London Mathematical Society
Lecture Note Series 97

Varieties of Constructive Mathematics

DOUGLAS BRIDGES and FRED RICHMAN

CAMBRIDGE UNIVERSITY PRESS

LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor J.W.S. Cassels, Department of Pure Mathematics and Mathematical Statistics, 16 Mill Lane, Cambridge CB2 1SB, England

The books in the series listed below are available from booksellers, or, in case of difficulty, from Cambridge University Press.

4 Algebraic topology, J.F.ADAMS
5 Commutative algebra, J.T.KNIGHT
11 New developments in topology, G.SEGAL (ed)
12 Symposium on complex analysis, J.CLUNIE & W.K.HAYMAN (eds)
13 Combinatorics, T.P.McDONOUGH & V.C.MAVRON (eds)
16 Topics in finite groups, T.M.GAGEN
17 Differential germs and catastrophes, Th.BROCKER & L.LANDER
18 A geometric approach to homology theory, S.BUONCRISTIANO, C.P.ROURKE & B.J.SANDERSON
20 Sheaf theory, B.R.TENNISON
21 Automatic continuity of linear operators, A.M.SINCLAIR
23 Parallelisms of complete designs, P.J.CAMERON
25 Lie groups and compact groups, J.F.PRICE
26 Transformation groups, C.KOSNIOWSKI (ed)
27 Skew field constructions, P.M.COHN
29 Pontryagin duality and the structure of LCA groups, S.A.MORRIS
30 Interaction models, N.L.BIGGS
31 Continuous crossed products and type III von Neumann algebras,A.VAN DAELE
32 Uniform algebras and Jensen measures, T.W.GAMELIN
34 Representation theory of Lie groups, M.F. ATIYAH et al.
35 Trace ideals and their applications, B.SIMON
36 Homological group theory, C.T.C.WALL (ed)
37 Partially ordered rings and semi-algebraic geometry, G.W.BRUMFIEL
38 Surveys in combinatorics, B.BOLLOBAS (ed)
39 Affine sets and affine groups, D.G.NORTHCOTT
40 Introduction to Hp spaces, P.J.KOOSIS
41 Theory and applications of Hopf bifurcation, B.D.HASSARD, N.D.KAZARINOFF & Y-H.WAN
42 Topics in the theory of group presentations, D.L.JOHNSON
43 Graphs, codes and designs, P.J.CAMERON & J.H.VAN LINT
44 Z/2-homotopy theory, M.C.CRABB
45 Recursion theory: its generalisations and applications, F.R.DRAKE & S.S.WAINER (eds)
46 p-adic analysis: a short course on recent work, N.KOBLITZ
47 Coding the Universe, A.BELLER, R.JENSEN & P.WELCH
48 Low-dimensional topology, R.BROWN & T.L.THICKSTUN (eds)
49 Finite geometries and designs,P.CAMERON, J.W.P.HIRSCHFELD & D.R.HUGHES (eds)
50 Commutator calculus and groups of homotopy classes, H.J.BAUES
51 Synthetic differential geometry, A.KOCK
52 Combinatorics, H.N.V.TEMPERLEY (ed)
54 Markov process and related problems of analysis, E.B.DYNKIN
55 Ordered permutation groups, A.M.W.GLASS
56 Journêes arithmêtiques, J.V.ARMITAGE (ed)
57 Techniques of geometric topology, R.A.FENN
58 Singularities of smooth functions and maps, J.A.MARTINET
59 Applicable differential geometry, M.CRAMPIN & F.A.E.PIRANI
60 Integrable systems, S.P.NOVIKOV et al
61 The core model, A.DODD
62 Economics for mathematicians, J.W.S.CASSELS
63 Continuous semigroups in Banach algebras, A.M.SINCLAIR
64 Basic concepts of enriched category theory, G.M.KELLY
65 Several complex variables and complex manifolds I, M.J.FIELD

