# The value of errors in proofs

Avi Wigderson
Institute for Advanced Study

# Plan

## Proofs and computations

## The value of errors in computations

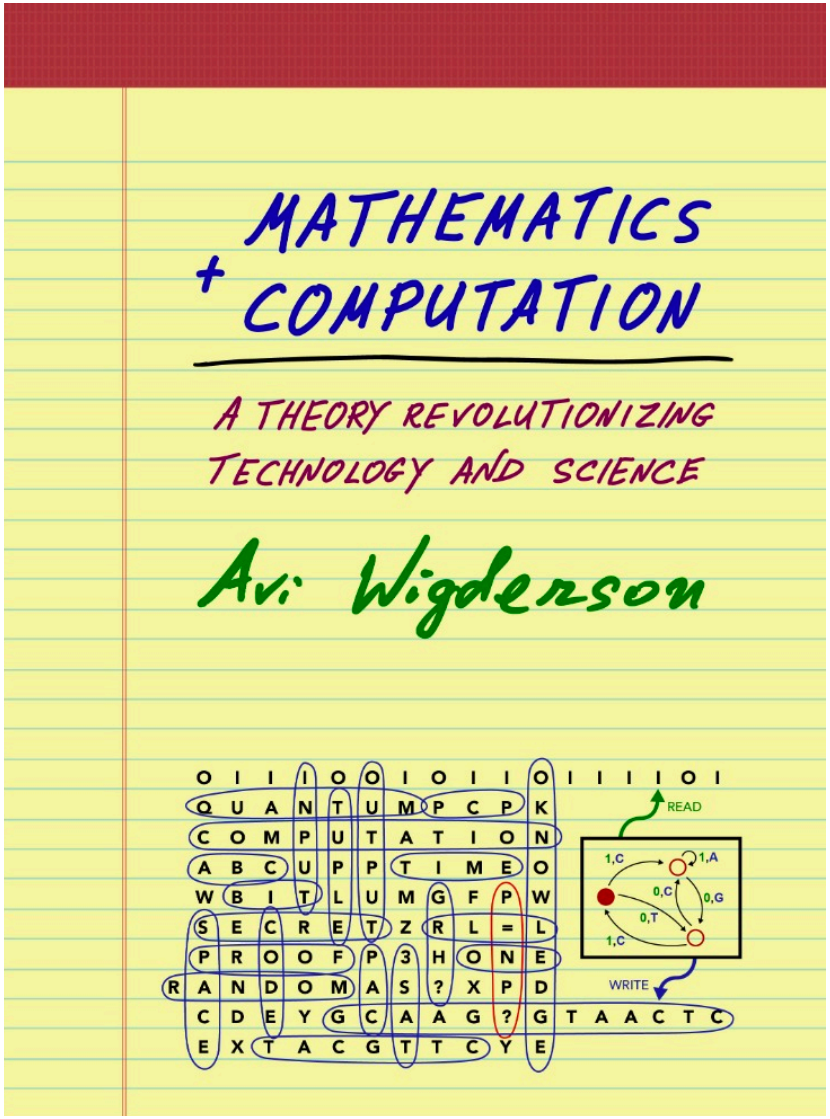
## The value of errors in proofs

Scientific impact: CS, Math, Physics, Optimization,…
Practical impact: Crypto, Clouds, Blockchains,…
Conceptual impact: Paradoxical properties of proofs

## The value of the complexity theory methodology

Modelling, classification, completeness, impracticality…

# Book ad




- Published by Princeton University Press

- Free (forever) on my website

- Comments welcome!

# Proofs and Computations

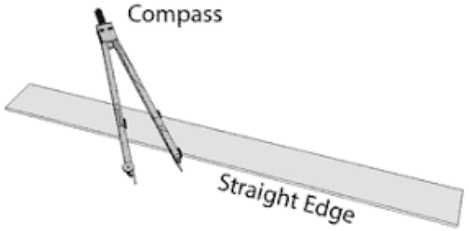
## Two points in a very long history

[Euclid, 300BC]: *The Elements*

{Proofs of theorems in Plane Geometry, deducible from 5 simple axioms}

=

{Constructions of planar point sets using Straightedge and Compass



Turn of the 20th century

Hilbert's *dream*: Truth = Provability = Computability

*...shattered*

[Gödel '31] Incompleteness Thm (= is wrong)

