LOGICAL FOUNDATIONS OF COMPLEXITY THEORY

Jan Krajíček, Charles U.

Begriffsschrift, *a formula language, modeled upon that of arithmetic, for pure thought*

GOTTLOB FREGE

(1879)

This is the first work that Frege wrote in the field of logic, and, although a mere booklet of eighty-eight pages, it is perhaps the most important single work ever written in logic. Its fundamental contributions, among lesser points, are the truth-functional propositional calculus, written with special symbols, "for pure thought", that is, free from rhetorical embellishments, "modeled upon that of arithmetic", that is, constructed from specific symbols that are manipulated according to definite rules. The last phrase does not mean that logic mimics arithmetic, and the analogies, uncovered

From Frege to Gödel

A Source Book in Mathematical Logic, 1879-1931

Frege, Peano, Dedekind, Burali-Forti, Cantor, Padoa, Russell, Hilbert, Zermelo, Richard, König, Whitehead and Russell, Wiener, Löwenheim, Skolem, Post, Fraenkel, Brouwer, von Neumann, Schönfinkel, Kolmogorov, Finsler, Weyl, Bernays, Ackermann, Herbrand, Gödel

Edited by Jean van Heijenoort

Hilbert's foundational program

→ consistency problem

→ Entscheidungsproblem

→ set th.: axiom & key principles

Entscheid.....

⇕

Algorithm to decide logical validity.

⇒ • Turing, Church '36

↓

T. machines, Halting problem

↓

negative solution of Hilbert's 10th probl.

consistency

⇝ formalize math and prove its consistency by finitary means

⇒ Gödel '31 : impossible

Gentzen '36 : "almost" possible

set theory

→ Zermelo , Fraenkel, ...

→ axiomatic system

→ Cantor's continuum problem , AC, ...

↳ for $X \subseteq \mathbb{R}$: either $\exists f : \mathbb{N} \twoheadrightarrow X$

or $\exists g : X \twoheadrightarrow \mathbb{R}$

Are these foundational problems relevant to CT?

[proof complexity]

YES, if we take "feasibility" into account

Entscheid....

$\Updownarrow$

$\exists$ $\underbrace{\text{Alg. } A}$ for FO logical validity ?

$\downarrow$ $\downarrow$

feasible A ... propositional ..... ?

$\Updownarrow$

$P =_? NP$

consistency

Can the consistency of Math w.r.t. proofs of size n be proved by a proof of size ~n?

$\Longleftrightarrow$ $NP \overset{?}{=} coNP$

or

$\Longleftrightarrow$ $\exists$? optimal prop. proo system

Consistency again

(A) Are the fundamental conjectures of CT consistent with CT?

(B) Where can we prove the soundness of an algorithm we define and does it matter?

Logic th's of Math:

key principles

↳ INDUCTION

↳ SET EXISTENCE

- Set th
- ⋮
- Π^1_1-CA — infinitary algebra or combinatorics
- Σ^1_1-AC — existence thms in analysis
- Peano Arith. ≈ finite set th
- WKL : completeness argument
- RCA : recursion th / alg's
- $I\Delta_0 + Exp$ ← combinatorics
- ⇐ CT : bounded arithmetic

Theories for CT → bounded f'las : Smullyan, Bennett 60s

↳ principal ex's

Parikh '73

Cook '75

Paris – Wilkie '70s + early 80s

Buss '85

⋮

INDuction :

$$\left[A(0) \wedge \forall y < x\,(A(y) \to A(y+1))\right] \to A(x)$$

2 key ax's:

language: f. symbol f_A for each p-time alg A

basic ax's: defining properties of As

IND: $\hookrightarrow$ for open flas $\rightsquigarrow$ theory P-IND ($\approx PV$, Cook '75)

$\hookrightarrow$ for Σ_1-flas $\rightsquigarrow$ NP-IND ($\approx T^1_2(PV)$, Buss '85)

$\exists y(|y| \le |t(x)|)\ldots$

Ex formalizations

$$P=NP \iff \text{for some } f_A:$$
$$Sat(x,y) \to Sat(x, f_A(x))$$

$$NP \subseteq P/poly \iff \forall z\ \exists C\ (|C| \le |z|^k)$$
$$\forall x,y\ (|x|, |y| \le |z|)$$
$$Sat(x,y) \to Sat(x, C(x))$$

[$P \neq NP$ can be also formalized by $\forall$-sentences.]

