PROOF THEORY AND CONSTRUCTIVE MATHEMATICS

Anne S. Troelstra
ILLC , University van Amsterdam ,Plantage Muidergracht 24 ,1018 TV Amsterdam , Netherlands

Keywords: Algebraical semantics, almost negative formula, axiom of open data, bar induction, Bishop's constructive mathematics, Brouwer-Heyting-Kolmogorov interpretation, choice sequence, Church's thesis, Church-Kleene ordinal, constructive recursive mathematics, constructivism, continuity axioms, contraction, cut elimination, disjunction property, elimination rule, explicit definability property, finitism, Gentzen sequent, Glivenko theorem, Gödel-Gentzen translation, Heyting arithmetic, Hilbert's program, Hilbert-type system, I-completeness, introduction rule, intuitionism, intuitionistic arithmetic, intuitionistic logic, inversion lemma, Kreisel-Lacombe-Shoenfield-Tsejtin theorem, Kripke forcing, Kripke semantics, lawless sequence, Markov's principle, Markov's rule, natural deduction, negative formula, normalization, order type, ordinal notation, predicativism, proof theory, proof-theoretic ordinal, realizability, semi-formal system, singular cover, Specker sequence, Tait calculus, topological semantics, truth-complexity, typed lambda-calculus, weakening.

Contents

UNESCO – EOLSS
SAMPLE CHAPTERS

Summary

An introduction to the constructive point of view in the foundations of mathematics, in particular intuitionism due to L.E.J. Brouwer, constructive recursive mathematics due to A.A. Markov, and Bishop’s constructive mathematics, is provided in this chapter. The constructive interpretation and formalization of logic is described. For constructive (intuitionistic) arithmetic, Kleene’s realizability interpretation is given; this provides an example of the possibility of a constructive mathematical practice, which diverges from classical mathematics. The crucial notion in intuitionistic analysis, choice sequence, is briefly described and some principles, which are valid for choice sequences, are discussed. The second half of the article deals with some aspects of proof theory, i.e. the study of formal proofs as combinatorial objects. Gentzen’s fundamental contributions are outlined: his introduction of the so-called Gentzen systems, which use sequents instead of formulas and his result on first-order arithmetic showing that (suitably formalized) transfinite induction up to the ordinal ε_0 cannot be proved in first-order arithmetic.

UNESCO – EOLSS
SAMPLE CHAPTERS

1. Introduction

1.1. Constructivism

Since the beginning of the twentieth century several positions w.r.t. the foundations of mathematics have been formulated which might be said to be versions of constructivism.

Typically, a constructivist view demands of mathematics some form of explicitness of the objects studied, they must be concretely representable, or explicitly definable, or capable of being viewed as mental constructions. We distinguish five variants of constructivism in this chapter: finitism, predicativism, intuitionism (INT), constructive recursive mathematics (CRM), and Bishop’s constructive mathematics (BCM). We will be brief about finitism and predicativism, and concentrate on the other three instead.

Finitism insists on concrete representability of the objects of mathematics and avoids the higher abstractions. Thus, particular functions from $\mathbb{N}$ to $\mathbb{N}$ are considered, but the notion of an arbitrary function from $\mathbb{N}$ to $\mathbb{N}$ is avoided, etc. This curtails the use of logic, in particular the use of quantifiers over infinite domains. Infinite domains are regarded as indefinitely extendable finite domains rather than as completed infinite totalities. Finitism is not only of interest as a version of constructivism, but also as a key ingredient in Hilbert’s original program: Hilbert wanted to establish consistency of formal mathematical theories by 'finitistic' means, since he regarded these as evidently justified and uncontroversial (see also below under 1.2).

Predicativism concentrates on the explicitness and non-circular character of definitions. As a rule, in the predicativist approach the natural numbers are taken for granted; but sets of natural numbers have to be explicitly defined, and in defining a mathematical entity A say, the definition should not refer to the totality of objects of which A is an element.

Intuitionism (INT). Intuitionism, as it is understood here, is due to the Dutch mathematician L.E.J. Brouwer (1881–1966). The basic tenets of intuitionism may be summarily described as follows.

1. Mathematics is not formal; the objects of mathematics are mental constructions in the mind of the (ideal) mathematician. Only the thought constructions of the (idealized) mathematician are exact.