[Turing '36] Undecidability Thm (= is wrong)

Def: algorithms ↔ Turing Machines

Corollary: Computer revolution

Set S ↔ Decision Problem { "is x ∈ S ?" }

R = {Sets *computable* by finite algorithms}

RE = {Sets *provable* to finite algorithms}

Thm: R ≠ RE

Halting = {TMs M which halt on empty input}

Polynomial time

P = {Sets *computable* by efficient algorithms}

NP = {Sets *provable* to efficient algorithms}

Otherwise, no cryptography!

Open: P ≠ NP?

# Examples: claims, arguments, proofs, proof systems, provers, verifiers…

What is true? In real life? In math?

What is a convincing argument?

**Claim:**

"$x \in S$"

# Volume comparison

Left

Right

**Claim:** Left > Right

**Verification:**
Fill Left with water (to the rim) and pour to Right
[if spills, ACCEPT, else, REJECT]

# Sudoku

**Claim:** This puzzle is solvable

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 8 | 6 | | | | | |
| | | | | | | | 6 | |
| | | | 4 | 8 | | | 2 | 3 |
| | | 5 | | 9 | | | | 8 |
| | 4 | 9 | | | | 2 | 1 | |
| 2 | | | | 4 | | 7 | | |
| 3 | 6 | | | 2 | 9 | | | |
| | 1 | | | | | | | |
| | | | | | 5 | 1 | | |

**Argument:**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 9 | 2 | 8 | 6 | 1 | 3 | 4 | 5 | 7 |
| 4 | 7 | 3 | 9 | 5 | 2 | 8 | 6 | 1 |
| 1 | 5 | 6 | 4 | 8 | 7 | 9 | 2 | 3 |
| 7 | 3 | 5 | 2 | 9 | 1 | 6 | 4 | 8 |
| 6 | 4 | 9 | 7 | 3 | 8 | 2 | 1 | 5 |
| 2 | 8 | 1 | 5 | 4 | 6 | 7 | 3 | 9 |
| 3 | 6 | 7 | 1 | 2 | 9 | 5 | 8 | 4 |
| 5 | 1 | 2 | 8 | 7 | 4 | 3 | 9 | 6 |
| 8 | 9 | 4 | 3 | 6 | 5 | 1 | 7 | 2 |

**Verification:** Check each row, column, square, AND that consistent with input. ACCEPT/REJECT

# Composite numbers

**Claim:** 147573952588676412927 composite

**Argument:** 193707721, 761838257287

**Verification:** Check if
193707721 x 761838257287 = 147573952588676412927

Again….

# Volume comparison

**Claim:** Left > Right

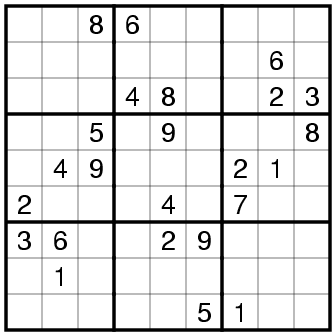
**Verification:** General Procedure

Fill Left with water (to the rim) and pour to Right

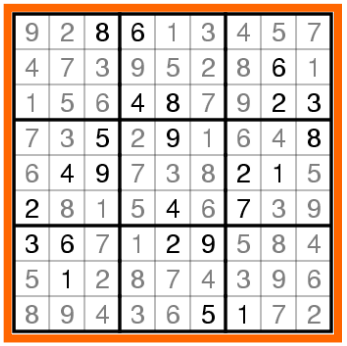
[if spills, ACCEPT, else, REJECT]

