LECTURE 17

Note Title 4/11/2007

TODAY: • Complete $IP \supseteq PSPACE$

• Few words on Knowledge

———— x ————

Admin: - No lecture on Monday - holiday

- I'll be away - Swastik will lecture (1st of 3 lectures on PCP).

———— x ————

Review from last lecture

Polynomial Construction Sequence

$P_0, P_1, P_2, \ldots P_\ell$ $\qquad$ ℓ

field $= \mathbb{F}$

- Each polynomial of degree $\leq d$
- " # variables $\leq m$
- P_0 computable in time $\leq t$
- P_i computable with oracle for P_{i-1} with # calls $\leq w$ in time t

$\Rightarrow$ Given $\bar{a} = (a_1 \ldots a_m) \in \mathbb{F}^m$ & $b \in \mathbb{F}$

Can prove interactively that "$P_\ell(\bar{a}) = b$"

in time poly$(\ell, d, \mathbb{F}, m, t, w)$.

provided $|\mathbb{F}|$ large.

Typical Phase of interaction

$$\text{“} P_i(a^{(i)}) = b^{(i)} \text{ ?”}$$

Verifier	Prover

Prover: Compute $v_1 \dots v_w$ s.t. $P_i(a^{(i)})$ can be computed from $P_{i-1}(v_1 \dots v_w)$.

Compute curve C s.t. $C(j) = v_j$;

$h \leftarrow P_{i-1}(C(t))$

$$\xleftarrow{\quad C,\ h \quad}$$

- Verify $C(i) = v_i$
- Verify $b^{(i)} = f_i(h(1) \dots h(w))$

Pick $t_0 \in \mathbb{F}$ at random

$a^{(i-1)} = C(t_0)$; $b^{(i-1)} = h(t_0)$

$$\xrightarrow{\quad t_0 \quad}$$

Poly Construction Sequence for PSPACE

Given: machine M, x s.t. configurations of machine are s bits long.

Goal: To decide if initial config $a_1 \dots a_s$ leads to (unique) accepting config $b_1 \dots b_s$ in 2^s steps.

Define: Function

$$F_0, F_1 \dots F_s : \mathbb{F}^{2s} \to \mathbb{F}$$

$$F_i(\bar{\sigma} = (\sigma_1 \dots \sigma_s), \tau = (\tau_1 \dots \tau_s)) = 1 \quad \text{if } \sigma \Rightarrow \tau \text{ in } 2^i \text{ steps}$$

$$= 0 \quad \text{if } \sigma, \tau \in \{0,1\}^s \text{ o.w.}$$

$$= \text{arbitrary for } \sigma, \tau \notin \{0,1\}^s$$

① Can define F_0 s.t. it is a polynomial of degree $O(1)$ in each variable; and is computable in polytime.

② $$F_i(\bar{x}, \bar{y}) = \sum_{z \in \{0,1\}^s} F_{i-1}(\bar{x}, \bar{z}) \cdot F_{i-1}(\bar{z}, \bar{y})$$

$\uparrow$

- F_i computable from F_{i-1} ☺
- degree in each variable $\leq c$ ☺
- F_i needs 2^s values of F_{i-1} ☹

$\uparrow$

Need to fix this

Breaking Exponential Sum into Smaller Pieces.

$$\begin{tikzcd}
F_{i-1} \arrow[rrr] \arrow[d] & & & F_i \\
G_{i,s} \arrow[r] & G_{i,s-1} \arrow[r] & \cdots & G_{i,0} \arrow[u]
\end{tikzcd}$$

$$G_{i,s}(x,y,z) = F_{i-1}(x,z) \cdot F_{i-1}(z,y)$$

$$G_{i,j}(x,y,z_1 \ldots z_j) = G_{i,j+1}(x,y,z_1 \ldots z_j,0) + G_{i,j+1}(x,y,z_1 \ldots z_j,1).$$

The sequence

$G_{0,0}, G_{1,s}, G_{1,s-1} \cdots G_{1,0}, G_{2,s} \cdots G_{2,0} \cdots \quad G_{s,0}$

Over every large field is good.

degree $\leq 4 \cdot c \cdot s$

length $\leq O(s^2)$

width $= 2$

time $= O(s)$

variables $\leq 3s$

$\boxtimes$

(ZERO) KNOWLEDGE

- Classical theory of Information [Shannon]:
  - if I send you the outcome of n unbiased coin tosses, that gives you n bits of information.

