中国科学院软件研究所学术年会 2023 暨计算机科学国家重点实验室开放周 学术论文

Randomness below complete theories of arithmetic

George Barmpalias - State Key Lab of Computer Science, Inst. of Software, Chinese Acad. Science, Beijing

Wei Wang - Inst. of Logic & Cognition and Dept. Philosophy, Sun Yat-Sen University, Guangzhou

Information and Computation 290 (2023) - NSFC 11750110425 - barmpalias@ios.ac.cn

Formal arithmetic (Peano Arithmetic)

Based on Peano's axioms and their variations

Axioms for PA

P1 $\forall x(sx \neq 0)$

P2 $\forall x \forall y(sx = sy \supset x = y)$ — s is 1-1 function

P3 $\forall x(x + 0 = x)$

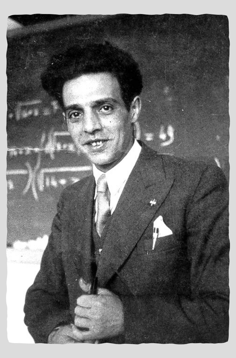
P4 $\forall x \forall y(x + sy = s(x + y))$ — (P3, P4) define $+$

P5 $\forall x(x \cdot 0 = 0)$

P6 $\forall x \forall y(x \cdot sy = (x \cdot y) + x)$ — (P5, P6) define $\cdot$

Induction Scheme: Let $Ind(A(x))$ be the sentence

$$\forall y_1 \cdots \forall y_k[(A(0) \land \forall x(A(x) \supset A(sx))) \supset \forall x A(x)]$$



Complexity of True Arithmetic

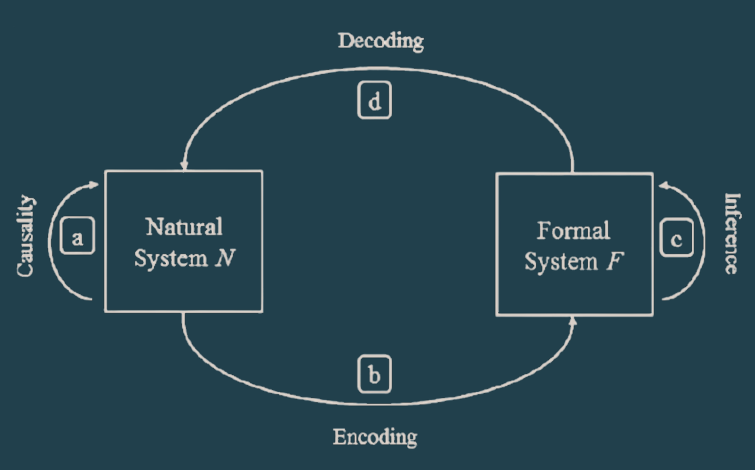
The computational complexity of the true sentences of arithmetic is overwhelming: it is as hard as infinitely many iterations of the halting problem.

However many complete extensions of arithmetic, though incomputable, are much easier to compute than many known problems, such as the halting problem.

Language, Coding, Computation

Theories of arithmetic can be written in binary, via coding of formulas into integers.

Then proofs can be viewed as computations.



Randomization in Arithmetic

Completions of arithmetic can be obtained probabilistically

But the probability of a successful outcome is as small as it can be

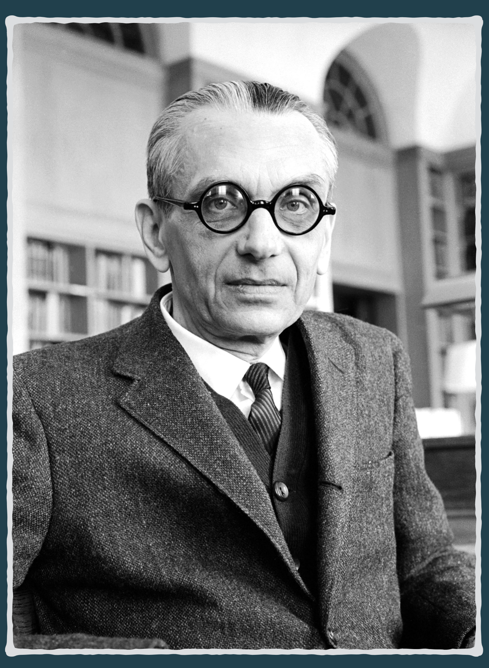
The same is true for completions of finite segments of arithmetic

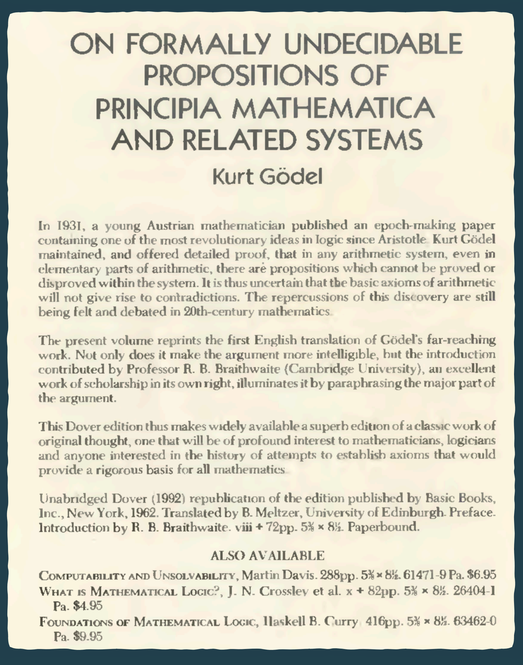
Random binaries do not encode complete theories of arithmetic (unless they compute the halting problem)

Complete theories of arithmetic are deep in the sense of Bennett: it is hard to obtain them probabilistically.