# Sudoku

**Claim:** This puzzle is solvable



**Argument:**



General

**Verification:** Check each row, column, square, AND that consistent with input. ACCEPT/REJECT

Efficient algorithm: simple pattern matching

| 1 |  |  | 2 | 3 | 4 |  |  | 12 |  | 6 |  |  |  | 7 |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  | 8 |  |  |  | 7 |  |  | 3 |  |  | 9 | 10 | 6 | 11 |
|  | 12 |  |  | 10 |  |  | 1 |  | 13 |  | 11 |  |  | 14 |  |
| 3 |  |  | 15 | 2 |  |  | 14 |  |  |  | 9 |  |  | 12 |  |
| 13 |  |  |  | 8 |  |  | 10 |  | 12 | 2 |  | 1 | 15 |  |  |
|  | 11 | 7 | 6 |  |  |  | 16 |  |  |  | 15 |  |  | 5 | 13 |
|  |  |  | 10 |  | 5 | 15 |  |  | 4 |  | 8 |  |  | 11 |  |
| 16 |  |  | 5 | 9 | 12 |  |  | 1 |  |  |  |  |  | 8 |  |
|  | 2 |  |  |  |  |  | 13 |  |  | 12 | 5 | 8 |  |  | 3 |
|  | 13 |  |  | 15 |  | 3 |  |  | 14 | 8 |  | 16 |  |  |  |
| 5 | 8 |  |  | 1 |  |  |  | 2 |  |  |  | 13 | 9 | 15 |  |
|  |  | 12 | 4 |  | 6 | 16 |  | 13 |  |  | 7 |  |  |  | 5 |
|  | 3 |  |  | 12 |  |  |  | 6 |  |  | 4 | 11 |  |  | 16 |
|  | 7 |  |  | 16 |  | 5 |  | 14 |  |  | 1 |  |  | 2 |  |
| 11 | 1 | 15 | 9 |  |  | 13 |  |  | 2 |  |  |  | 14 |  |  |
|  | 14 |  |  |  | 11 |  | 2 |  |  | 13 | 3 | 5 |  |  | 12 |

# Composite numbers

**Claim:** 147573952588676412927 composite

**Argument:** 193707721, 761838257287
Crypto rests on the difficulty of finding such

**Verification:** Check if General
193707721 x 761838257287 = 147573952588676412927
Efficient algorithm: simple arithmetic

# Deductive proof systems e.g. Peano Arithmetic

Numerous others

**Objects:** Formulas/expressions over integers (A,B,..)

**Axioms:** E.g.

- x+y = y+x
- x+1 > x
- (x+y)z = xz+yz
- Induction Principle

You've got to believe/trust something!

Proofs are reductions of complex statements to simple truths via simple local sound steps

**Deduction rules:** E.g. if A, A→B true, then B is true.

**Argument:** $A_1, A_2, \ldots, A_m$

**Verification:** Check that each $A_i$ is an axiom, or follows from previous ones by a deduction rule.

**Theorems:**

- There are infinitely many primes
- Fermat's last theorem: no solution to $x^n+y^n=z^n$, $n>2$

# Essentials of proof systems

**Completeness:** True claims have proofs

**Soundness:** False claims don't

**Easy to check:** Distinguishing convincing and faulty **arguments** by an efficient Verifier algorithm

*A complexity theoretic view*

# Proof System [Cook-Reckhow '79]

An efficient Verifier V(claim, argument) satisfies:

**Completeness**: If claim is true then, for *some* argument
V(claim, argument) = ACCEPT
(in which case claim=theorem, argument=proof)

**Soundness**: If claim is false then, for *every* argument
V(claim, argument) = REJECT

$T_V$ : the set of theorems in this system.

[CR'79] NP = {$T_V$ : V deterministic}

# Probabilistic computation & error

"Axiom": Nature provides free access to randomness
(so, let algorithms make random choices!)

Def: A deterministic algorithm $A$ computes a function $f$ if
for all $x$, $A(x) = f(x)$ always

Def: A probabilistic algorithm $B$ computes a function $f$ if
for all $x$, $B(x) = f(x)$ WHP (eg > 2/3) errors in algs

Error can be efficiently reduced arbitrarily!
$\Pr[B(x) \neq f(x)] < 1/3 \Rightarrow \forall k, \Pr[B_k(x) \neq f(x)] < \exp(-k)$

Rationale for allowing errors: (1) "Axiom" reasonable, and
(2) We tolerate uncertainty in life, why not in algs?

