The Early Days of Interactive Proofs

Lance Fortnow
Illinois Institute of Technology
The Death of Proof

Computers are transforming the way mathematicians discover, prove and communicate ideas, but is there a place for absolute certainty in this brave new world?

By John Horgan
A Model-Theoretic Analysis of Knowledge: Preliminary Report

Ronald Fagin
Joseph Y. Halpern
Moshe Y. Vardi

IBM Research Laboratory
San Jose, CA 95193
THE KNOWLEDGE COMPLEXITY OF INTERACTIVE PROOF SYSTEMS*

SHAFI GOLDWASSER†, SILVIO MICALI†, AND CHARLES RACKOFF‡

Abstract. Usually, a proof of a theorem contains more knowledge than the mere fact that the theorem is true. For instance, to prove that a graph is Hamiltonian it suffices to exhibit a Hamiltonian tour in it; however, this seems to contain more knowledge than the single bit Hamiltonian/non-Hamiltonian.

In this paper a computational complexity theory of the “knowledge” contained in a proof is developed. Zero-knowledge proofs are defined as those proofs that convey no additional knowledge other than the correctness of the proposition in question. Examples of zero-knowledge proof systems are given for the languages of quadratic residuosity and quadratic nonresiduosity. These are the first examples of zero-knowledge proofs for languages not known to be efficiently recognizable.

Key words. cryptography, zero knowledge, interactive proofs, quadratic residues

AMS(MOS) subject classifications. 68Q15, 94A60
Interactive Proofs

All Powerful

Computationally Limited
Arthur–Merlin Games: A Randomized Proof System, and a Hierarchy of Complexity Classes

László Babai

Eötvös University, Budapest, Hungary and
University of Chicago, Chicago Illinois

AND

Shlomo Moran

Technion, Haifa, Israel

Received June 24, 1986; revised August 3, 1987
1986
Interactive Proofs

All Powerful

Computationally Limited
Goldwasser-Sipser
Public vs Private Coins

All Powerful

Computationally Limited
How to Prove All NP Statements in Zero-Knowledge
and
a Methodology of Cryptographic Protocol Design

(Extended Abstract)

Oded Goldreich
Dept. of Computer Sc.
Technion
Haifa, Israel

Silvio Micali
Lab. for Computer Sc.
MIT
Cambridge, MA 02139

Avi Wigderson
Inst. of Math. and CS
Hebrew University
Jerusalem, Israel
The Complexity of Perfect Zero-Knowledge

(extended abstract)

Lance Fortnow*
MIT Math Dept.†
Cambridge, MA 02139
1988
Multi-Prover Interactive Proofs:
How to Remove Intractability Assumptions

Michael Ben-Or*  
Hebrew University

Shafi Goldwasser†
MIT

Joe Kilian‡
MIT

Avi Wigderson§
Hebrew University
Interactive Proofs

All Powerful

Computationally Limited
Multiple Provers
On the Power of Multi-Prover Interactive Protocols

Lance Fortnow*
John Rompel†
Michael Sipser‡

Laboratory for Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139
Multiple Provers
A PARALLEL REPETITION THEOREM

RAN RAZ

Abstract. We show that a parallel repetition of any two-prover one-round proof system (MIP(2,1)) decreases the probability of error at an exponential rate. No constructive bound was previously known. The constant in the exponent (in our analysis) depends only on the original probability of error and on the total number of possible answers of the two provers. The dependency on the total number of possible answers is logarithmic, which was recently proved to be almost the best possible [U. Feige and O. Verbitsky, Proc. 11th Annual IEEE Conference on Computational Complexity, IEEE Computer Society Press, Los Alamitos, CA, 1996, pp. 70-76].
1989
\[
\begin{array}{cccc}
x_{11} & x_{12} & \cdots & x_{1n} \\
x_{21} & x_{22} & \cdots & x_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
x_{n1} & x_{n2} & \cdots & x_{nn} \\
\end{array}
\]

\[
Det(X) = \sum_{\sigma} (-1)^{\sigma} x_{1\sigma(1)}x_{2\sigma(2)}\cdots x_{n\sigma(n)}
\]

\[
Perm(X) = \sum_{\sigma} x_{1\sigma(1)}x_{2\sigma(2)}\cdots x_{n\sigma(n)}
\]
Algebraic Methods for Interactive Proof Systems

Carsten Lund*
Lance Fortnow†
Howard Karloff‡
University of Chicago

Noam Nisan§
Hebrew University
IP=PSPACE

Adi Shamir

Applied Mathematics Department
The Weizmann Institute of Science
Rehovot, Israel
Non-Deterministic Exponential Time has Two-Prover Interactive Protocols

László Babai\textsuperscript{*}\textdagger  Lance Fortnow\textsuperscript{†}  Carsten Lund\textsuperscript{§}
Interactive Proofs and the Hardness of Approximating Cliques

URIEL FEIGE
The Weizmann Institute, Rehovot, Israel

SHAFI GOLDWASSER
Massachusetts Institute of Technology, Cambridge, Massachusetts

LASZLO LOVÁSZ
Yale University, New Haven, Connecticut

SHMUEL SAFRA
Tel-Aviv University, Tel-Aviv, Israel

AND

MARIO SZEGEDY
AT&T Bell Laboratories, Murray Hill, New Jersey
Proof Verification and the Hardness of Approximation Problems

SANJEEV ARORA
Princeton University, Princeton, New Jersey

CARSTEN LUND
AT&T Bell Laboratories, Murray Hill, New Jersey

RAJEEV MOTWANI
Stanford University, Stanford, California

MADHU SUDAN
Massachusetts Institute of Technology, Cambridge, Massachusetts

AND

MARIO SZEGEDY
AT&T Bell Laboratories, Murray Hill, New Jersey
And More...

• Program Checking
  • Babai-Fortnow-Levin-Szegedy 1991

• Unique Games
  • Subhash Khot 2002

• Quantum Proof Systems
  • Anand Natarajan and John Wright 2019
The Death of Proof

Computers are transforming the way mathematicians discover, prove and communicate ideas, but is there a place for absolute certainty in this brave new world?

By John Horgan