Interactive Proofs (IP) and Zero Knowledge (ZK)

Last Time: Pairings

- $e: G_1 \times G_1 \to G_T$
  - Properties
    1. Bilinear
    2. Efficient
    3. Non-trivial
  - Applications
    - signatures
    - 3-party key exchange
    - more! (see lecture 11)

This time:

[1] Interactive Proofs

[2] Zero Knowledge

[3] Zk-proof for HAMCYCLE

What is a Proof?

Some one ("prover")
convinces someone else ("verifier")
that something ("a statement")
is true

formalizing statements:
define languages: $\mathcal{L} \subseteq \{0,1\}^*$
statements have form $x \in \mathcal{L}$

Examples
"15 is biprime"
$15 \in \{pq : \text{primes } p, q\}$

"Pythagoras' Theorem is true"

PYTHAG $\in$ {true theorems}

"ϕ is a satisfiable boolean formula"

$\phi \in$ {satisfiable formulas}

$\phi \in$ SAT $\quad \phi = a \wedge b \wedge \neg c$

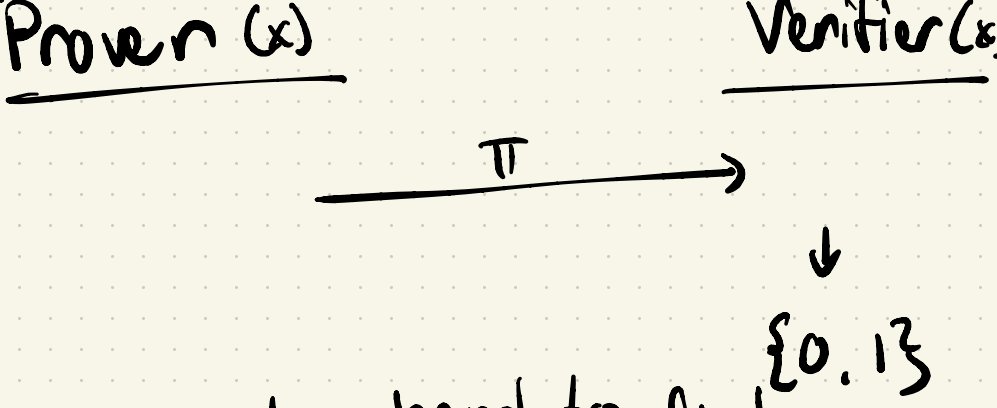
"ϕ is an unsatisfiable boolean formula"

$\phi \in$ coSAT $\quad \phi = a \wedge \neg a$

Observation some statements (e.g. $\phi \in$ SAT) are easy to prove others (e.g. $\phi \in$ coSAT) seem hard...

Short, conventional proofs: "NP"

Defn.



1. π may be hard to find.
2. It must be easy to check!
   - polytime, deterministic V, poly-length π

Complexity class "NP":

$L \in NP$ if $\exists\ V$ such that

completeness: $x \in L \rightarrow V(x, \pi) = 1$ for some π

soundness: $x \notin L \rightarrow V(x, \pi) = 1$ for <u>no</u> π

More formally:

$L \in NP \iff \exists$ deterministic, poly-time V.

$\forall x \quad x \in L \iff$

$\exists \pi \in \{0,1\}^{poly(|x|)}$

$V(x, \pi) = 1$

Example:

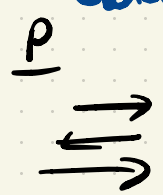
a. for SAT, π is the assignment.

b. we believe $coSAT \notin NP$

(coNP $\neq$ NP assumption)

Interactive Proofs (IP) [Micali Goldwasser]

With interaction?



⇒ Still NP (see HW)

With interaction + randomness?