2. Mathematics is independent of experience in the outside world, and mathematics is in principle also independent of language. Communication by language may serve to suggest similar thought constructions to others, but there is no guarantee that these other constructions are the same. (This is a solipsistic element in Brouwer's philosophy.)

3. Mathematics does not depend on logic; on the contrary, logic is part of mathematics.

The first item not only leads to the rejection of certain theorems of classical logic, but also opens a possibility for admitting deviant objects, the "forever incomplete" choice sequences. Just as for Constructive Recursive Mathematics (CRM), the mathematical theories of INT are not simply sub-theories of their classical counterparts, but may actually be incompatible with the corresponding classical theory.

Constructive Recursive Mathematics (CRM). A.A. Markov (1903–1979) formulated in 1948–49 the basic ideas of constructive recursive mathematics (CRM for short). They are the following:

1. Objects of constructive mathematics are constructive objects, concretely: words in various alphabets.

2. The abstraction of potential existence (potential realizability) is admissible but the abstraction of actual infinity is not allowed. Potential realizability means e.g., that we may regard addition as a well-defined operation for all natural numbers, since we know how to complete it for arbitrarily large numbers. This admissibility is taken to include acceptance of 'Markov's Principle': if it is impossible that an algorithmic computation does not terminate, it does in fact terminate. The rejection of actual infinity is tantamount to the rejection of classical logic.

UNESCO – EOLSS SAMPLE CHAPTERS

3. A precise notion of algorithm is taken as a basis (Markov chose for this his own notion of 'Markov-algorithm'). Since Markov-algorithms are encoded by words in suitable alphabets, they are objects of CRM; conversely, each word in some definite alphabet may be interpreted as a Markov algorithm.

4. Logically compound statements have to be interpreted so as to take the preceding points into account.

Markov's principle holds neither in INT nor in Bishop's Constructive Mathematics (BCM).

Bishop's Constructive Mathematics (BCM). Errett Bishop (1928–1983) formulated his version of constructive mathematics around 1967. There is a single "ideological" principle underlying BCM:

1. proofs of existential statements must provide a method of constructing the object satisfying the specifications,

   and three more pragmatic guiding rules for the development of BCM:

2. avoid concepts defined in a negative way;

3. avoid defining irrelevant concepts — that is to say, among the many possible classically equivalent, but constructively distinct definitions of a concept, choose the one or two which are mathematically fruitful ones, and disregard the others;

4. avoid pseudo-generality, that is to say, do not hesitate to introduce an extra assumption if it facilitates the theory and is satisfied by the examples one is interested in.

Starting from the principles outlined above, three distinct versions of mathematics have been developed, which differ notably in their respective theories of the continuum, as will be explained further on.

1.2. Proof Theory

Proof theory owes its origin to Hilbert's Program, i.e., the project of establishing freedom of contradiction for formally codified (substantial parts of) mathematics, using elementary, "evident" reasoning (finitistic reasoning). As shown by Gödel, in its original form this program was bound to fail. However, a modification of the program has been successful; one then asks to establish consistency using "evident" means of proof, possibly stronger than the system whose consistency is to be established.

Structural proof theory studies formal mathematical (logical) proofs as combinatorial structures; various styles of formalization are compared.

UNESCO – EOLSS SAMPLE CHAPTERS

Hilbert-Schütte style proof theory takes its starting point from Gentzen's consistency proof for arithmetic, and compares formal systems with respect to their proof-theoretic strength, by analyzing the structure of suitably devised deduction systems.

Interpretational proof theory compares formalisms via syntactic translations or interpretations. We shall encounter various examples below.

2. Intuitionistic Logic, I

Although Brouwer was positively averse to formalization of mathematics, he was nevertheless the first to formulate and establish some principles of intuitionistic logic. But Kolmogorov in 1925 and Heyting in 1930 demonstrated that intuitionistic logic could be studied as a formalism. Formalizations of intuitionistic logic need an informal interpretation to justify them as codifications of *intuitionistic* logic. Heyting (1930, 1934) and Kolmogorov (1932) each developed such an interpretation; their interpretations were later to be seen to be essentially equivalent. Heyting in particular built on some of Brouwer's early papers.

2.1. The BHK-interpretation

The need for a different logic in the setting of INT, BCM and CRM becomes clear by considering some informal examples.

