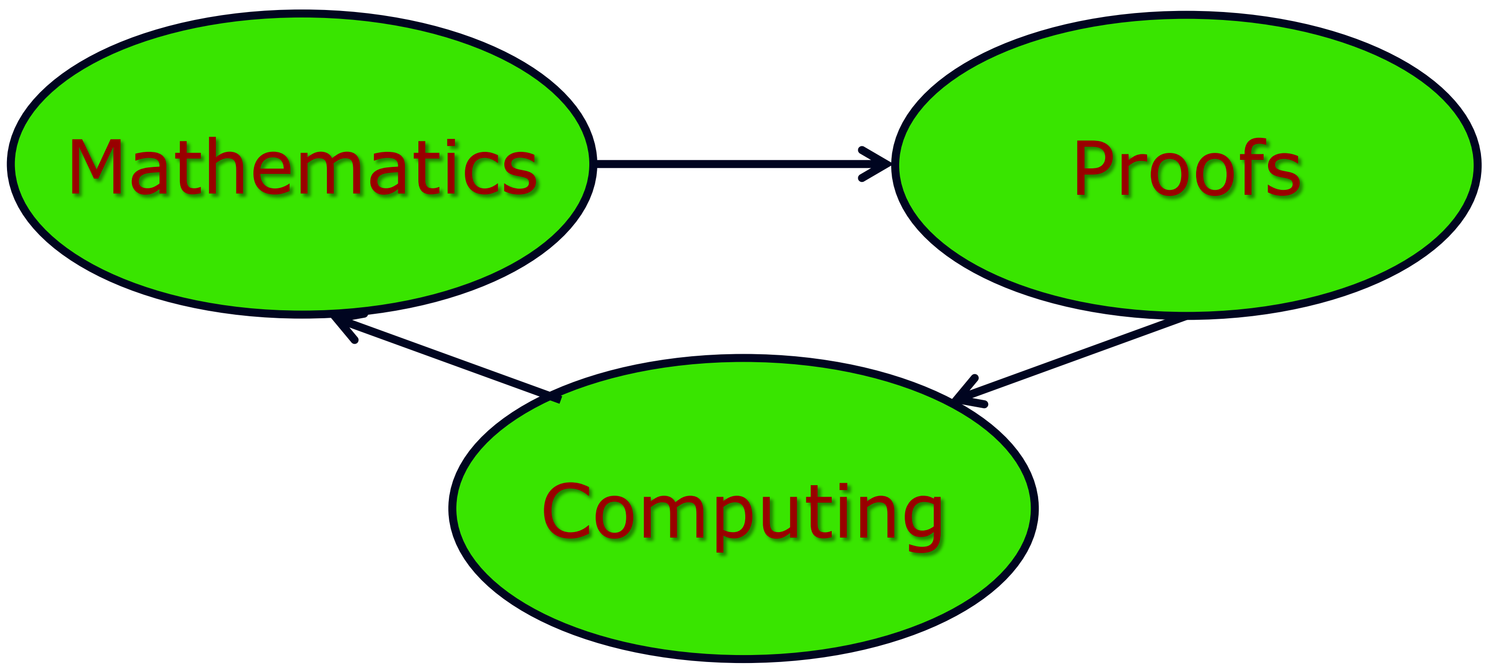
Proofs and Computation

Madhu Sudan
Harvard

In this talk: Proofs and Computation

- "Computer Assisted Proofs ?"
  - [Appel-Haken] – 4-color theorem
  - [Hales] – Kepler Conjecture
  - [Petkovsky,Wilf,Zeilberger] – "A=B"

No!



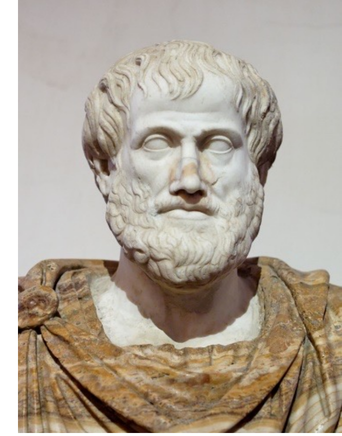
Outline of this talk

- I. Prehistoric stuff ($-\infty$ to 1950)
  - Logic & (Theory of) Computing
- II. Ancient history (1950-1980)
  - P, NP, and Optimization
- III. Recent history (1980-2010)
  - Interaction, Randomness
  - Connections to approximate optimization
- IV. Current themes:
  - Unique games conjecture + progress
  - Proving Quantum Behavior
- V. Future?