- If Goal of a website is to spread information, then would have websites filled with coin tosses....

- What do intelligent entities "trade" when they exchange bits?

  Claim: Want "knowledge", not "information".

- **Claim**: Sequence of n random coin tosses has 0 bit of knowledge ; (vs. n bits of information).

- **(More interesting) Claim**: If I take Primes P, Q (n bits each) & send you N ($= P.Q$) then you don't know P (or Q).

- **Anecdotal Story***: Micali posed variant of above as question in problem set in U. Toronto in ~82 ; Cook responded "I don't know how to prove I don't know."

- Formal theory of knowledge emerged. [Goldwasser Micali Rackoff]

* Anonymous source; unreliable

Definition by Example :

- ZK proof of Graph Isomorphism

[Goldreich
Micali
Wigderson]

Given : G_1, G_2

Goal : Prover $\longleftrightarrow$ Verifier

- Completeness : if $G_1 \approx G_2$ then V must accept w.h.p.
- Soundness : if $G_1 \not\approx G_2$ then V must reject w.h.p
- Zero Knowledge : if $G_1 \approx G_2$ then V must not know isomorphism ; or learn anything other than this fact from conv.

Protocol : Now P Randomized !

V $\xleftarrow{\quad}$ G_1, G_2 $\xrightarrow{\quad}$ P

[say $G_1 = \pi_0(G_2)$]

Pick $i \in_U \{1,2\}$

$\pi \in_U S_n$

$H = \pi(G_i)$ $\longleftarrow$

$b \in_U \{1,2\}$

$\longrightarrow$

$\longleftarrow$

- π if $b = i$
- $\pi \circ \pi_0$ if $i = 1$, $b = 2$
- $\pi \circ \pi_0^{-1}$ if $i = 2$, $b = 1$

Claim : Sound : Know what this means

Claim : Zero-Knowledge : Don't know yet !

Definition of Zero-Knowledge

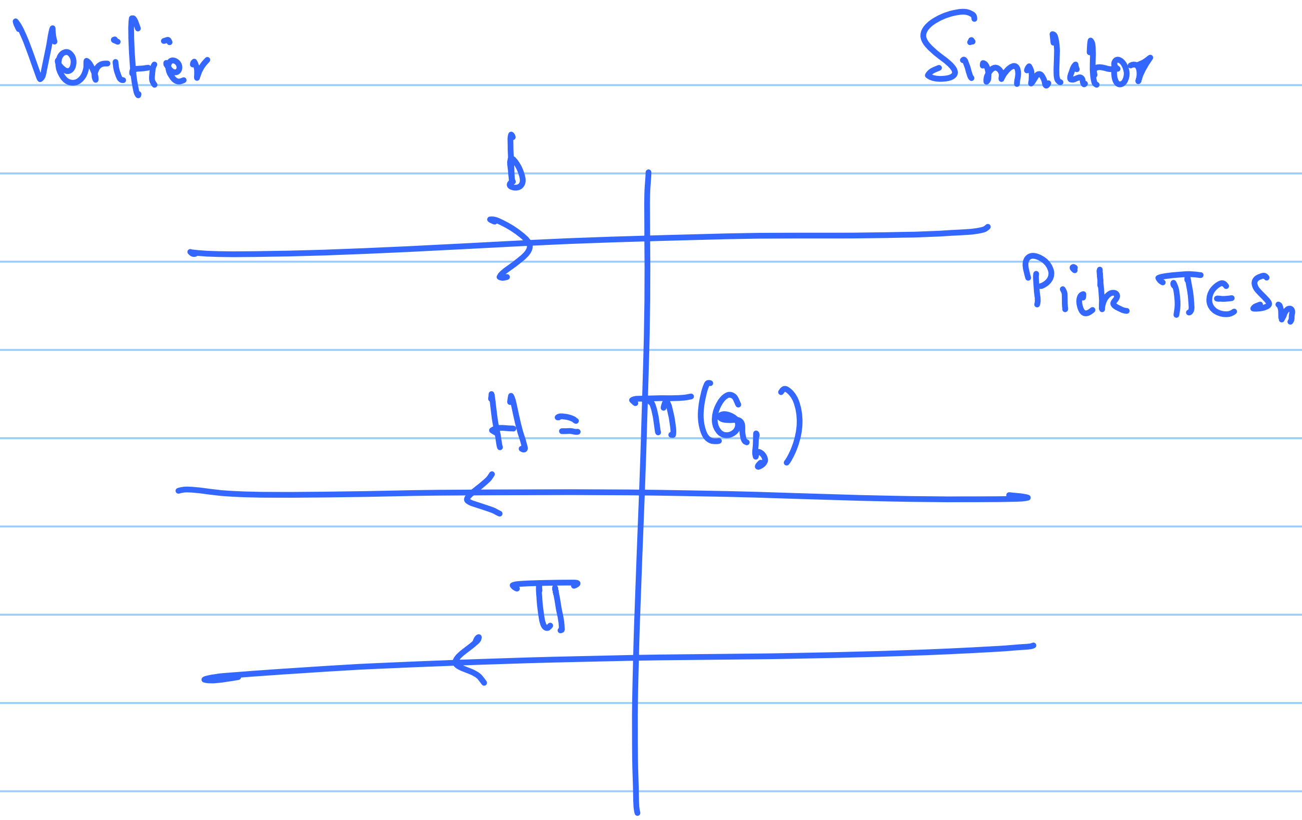
1. Fix verifier's coins R
2. Transcript is still random variable with distribution D_R

