This week:

The Evolution of Proofs in Computer Science

Last class: ZK Proofs

Today: Aftermath!
Classical proofs

(Zero-knowledge) Interactive proofs

Multi-prover interactive proofs

Probabilistically checkable proofs (PCPs)

Succinct non-interactive arguments (SNARGs)
Interactive Proofs

[Goldwasser-Micali-Rackoff85]

\[ P \quad V \]

[Goldreich-Micali-Wigderson87]: Every statement that has a classical proof has zero-knowledge (ZK) interactive proof, assuming one-way functions exist.
Interactive Proofs are more efficient!
Classical Proofs
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!

*Interactive Proofs* are more efficient to verify than traditional proofs. The time to verify a computation and the space required to do the computation are approximately equal. This is represented by the equation:

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

This result, known as the *IP = PSPACE* theorem, was established by Lund, Fortnow, Karloff, and Nissan in 1990, as well as by Shamir in the same year.

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

correctness of any computation can be proved:

Time to verify

$\approx$

Space required to do the computation

Succinct space $\rightarrow$ succinct interactive proof
Interactive Proofs are More Efficient!

[Lund-Fortnow-Karloff-Nissan90, Shamir90]

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

$\exists x \in L$

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

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:

\[ x \in L \]

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

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

[BenOr-Goldwasser-Kilian-Wigderson88]

Theorem [Babai-Fortnow-Lund90]:

Any proof can be made exponentially shorter with a 2-prover interactive proof!

∀f computable in time T:

2-provers can convince verifier that f(x) = y, where the runtime of the verifier is only |x| \cdot polylog(T) and the communication is polylog(T)
[Fortnow-Rompel-Sipser88]:

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]

\[
\begin{array}{cccc}
  a_1 & a_2 & a_3 & a_4 \\
\end{array}
\]
Probabilistically Checkable Proofs

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

Succinct Interactive Arguments
[Micali14]

$P(w)$

$x \in L$

$V$

$HT_h(\pi)$

Compute PCP $\pi$ for $x \in L$

Compute corresponding openings $o_1, o_2, o_3$

Sample PCP queries: $q_1, q_2, q_3$

$\pi_{q_1}, \pi_{q_2}, \pi_{q_3}$

Theorem: This protocol is computationally sound assuming $h$ is collision resistant.
Succinct Interactive Arguments

\[ P(w) \quad x \in L \quad V \]

\[ \text{Compute PCP } \pi \text{ for } x \in L \]

\[ \text{Sample PCP queries: } q_1, q_2, q_3 \]

\[ \text{Compute corresponding openings } o_1, o_2, o_3 \]

\[ HT_h(\pi) \]

Obtain a Succinct Non-Interactive Argument (SNARG) by applying the Fiat-Shamir Paradigm.

Computationally Sound Proofs
Classical proofs

(Zero-knowledge) Interactive proofs

Multi-prover interactive proofs

Probabilistically checkable proofs (PCPs)

Succinct non-interactive arguments (SNARGs)