66 Several complex variables and complex manifolds II. M.J.FIELD
67 Classification problems in ergodic theory, W.PARRY & S.TUNCEL
68 Complex algebraic surfaces, A.BEAUVILLE
69 Representation theory, I.M.GELFAND et al.
70 Stochastic differential equations on manifolds, K.D.ELWORTHY
71 Groups - St Andrews 1981, C.M.CAMPBELL & E.F.ROBERTSON (eds)
72 Commutative algebra: Durham 1981, R.Y.SHARP (ed)
73 Riemann surfaces: a view towards several complex variables,A.T.HUCKLEBERRY
74 Symmetric designs: an algebraic approach, E.S.LANDER
75 New geometric splittings of classical knots, L.SIEBENMANN & F.BONAHON
76 Spectral theory of linear differential operators and comparison algebras, H.O.CORDES
77 Isolated singular points on complete intersections, E.J.N.LOOIJENGA
78 A primer on Riemann surfaces, A.F.BEARDON
79 Probability, statistics and analysis, J.F.C.KINGMAN & G.E.H.REUTER (eds)
80 Introduction to the representation theory of compact and locally compact groups, A.ROBERT
81 Skew fields, P.K.DRAXL
82 Surveys in combinatorics, E.K.LLOYD (ed)
83 Homogeneous structures on Riemannian manifolds, F.TRICERRI & L.VANHECKE
84 Finite group algebras and their modules, P.LANDROCK
85 Solitons, P.G.DRAZIN
86 Topological topics, I.M.JAMES (ed)
87 Surveys in set theory, A.R.D.MATHIAS (ed)
88 FPF ring theory, C.FAITH & S.PAGE
89 An F-space sampler, N.J.KALTON, N.T.PECK & J.W.ROBERTS
90 Polytopes and symmetry, S.A.ROBERTSON
91 Classgroups of group rings, M.J.TAYLOR
92 Representation of rings over skew fields, A.H.SCHOFIELD
93 Aspects of topology, I.M.JAMES & E.H.KRONHEIMER (eds)
94 Representations of general linear groups, G.D.JAMES
95 Low-dimensional topology 1982, R.A.FENN (ed)
96 Diophantine equations over function fields, R.C.MASON
97 Varieties of constructive mathematics, D.S.BRIDGES & F.RICHMAN
98 Localization in Noetherian rings, A.V.JATEGAONKAR
99 Methods of differential geometry in algebraic topology, M.KAROUBI & C.LERUSTE
100 Stopping time techniques for analysts and probabilists, L.EGGHE
101 Groups and geometry, ROGER C.LYNDON
102 Topology of the automorphism group of a free group, S.M.GERSTEN
103 Surveys in combinatorics 1985, I.ANDERSEN (ed)
104 Elliptic structures on 3-manifolds, C.B.THOMAS
105 A local spectral theory for closed operators, I.ERDELYI & WANG SHENGWANG
106 Syzygies, E.G.EVANS & P.GRIFFITH
107 Compactification of Siegel moduli schemes, C-L.CHAI
108 Some topics in graph theory, H.P.YAP
109 Diophantine analysis, J.LOXTON & A.VAN DER POORTEN (eds)
110 An introduction to surreal numbers, H.GONSHOR
111 Analytical and geometric aspects of hyperbolic space, D.B.A.EPSTEIN (ed)
112 Low dimensional topology and Kleinian groups, D.B.A.EPSTEIN (ed)
113 Lectures on the asymptotic theory of ideals, D.REES
114 Lectures on Bochner-Riesz means, K.M.DAVIS & Y-C.CHANG
115 An introduction to independence for analysts, H.G.DALES & W.H.WOODIN
116 Representations of algebras, P.J.WEBB (ed)
117 Homotopy theory, E.REES & J.D.S.JONES (eds)
118 Skew linear groups, M.SHIRVANI & B.WEHRFRITZ

London Mathematical Society Lecture Note Series. 97

Varieties of Constructive Mathematics

DOUGLAS BRIDGES
University of Buckingham

FRED RICHMAN
New Mexico State University

The right of the University of Cambridge to print and sell all manner of books was granted by Henry VIII in 1534. The University has printed and published continuously since 1584.

