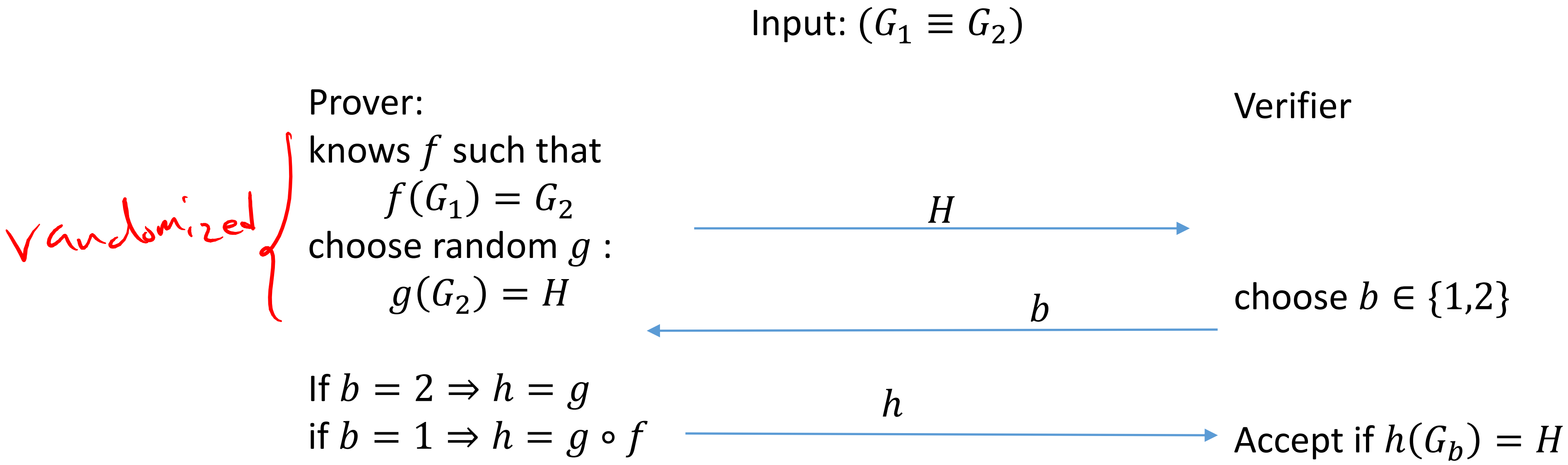
Computational Complexity

Mohammad Mahmoody

Session 27
April 2014

Zero-Knowledge Proofs

- ZK Proof for Graph Isomorphism:



Input: $(G_1 \equiv G_2)$

Prover:

knows f such that

$f(G_1) = G_2$

choose random g :