Ex's of formalizations:

- NP-completeness of SAT
- PCP thm
- Goldreich-Levin thm
- OWF → PRNG constr.
- derandomization via NW gen's
- natural proofs
- sorting networks
- expander constructions
- circuit & proof lower bounds

dWPHP : $f_A : a = \{0,1\}^n \not\twoheadrightarrow a^2 = \{0,1\}^{2n}$

[Used to formalize probabilistic concepts ....]

Ex. $\underline{tt_{s,k}}$: $\left. \begin{array}{c} C(x_1, \dots, x_k) \\ |C| \leq s \end{array} \right\} \longrightarrow \underset{\text{truth-table}}{tt(C) \in \{0,1\}^{2^k}}$

Then: $\exists b \in \{0,1\}^{2^k} \setminus Rng(tt_{s,k})$

$\Updownarrow$

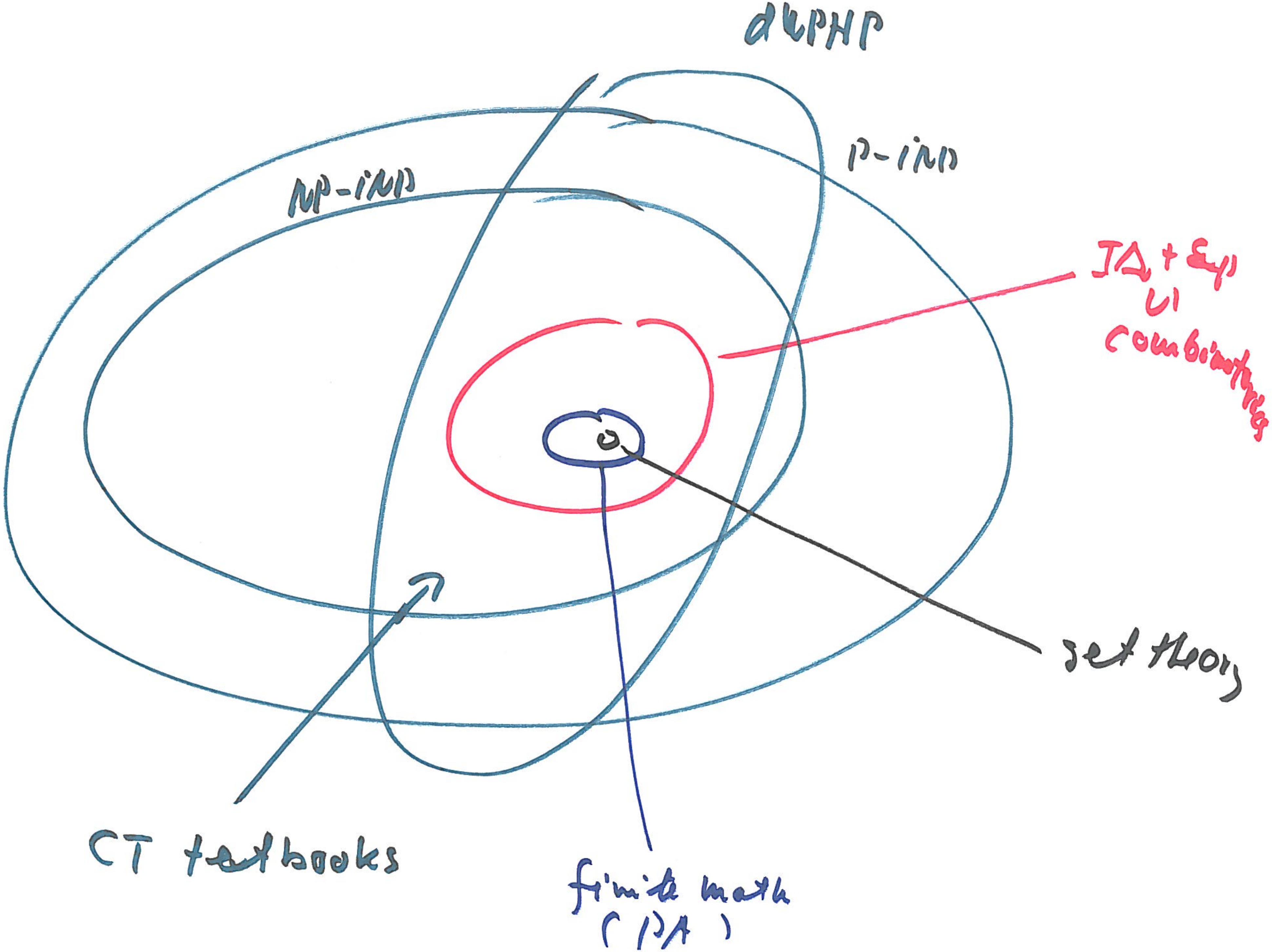
b is a Bool. f. requiring circuits of $\underline{\text{size} > s}$