I. Prehistory

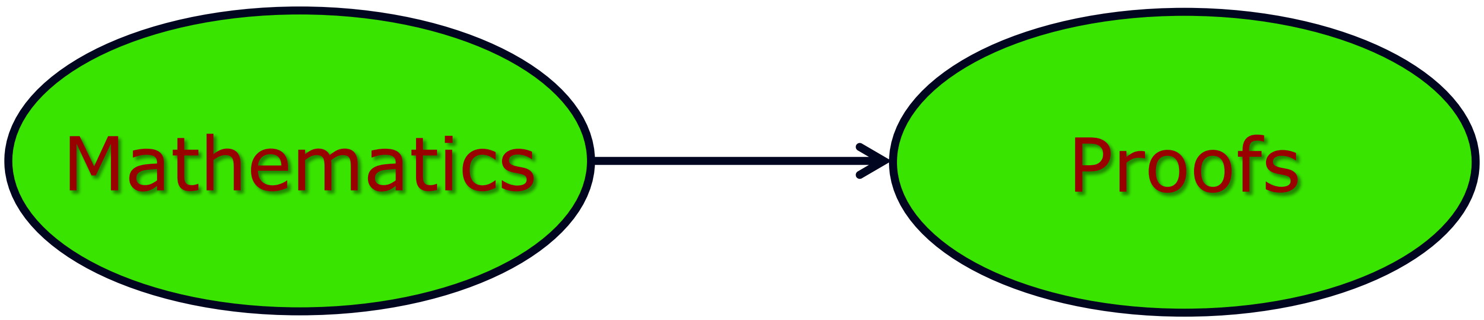
Provable statements

Formal Logic

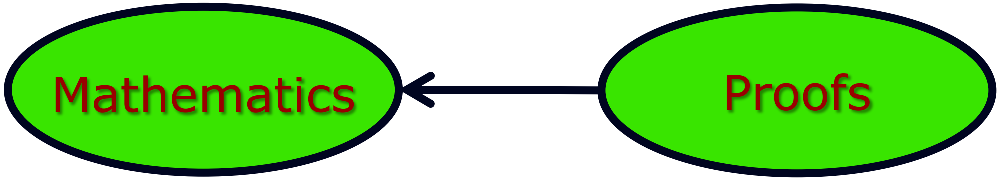


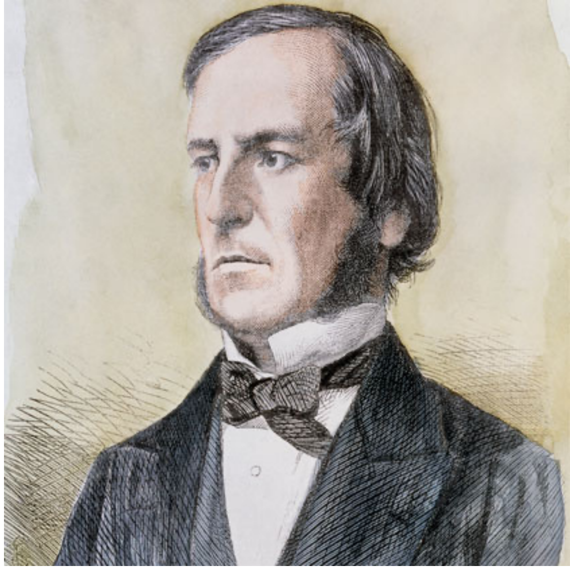
- Attempts to convert reasoning to symbolic manipulation.
- Remarkably powerful.