CAMBRIDGE UNIVERSITY PRESS
Cambridge
New York New Rochelle
Melbourne Sydney

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore,
São Paulo, Delhi, Dubai, Tokyo, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by
Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521318020

First published 1987
Reprinted 1988

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication Data

Bridges, D. S. (Douglas S.), 1945–
Varieties of constructive mathematics.
(London Mathematical Society lecture note series ;97)
1. Constructive mathematics.
I. Richman, Fred. II. Title. III. Series
QA9.56.B75 1986 511.3 85–26904

ISBN 978-0-521-31802-5 Hardback
ISBN 978-0-521-31802-0 Paperback

Preface

In Hilary Term, 1981, Douglas Bridges gave a course of lectures on Intuitionism and constructive mathematics in the Mathematical Institute of Oxford University. Shortly afterwards, he invited Fred Richman to join in the writing of a book based (as it turns out, rather loosely) on those lectures. The book now lies in front of the reader, as an introduction to the spirit and practice of modern constructive mathematics.

There are several excellent works - such as Beeson's *Foundations of Constructive Mathematics* and Dummett's *Elements of Intuitionism* - on the logical and philosophical foundations of constructive mathematics; and there are others, such as Bishop's seminal treatise *Foundations of Constructive Analysis*, dealing with the detailed development of major portions of mathematics within a constructive framework. The present book is intended to land between those two positions: specifically, we hope that, with a minimum of philosophy and formal logic, and without requiring of the reader too great an investment of time and effort over technical details, it will leave him with a clear conception of the problems and methods of the three most important varieties of modern constructive mathematics.

Since classical mathematics, as practised by all but a tiny minority of mathematicians, appears to offer a much less arduous route to discovery, and a far greater catalogue of successes, than its constructive counterpart, one may well ask: Why should anyone, other than a devotee of a constructivist philosophy, be interested in learning about constructive mathematics? We believe there are several reasons why one might be so interested.

First, there is the richer structure of constructive mathematics that flows from the deepened meaning of existence. In the classical interpretation, an object exists if its non-existence is contradictory. There is a clear distinction between this meaning of existence and the constructive, algorithmic one, under which an object exists only if we can construct it, at least in principle. As Bishop has said, such 'meaningful distinctions deserve to be maintained'.

Second, there is the unexpected role played by intuitionistic logic and constructive methods in topos theory. Any theorem in constructive mathematics may be interpreted as a classical theorem about a topos; if the topos is suitably chosen, then the theorem may have classical interest outside of topos theory. For example, constructive theorems about diagonalizing matrices over the reals may be interpreted as classical theorems about diagonalizing matrices over the ring of continuous functions on a compact metric space.

Finally, there is the possibility of applications of constructive mathematics to areas such as numerical mathematics, physics, and computer science. For computer science, we refer the reader to Martin-Löf's paper *Constructive mathematics and computer programming* (in: *Logic, Methodology and the Philosophy of Science* VI, North-Holland, 1982), and to the recent book *Implementing Mathematics with the Nuprl Proof Development System*, by Constable et al. (Prentice-Hall, 1986).

We now outline the contents of our book. In Chapter 1 we introduce the three varieties of constructive mathematics with which we shall be concerned: Bishop's constructive mathematics, Brouwer's intuitionistic mathematics, and the constructive recursive mathematics of the Russian school of Markov; we also construct the real line $\mathbb{R}$ and examine its basic properties.

In Chapter 2 we discuss, within Bishop's mathematics, a range of topics in analysis. These topics are chosen to illustrate distinctive features of the practice of constructive mathematics, such as the splitting of one classical theorem (for example, Baire's theorem) into several inequivalent constructive ones, and the investigation of important notions, like locatedness, with little or no classical significance. A similar approach to constructive algebra is found in Chapter 4, which culminates in a constructive treatment of the Hilbert basis theorem. Chapter 4 also offers some comparisons between constructive algebra and classical recursive algebra.

Chapter 3 contains the essentials of constructive recursive mathematics, and is based on Richman's axiomatic approach to Church's thesis. This approach greatly simplifies the presentation of mathematics within the recursive framework, and leads to particularly perspicuous proofs of Specker's theorem and the existence of a compact subset of $\mathbb{R}$ that is not Lebesgue measurable.

Chapter 5 deals with intuitionistic mathematics, by formulating axioms which capture the mathematical essence of Brouwer's approach. The elements of intuitionistic mathematics are developed, including Brouwer's famous theorem that every real-valued function on a compact interval is uniformly continuous.