consistency revisited (A)

(A) Show that standard conjectures are true (individually, at least) in some model of P-IND, LL IND, rdWPHP, ...

$\Updownarrow$

Interpretation: the conj's are not refutable in CT. This counts towards the truth of the conjectures.


dWPHP
P-IND
NP-IND
IΔ₀ + Exp
∪|
combinatorics
set theory
CT textbooks
finite math
(PA)

Ex's of unconditional consistency results:

- $\exists n_0$ "ER is quasi-poly bounded for $|\tau| \geq n_0$" [K.-Pudlák]
- $NP \subsetneq Size(n^k)$
- $\Delta^p_2 \subsetneq Size(n^k)$ $\longleftarrow$ with NP-IND
- $P \subsetneq Size(n^k)$ [K.-Oliveira]

with PV (= P-IND)

[Cook-K.]

consistency revisited (B)

(B) Consistency of $P \neq NP$: want a model in which all universal statements

$$\mathrm{Sound}_{f_A}: \quad \mathrm{Sat}(x,y) \longrightarrow \mathrm{Sat}(x, f_A(x))$$

fail.

[No $\exists$-quantifier to analyze.]

Does it matter where we prove Sound_{f_A}?

Ex. situation: f_A exists and Sound_{f_A} is true

but $\text{P-IND} \nvdash \mathrm{Sound}_{f_A}$

while $\text{NP-IND} \vdash \mathrm{Sound}_{f_A}$

Can one still maintain that A is feasible?

FEASIBLY CONSTRUCTIVE PROOFS AND THE PROPOSITIONAL CALCULUS

Preliminary Version

Stephen A. Cook
University of Toronto

1. Introduction

The motivation for this work comes from two general sources. The first source is the basic open question in complexity theory of whether *P* equals *NP* (see [1] and [2]). Our approach is to try to show they are not equal, by trying to show that the set of tautologies is not in *NP* (of course its complement is in *NP*). This is equivalent to showing that no proof system (in the general sense defined in [3]) for the tautologies is "super" in the sense that there is a short proof for every tautology. Extended resolution is an example of a powerful proof system for tautologies that can simulate most standard proof systems (see [3]). The Main Theorem (5.5) in this paper describes the power of extended resolution in a way that may provide a handle for showing it is not super.

The second motivation comes from constructive mathematics. A constructive proof of, say, a statement $\forall xA$ must provide an effective means of finding a proof of A for each value of x, but nothing is said about how long this proof is as a function of x. If the function is exponential or super exponential, then for short values of x the length of the proof of the instance of A may exceed the number of electrons in the universe. Thus one can question the sense in which our original "constructive" proof provides a method of verifying $\forall xA$ for such values of x. Parikh [4] makes similar points, and goes on to suggest an "anthropomorphic" formal system for number theory in which induction can only be applied to formulas with bounded quantifiers. But even a quantifier bounded by n may require time exponential in the length of (the decimal notation for) n to check all possible values of the quantified variable (unless $P = NP$), so Parikh's system is apparently still not feasibly constructive.