- Originated independently, and with different levels of impact, in different civilizations …



George Boole (1815-1864)





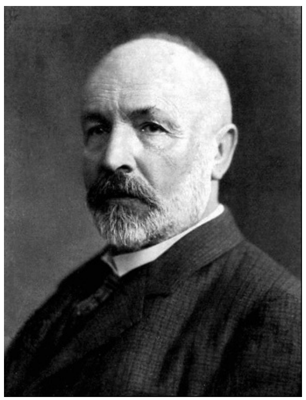
- The strange math of $(\{0,1\}; \vee, \wedge, \neg)$
- Typical Derivation:
  - Axiom: Repetition does not add knowledge
    - Formally: $xx = x$
    - Example: Object is Good and Good ≡ Object is Good
  - Consequence: Principle of Contradiction
    - "… it is impossible for any being to possess a quality and at the same time to not possess it."
    - Proof: $x^2 = x \Rightarrow x^2 - x = 0 \Rightarrow x(x-1) = 0$

      $\Rightarrow x = 0$ or $\neg x \overset{\text{def}}{=} 1 - x = 0$ (page 34)

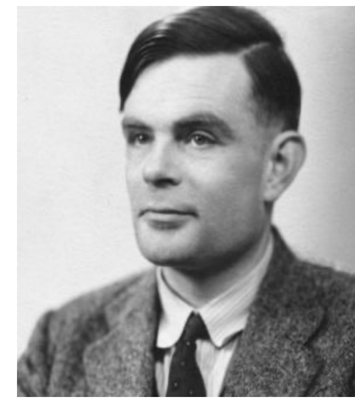
      $\Rightarrow x$ or $\neg x$ does not hold

Whither Computing?

- How well does the logic capture mathematics?







Cantor`1890: Logic may face some problems?

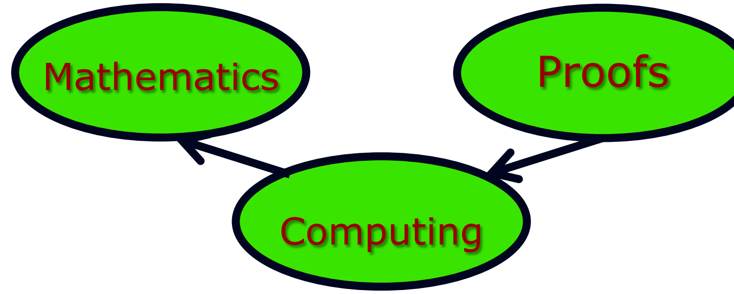
Hilbert `1900: Should capture everything!

Godel `1920s: Incompleteness

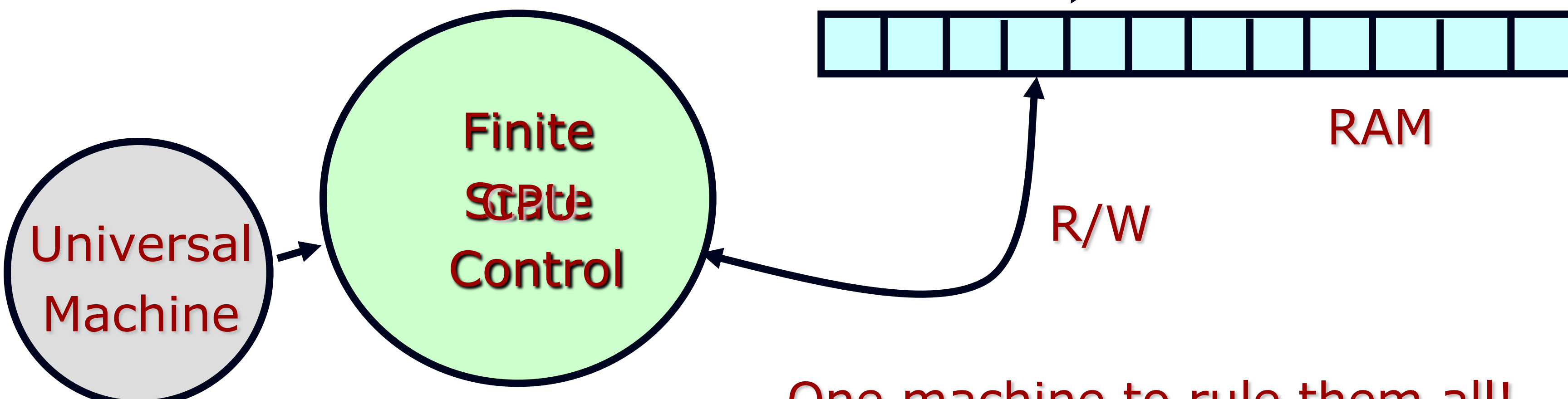
THIS STATEMENT IS NOT PROVABLE

Church-Turing 1930s: Incompleteness holds for any effective reasoning procedure.