In Chapter 6 the three varieties of constructive mathematics are compared by an examination of the status within each of the classical proposition

if f is a uniformly continuous mapping of [0,1] *into the positive real line, then the infimum of f is positive.*

The final chapter deals with intuitionistic logic and topos models, mainly through the presentation of a few examples. We treat this material somewhat superficially, not wishing to involve the reader in a detailed development of the logic and category theory necessary for a fully rigorous treatment.

A remark about our style of references is in order here. With few exceptions, references are found in the notes at the end of each chapter, in which case they are normally described in detail. There are certain works to which we refer so often, or which are indispensable to the practising constructive mathematician, that we chose to give them special names, printed in bold face; these are

Beeson	Michael J. Beeson, *Foundations of Constructive Mathematics* (Springer, 1985)
Bishop	Errett Bishop, *Foundations of Constructive Analysis*, (McGraw-Hill, 1967)
Bishop-Bridges	Errett Bishop and Douglas Bridges, *Constructive Analysis* (Springer, 1985)
Brouwer	*Brouwer's Cambridge lectures on intuitionism*, (Dirk Van Dalen ed., Cambridge University Press, 1981)
Dummett	Michael Dummett, *Elements of Intuitionism* (Oxford University Press, 1977)

Kushner	B.A. Kushner, *Lectures on Constructive Mathematical Analysis* (American Mathematical Society, 1985)
MRR	Ray Mines, Fred Richman, Wim Ruitenberg, *A Course on Constructive Algebra* (Springer, forthcoming)
Springer 873	*Constructive Mathematics* (Fred Richman ed., Springer Lecture Notes in Mathematics 873)

During the writing of this book, we received support from the University of Buckingham and from New Mexico State University. As usual, we have had many hours of stimulating discussion with Bill Julian and Ray Mines. Bill and Nancy Julian kindly provided hospitality when Bridges visited New Mexico to work with Richman. David Tranah, of Cambridge University Press, has been unbelievably patient with us, as deadline after deadline has passed by.

Perhaps the most long-suffering have been our families, who have had to share the birth pangs of this book over an unusually long labour; we dedicate this work to them.

Douglas S. Bridges
Fred Richman

Buckingham, England
Las Cruces, New Mexico

Contents

Chapter 1. Foundations of Constructive Mathematics

In which the reader is introduced to the three varieties of constructive mathematics that will be studied in detail in subsequent chapters; the framework of Bishop's constructive mathematics is erected; and the elementary theory of the real numbers is developed.

1. Existence and omniscience

We engage in constructive mathematics from a desire to clarify the meaning of mathematical terminology and practice – in particular, the meaning of existence in a mathematical context. The classical mathematician, with the freedom of methodology advocated by Hilbert, perceives an object x to exist if he can prove the impossibility of its nonexistence; the constructive mathematician must be presented with an algorithm that constructs the object x before he will recognize that x exists.

What do we mean by an *algorithm*? We may think of an algorithm as a specification of a step-by-step computation, such as a program in some computer language, which can be performed, at least in principle, by a human being or a computer in a finite period of time; moreover, the passage from one step to another should be deterministic. Note that we say 'performed, at least in principle', for it is possible for an algorithm to require an amount of time greater than the age of the universe for its complete execution. We are not concerned here with questions of complexity or efficiency.

In Bishop's constructive mathematics (**BISH**), and in Brouwer's intuitionism (**INT**), the notion of an algorithm, or finite routine, is taken as primitive. Russian constructivism (**RUSS**), on the other hand, operates within a fixed programming language, and an algorithm is a sequence of symbols in that language.

While BISH is only one of the three varieties of constructive mathematics that we shall consider, it is the one to which we shall devote the most attention. There are at least two reasons for this. First, BISH is consistent with **CLASS**, the classical mathematics practised by most mathematicians today. Every proposition P in BISH has an immediate interpretation in CLASS, and a proof of P in BISH is also a proof of P in CLASS. This is not true in our other two varieties: Russian constructivism (RUSS) and Brouwer's intuitionism (INT). For example, in both RUSS and INT it is proved that every real valued function on the interval [0,1] is pointwise continuous.

