Gamma_2 \vdash_i \gamma$ and, again by the induction hypothesis, $\mathcal{M}_{\Gamma_2} \Vdash \gamma$. ($\Rightarrow$) Second suppose $\Gamma \nvdash_i \chi \supset \gamma$. By Lemma 7, since $\Gamma \cup \{\chi\} \nvdash_i \gamma$, there is a $\mathcal{M}_{\Gamma_2} \succcurlyeq \mathcal{M}_\Gamma$ such that $\chi \in \Gamma_2$ and $\Gamma_2 \nvdash_i \gamma$. Now, by the induction hypothesis twice, $\mathcal{M}_{\Gamma_2} \Vdash \chi$ and $\mathcal{M}_{\Gamma_2} \nVdash \gamma$; so $\mathcal{M}_\Gamma \nVdash \chi \supset \gamma$.

Case (6): ψ is $(\forall x)\chi(x)$. ($\Leftarrow$) First suppose $\Gamma \vdash_i (\forall x)\chi(x)$. Further suppose $\mathcal{M}_{\Gamma_2} \succcurlyeq \mathcal{M}_\Gamma$, Γ_2 is C_2-saturated and $c \in C_2$. Then $\Gamma_2 \vdash_i \chi(c)$ since $\Gamma_2 \supseteq \Gamma$ and by the induction hypothesis, $\mathcal{M}_{\Gamma_2} \Vdash \chi(c)$. Hence $\mathcal{M}_\Gamma \Vdash (\forall x)\chi(x)$. ($\Rightarrow$) Second suppose $\Gamma \nvdash_i (\forall x)\chi(x)$. If c is a new constant symbol not in C, then $\Gamma \nvdash_i \chi(c)$. By Lemma 7 there is a world $\mathcal{M}_{\Gamma_2} \succcurlyeq \mathcal{M}_\Gamma$ such that $\Gamma_2 \nvdash_i \chi(c)$ with c a constant symbol in the language of Γ_2. Now by the induction hypothesis, $\mathcal{M}_{\Gamma_2} \nVdash \chi(c)$ so $\mathcal{M}_\Gamma \nVdash (\forall x)\chi(x)$.

Q.E.D. Lemma 8 and the Completeness Theorem.

It is interesting to ask whether there are analogues of our completeness and soundness theorems for IPV^+ w.r.t. CPV-normal Kripke models that apply to Peano arithmetic (PA) and Heyting arithmetic (HA). Let PA and HA be formulated in the first-order language of PRA so there is a function symbol for every primitive recursive function symbol: as usual, PA and HA have induction axioms for all arithmetic (first-order) formulas. PA is a classical theory and HA is an intutionistic theory and has the law of excluded middle for quantifier-free formulas. If we define a PA-normal Kripke model to be one in which each world is a classical model of Peano arithmetic, then it is natural to inquire whether Heyting arithmetic is complete and sound with respect to PA-normal Kripke models. It turns out that with some minor modifications the proof above shows that Heyting arithmetic is complete with respect to PA-normal Kripke models:

Theorem 9 *(Completeness Theorem for HA with respect to PA-normal Kripke models)*

Let φ be any sentence. If $HA \nvdash_i \varphi$ then there is a PA-normal Kripke model $\mathcal{K}$ such that $\mathcal{K} \Vdash HA$ and $\mathcal{K} \nVdash \varphi$.

We shall give the proof of Theorem 9 is a future paper; we also shall show that the converse fails: that is to say, there is a PA-normal Kripke model which is not a model of Heyting arithmetic.