In section 2, I introduce the system PV for number theory, and it is this system which I suggest properly formalizes the notion of a feasibly constructive proof. The formulas in PV are equations $t = u$, (for example, $x\cdot(y+z) = x\cdot y + x\cdot z$) where t and u are terms built from variables, constants, and function symbols ranging over $\mathcal{L}$, the class of functions computable in time bounded by a polynomial in the length of their arguments. The system PV is the analog for $\mathcal{L}$ of the quantifier-free theory of primitive recursive arithmetic developed by Skolem [5] and formalized by others (see [6]). A result necessary for the construction of the system is Cobham's theorem [7] which characterizes $\mathcal{L}$ as the least class of functions containing certain initial functions, and closed under substitution and limited recursion on notation (see section 2). Thus all the functions in $\mathcal{L}$ (except the initial functions) can be introduced by a sequence of defining equations. The axioms of PV are these defining equations, and the rules of PV are the usual rules for equality, together with "induction on notation".

All proofs in PV are feasibly constructive in the following sense. Suppose an identity, say $f(x) = g(x)$, has a proof Π in PV. Then there is a polynomial $p_\Pi(n)$ such that Π provides a uniform method of verifying within $p_\Pi(|x_0|)$ steps that a given natural number x_0 satisfies $f(x_0) = g(x_0)$. If such a uniform method exists, I will say the equation is <u>polynomially verifiable</u> (or p-verifiable).

The reader's first reaction might be that if both f ang g are in $\mathcal{L}$, then there is always a polynomial p(n) so that the time required to evaluate them at x_0 is bounded by $p(|x_0|)$, and if $f(x) = g(x)$ is a true identity, then it should be p-verifiable. The point is that the verification method must be uniform, in the sense that one can see (by the proof Π) that the verification will always succeed. Not all true identities are provable, so not all are p-verifiable.

There is a similar situation in constructive (or intuitionistic) number theory. The Kleene-Nelson theorem ([8], p. 504) states that if a formula $\forall xA$ has a

$$\underbrace{A(z) \text{ open}\ ,\ 1^{(n)}}$$

$\downarrow$ p-time

prop. f'la $\|A\|^n(p_1, \dots, p_n)$ s.t.

(i) $a \in \{0,1\}^n$: $A(a)$ true $\iff \|A\|^n(a) \in TAUT$

(ii) $p\text{-}IND \vdash \forall z A(z)$

$\implies$ $\|A\|^n$ have p-size ER-proofs

[Cook '75]

Proof Complexity fact:

Assume $P \geq ER$ proves all $\|Sound_{f_A}\|^n, n \geq 1$, shortly for some alg A then P proves all tautologies shortly.

Hence: a super-poly l. bound for ER-proofs of any sequence of tautologies.

$\Downarrow$

$P \neq NP$ is consistent with PV

[~ logical $P \neq NP$]

function classes

p-time f's / PLS

$\exists_1$:

compl. class

P / NP

theory

P-ind / NP-ind

$\forall_1$: prop. proof systems

ER / G_1

A proof complexity fact:

Cook's simulation of PV by ER can be extended:

theory T $\longrightarrow$ pps P_T

$\uparrow$

any consistent
r.e. theory $\supseteq$ PV
(e.g. L_{PV} - consequences of ZFC)

Further facts:

- $T \vdash Con_{P_T}$, so $P_T \vdash_{\text{shortly}}$ "$\| Con_{P_T} \|^n$"

  [i.e. no analogy to Gödel's 2nd thm]

- $T \vdash Con_Q \Rightarrow Q \leq_p P$ [simulation]

  $\Uparrow$

  $T \vdash$ lower bound for Q

  [i.e. l.bounds $\Rightarrow$ simulation]


PERSPECTIVES IN LOGIC
Stephen Cook
Phuong Nguyen
LOGICAL FOUNDATIONS
OF PROOF COMPLEXITY
ASL
CAMBRIDGE

Proof complexity is a rich subject drawing on methods from logic, combinatorics, algebra and computer science. This self-contained book presents the basic concepts, classical results, current state of the art and possible future directions in the field. It stresses a view of proof complexity as a whole entity rather than a collection of various topics held together loosely by a few notions, and it favors more generalizable statements.