A second reason for paying particular attention to BISH is that every proof of a proposition P in BISH is a proof of P in RUSS and in INT. Indeed, the last two varieties may be regarded as extensions of BISH. In RUSS, the main principle adjoined to BISH is a form of Church's thesis that all sequences of natural numbers are recursive. In INT, two principles are added which ensure strong continuity properties of arbitrary real-valued functions on intervals of the line.

From a philosophical point of view, there is more to RUSS and INT than the mere adjunction of certain principles to BISH. In RUSS, every mathematical object is, ultimately, a natural number: constructions take place within a fixed formal system, functions are Gödel numbers of the algorithms that compute them, and so on. On the other hand, INT is based on Brouwer's intuitionistic philosophy, including an analysis of the notion of an infinitely proceeding, or free choice, sequence. For the most part we shall ignore the philosophical aspects by abstracting in each case the features essential for the development of the associated mathematics; we are writing for mathematicians rather than for philosophers or logicians.

The essential difference between BISH and CLASS is illustrated by considering the simplest kind of statement concerning existence in an infinite context. A **binary sequence** is a finite routine that assigns to each positive integer an element of $\{0,1\}$. Let α be a binary sequence, and consider the statements

$$\begin{aligned} P(\alpha) &: \ a_n = 1 \text{ for some } n, \\ \neg P(\alpha) &: \ a_n = 0 \text{ for all } n, \\ P(\alpha) \vee \neg P(\alpha) &: \ \text{Either } P(\alpha) \text{ or } \neg P(\alpha), \end{aligned}$$

$$\forall\alpha(P(\alpha) \vee \neg P(\alpha)) : \text{ For all } \alpha, \text{ either } P(\alpha) \text{ or } \neg P(\alpha).$$

Note that $\neg P(\alpha)$ is the denial of $P(\alpha)$. A constructive proof of $P(\alpha) \vee \neg P(\alpha)$ must provide a finite routine which either shows that $a_n = 0$ for all n, or computes a positive integer n with $a_n = 1$. (Note the constructive meaning of disjunction, which follows from the constructive interpretation of existence: $P_1 \vee P_2$ holds if and only if there exists i such that P_i; to prove $P_1 \vee P_2$, it is not enough to show that P_1 and P_2 cannot both be false.) In particular, if α is the binary sequence defined by setting

$$a_n = 0 \quad \text{if } x^{m+2} + y^{m+2} \neq z^{m+2} \text{ for all positive integers } x,y,z,m \leq n,$$
$$= 1 \quad \text{otherwise,}$$

then a constructive proof of $P(\alpha) \vee \neg P(\alpha)$ would give a method for deciding the Fermat conjecture, $\neg P(\alpha)$, by providing a construction that either establishes the Fermat conjecture or produces an explicit counterexample to it; unless we have such a construction, we are not entitled to assert $P(\alpha) \vee \neg P(\alpha)$ within BISH. We say that α is a **Brouwerian example** of a binary sequence for which $P(\alpha) \vee \neg P(\alpha)$ does not hold, or that α is a **Brouwerian counterexample** to the statement $\forall\alpha(P(\alpha) \vee \neg P(\alpha))$. Note that a Brouwerian counterexample is not an counterexample in the usual sense; it is *evidence* that a statement does not admit a constructive proof.

The use of Fermat's conjecture in the above example is not essential. If Fermat's conjecture were resolved tomorrow, we could then assert $P(\alpha) \vee \neg P(\alpha)$; however, by referring to another open problem, such as the Riemann hypothesis or the Goldbach conjecture, we could construct another binary sequence α for which we could not assert $P(\alpha) \vee \neg P(\alpha)$

More generally, a **Brouwerian counterexample** to an assertion A is a proof that A implies some principle that is unacceptable, or at least highly dubious, in the context of constructive mathematics. The two most popular principles were introduced by Brouwer; we present them here under the names given them by Bishop. The first is simply the assertion $\forall\alpha(P(\alpha) \vee \neg P(\alpha))$; the second is a little subtler.

LPO **The limited principle of omniscience:** *If* (a_n) *is a binary sequence, then either there exists* n *such that* $a_n = 1$*, or else* $a_n = 0$ *for each* n.