The following is not acceptable as a constructive definition of a natural number:
$n = 2 \text{ if } R \text{ holds}, \quad n = 3 \text{ if } \neg R \text{ holds},$

where R stands for some mathematically unsolved problem, e.g., R = The Riemann hypothesis. This is not a constructive definition because we cannot identify n with one of the explicitly given natural numbers 0,1,2,3,4,…; for such an identification to be possible, we have to decide whether R or $\neg R$ holds, i.e., to decide the Riemann hypothesis. Note that the definition becomes acceptable as soon as problem R has been solved.

Example of a non-constructive proof: Consider the following statement: there exist irrational numbers a,b such that a^b is rational. This statement has a very simple proof: $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational. In the first case, take $a = b = \sqrt{2}$. In the second case, take $a = \sqrt{2}^{\sqrt{2}}, b = \sqrt{2}$. The proof is obviously non-constructive, since it does not permit us to compute a with any desired degree of accuracy. A constructive proof of the statement is possible, for example, by an appeal to a non-trivial theorem of Gelfond: if $a \notin \{0,1\}$, a algebraic, b irrational algebraic, then a^b is irrational, even transcendental.

INT, BCM and CRM have the same logical basis, called intuitionistic logic or constructive logic, and which is a subsystem of classical predicate logic. The standard informal interpretation of logical operators in intuitionistic logic is the so-called *proof-interpretation* or *Brouwer-Heyting-Kolmogorov interpretation* (BHK-*interpretation* for short). The formalization of intuitionistic logic started before this interpretation was

UNESCO – EOLSS SAMPLE CHAPTERS

actually formulated, but it is preferable to discuss the BHK-interpretation first since it facilitates the understanding of the more technical results.

We use capitals $A, B, C, \ldots$ for arbitrary formulas. Our logical operators are $\wedge, \vee, \rightarrow, \perp, \forall, \exists$. We treat $\neg A$ as an abbreviation of $A \rightarrow \perp$, and we use $\equiv$ denotes identity of strings and $:\equiv$ for definitions If $\mathcal{E}$ is a syntactic expression, we write $\mathcal{E}[x/t]$ for the result of substituting the term t for the free variable x in $\mathcal{E}$; it is tacitly assumed that t is free for x in $\mathcal{E}$, that is to say, no variable free in t becomes bound after substitution. We often use a more informal notation: if $\mathcal{E}(x)$ has been introduced in the discourse as an expression $\mathcal{E}$ with some free occurrences of the variable x, we write $\mathcal{E}(t)$ for $\mathcal{E}[x/t]$.

On the BHK-interpretation, the meaning of a statement A is given by explaining what constitutes a proof of A, and *proof of A* for logically compound A is explained in terms of what it means to give a proof of its constituents. Thus:

1. A proof of $A \wedge B$ is given as a pair of proofs $\langle p, q\rangle$, where p is a proof of A and q is a proof of B.

2. A proof of $A \vee B$ is of the form $\langle 0, p\rangle$, where p is a proof of A, or $\langle 1, q\rangle$, where q a proof of B.
3. A proof of $A \rightarrow B$ is a construction q which transforms any proof p of A into a proof $q(p)$ of B.

4. Absurdity $\perp$ ('the contradiction') has no proof; a proof of $\neg A$ is a construction which transforms any supposed proof of A into a proof of $\perp$.

To understand the meaning of the last chance for negation, note that this amounts to saying that *A* has *no* proof; and in this case every functional construction will do as a proof of $\neg A$.
In the quantifier clauses, we assume the individual variables to range over a domain D; the fact that $d \in D$ for some d is not supposed to need further proof. (This is sometimes expressed by calling D a *basic* domain; $\mathbb{N}$ is an example.)

5. A proof p of $\forall x A(x)$ is a construction transforming any $d \in D$ into a proof $p(d)$ of $A(d)$.

6. A proof p of $\exists x A(x)$ is a pair $\langle d, q\rangle$ with $d \in D$, q a proof of $A(d)$.

The concepts of *proof* and *construction* in these explanations are to be taken as primitive; "proof" is not to be identified with any notion of deduction in any formal system. Obviously, the constructions in the clauses for implication and the universal quantifier are (constructive) functions.

UNESCO – EOLSS
SAMPLE CHAPTERS

Let us write $\lambda x.t(x)$ for $t(x)$ as a function of x (so $(\lambda x.t(x))(d) = t(d)$). As an example of the BHK-interpretation, let us argue that $\neg\neg(A \vee \neg A)$ is valid on this interpretation.