Lower bounds for lengths of proofs, often regarded as the key issue in proof complexity, are of course covered in detail. However, upper bounds are not neglected: this book also explores the relations between bounded arithmetic theories and proof systems and how they can be used to prove upper bounds on lengths of proofs and simulations among proof systems. It goes on to discuss topics that transcend specific proof systems, allowing for deeper understanding of the fundamental problems of the subject.

Jan Krajíček is Professor of Mathematical Logic in the Faculty of Mathematics and Physics at Charles University, Prague. He is a member of the Academia Europaea and of the Learned Society of the Czech Republic. He has been an invited speaker at the European Congress of Mathematicians and at the International Congresses of Logic, Methodology and Philosophy of Science.

CAMBRIDGE
UNIVERSITY PRESS
www.cambridge.org

ISBN 978-1-108-41684-9
9 781108 416849

9781108416849 KRAJÍCEK – PROOF COMPLEXITY PPC C M Y K

170

Krajíček

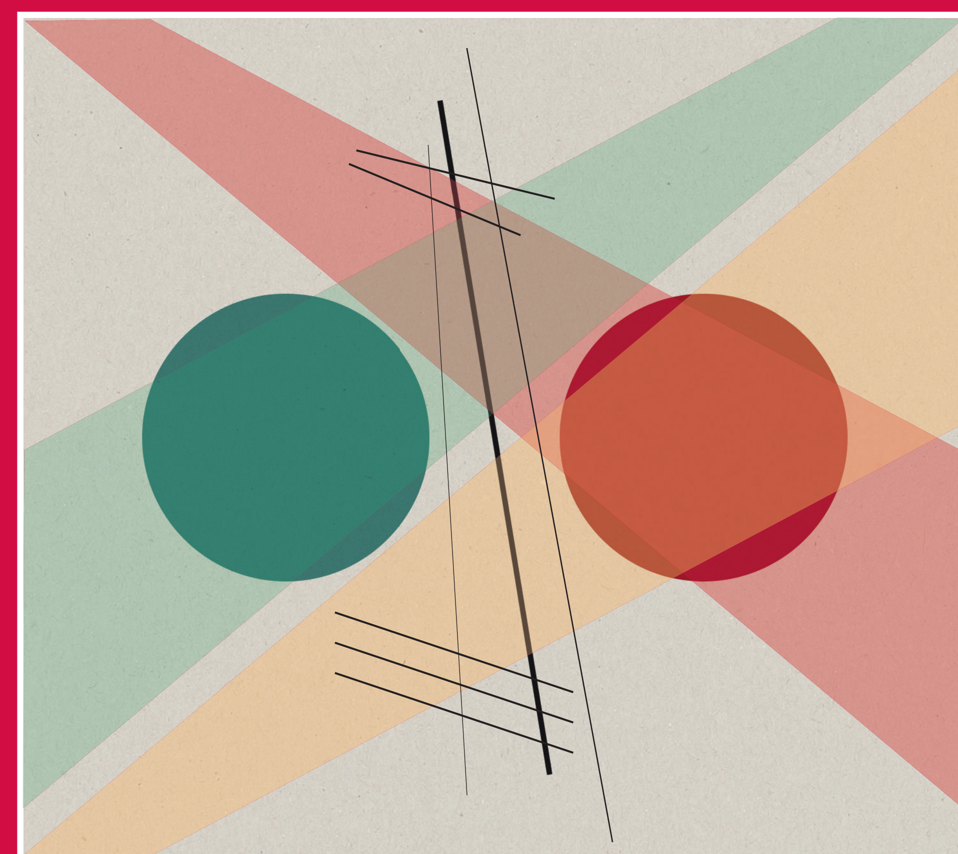
PROOF COMPLEXITY

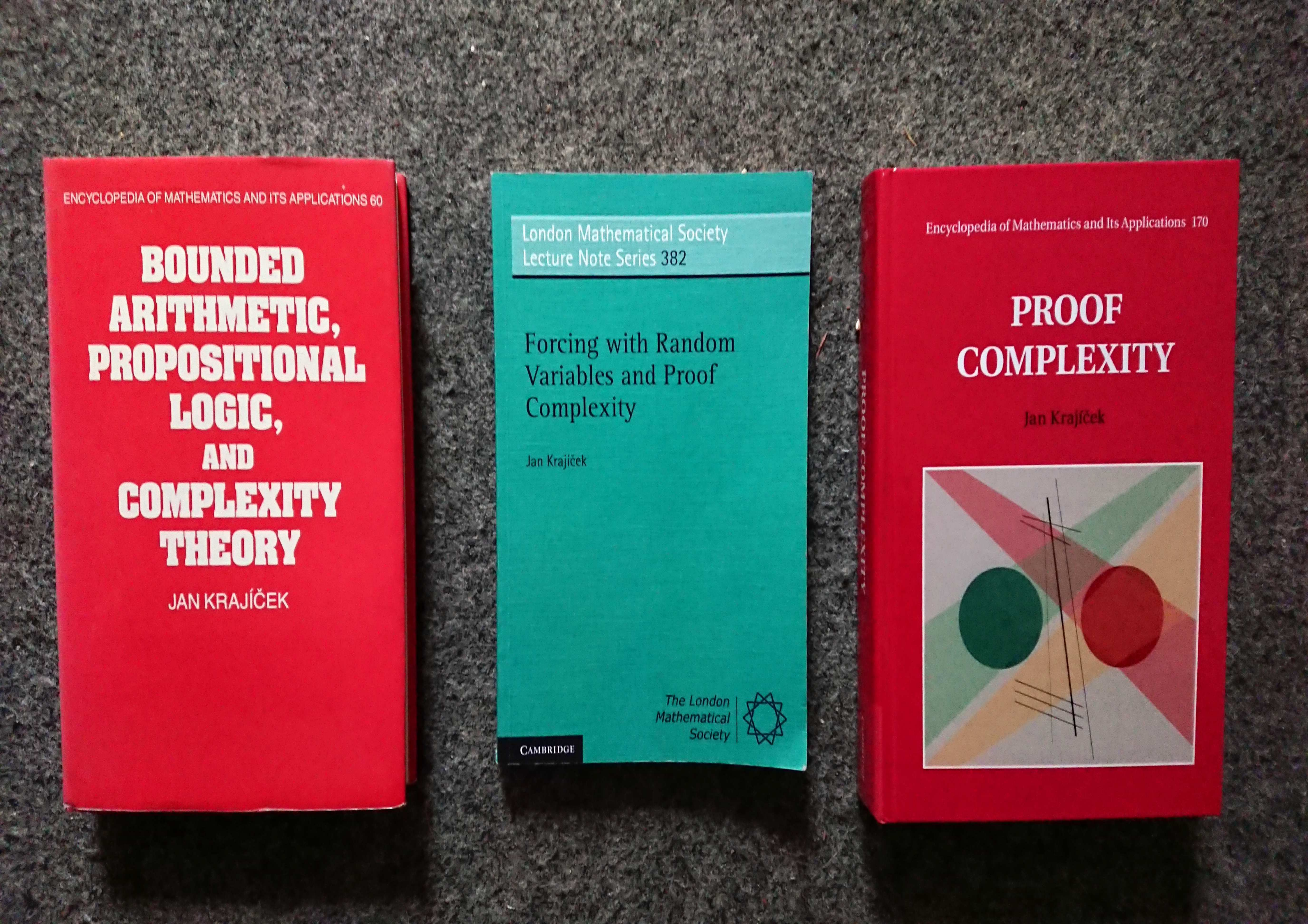
CAMBRIDGE

Encyclopedia of Mathematics and Its Applications 170

PROOF COMPLEXITY

Jan Krajíček




ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS 60
BOUNDED ARITHMETIC, PROPOSITIONAL LOGIC, AND COMPLEXITY THEORY
JAN KRAJÍČEK
London Mathematical Society Lecture Note Series 382
Forcing with Random Variables and Proof Complexity
Jan Krajíček
The London Mathematical Society
CAMBRIDGE
Encyclopedia of Mathematics and Its Applications 170
PROOF COMPLEXITY
Jan Krajíček
PROOF COMPLEXITY