LLPO **The lesser limited principle of omniscience:** *If* (a_n) *is a binary sequence containing at most one* 1, *then either* $a_{2n} = 0$ *for each* n, *or else* $a_{2n+1} = 0$ *for each* n.

A constructive proof of LPO would provide a finite decision procedure for a vast number of unsolved problems in mathematics, including the conjectures of Fermat, Riemann, and Goldbach. The unlikelihood of finding a method of such power and scope is an argument for excluding LPO from constructive mathematics, at least provisionally; were such a method found, our ideas concerning constructive mathematics would have to be drastically revised, especially as LPO and LLPO are provably false within INT and RUSS.

The **law of excluded middle**, which asserts that $P \vee \neg P$ holds for any statement P, implies LPO, and so is rejected in constructive mathematics.

Given a real number r, for each positive integer n compute a rational number r_n such that $|r - r_n| < 1/n$. If $|r_n| \leq 1/n$, set $a_n \equiv 0$, and if $|r_n| > 1/n$, set $a_n \equiv 1$. Then the resulting binary sequence $a \equiv (a_1, a_2, \ldots)$ has the property that

$$(*) \qquad \begin{aligned} |r| > 0 &\text{ if and only if } \exists n(a_n = 1), \text{ and} \\ r = 0 &\text{ if and only if } \forall n(a_n = 0). \end{aligned}$$

Conversely, to each binary sequence a there corresponds a real number $r \equiv \sum_{n=1}^{\infty} 2^{-n} a_n$ such that $(*)$ obtains. Thus the limited principle of omniscience is equivalent to the assertion that each real number is either 0 or different from 0. Another assertion equivalent to LPO is the **trichotomy law:** $[-1,1] = [-1,0) \cup \{0\} \cup (0,1]$.

The lesser limited principle of omniscience says that for any binary sequence, either the first nonzero term, if it exists, has even index, or the first nonzero term, if it exists, has odd index. This is equivalent to the assertions

$$[-1,1] = [-1,0] \cup [0,1],$$

and

$$\text{for each real number } r, \text{ either } r \leq 0 \text{ or } r \geq 0.$$

Another assertion equivalent to LLPO is that if the product of two real numbers is 0, then one or the other of them is 0.

Many other familiar results of CLASS are equivalent to some principle that is rejected in BISH. The intermediate value theorem for uniformly continuous functions is equivalent to LLPO, while LPO is equivalent to the assertion that every real number is either rational or irrational. The law of excluded middle is a consequence of the statement that every ideal in the ring of integers is finitely generated.

It is helpful to formulate omniscience principles in the notation of the (intuitionistic) propositional calculus, in terms of the simplest kind of assertion of existence in an infinite context. Let us call an assertion A **simply existential** if we can construct a binary sequence α such that A holds if and only if there exists n such that $\alpha_n = 1$. For arbitrary simply existential statements A and B, the principles LPO and LLPO take the forms:

$$\text{LPO:} \quad A \vee \neg A,$$

$$\text{LLPO:} \quad \neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B.$$

It is easily seen that if A and B are simply existential, then so is $A \wedge B$. Thus LLPO can be extended, by induction on n, to read

$$\neg(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \Leftrightarrow \neg A_1 \vee \neg A_2 \vee \cdots \vee \neg A_n.$$

Two other omniscience principles, stated for an arbitrary simply existential statement A, are the **weak limited principle of omniscience**

$$\text{WLPO:} \quad \neg A \vee \neg\neg A,$$

and **Markov's Principle**

$$\text{MP:} \quad \neg\neg A \Leftrightarrow A.$$

These two principles were also rejected by Brouwer, and are commonly used by constructive mathematicians for counterexamples. It is not difficult to show that LPO implies WLPO, and that WLPO implies LLPO. These three principles are false in RUSS, unlike Markov's principle, which is used freely by the practitioners of that school.

The reader should not be misled into thinking that constructive mathematics is largely a criticism of classical mathematics by means of Brouwerian counterexamples, although such counterexamples do play an important role in establishing the direction of constructive research. The main task of the constructive mathematician is the positive