- An IP, (P, V) is a pair of randomized machines
- V is efficient
- If $\langle P, V \rangle(x)$ denote's V's output

completeness:

$$\forall x \in L \quad \Pr_{P,V}[\langle P, V \rangle(x) = 1] \geq 2/3$$

"perfect" if ≥ 1

soundness:

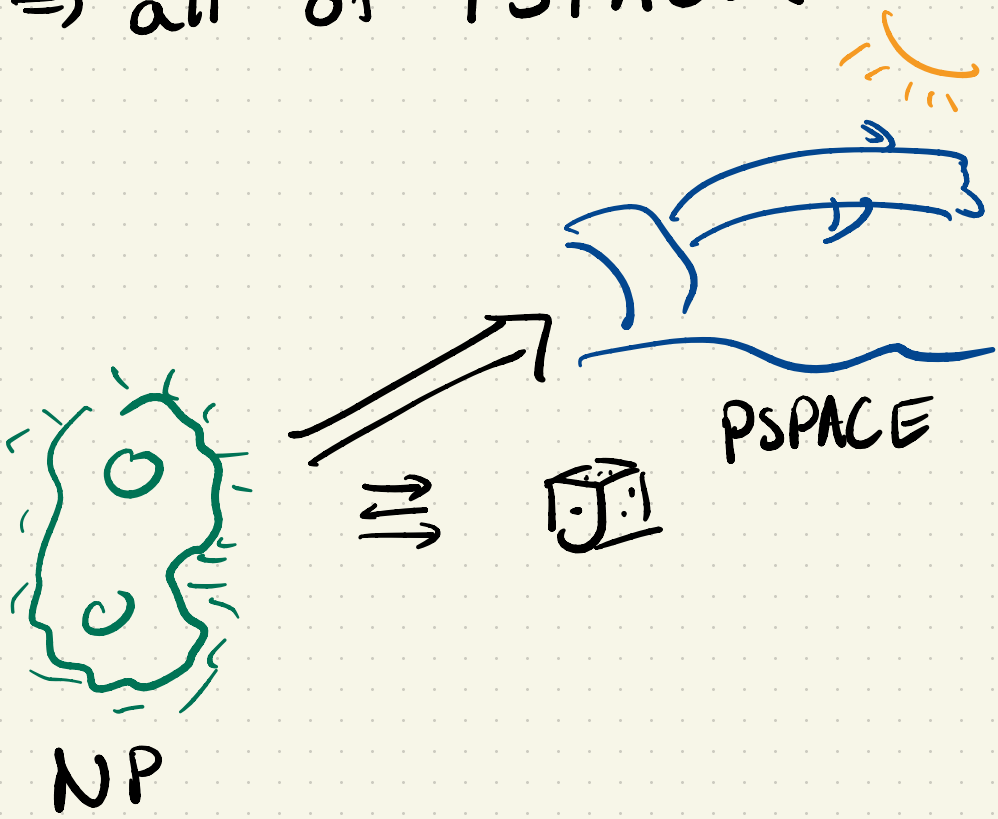
$$\forall x \notin L \quad \forall P^* \quad \Pr_{V}[\langle P, V \rangle(x) = 1] \leq \epsilon$$

"soundness error" (e.g. $\leq 1/3$). Repeat to boost.

Which Languages are in IP?

[Shamir '92] [Shen '92]

$\Rightarrow$ all of PSPACE!



Zero Knowledge Proofs

- IP where V learns

  $x \in \mathcal{L}$ and nothing else

Examples:

Prove a graph is 3-colorable without revealing the coloring ↗ today.

Prove a formula is SAT without revealing the assignment

Prove you know an unspent coin's id without revealing which coin (=> zcash)

Formalizing ZK

Idea: the "how was school?" principle?

Dad: "How was school"
Kid: "fine" ← Dad could have guessed this
→ if $\mathcal{V}$ can fake the transcript, protocol is ZK.

Defn: (P, V) is ZK if for all efficient V^*, there exists an effisient Sim

$$\{\text{View}_{V^*}[(P, V^*)(x)]\} \approx \{\text{Sim}(x)\}$$

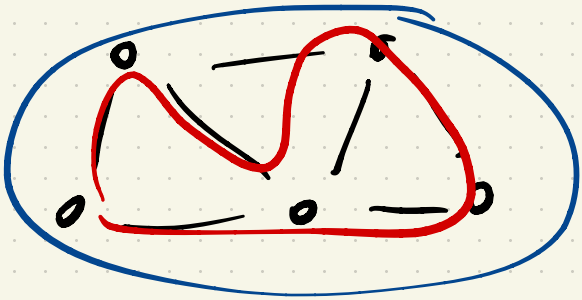
statistically, computationally, perfectly

tip: relax this defn by giving Sim more inputs.

⇒ We'll show all $\mathcal{L}$ ∈ NP have a ZK proof system!

HAMCYCLE

HAMCYCLE is the set of graphs with a hamiltonian cycle: a cycle that visits each vertex exactly once.