Turing's Machine



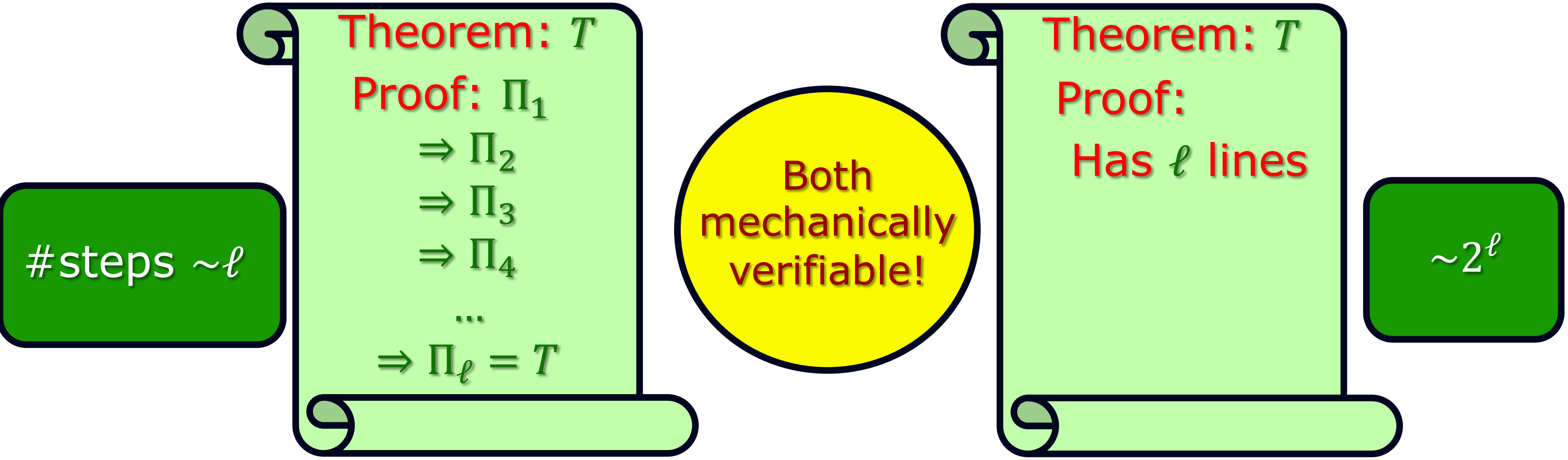
- Model of computer - Universal!
  → von Neumann architecture



One machine to rule them all!

Proofs: Story so far

- Proof: Has to be mechanically verifiable.
- Theorem: Statement with a proof.
- Incompleteness: There exist statements consistent with the system of logic that do not admit a proof.
- Unaddressed: What difference does proof make?

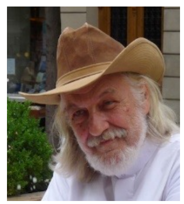
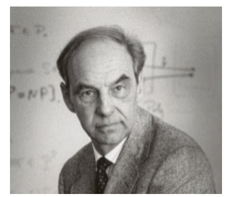


II. Ancient History

Efficient Verification

Origins of Modern Complexity

- [Gödel 1956] in letter to von Neumann: "Is there a more "effective" procedure to find proof of length ℓ if one exists?" (in ℓ^2 steps? $\ell^3 + 10\ell^2$?)


- [Cobham, Edmonds, Hartmanis, Stearns – 60s]:
  - Time Complexity is a (coarse) measure. $10\ell^2 = 5\ell^2$! But $\ell^2 > \ell^{1.9}$.
  - $P \stackrel{\text{def}}{=}$ problems solvable in time ℓ^c for constant c
- Edmonds Conjecture: Travelling Salesman Problem is not solvable in P

Proofs, Complexity & Optimization!

