This week:

The Evolution of Proofs in Computer Science

Last class: ZK Proofs

Today: Aftermath!

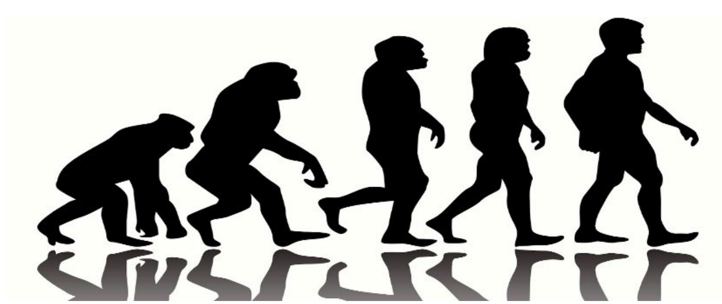
Classical proofs

(Zero-knowledge)
Interactive proofs

Multi-prover
interactive proofs

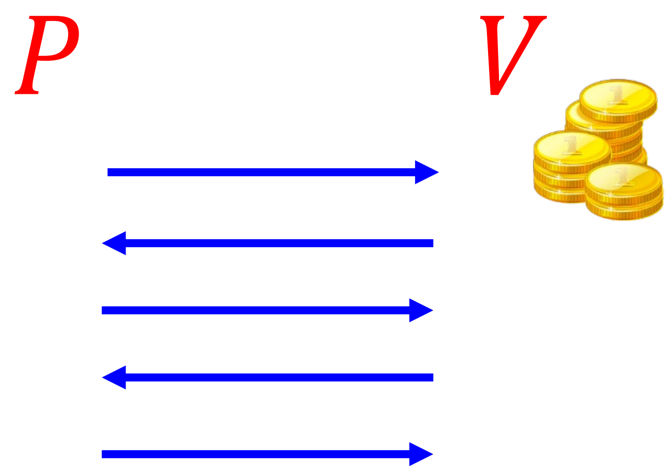
Probabilistically
checkable proofs (PCPs)

Succinct non-interactive arguments
(SNARGs)



Interactive Proofs

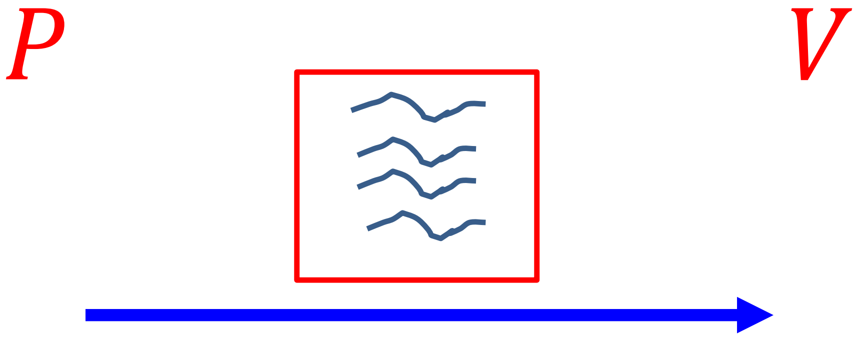
[Goldwasser-Micali-Rackoff85]



[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



Classical Proofs

P V

$$\frac{a}{\vdash a = a}$$

$$\frac{\Gamma \vdash a = b;\ \Delta \vdash b' = c}{\Gamma \cup \Delta \vdash a = c}$$

$$\frac{\Gamma \vdash f = g;\ \Delta \vdash a = b}{\Gamma \cup \Delta \vdash f\,a = \ldots}$$

