This week:

The Evolution of Proofs in Computer Science
Classical proofs

(Zero-knowledge) Interactive proofs

Multi-prover interactive proofs

Probabilistically checkable proofs (PCPs)

Succinct non-interactive arguments (SNARGs)
Zero-Knowledge Proofs
[Goldwasser-Micali-Rackoff85]

Proofs that reveal no information beyond the validity of the statement
Zero-Knowledge Proofs
[Goldwasser-Micali-Rackoff85]

Impossible!

This is information!
Interactive Proofs
[Goldwasser-Micali-Rackoff85]

Completeness: \( \forall x \in L \quad \Pr[(P, V)(x) = 1] \geq 2/3 \)

Soundness: \( \forall x \notin L, \forall P^* \quad \Pr[(P^*, V)(x) = 1] \leq 1/3 \)

Note: By repetition, we can get completeness \( 1 - 2^{-k} \) and soundness \( 2^{-k} \)
Interactive Proofs

[Goldwasser-Micali-Rackoff85]

For ZK the prover needs to be randomized

[Goldreich-Micali-Wigderson87]: Every statement that has a classical proof has zero-knowledge (ZK) interactive proof, assuming one-way functions exist
Defining Zero-Knowledge

Formally: There exists a PPT algorithm $S$ (called a simulator), such that for every PPT (cheating) verifier $V^*$ and for every $x \in L$:

$$S(x) \approx (P, V^*)(x)$$

Denotes the transcript

This transcript reveals no information
Focus on the NP-complete language of all 3-colorable graphs:

\[ G = (Ver, E) \]

Randomly permute the coloring, to obtain valid coloring \((c_1, \ldots, c_n)\)

Choose a random edge \((i, j) \in E\)

Open safes \(i, j\)

**Soundness:** Only \(1 - \frac{1}{|E|}\) but can be amplified via repetition.
ZK Proofs for NP

Focus on the $NP$-complete language of all 3-colorable graphs:

\[ G = (\text{Ver}, E) \]

\[ S(G): \]
1. Choose a random $(i, j) \in E$
2. Choose random distinct colors $c_i, c_j$
3. The simulated transcript is:
   
   \[ (i, j) \in E \]
   
   Open safes $i, j$

For honest $V$

\[ (i, j) \in E \]

Open safes $i, j$
Implementing Digital Safes: Commitment Scheme

Commitment scheme is a randomized algorithm $Com$ s.t.

• Computationally Hiding:
  \[ \forall m, m' \quad Com(m; r) \approx Com(m'; r') \]

• Statistically Binding: \( \mathcal{A}(m, r), (m', r') \) s.t. \( m \neq m' \) and
  \[ Com(m; r) = Com(m'; r') \]
Constructing a Commitment Scheme

**Construction 1:**

Let $f: \{0,1\}^* \rightarrow \{0,1\}^*$ be an injective OWF, and $p: \{0,1\}^* \rightarrow \{0,1\}$ be a corresponding hardcore predicate.

$$\text{Com}(b; r) = (f(r), p(r) \oplus b)$$

**Binding:** Follows from the fact that $f$ is injective

**Hiding:** Relies on the fact that if $f$ is one-way then:

$$(f(r), p(r)) \approx (f(r), U)$$
Constructing a Commitment Scheme

Construction 2: computationally hiding, and statistically binding [Pederson]

Let $G$ be a group of prime order $p$, let $g \in G$ be any generator, and $h$ be a random group element.

$$Com_{g,h}(m, r) = g^m h^r$$

**Hiding:** Information theoretically!

**Binding:** Follows from the Discrete Log assumption.
Perfect ZK Computationally Sound Proofs

For the \( NP \)-complete language of all 3-colorable graphs

\[ G = (V, E) \]

Randomly permute the coloring, to obtain valid coloring \((c_1, ..., c_n)\)

Choose a random edge \((i, j) \in E\)

Reveal \(c_i, c_j\), with corresponding randomness

\[ \text{Com}_{g,h}(c_1), ..., \text{Com}_{g,h}(c_n) \]
So Far...

• Constructed ZK proofs for all of NP
  – using commitment schemes
Interactive Proofs are more efficient!
Classical Proofs

$P \quad V$

Diagram with a box in the middle and arrows pointing from $P$ to $V$.
Conjecture: There is no succinct classical proof for correctness of any computation $M(x) = 1$ within $T$ steps.
Interactive Proofs are More Efficient!

[Lund-Fortnow-Karloff-Nissan90, Shamir90]

Example: Chess
Interactive Proofs are More Efficient! [Lund-Fortnow-Karloff-Nissan90, Shamir90]

correctness of any computation can be proved:

\[ \text{Time to verify} \approx \text{Space required to do the computation} \]

\[ \text{Interactive Proof} \]

\[ IP = PSPACE \]
Interactive Proofs are More Efficient!

[Lund-Fortnow-Karloff-Nissan90, Shamir90]

correctness of any computation can be proved:

\[
\text{Time to verify} \approx \text{Space required to do the computation}
\]

Succinct space \rightarrow \text{succinct interactive proof}
Interactive Proofs are More Efficient!

[Lund-Fortnow-Karloff-Nissan90, Shamir90]

Fix any language $L$ computable in time $T$ and space $S$

Runs in time $\approx 2^{S^2}$

$P$

$x \in L$

$V$

Runs in time $\approx S \cdot \text{polylog } T$
Open Problem:

Does there exist an interactive proof for any time-$T$ space-$S$ computation where the verifier runs in time $\approx S \cdot \text{polylog}(T)$ and the prover runs in time $\text{poly}(T)$?

Is proving harder than computing??
Open Problem:

$P \in L$

Runs in time $\approx S \cdot \text{polylog}T$

Runs in time $\text{poly}(T)$
Multi-Prover Interactive Proofs

[BenOr-Goldwasser-Kilian-Wigderson88]

\[ \forall f \text{ computable in time } T: \]

2-provers can convince verifier that \( f(x) = y \),
where the runtime of the verifier is only \( |x| \cdot \text{polylog}(T) \)
and the communication is \( \text{polylog}(T) \)

\( P_1 \)
\[ a_1 \]
\[ q_1 \]
\( P_2 \)
\[ a_2 \]
\[ q_2 \]
\( V \)

motivated by constructing perfect ZK proofs
[Fortnow-Rompel-Sipser88]:

\[ V \]

\[ q_1 \]

\[ q_2 \]

\[ a_1 \]

\[ a_2 \]

\[ P_1 \]

\[ P_2 \]

\[ a_1 \ a_2 \ a_3 \ a_4 \]

\[ a_1 \ a_2 \ a_3 \ a_4 \]
Probabilistically Checkable Proofs


Read only 3 bits of the proof, and obtain soundness 1/8
Classical proofs

(Zero-knowledge) Interactive proofs

Multi-prover interactive proofs

Probabilistically checkable proofs (PCPs)

Succinct non-interactive arguments (SNARGs)
THANK YOU