[Cook '71]
Complexity of Theorem Proving

[Levin '73]
Universal Search problems

- Formalized Edmond's Conjecture:
  - NP = Problems w. efficiently verifiable solutions
  - NP-complete = Hardest problem in NP
    - *Theorem-Proving* NP-Complete
    - *SAT* (simple format of proofs) NP-complete
    - *Domino tiling* NP-Complete
    - Godel's question ≡ "Is $NP = P$?"

Proofs, Complexity & Optimization - 2

[Karp ‘72] Reducibility among combinatorial optimization problems

- Showed central importance of NP.
  - Nineteen problems NP-Complete!
  - Cover optimization, logic, combinatorics, graph theory, chip design.

Some NP-complete Problems

- Map Coloring: Can you color a given map with 3-colors, s.t. bordering states have diff. colors?

Some NP-Complete Problems

- Travelling Salesman Problem: (TSP) – Find tour of minimum length visiting given set of cities.

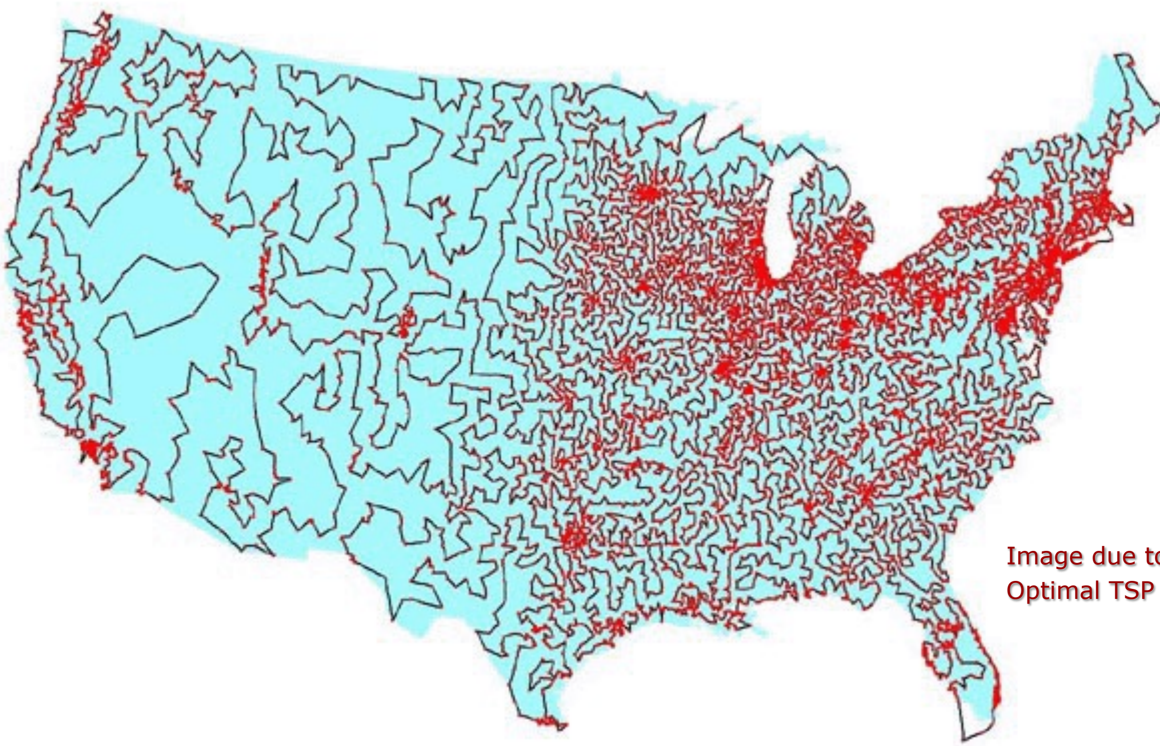


Image due to [Applegate, Bixby, Chvatal, Cook].
Optimal TSP visiting ~13000 most populated cities in US.

Some NP-Complete Problems

- Biology: Fold DNA sequence so as to minimize energy.
- Economics: Finding optimal portfolio of stocks subject to budget constraint.
- Industrial Engineering: Schedule tasks subject to precedence constraints to minimize completion time.
- …

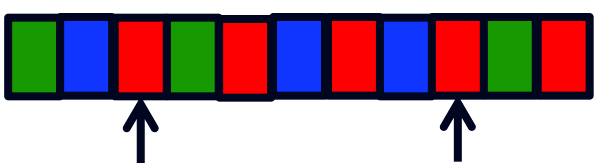
Consequences to Proof Checking

- NP-Complete problem ≡ Format for proofs.
  - 3-coloring is NP-complete ⇒ exists function f

    $f(T, \ell)$ = Map with ℓ^c regions s.t.