Value of allowing errors: Solve many more problems, ++

# Probabilistic Proof System
## [Babai '85, Goldwasser-Micali-Rackoff '85]

probabilistic

An efficient Verifier V(claim, argument) satisfies:

**Completeness**: If claim is true then, for *some* argument
V(claim, argument) = ACCEPT always
(in which case claim=theorem, argument=proof)

**Soundness**: If claim is false then, for *every* argument
V(claim, argument) = REJECT WHP

errors in proofs

$T_V$ : the set of theorems in this system.

IP $\triangleq$ {$T_V$ : V probabilistic + *interactive*}

# IP = (Probabilistic) Interactive Proofs

## [Babai'85, Goldwasser-Micali-Rackoff'85]

claim

Prover

Verifier (deterministic)

NP

argument

ACC/REJ correctly always

---

Prover

Verifier (probabilistic)

IP

Reasonable

$q_1$

$a_1$

.....

$q_r$

$a_r$

ACC/REJ correctly WHP

**A revolutionary scientific notion!**

# Value of errors in proofs: Impact of interactive proofs

Conceptual

Scientific

Mathematical

Technological

Proof with paradoxical properties

ZK: Convincing proofs need not convey information

PCP: Convincing proofs need not be read

The amazing journey from ZK to PCP

# ZKIP: Zero-Knowledge Interactive Proofs

## [Goldwasser-Micali-Rackoff '85]

claim

Prover $q_1$ Verifier

$a_1$

.....

$q_r$

$a_r$

ZKIP

Formal def non-trivial!

ZKIP = IP +

V ACC. → V learns nothing else

Possible? Can a convincing proof be uninformative?

[Goldreich-Micali-Wigderson '86]

1-way functions exist → NP ⊆ ZKIP

Every proof can be made into a ZK proof!

Crypto is used! Is it necessary?

# ZK impacts

Crypto: [Goldreich-Micali-Wigderson '87, …]
Cryptographic protocol design, completeness thm

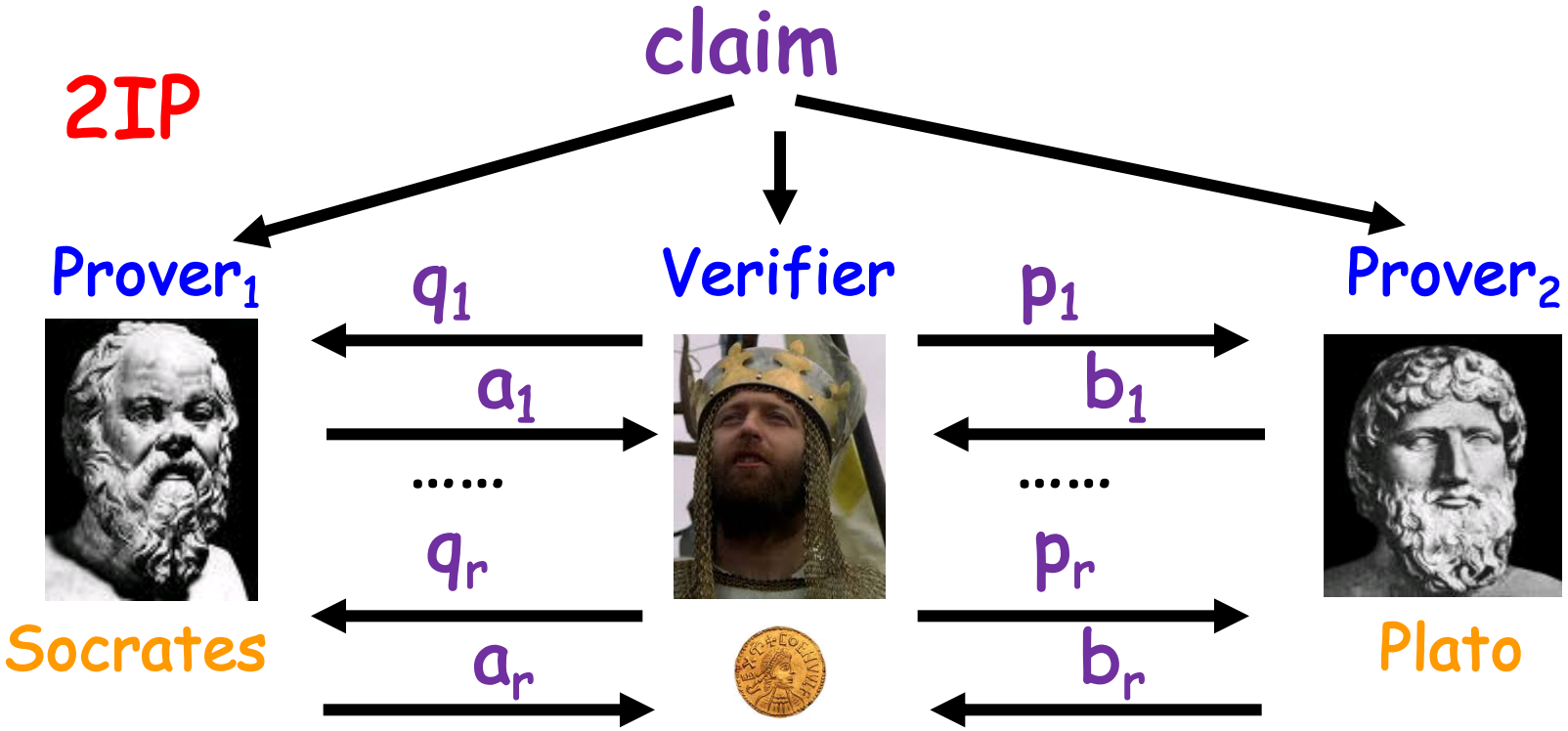
Practical applications:
Anonymous cash, Blockchains, Public ledgers …