$$\frac{\ldots}{\vdash (\lambda x.\, a)\, x = a}$$

$$\frac{p{:}bool}{p \vdash p}$$

$$\frac{\Gamma \vdash p;\ \Delta \vdash p' = q}{\Gamma \cup \Delta \vdash q}$$

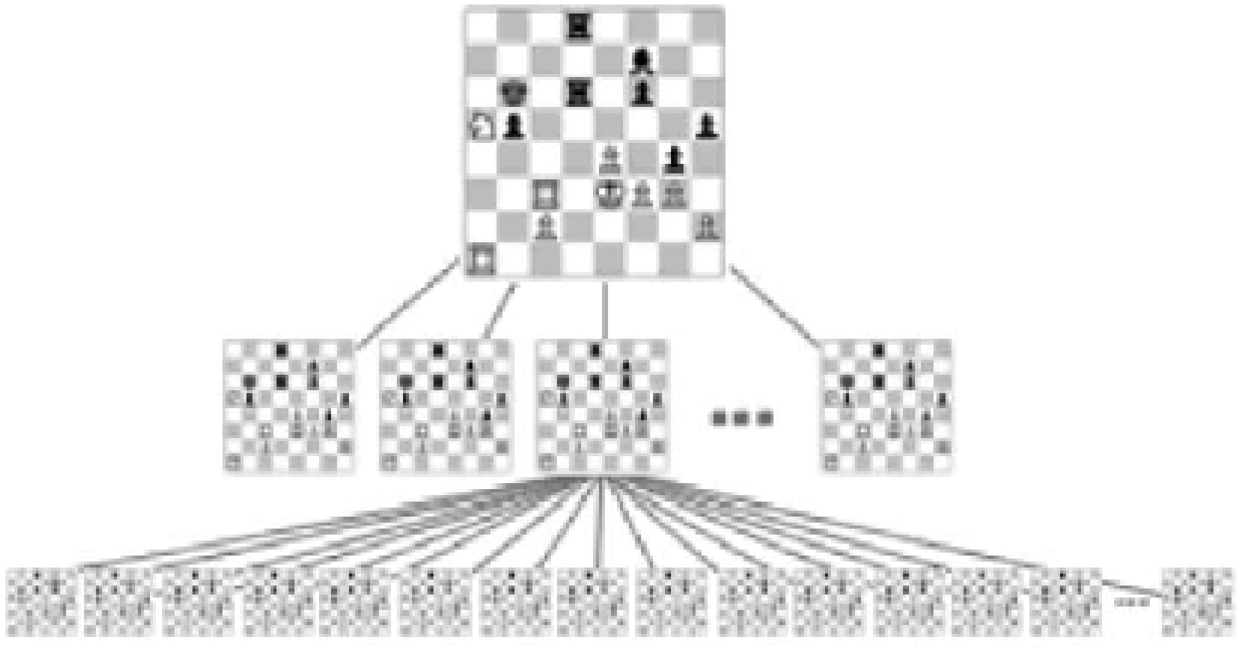
$$\frac{\Gamma \vdash p;\ \Delta \vdash q}{(\Gamma \setminus q) \cup (\Delta \setminus p) \vdash p = q}$$

Conjecture: $\nexists$ **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:

Time to verify

$\approx$

Space required to do the computation

Interactive Proof

$$\boldsymbol{IP = PSPACE}$$

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 ⟹ 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 $\approx 2^{S^2}$