$g(G_2) = H$

randomized

If $b = 2 \Rightarrow h = g$

if $b = 1 \Rightarrow h = g \circ f$

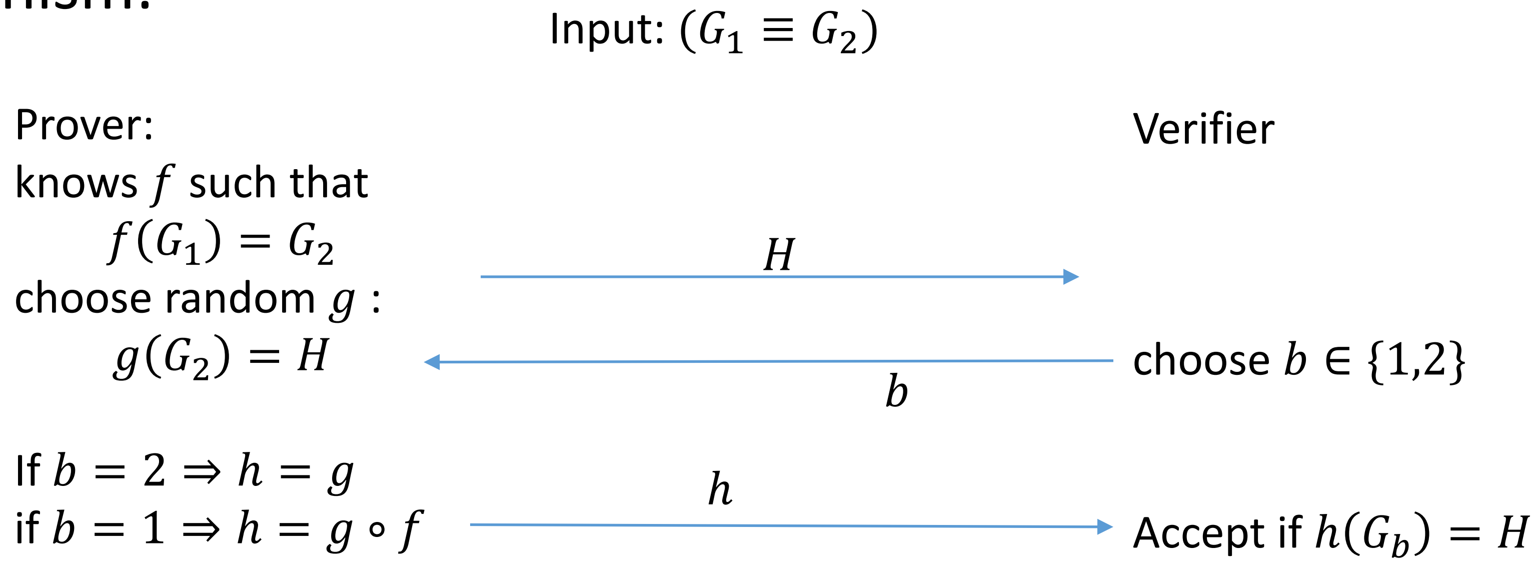
Verifier

choose $b \in \{1,2\}$

Accept if $h(G_b) = H$

Zero-Knowledge Proofs

- ZK Proof for Graph Isomorphism:



Input: $(G_1 \equiv G_2)$

Prover:
knows f such that
$f(G_1) = G_2$
choose random g :
$g(G_2) = H$

Verifier

H

choose $b \in \{1,2\}$

b

If $b = 2 \Rightarrow h = g$
if $b = 1 \Rightarrow h = g \circ f$

h

Accept if $h(G_b) = H$

- Soundness:
  if $G_1 \neq G_2$ for at least one of $b \in \{0,1\}$ no h exists.

$x = (G_1, G_2) \notin GI \Longrightarrow$

$\forall P^* \quad \Pr[\text{Ver rej}] \geq \frac{1}{2}$

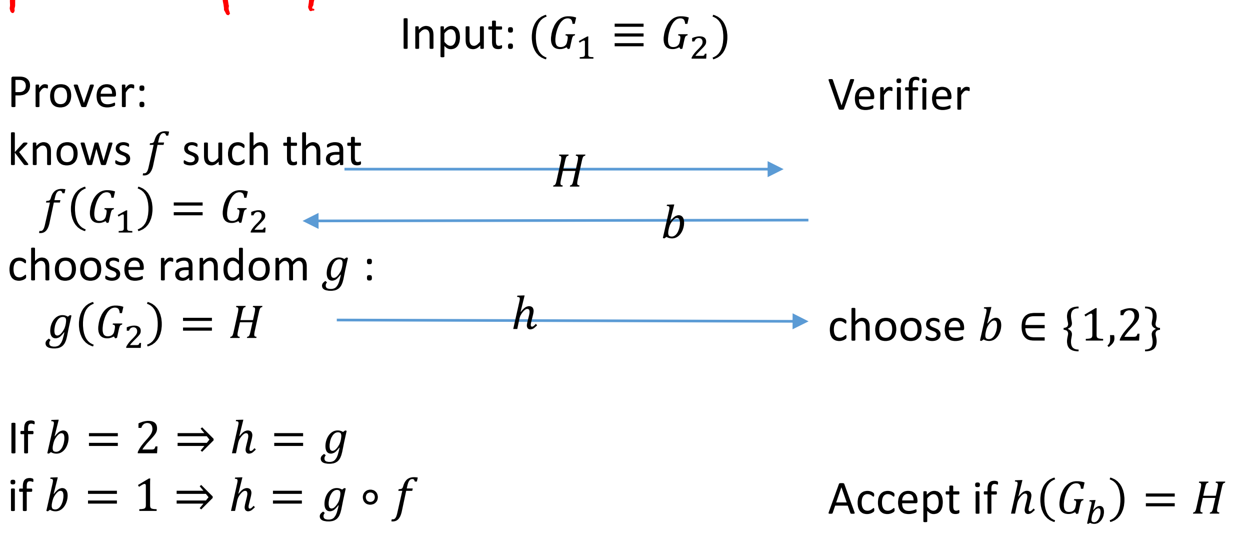
- Zero-Knowledge: What verifier gets to see?
- A random isomorphism for one of G_1 or G_2 of her choice!
- This is something she could generate on her own efficiently!

$b' \leftarrow X \rightarrow H \longleftrightarrow b$

Proof of Zero-Knowledge of GI Protocol

expected poly-time

- For any (perhaps malicious) verifier V^* there is an efficient "simulator" S that generates what V^* observes (called view).



Input: $(G_1 \equiv G_2)$

Prover:

knows f such that $f(G_1) = G_2$

choose random g : $g(G_2) = H$

If $b = 2 \Rightarrow h = g$

if $b = 1 \Rightarrow h = g \circ f$

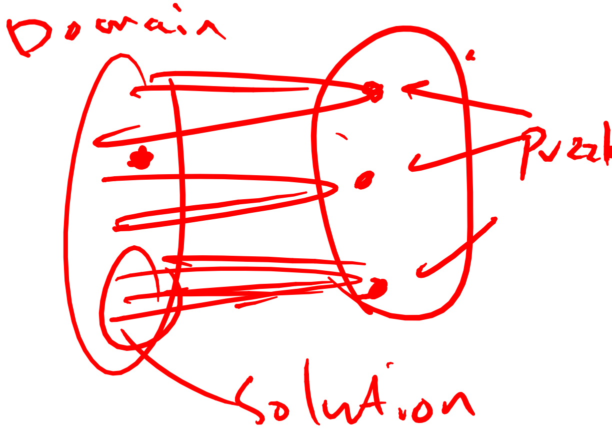
Verifier

choose $b \in \{1,2\}$

Accept if $h(G_b) = H$

- Proof: if $G_1 \equiv G_2$
  - S chooses $b' \in \{1,2\}$ at random and sends it to V^*
  - S sends a random isomorphism H of G_b to V^* and gets back b
  - If $b = b'$ (happens with prob. ½) S sends mapping of G_b to H
  - IF $b \neq b'$ simulator repeats the game
- Expected repetitions of game: 2