Physical ZK proofs:
[Barak-Glaser-Goldstone'14] Nuclear disarmament
[Fisch-Freund-Naor '14] Anonymous DNA testing,…

New proof systems:
MIP: allowing multiple provers

# 2IP: 2-Prover Interactive Proofs

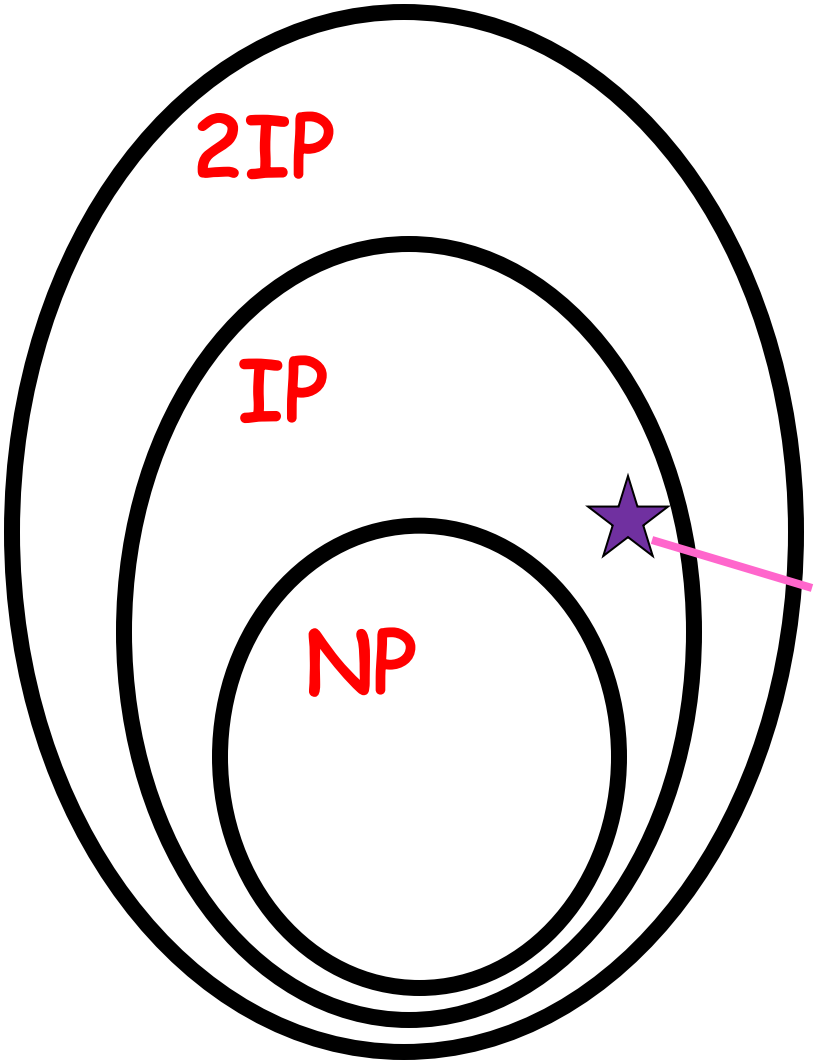
## [BenOr-Goldwasser-Kilian-Wigderson '89]