    T has proof of length ℓ ⇒ Map is 3-colorable

    … no proofs of length ℓ ⇒ Map not 3-colorable
- Format?
  - Rather than conventional proof, can simply give coloring of map!



Verifier computes $f(T, \ell)$ and verifies coloring is good

  - Advantage: Error is local (two improperly colored regions)

Is P=NP?

- Don't know …
- If P=NP …

"Of all the Clay Problems, this might be the one to find the shortest solution, by an amateur mathematician."

\- Devlin, *The Millenium Problems (Possibly thinking P=NP)*

  - Mathematicians replaced by computers.

"If someone shows P=NP, then they prove any theorem they wish. So they would walk away not just with \$1M, but \$6M by solving all the Clay Problems!"

\- Lance Fortnow, *Complexity Blog*

"P = NP?" is Mathematics-Complete !!

III. Recent History

Proofs and Randomness

Randomness & Modern Complexity

- Emphasis on Randomness.
  - Randomness can potentially speed up algorithms.
  - Essential for
    - Equilibrium behavior
    - Coordination among multiple players
    - Cryptography

- But it probably can't help with Logic – right?
  - Actually – it does!!

Interactive Proofs




- [Goldwasser, Micali, Rackoff], [Babai] ~1985
- Verifier asks questions and Prover responds:
  - Space of questions exponentially large in the length!
  - Prover has to be ready for all!
- Many striking examples:
  - Pepsi ≠ Coke! ("Graphs not isomorphic")
  - Can prove "theorem has no short proof".
  - "IP = PSPACE" [LFKN, Shamir]
- "Zero Knowledge Protocols" – Foundations of Secure communication

Probabilistically Checkable Proofs

- Do proofs have to be read in entirety to verify?

$$\begin{aligned} a &= b \\ a^2 &= ab \\ a^2 - b^2 &= ab - b^2 \\ (a+b)(a-b) &= b(a-b) \\ a+b &= b \\ 2b &= b \\ 2 &= 1 \end{aligned}$$

$$\begin{aligned} x &= (\pi+3)/2 \\ 2x &= \pi+3 \\ 2x(\pi-3) &= (\pi+3)(\pi-3) \\ 2\pi x - 6x &= \pi^2 - 9 \\ 9 - 6x &= \pi^2 - 2\pi x \\ 9 - 6x + x^2 &= \pi^2 - 2\pi x + x^2 \\ (3-x)^2 &= (\pi - x)^2 \\ 3 - x &= \pi - x \\ \pi &= 3 \end{aligned}$$

Probabilistically Checkable Proofs

- Do proofs have to be read in entirety to verify?
  - Conventional formats for proofs – YES!
  - But we can change the format!
- Format ≡ Verification Algorithm
  - Any verifier is ok, provided:
    - If T has proof of length ℓ in standard system, then V should accept some proof of length $\text{poly}(\ell)$
    - If T has no proofs, then V should not accept any proof with probability $\geq$ ~~$\frac{1}{2}$~~ $.001$
- PCP Theorem [Arora, Lund, Motwani, Safra, Sudan, Szegedy '92]:

A format exists where V reads only constant number of bits of proof!

An Analogy

- Inspecting a building:
  - "Building = $O(n)$ atoms" … OR
  - "Building = $O(1)$ rooms = $O(1)$ walls"
- Former view:
  - Verifying stability takes $\Omega(n)$-checks.
- Latter view:
  - Verifying stability takes $O(1)$-checks +
  - $O(1)$-"stability of wall-checks".

- Polynomials ≡ Walls!