6 On Independence Results

6.1 Independence Results in Computational Complexity from Feasible Theories

The main motivation for the independence results discussed below comes from the question of whether P = NP. Hartmanis and Hopcroft [8] suggested that P =?NP might be independent of set theory. Although this question is still open (and the natural conjecture is that it is not independent of set theory) there have been a number of results on independence of P =?NP and NP =?coNP from theories related to Bounded Arithmetic. DeMillo and Lipton [6, 7] proved that P = NP is consistent with the fragment of arithmetic ET which has function symbols for addition, subtraction, multiplication, exponentiation, maximization and minimization and has a predicate symbol for each polynomial time function. Sazanov [13] proved that there is a model of the true universal sentences of PV in which exponentiation is not total and yet there is a deterministic Turing machine which can find satisfying assignments to satisfiable propositional formulas. Recently, Cook and Urquhart [5] and Krajíček and Pudlák [11] have independently proved that it is consistent with IPV and PV_1 that extended Frege proof systems are almost super. By "almost super" is meant that for sufficiently large tautologies there are extended Frege proofs with size bounded by any provably super-polynomial growth rate function.

The point of these independence results is not to provide exidence that perhaps P = NP or the polynomial time hierarchy collapses; instead, the goal is to show why it seems so difficult to prove that P $\neq$ NP. However, it is difficult to know how much significance to attach to these independence results. DeMillo and Lipton's construction was criticized extensively by Joseph [10]; in particular, the standard integers are definable in DeMillo and Lipton's model by an atomic formula with a nonstandard parameter and hence induction fails for such formulas. Sazanov's model does have induction for all atomic (polynomial time) formulas with parameters, but his model only indirectly satisfies P = NP in that there is no polynomial time predicate that defines the set of satisfiable formulas. Furthermore, in Sazanov's model there is a polynomial time function mapping the set unary integers *onto* the integers in binary notation in spite of the fact that exponentiation is not total. The constructions of Cook and Urquhart and of Krajíček and Pudlák avoid

such overtly pathological features but they only indirectly make NP = coNP. They show that there is a Π_3-formula *NPB* which is not a consequence of either PV_1 or *IPV*; *NPB* states that an extended Frege proof system is not super. It is open whether the theory $CPV = S^1_2(PV)$ can prove *NPB*. It seems that PV_1 and *IPV* are too weak for these latter independence results to be very meaningful.

There are a number of other independence results in computer science which we have not discussed because they are not related to Bounded Arithmetic; Joseph [9] contains a survey of this area.

6.2 Independence Results for PV_1 and IPV via Kripke models

Let $f(x)$ be a unary integer function such that the predicates $y = f(x)$ and $y \leq f(x)$ are polynomial time computable and hence definable by atomic formulas in PV_1. Also suppose f is provably an increasing function and provably dominates any polynomial growth rate function; i.e., for each $n \in \mathbb{N}$, there is an $m \in \mathbb{N}$ such that

$$PV_1 \vdash_c (\forall y \geq m)(\forall z)(f(y) = z \supset |z| \geq |y|^n).$$

Since this is a universal statement, *IPV* also proves this. Note that this growth rate implies that f is not provably total in PV_1 or *IPV*. An example of such a function is $f(x) = x^{|x|}$.

The independence results of Krajíček-Pudlák and Cook-Urquhart state that it is not the case that $f(x)$ is provably not an upper bound to the size of extended Frege proofs of tautologies: more precisely, let *NPB* ("Not Polynomially Bounded") be the formula

$$(\forall x)(\exists y \geq x)[Taut(y) \wedge (\forall z)(z \leq f(y) \supset \neg z \vdash_{e\mathcal{F}} y)]$$

where $Taut(y)$ states that y is the Gödel number of a propositional tautology and "$z \vdash_{e\mathcal{F}} y$" states that z is the Gödel number of an extended Frege proof of the formula coded by y. So *NPB* states that there are arbitrarily large tautologies y whose shortest (if any) extended Frege proofs have Gödel number greater than $f(y)$.