(i) If u proves A, then $\langle 0, u\rangle$ proves $A \vee \neg A$.
(ii) If v proves $\neg(A \vee \neg A)$ and $\langle 0, u\rangle$ proves $A \vee \neg A$, then $v\langle 0, u\rangle$ proves $\perp$.
(iii) If v proves $\neg(A \vee \neg A)$, then $\lambda u.v\langle 0, u\rangle$ proves $\neg A$ (by (i) and (ii)).
(iv) If w proves $\neg A$, then $\langle 1, w\rangle$ proves $A \vee \neg A$, so $\langle 1, \lambda u.v\langle 0, u\rangle\rangle$ proves $A \vee \neg A$ by (iii).
(v) If v proves $\neg(A \vee \neg A)$, then $v\langle 1, \lambda u.v\langle 0, u\rangle\rangle$ proves $\perp$ by (iv).
(vi) $\lambda v.v\langle 1, \lambda u.v\langle 0, u\rangle\rangle$ proves $\neg\neg(A \vee \neg A)$ (by (v)).

-
-
-

TO ACCESS ALL THE **47 PAGES** OF THIS CHAPTER,
Visit: http://www.eolss.net/Eolss-sampleAllChapter.aspx

UNESCO – EOLSS SAMPLE CHAPTERS

Bibliography

E. Bishop and D. Bridges.(1985) *Constructive Analysis*. Springer-Verlag, Berlin. [Develops a substantial body of mathematical analysis within the framework of BCM.]

W. Buchholz, S. Feferman, W. Pohlers and W. Sieg (1981) *Iterated Inductive Definitions and Subsystems of Analysis: Recent Proof-Theoretical Studies*. Lecture Notes in Mathematics 897. Springer-Verlag, Berlin, Heidelberg, New York. [A monograph on subsystems of analysis, in particular those generated by various principles of generalized inductive definition.]

D. Bridges and F. Richman. (1987) *Varieties of Constructive Mathematics*. Cambridge University Press, Cambridge. [A concise introduction to the mathematical practice of BCM, INT and CRM.]

L. E. J. Brouwer. (1975) *Collected Works 1. Philosophy and Foundations of Mathematics*. North-Holland Publ. Co., Amsterdam, and American Elsevier Publ. Co., New York. [Contains all Brouwer's papers on philosophy and intuitionism.]

S. R. Buss, editor. (1998) *Handbook of Proof Theory*. Elsevier, Amsterdam. [The papers in this volume represent an up to date survey of the field.]

A. G. Dragalin. (1987) *Mathematical Intuitionism. Introduction to Proof Theory*. Translations of Mathematical Monographs, volume 67. American Mathematical Society, Providence Rh.I.. Translated from the Russian original, published by Nauka, Moscow 1979. [Deals with the metamathematics of systems based on intuitionistic logic.]

M. A. E. Dummett. (1977) *Elements of Intuitionism*. Clarendon Press, Oxford. 2nd ed. 2000. [Treats intuitionism from the authors philosophical point of view. Contains the most accessible exposition of the authors philosophy of intuitionistic logic.]

M. D. Fitting. (1969) *Intuitionistic Logic, Model Theory and Forcing*. North-Holland Publ. Co., Amsterdam. [An elegant treatment of completeness questions for intuitionistic logic w.r.t. Beth and Kripke semantics, and a treatment of forcing in set theory.]

G. Gentzen. (1969) *The Collected Papers of Gerhard Gentzen*. North-Holland Publ. Co., Amsterdam. English translation of Gentzen's papers, edited and introduced by M. E. Szabo. [Gentzen's classic papers.]

J.-Y. Girard. (1987) *Proof Theory and Logical Complexity, Volume 1*. Bibliopolis, Napoli. [A monograph on proof theory, especially of analysis, containing material not easily found elsewhere.]

D. Hilbert and P. Bernays. (1934) *Grundlagen der Mathematik, Bd. I*. Springer-Verlag, Berlin, Heidelberg, New York. 2nd edition 1968. [The first monograph on proof theory, still a valuable source for its detailed discussion of ideas, and careful exposition of basic techniques.]

D. Hilbert and P. Bernays. (1939) *Grundlagen der Mathematik, Bd. II*. Springer-Verlag, Berlin, Heidelberg, New York,. 2nd edition 1970. [See preceding item.]