10^6-mile view of PCPs: Polynomials

- A (NP-)complete statement:
  - Graph $G \in \{0,1\}^{n \times n}$ is 3-colorable.
  - Proof: Coloring ($\Theta(n)$-bits).
  - Verification: Read entire coloring.
- PCP Idea: Glue n bits using polynomials (deg. n)
  - Key fact: Non-zero polynomial usually non-zero.
- Equivalent (NP-)complete statement:
  - Given: Φ local map from poly's to poly's
  - ∃ poly's A, B, C, D s.t. $\Phi(A, B, C, D) \equiv 0$
  - Verification:
    - Step 1: Test A, B, C, D are polynomials
    - Step 2: Verify $\Phi(A, B, C, D)[r] = 0$ for random r.

Polynomials = Wall - II

- Reduction from 3-coloring to polynomial satisfiability [Ben-Sasson-S.'04]
- $\Phi(A,B,C,D)[x_0,\boldsymbol{x},\boldsymbol{y}] = \Phi_E(A,B,C,D)[x_0,\boldsymbol{x},\boldsymbol{y}]$

$$= (A[\boldsymbol{x}](A[\boldsymbol{x}]-1)(A[\boldsymbol{x}]-2)\ - B[\boldsymbol{x}]\Pi_{v\in V}(\boldsymbol{x}-v))$$
$$+ x_0\cdot (E(\boldsymbol{x},\boldsymbol{y})\cdot \Pi_{i\in\{-2,-1,1,2\}}(A[\boldsymbol{x}]-A[\boldsymbol{y}]-i)$$
$$- C[\boldsymbol{x},\boldsymbol{y}]\Pi_{v\in V}(\boldsymbol{x}-v) - D(\boldsymbol{x},\boldsymbol{y})\Pi_{v\in V}(\boldsymbol{y}-v))$$

Improved (Optimal) PCPs

- [Raz'94, Hastad'97, Dinur'06, Moshkovitz-Raz'08]: Series of remarkable improvements: Reduced error, reduced #queried bits, Reduced size of PCP:
  - Current: For barely super-linear blowup in size, PCP can be verified reading 3 bits to get error ½.
- Ingredients: Fourier analysis, Expander graphs, Error-correcting codes, Information Theory

PCPs and Approximate Optimization

- Classical connection: [Cook → Karp]:
  - Solving optimization problems ≡ finding proofs
- New Connection: [Feige et al., Arora et al.]
  - Solving optimization problems <u>approximately</u> ≡ finding <u>nearly valid</u> proofs.
  - Existence of nearly valid proofs ≡ Existence of perfectly valid proofs (due to PCPs)!
  - Conclude: Solving (some/many) optimizations approximately is as hard as solving them exactly!
- 1992-today: PCP-induced revolution in understanding approximability!!