Theorem 10

(a) *(Cook-Urquhart [5]) IPV* $\nvdash_i$ *NPB.*

(b) *(Krajíček-Pudlák [11])* $PV_1 \nvdash_c$ *NPB.*

In other words, IPV and PV_1 do not prove that extended Frege systems are not super. (Cook and Urquhart state their result for IPV^ω but this is equivalent since they also show that IPV^ω is conservative over IPV.)

Both parts of Theorem 10 were proved with the aid of Cook's theorem that PV-provable polynomial time identities give rise to tautologies with polynomial size extended Frege proofs. Krajíček and Pudlák proved part (b) by constructing a chain of models $\mathcal{M}_0, \mathcal{M}_1, \ldots$ of CPV such that for $i \leq j$, $\mathcal{M}_i$ is a substructure of $\mathcal{M}_j$ and such that for any $d \in \mathcal{M}_i$ there is a $j \geq i$ such that $\mathcal{M}_j \vDash (\exists z)(z \vdash_{e\mathcal{F}} d)$ or $\mathcal{M}_j \vDash \neg Taut(d)$. Furthermore, there is a nonstandard element $a \in |\mathcal{M}_0|$ such that a, $a\#a$, $a\#a\#a$,... is cofinal in every $\mathcal{M}_i$. By taking the union of the $\mathcal{M}_i$'s a model of PV_1 is obtained in which NPB is false; thus proving Theorem 10(b).

The natural question then arises of what is true in the Kripke model $(\{\mathcal{M}_i\}_{i\in\mathbb{N}}, \preccurlyeq)$ where $\mathcal{M}_i \preccurlyeq \mathcal{M}_j$ if and only if $i \leq j$. Since it is CPV-normal, IPV^+ is valid in this Kripke model; it turns out that NPB is not valid. By pulling out the universal quantifiers and combining like quantifiers we rewrite NPB as

$$(\forall x)(\exists y)(\forall z)NPB_M$$

where $NPB_M(x, y, z)$ is an atomic formula formalizing "$y \geq x$ and z is not a satisfying assignment of y and if $z \leq f(y)$ then z is not an extended Frege proof of y".

Theorem 11

(a) $IPV^+ \nvdash_i \neg\neg NPB$

(b) $IPV^+ \nvdash_i \neg(\exists x)(\forall y)\neg(\forall z)NPB_M(x, y, z)$

(c) $IPV^+ \nvdash_i \neg(\exists x)(\forall y)\neg\neg(\exists z)\neg NPB_M(x, y, z)$.

Of course, Theorem 11 represents a slight strengthening of Theorem 10(a); firstly, because IPV has been replaced by IPV^+ and, secondly, since negation signs have been introduced.

Proof Let $\mathcal{K}$ be the Kripke model $(\{\mathcal{M}_i\}_{i\in\mathbb{N}}, \preccurlyeq)$ as above. Since $\mathcal{K}$ is CPV-normal and hence IPV^+ is valid in $\mathcal{K}$ it will suffice to show that the formulas (a), (b) and (c) are not valid in $\mathcal{K}$. For (a), suppose for a contradiction that $\mathcal{K} \Vdash \neg\neg NPB$. Then by the definition of forcing, $\mathcal{M}_i \Vdash NPB$ for sufficiently large i. But taking $x = a$ where $a, a\#a, \ldots$ is cofinal in $\mathcal{M}_i$, $\mathcal{M}_i \Vdash (\exists y)(\forall z)NPB_M(a, y, z)$ and so for some $y_0 \in |\mathcal{M}_i|$ such that $y_0 \geq a$ and $\mathcal{M}_i \Vdash (\forall z)NPB_M(a, y_0, z)$. But, by contruction of the $\mathcal{M}_i$'s, there is some $j \geq i$ and some $z_0 \in \mathcal{M}_j$ such that z_0 is either an extended Frege proof of y_0 or z_0 is not an satisfying assignment for y_0. Also, $z_0 \leq f(y_0)$

as $y_0 \geq a$, f is increasing, and $|z| \leq |a|^n < |f(a)|$ for some standard n. Thus $\mathcal{M}_j \nVdash NPB_M(a, y_0, z_0)$, contradicting $\mathcal{M}_i \Vdash (\forall z) NPB_M(a, y_0, z)$. That proves that (a) is not valid in $\mathcal{K}$. The proofs for (b) and (c) are similar. $\Box$.