Incompleteness in arithmetic

Discovered by Gödel: there is no computable binary predicate consistently evaluating the truth of each arithmetical sentence.





ON FORMALLY UNDECIDABLE PROPOSITIONS OF PRINCIPIA MATHEMATICA AND RELATED SYSTEMS

Kurt Gödel

In 1931, a young Austrian mathematician published an epoch-making paper containing one of the most revolutionary ideas in logic since Aristotle. Kurt Gödel maintained, and offered detailed proof, that in any arithmetic system, even in elementary parts of arithmetic, there are propositions which cannot be proved or disproved within the system. It is thus uncertain that the basic axioms of arithmetic will not give rise to contradictions. The repercussions of this discovery are still being felt and debated in 20th-century mathematics.

The present volume reprints the first English translation of Gödel's far-reaching work. Not only does it make the argument more intelligible, but the introduction contributed by Professor R. B. Braithwaite (Cambridge University), an excellent work of scholarship in its own right, illuminates it by paraphrasing the major part of the argument.

This Dover edition thus makes widely available a superb edition of a classic work of original thought, one that will be of profound interest to mathematicians, logicians and anyone interested in the history of attempts to establish axioms that would provide a rigorous basis for all mathematics.

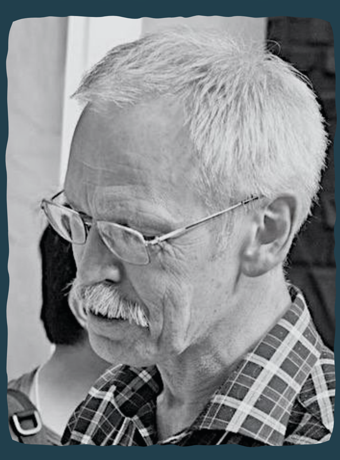
Unabridged Dover (1992) republication of the edition published by Basic Books, Inc., New York, 1962. Translated by B. Meltzer, University of Edinburgh. Preface. Introduction by R. B. Braithwaite. viii + 72pp. 5⅜ × 8½. Paperbound.

ALSO AVAILABLE

COMPUTABILITY AND UNSOLVABILITY, Martin Davis. 288pp. 5⅜ × 8½. 61471-9 Pa. $6.95

WHAT IS MATHEMATICAL LOGIC?, J. N. Crossley et al. x + 82pp. 5⅜ × 8½. 26404-1 Pa. $4.95

FOUNDATIONS OF MATHEMATICAL LOGIC, Haskell B. Curry. 416pp. 5⅜ × 8½. 63462-0 Pa. $9.95



Kucera pioneered the study of interactions between randomness and extensions of formal arithmetic

Stephan & Levin: weakness of randomization for completing arithmetic and binary predicates

Barmpalias, Lewis-Pye, Ng: complete theories are computable from two random bit-sequences

This is all that was known about computing complete theories of arithmetic with the use of random binaries...

True but unprovable statements

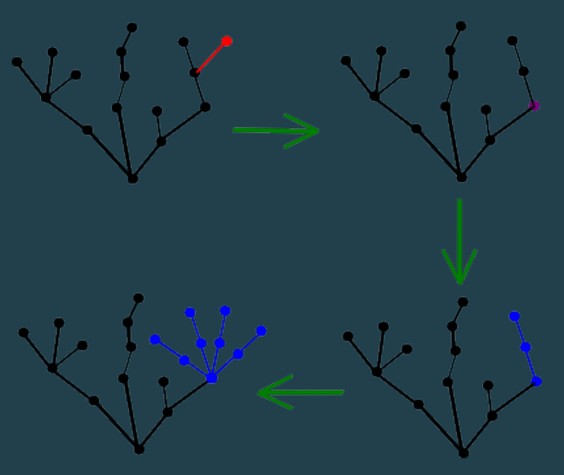
(a) Kruskal's theorem: the finite trees over a well-quasi-order is well-quasi-ordered under homeomorphic embedding.

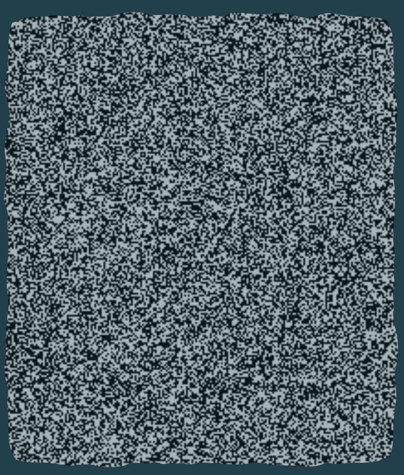
(b) Ramsey: there are monochromatic cliques in any coloring of sufficiently large complete graphs.

(c) Graph minor: the undirected graphs, partially ordered by the graph minor relationship, form a well-quasi-ordering

Research problem

Given a complete theory of arithmetic and any random binary that it computes, is there another random binary that computes the theory with the help of the first one?





Complete extensions of Arithmetic

There are arithmetical sentences whose validity cannot be decided from the axioms. A complete extension is obtained by adding such sentences (or their negation) to the theory, while maintaining consistency.

Extensions of arithmetic may not be consistent with each other: some may include a certain undecidable sentence, while others may include its negation.

Outcome and Methodology

- Coding deep (Bennett's logical depth) information into unstructured (random) binary sequences
- Random coding technology was not up to this task
- Randomizing the method of Kucera, we obtained the required coding method to give a positive answer.