J. Herbrand. (1971) *Écrits Logiques*. Presses Universitaires de France, Paris, 1968. Translated as *Logical Writings*, Harvard University Press, Cambridge, MA. [Herbrand's collected works, a historically important source.]

J. R. Hindley. (1997) *Basic Simple Type Theory*. Cambridge University Press, Cambridge, UK. [A clear exposition of the connections between type theory and intuitionistic prepositional logic.].

S. C. Kleene. (1952) *Introduction to Metamathematics*. North-Holland Publ. Co., Amsterdam. [A classic textbook still to be recommended for its reliability and careful treatment of many important topics concerning intuitionistic logic.]

B. A. Kushner. (1984) *Lectures on Constructive Mathematical Analysis*. Translations of Mathematical Monographs, volume 60. American Mathematical Society, Providence Rh.I.. Translated from the Russian original, published by Nauka, Moscow 1973. [An elegant treatment of a substantial part of mathematical analysis in CRM.]

S. C. Kleene and R. E. Vesley. (1965) *The Foundations of Intuitionistic Mathematics*. North-Holland Publ. Co. [A detailed formalization and metamathematical investigation of intuitionistic analysis based on choice sequences. Especially valuable for tits careful discussion of bar induction.].

G. E. Mints. (1992) *Selected Papers in Proof Theory*. North-Holland Publ. Co., Amsterdam; Bibliopolis, Napoli. [Contains material on the connections between intuitionistic logic and category theory, and continuous cut elimination for infinitary derivations.]

G. E. Mints. (1992) *Selected Papers in Proof Theory*. Bibliopolis, Napoli and North-Holland, Amsterdam.

W. Pohlers. (1989) *Proof Theory*. *An Introduction*. Springer-Verlag, Berlin. [A very elegant introduction to the proof theory of subsystems of analysis.]

D. Prawitz. (1965) *Natural Deduction. A Proof-Theoretical Study*. Almquist and Wiksell, Stockholm.

K. Schütte. (1968) *Vollständige Systeme modaler and intuitionistischer Logik*. Springer-Verlag, Berlin, Heidelberg, New York. [Covers to some extent the same ground as Fitting's monograph, but also deals with the connections with modal logic.]

K. Schütte. (1977) *Proof Theory*. Springer-Verlag, Berlin, Heidelberg, New York. [Deals with Gödel's Dialectica interpretation and the ordinals of predicative and Π^1_1-analysis.]

G. Takeuti. (1987) *Proof Theory*. 2nd edition. North-Holland Publ. Co., Amsterdam. [Hilbert-Schutte proof theory of arithmetic and analysis by means of the author's 'ordinal diagrams'; cut elimination for simple type theory and determinate logic.]

A. S. Troelstra. Editor (1973) *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis.* Lecture Notes in Mathematics 344. Springer-Verlag, Berlin, Heidelberg, New York. [Surveys much of what was known of the metamathematics of intuitionistic formal systems at the time and contains results not found in more recent monographs.]

A. S. Troelstra and H. Schwichtenberg. (2000) *Basic Proof Theory*. 2nd revised edition., Cambridge University Press, Cambridge UK. [Detailed treatment of structural proof theory for intuitionistic and classical predicate logic, with an introduction tot he proof theory of first-order arithmetic.]

A. S. Troelstra and D. van Dalen. (1988) *Constructivism in Mathematics*. Studies in Logic and the Foundations of Mathematics. Vol.I and II, North-Holland Publ. Co., Amsterdam. [A thorough

UNESCO – EOLSS
SAMPLE CHAPTERS

introduction to BCM, INT and CRM, both mathematical practice as well as the metamathematics. Not much structural proof theory, but a long discussion of completeness questions and semantics.]

Biographical Sketch

Anne S. Troelstra is Emeritus Professor of Pure Mathematics and Foundations of Mathematics, at the Institute of Logic, Language and Information (ILLC) of the University of Amsterdam. He has worked primarily in Proof Theory and Constructive Mathematics, and he has written with Dirk van Dalen one of the classic textbooks in this area. He has been a member of the Royal Dutch Academy of Sciences since 1976, and in 1996 he was awarded the F.L. Bauer-prize of the "Bund der Freunde der Technischen Universita"t Mu"nchen" for internationally outstanding contributions to Computer Science.

UNESCO – EOLSS
SAMPLE CHAPTERS