Vertices $V = \{1, 2, \ldots, n\}$

edeges represented by adjacency matrix:

$$G_{ij} = \begin{cases} 1 & i \sim j \\ 0 & \text{otherwise} \end{cases}$$

ham cycle is an $\ell \in \mathbb{N}^n$ without repeats, such that $\forall i \in \{1, 2, \ldots, n-1\}$ $G_{\ell_i, \ell_{i+1}} = 1$

HAMCYCLE $\in$ NP:

$\underline{P(G)}$ $\qquad\qquad\qquad\qquad$ $\underline{V(G)}$

$\ell \leftarrow ?$

$\xrightarrow{\ell}$

checks ℓ

↑ not a ZK proof unless P=NP

HAMCYCLE is NP-hard [Karp '72]

HAMCYCLE → directed HAMCYCLE

→ vertex cover → clique

→ SAT

→ NP [Cook-Levin '71]

So a ZK-proof for HAMCYCLE can be extended to <u>all</u> of NP.

* (w/ invertible reductions)

ZK Proof for HAMCYCLE

P(G, ℓ)	V(G)
$\sigma \xleftarrow{\$}$ permutations(V)	
$G' \leftarrow \sigma(G)$	
$c_{i,j} \leftarrow \text{Commit}(G'_{i,j})$	
$d_i \leftarrow \text{Commit}(\sigma(i))$ →	
	show commits ↓
	$b \xleftarrow{\$} \{0,1\}$
← b	
	show cycle
if $b=0$: open all commits	
if $b=1$: open the commits of G' which show the cycle $\sigma(\ell)$ →	- check all openings - if $b=0$: check σ is a permutations if $b=1$: check that openings form a HAMCYCLE

Analysis

Completeness:

1. σ is always a permutation
2. ℓ is always a cycle
3. commitments are always legit

Soundness:

if $G \notin$ HAMCYCLE, no permutation of it has a HAMCYCLE either

so the permutation is invalid

<u>or</u> the cycle is invalid

$\Rightarrow$ 50% chance of getting caught.

$\Rightarrow$ repeat to improve

Zero-knowledge:

Sim(G):

$b' \xleftarrow{\$} \{0,1\}$

if $b'=0$:

commit to random permutation of G

else:

commit to random permutation of an n-vertex cycle graph.

$b \leftarrow V^*$(commitments) ↕ $G' = I$

if $b' \neq b$: ← fixes distribution for V^* which does not chose $b \xleftarrow{\$} \{0,1\}$

restart (up to λ times) ← else FAIL

if $b=0$:

open all commits

if $b=1$:

open cycle commitments

(open $C_{i,\sigma(i)}$ for $i \in [n]$ and permutation I)

Need to show

$$\{\text{View}_{V^*}[\langle P, V\rangle(x)]\} \approx_c \{\text{Sim}(G)\}$$

$$D \approx D'$$

Sketch

$\{(G, (c_{1,1}, \ldots, c_{n,n}), (d_1, \ldots, d_n), b, \text{openings})\}$

- these are all $\approx$ in D, D' (conditioned on prior entries)
- need to show these are $\approx$ in D, D'
  - → use commitment hiding & $n^2 + n$ hybrids
  - → each hybrid replaces one commitment

More formally:

→ Assume commitment scheme is perfectly binding & computationally binding.

→ then Sim's $\{(G, \{c_{i,j}\}, \{d_i\})\}$ and the real distribution are identically distributed.

→ thus, b' and b are independent

→ thus, $Pr[b' = b] = 1/2$

→ thus, Sim fails w/ prob $\leq (1/2)^\lambda \leq negl(\lambda)$.

→ when Sim does not fail:

suffices to show that the openings are identically distributed.

→ if $b - b' = 0$:

both are commitments to a perm. of G_1

if $b = b' = 1$:

both are commitments to a random cycle sub-graph.

✓

- So Sim's output is identically distributed except w/ negl(λ) probability

→ "statistically indistinguishable"

Recap:

[0] NP-proofs

[1] Interactive Proofs

[2] IP: Zero knowledge

[3] ZK for all of NP

(via HAMCYCLE + commitments)

Rest of unit: other IP properties

Mon: Proof of knowledge

Wed.: Non-interactivity

Mon & Wed.: Succinctness