[BGKW '89] NP $\subseteq$ ZK 2IP

Physical separation replaces computational assumptions

# What is the power of Randomness and Interaction in Proofs?




Trivial inclusions

$IP \subseteq PSPACE$ Polynomial Space

$2IP \subseteq NEXP$ Nondeterministic Exponential Time

Few nontrivial examples

Graph non-isomorphism

……

Few years of stalemate

wonders of polynomials

# Avalanche of Characterizations

## + Conceptual meaning

[Lund-Fortnow-Karloff-Nisan, Shamir '90] IP = PSPACE

Winning strategies are efficiently verifiable!

[Babai-Fortnow-Lund '91] 2IP = NEXP

Intractable problems are efficiently verifiable!

[Arora-Lund-Motwani-Safra-Sudan-Szegedy'92] PCP = NP

Written proofs verifiable from constant-size snapshots!

Same for transcripts of program execution

No crypto!

# PCP (Probabilistically Checkable Proofs)

claim

Prover

Verifier (probabilistic)

NP=PCP

argument

ACC/REJ
Correctly WHP
Reads only 20 bits of the argument

Possible? Finding a single bug in a 100-page proof?

Yes!! Every proof can be turned into a PCP!

Optimization Hardness of approximation!
Coding theory
Complexity theory,...

Technology cloud computing, blockchains,...

# Quantum computation

"Axiom": Nature provides access to quantum phenomena

[Manin '80, Feynman '82] Suggest building computers, that manipulate quantum superpositions with unitary operations.

[..., Deutsch '85, Bernstein-Vazirani '97,...] Formalize it.
BQP: efficient quantum algorithms ( > probabilistic ones)

[Shor '94] Factoring, Discrete Log $\in$ BQP

Frenzy attempts to develop:
- Supporting technology (billions invested)
- "Post-quantum" cryptography (e.g. harness assumptions)
- New quantum algorithms (not so much...)
- New models (plenty)

# Quantum proof systems

Verifier is an efficient quantum algorithm

One prover: IP*, Many provers: MIP*

[Jain-Ji-Updahyay-Watrous'09] IP* = PSPACE

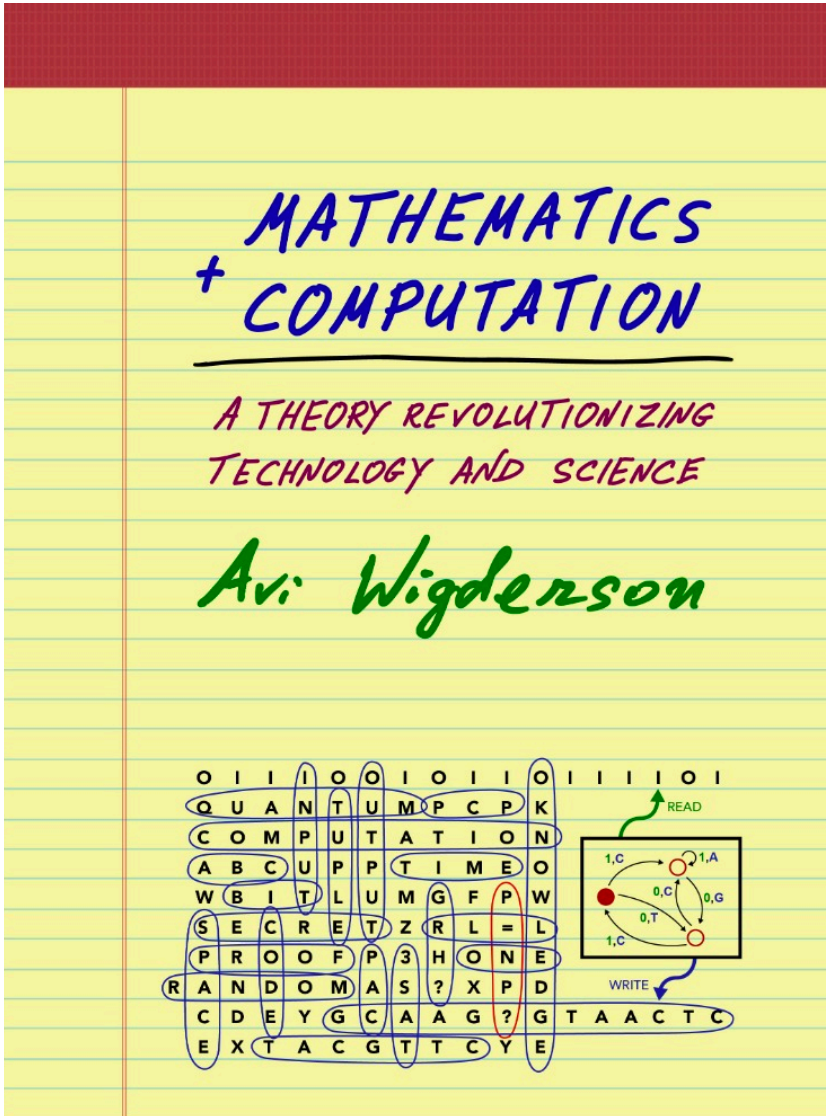
[…,Ji-Natarajan-Vidick-Wright-Yuen'20] MIP* = RE