Zero-Knowledge for all of **NP**



- Goldreich-Micali-Wigderson 87:
  If “one-way functions” exist → all of NP has “zero-knowledge” proofs

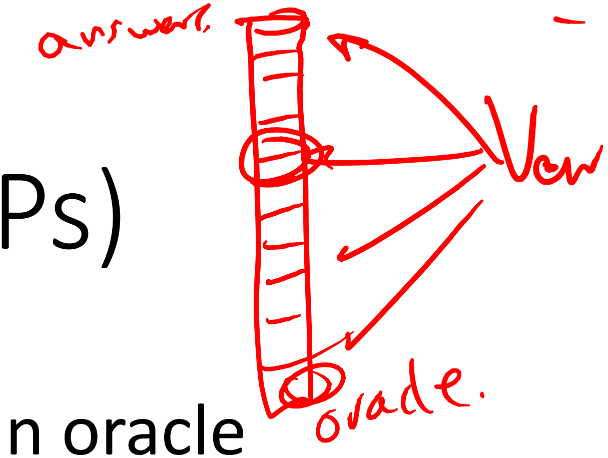
- An efficiently computable function $f: \{0,1\}^n \rightarrow \{0,1\}^n$ is one-way if:
  The probability that f could be “inverted” efficiently $\le 1/2$

- Formally: for every randomize efficient A if $x \leftarrow \{0,1\}^n, y = f(x)$ then

$$\Pr_{x}\left[\underbrace{f\big(A(y)\big) = y}_{\text{inverting}}\right] \le 1/2$$

- Note: if $\mathbf{P} = \mathbf{NP}$ no one-way function exists.

Probabilistic Checkable Proofs (PCPs)



- A form of interactive proofs in which the prover is an oracle

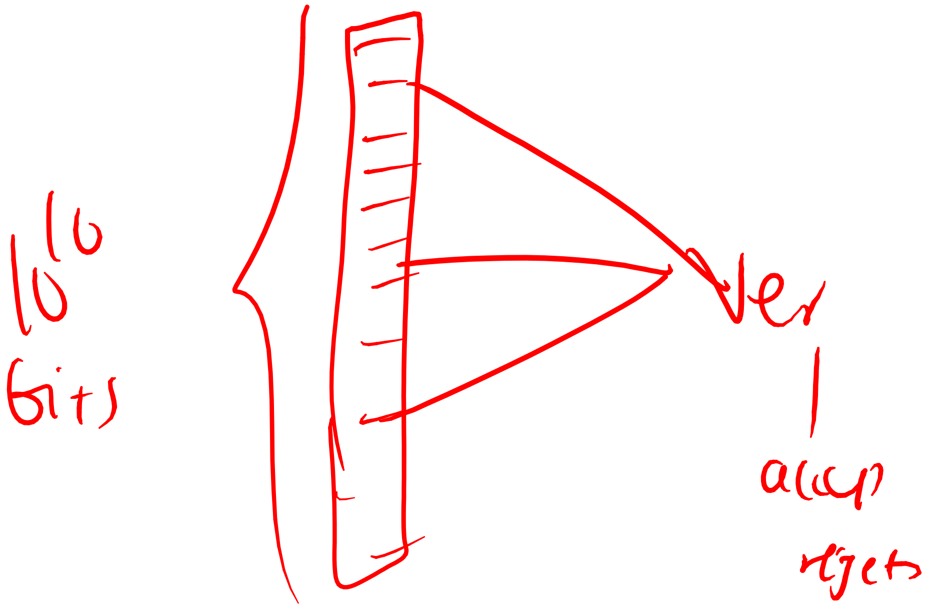
Equivalent to saying : a proof is "written" and efficient verifier "reads" it

L has a PCP

- Completeness: $x \in L \rightarrow \exists$ oracle O : $P[V^O(x) = 1] = 1$
- Soundness: $x \notin L \rightarrow \forall$ oracle O : $P[\underset{=1}{V^O(x)}] \leq \frac{1}{2}$

- PCP Theorem 1 [BFL90]: $\supseteq$ EXP $\supseteq$ PSPACE
  languages with PCPs = **NEXP** = languages with ≥ 2 provers

PCPs for **NP**



- PCPs in general are trivial for **NP**
- PCP Theorem 2 [ALMSS98]:
  Any L ∈ **NP** has a PCP in which verifier reads **only 3 bits** of “proof”
- Main applications: “hardness of approximation” (e.g. of MAX-3SAT)

Theom MAX-3AT hard to approx $(1 \pm \frac{1}{100})$