if Verifier can sample from D_R on its own, then Verifier gains no knowledge from prover.

"Simulator" $\equiv$ Sampler of D_R

[Perfect Zero Knowledge]

Simulator for GI



Output $\underbrace{(H, b, \pi)}$

exactly same distribution as with prover!
(for every $b \in \{0,1\}$.)

Sequence important for soundness!

Complexity - Theory of Knowledge

1. Can weaken definition of Zero-Knowledge.

(i) Simulator produces

$$D'_R \approx_\epsilon D_R$$

i.e, $\sum_x |D'(x) - D(x)| \le 2\epsilon$

"Statistical ZK" (SZK)

equivalently $\forall$ tests $T : \{0,1\}^n \to \{0,1\}$

$$\left| \Pr_{x \in D_R} [T(x) = 1] - \Pr_{x \in D'_R} [T(x) = 1] \right| \le \epsilon$$

(ii) Simulator produces D_R'' s.t.

$\forall$ polytime alg. A

$$\left| \Pr_{x \in D_R}[A(x) = 1] - \Pr_{x \in D_R''}[A(x) = 1] \right| \le \epsilon.$$

"Computational ZK" (CZK)

Results

- [GMR]: Definitions + protocols for NP-Comp. problems.
- [GMW]: GI $\in$ PZK $\subseteq$ SZK $\leftarrow$ statistical

IP $\subseteq$ CZK if o.w.f. exist.

$\uparrow$

cryptographic

- [Fortnow, Boppana Håstad]:

$$SZK \subseteq \text{co-}AM$$

$\Rightarrow$ $\Pi \in SZK$ can't be NP-hard unless PH collapses

- [Okamoto]:

$$SZK = \text{co-}SZK$$

- [Sahai-Vadhan]; [Goldreich-S-V] etc:

SZK complete problems.

E.g. $SD = \left\{ (C_1, C_2) \;\middle|\; \begin{array}{l} C_1, C_2 : \{0,1\}^n \to \{0,1\}^m \\ \text{circuits poly size} \\ \{C_1(x)\} \not\approx_{\frac{1}{3}} \{C_2(x)\} \end{array} \right\}$

Easy: $SD \subseteq SZK$

Harder: $SD \leq \overline{SD}$.

$\Big((C_1, C_2) \longrightarrow (D_1, D_2)$

s.t. $C_1 \approx_\epsilon C_2 \iff D_1 \not\approx_\epsilon D_2$! $\Big)$

Recently rich theory of CZK

$L_1 \in CZK$ & $L_2 \in CZK$

$\Rightarrow L_1 \cup L_2 \in CZK$. [Vadhan].