Note that Theorems 4(a) and 11(b) imply Theorem 10(b). What we have done is adapted Krajìček and Pudlàk's proof technique to to prove a strengthening of Cook and Urquhart's independence result and then used Theorem 4 to rederive Krajíček and Pudlák's theorem. This shows that there is a very close link between their two independence results.

It is open whether $\neg(\exists x)(\forall y)(\exists z)\neg NPB_M$ is independent of IPV; if so, then it is also independent of CPV and S^1_2. This is immediate from Theorem 1 since $(\exists z)(\forall y)(\exists z)\neg NPB_m$ is equivalent to a positive formula.

References

[1] S. R. Buss, *Bounded Arithmetic*, Bibliopolis, 1986. Revision of 1985 Princeton University Ph.D. thesis.

[2] ——, *The polynomial hierarchy and intuitionistic bounded arithmetic*, in Structure in Complexity, Lecture Notes in Computer Science #223, Springer-Verlag, 1986, pp. 77–103.

[3] ——, *A note on bootstrapping intuitionistic bounded arithmetic*, in Proof Theory: A selection of papers from the Leeds Proof Theory Programme 1990, Cambridge University Press, 1992, pp. 149–169.

[4] S. A. Cook, *Feasibly constructive proofs and the propositional calculus*, in Proceedings of the Seventh Annual ACM Symposium on Theory of Computing, 1975, pp. 83–97.

[5] S. A. Cook and A. Urquhart, *Functional interpretations of feasibly constructive arithmetic*, Annals of Pure and Applied Logic, 63 (1993), pp. 103–200.

[6] R. A. DeMillo and R. J. Lipton, *Some connections between mathematical logic and complexity theory*, in Proceedings of the 11th ACM Symposium on Theory of Computing, 1979, pp. 153–159.

[7] ——, *The consistency of "P=NP" and related problems with fragments of number theory*, in Proceedings of the 12th ACM Symposium on Theory of Computing, 1980, pp. 45–57.

[8] J. Hartmanis and J. Hopcroft, *Independence results in computer science*, SIGACT News, 8 (1976), pp. 13–24.

[9] D. Joseph, *On the Power of Formal Systems for Analyzing Linear and Polynomial Time Program Behavior*, PhD thesis, Purdue University, August 1981.

[10] ——, *Polynomial time computations in models of ET*, Journal of Computer and System Sciences, 26 (1983), pp. 311–338.

[11] J. Krajíček and P. Pudlák, *Propositional provability and models of weak arithmetic*. Typewritten manuscript, 1989.

[12] J. Krajíček, P. Pudlák, and G. Takeuti, *Bounded arithmetic and the polynomial hierarchy*, Annals of Pure and Applied Logic, 52 (1991), pp. 143–153.

[13] V. Y. Sazanov, *A logical approach to the problem "P=NP?"*, in Mathematics Foundations of Computer Science, Lecture Notes in Computer Science #88, Springer-Verlag, 1980, pp. 562–575. There is an unfixed problem with the proof of the main theorem in this article; see [14] for a correction.

[14] ——, *On existence of complete predicate calculus in matemathematics without exponentiation*, in Mathematics Foundations of Computer Science, Lecture Notes in Computer Science #118, Springer-Verlag, 1981, pp. 383–390.

[15] A. S. Troelstra and D. van Dalen, *Constructivism in Mathematics: An Introduction*, vol. I, North-Holland, 1988.

Samuel R. Buss
Department of Mathematics
University of California, San Diego
La Jolla, California 92093
U.S.A.