$x \in L$

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

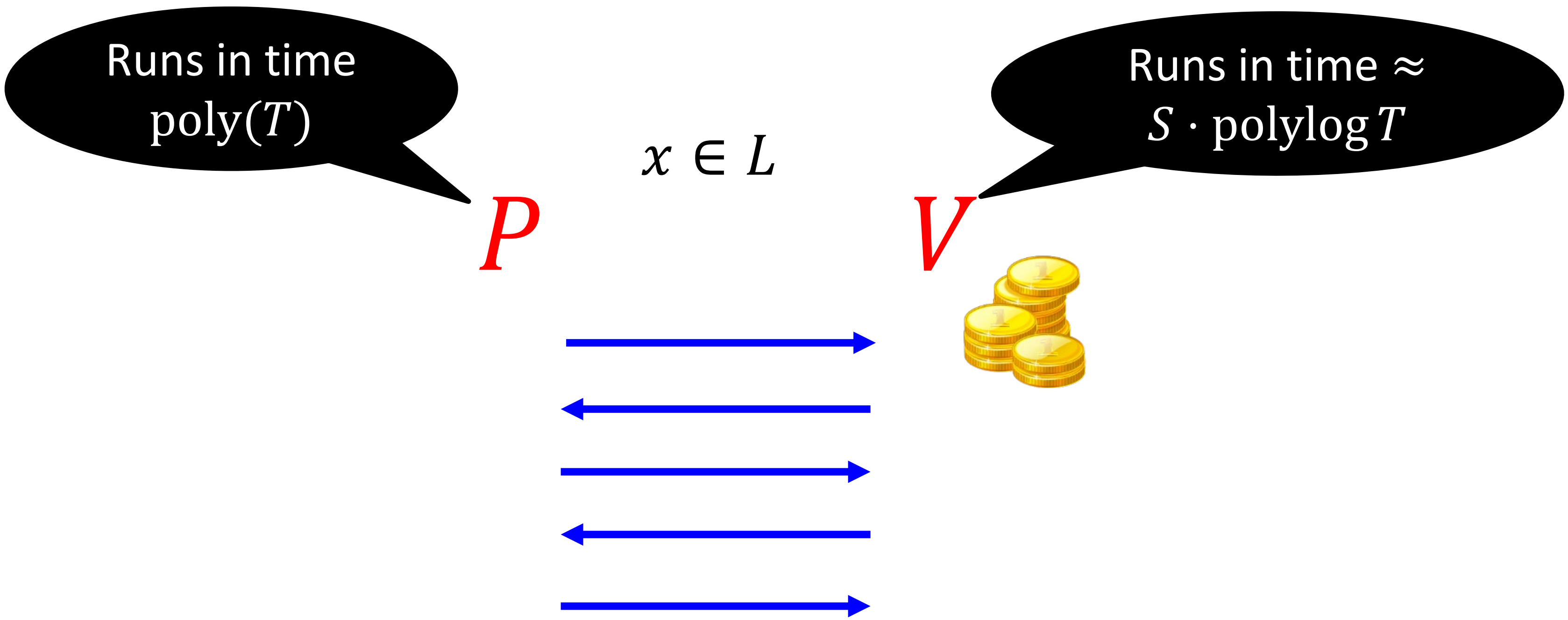
P V

Open Problem:

Is proving harder than computing??

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

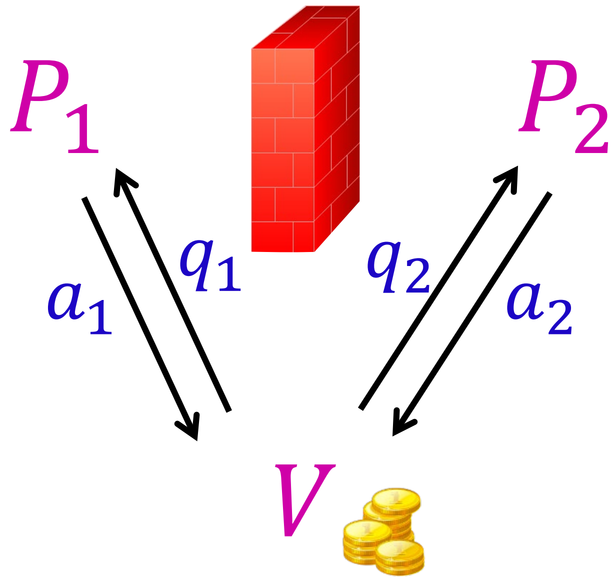
Open Problem:



Multi-Prover Interactive Proofs

[BenOr-Goldwasser-Kilian-Wigderson88]

motivated by constructing **perfect ZK proofs**



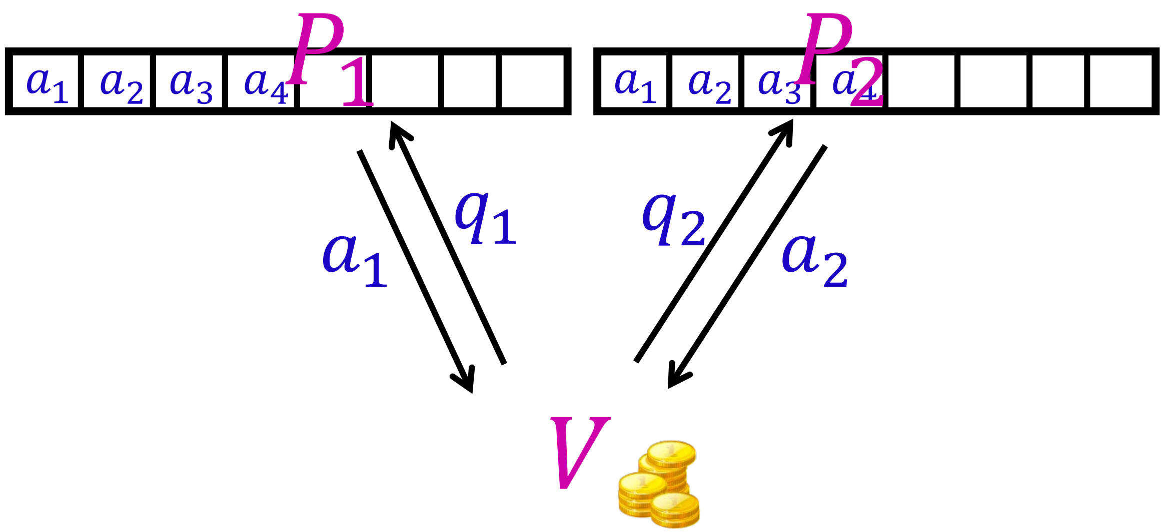
$\forall f$ computable in time T:

2-provers can convince verifier that $f(x) = y$,

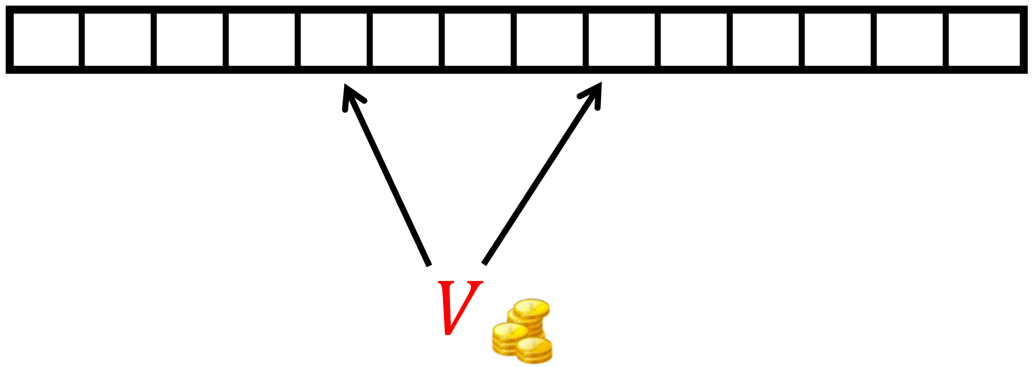
where the **runtime** of the **verifier** is only $|x| \cdot polylog(T)$

and the **communication** is $polylog(T)$

[Fortnow-Rompel-Sipser88]:



Probabilistically Checkable Proofs



[Feige-Goldwasser-Lovasz-Safra-Szegedy91, Babai-Fortnow-Levin-Szegedy91, Arora-Safra92, Arora-Lund-Mutwani-Sudan-Szegedy92]

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

Succinct Interactive Arguments [Micali14]

Computationally Sound Proofs

$x \in L$

$P(w)$ V

$\xleftarrow{h}$

Compute PCP π **for** $x \in L$

$\xrightarrow{HT_h(\pi)}$ ← **Hash tree**

Sample PCP queries: q_1, q_2, q_3

$\xleftarrow{q_1, q_2, q_3}$

Compute corresponding openings o_1, o_2, o_3

$\xrightarrow[o_1, o_2, o_3]{\pi_{q_1}, \pi_{q_2}, \pi_{q_3}}$

Theorem: This protocol is computationally sound assuming h is collision resistant.

Succinct Interactive Arguments [Micali14]

Computationally Sound Proofs

$\boldsymbol{x \in L}$

$P(w)$ V

$\xleftarrow{\quad \boldsymbol{h} \quad}$

Compute PCP $\boldsymbol{\pi}$ for $\boldsymbol{x \in L}$

$\xrightarrow{\quad \boldsymbol{HT_h(\pi)} \quad}$ **Hash tree**

$\xleftarrow{\quad \boldsymbol{q_1, q_2, q_3} \quad}$

Sample PCP queries: $\boldsymbol{q_1, q_2, q_3}$

Compute corresponding openings $\boldsymbol{o_1, o_2, o_3}$

$\xrightarrow[\boldsymbol{o_1, o_2, o_3}]{\quad \boldsymbol{\pi_{q_1}, \pi_{q_2}, \pi_{q_3}} \quad}$

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

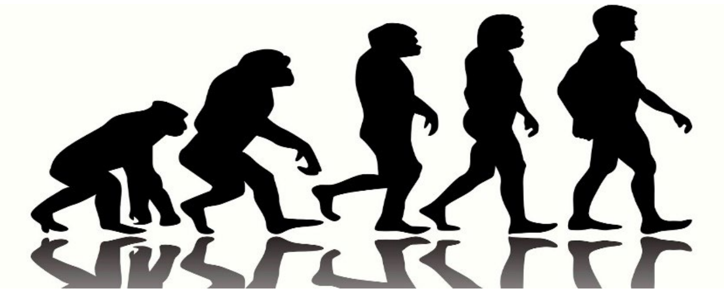
Classical proofs

(Zero-knowledge)
Interactive proofs

Multi-prover
interactive proofs

Probabilistically
checkable proofs (PCPs)

Succinct non-interactive arguments
(SNARGs)




THANK
YOU