Quantum Information theory: power of entanglement

Halting ≡ approx. the value of a non-local game!

Math ➔ Connes' embedding conjecture in von-Neumann algebras is false!

# Book ad

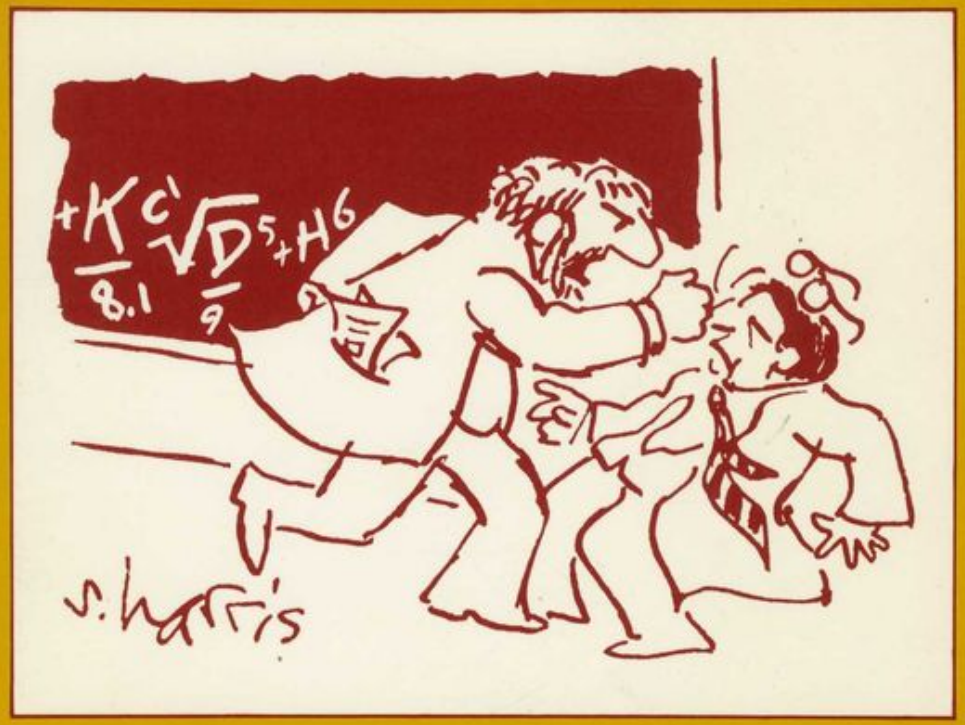



- Published by Princeton University Press

- Free (forever) on my website

- Comments welcome!

# "You want proof? I'll give you proof!"




## *More cartoons from*

# SIDNEY HARRIS

• • •

There's no proof the FOREWORD is BY ALBERT EINSTEIN