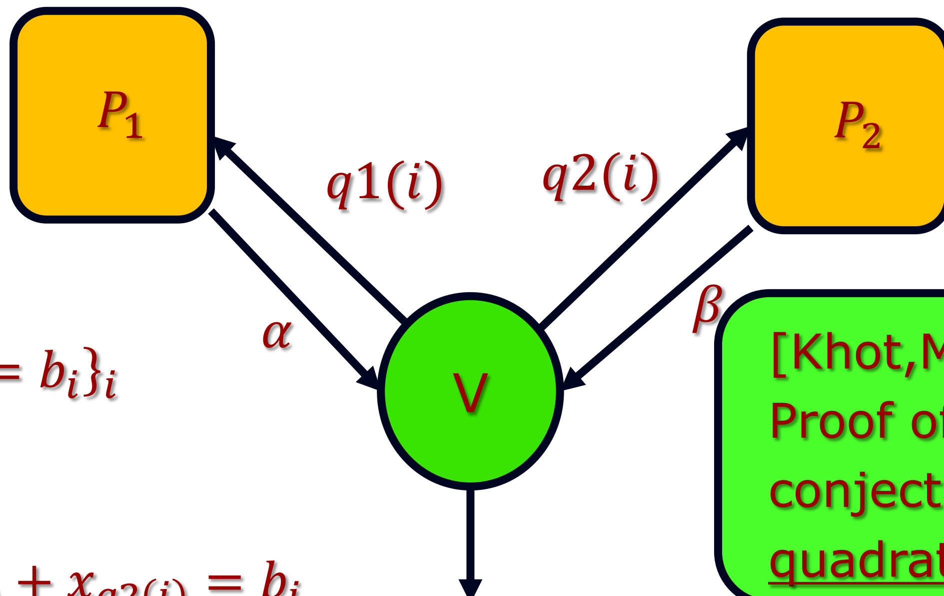
IV. Current Directions

Unique Games and a Conjecture

- Given linear equations $Ax = b \pmod p$, distinguish:
  - $1 - \epsilon$ fraction of equations satisfiable.
  - $\frac{1}{p} + \epsilon$ fraction of equations satisfiable.
  - Thm [Hastad '97]: NP-hard even if each equation has only 3 variables.
- Unique Game setting: 2 variables/equation
- Conjecture [Khot]: Still NP-hard …
- Implications: Many!
  - Roughly – for very broad class of optimization problems, a natural "convex relaxation and rounding" is best possible.

Unique? Game?

- Inspires "2-prover proof system" (game):



$Ax = b \Leftrightarrow \{a_i \cdot x = b_i\}_i$

Pick random i

$a_i \cdot x = b_i \,:\, x_{q1(i)} + x_{q2(i)} = b_i$

Accept iff $\alpha + \beta = b_i$

[Khot,Minzer,Safra'17]: Proof of analogous conjecture for system of quadratic equations

UGC ⇒ Perfect+Sound Proof system with negligible error

Unique? Condition on answer of P_1 answer to P_2 unique + vice versa!

Proofs & Quantumness

- CHSH game: Proving laws of quantum mechanics to a skeptic.
  - $V \to A : x$; $V \to B : y$
  - $A \to V : a$; $B \to V : b$
  - Accept iff $x \wedge y = a \oplus b$
  - Classical strategy wins w.p. ¾
  - Quantum strategy (A & B share entanglement) wins w.p. ~.85
- Modern "extensions":
  - [Mahadev]: Classical verification of quantum computation.
  - [Ji,Natarajan,Vidick,Wright,Yuen]: Interactive verification of all computable functions.
    - Ingredient: Alice and Bob can prove to V that they have n qubits of entanglement by consuming tiny number of qubits. (e.g, $\log\log\log\log\log n$ qubits)

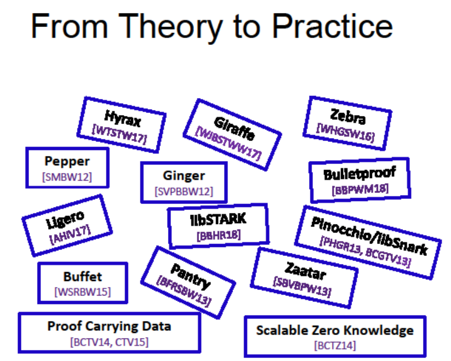
V. Future

Some context

- PCPs as method to understand (in)approximability: HUGELY successful

- PCPs as a positive method:
  - Make verification easier …
  - … much more limited
  - (Actually used in blockchain/cryptocurrencies)

- Why so limited?



(from Yael Kalai: "Evolution of Proofs")

Proofs: Standard Assumption

A	T	Π

- Small (Constant) Number of Axioms
  - $X \to Y, Y \to Z \Rightarrow \; X \to Z$, Peano, etc.
- Medium Sized Theorem:
  - $\forall x, y, z, n \in \mathbb{N}, \quad x^n + y^n = z^n \to n \leq 2$ …
- Big Proof:
  - Blah blah blah blah blah blah bla blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah

The truth

- Mathematical proofs assume large context.
  - "*By some estimates a proof that 2+2=4 in ZFC would require about 20000 steps … so we will use a huge set of axioms to shorten our proofs – namely, everything from high-school mathematics*"

  [Lehman,Leighton,Meyer – Notes for MIT 6.042]
- Context (= huge set of axioms) shortens proofs.
- But context is uncertain!
  - What is "high school mathematics"?
- Need to understand how this works?
  - Context, uncertainty, communication
  - Mind, reasoning, knowledge

Summary and Conclusions

- Computing as a science:
  - Goes to the very heart of scientific inquiry.
    - What big implications follow from local steps?
- Search for proofs captures essence of all search and optimization.
- “Is P=NP?” Central mathematical question.
  - Still open.
- What are proofs?
  - Many implications of randomness & interaction
  - Not yet totally understood … ☹
  - ☺ … Up to us to define and design!

Thank You!