LECTURE 16

Note Title

TODAY : - WORST-CASE to Avg. Case Reduction of Permanent

- #P $\subseteq$ IP

- Towards IP = PSPACE

WORST-CASE TO Avg. Case Reduction for Permanent

- $\text{Permanent}\begin{pmatrix} y_{11} & \cdots & y_{1n} \\ \vdots & & \\ y_{n1} & \cdots & y_{nn} \end{pmatrix} = \sum_{\pi} \prod_{i} y_{i\pi(i)}$

- Permanent is a degree n polynomial in n^2 variables.

- **Key Observation:** [Beaver Fergenbaum ; Lipton]

$f(x_1, \ldots x_n)$ is poly of degree d in n variables

$\Rightarrow \forall\ a_1 \ldots a_n,\ b_1 \ldots b_n$

$$f_{\bar{a},\bar{b}}(t) = f(a_1 + t \cdot b_1, \ldots a_n + t \cdot b_n)$$

$$= \text{poly of deg. } d \text{ in } 1 \text{ variable.}$$

- **Interpolation:** Can compute $f_{a,b}(0) = f(a_1 \ldots a_n)$ from

$$f(a_1 + b_1 \ldots a_n + b_n) = f_{a,b}(1)$$
$$f(a_1 + 2b_1, \ldots a_n + 2b_n) = f_{a,b}(2)$$
$$\vdots$$
$$f(a_1 + (d+1)b_1, \ldots, a_n + (d+1)b_n) = f_{a,b}(d+1)$$

- But in a field containing $1, 2, \ldots d+1$

  $\bar{a} + i\bar{b}$ is random ind. of $\bar{a}$

  when $\bar{b}$ is chosen

  at random.

Conclusion:

Can compute $f(\bar{a})$ from values of f

at random places.

... Now lets do this formally.

Given: ① Oracle / Program / Algorithm "A" such that

$$\Pr_{R \in_R \mathbb{Z}_p^{n \times n}} [A(R) = \text{Perm}(R)] \geq 1 - \delta ;$$

② Matrix $M \in \mathbb{Z}_p^{n \times n}$

Goal: Compute $\text{Perm}(M)$

Alg:

- Pick $R \in_U \mathbb{Z}_p^{n \times n}$
- let $y_i = A(M + iR)$ $\quad i = 1 \ldots n+1$
- let $h(t)$ be poly of deg. n s.t.

  $h(i) = y_i \quad \forall\ i = 1 \ldots n+1$;
- Output $h(0)$;

Analysis: Assume $p > n+1$

1. $\forall i \in \{1 \ldots n+1\}$ $\Pr_R \left[y_i \neq \text{Perm}(M+iR) \right] \leq \delta$

   [Since $M+iR$ is random]

2. $\Pr \left[\exists i \text{ s.t. } y_i \neq \text{Perm}(M+iR) \right] \leq (n+1)\delta$

3. if $\forall i \quad y_i = \text{Perm}(M+iR)$ then

   $h(t) = \text{Perm}(M + t \cdot R)$ [both are deg. n polys & agree at $n+1$ places]

   & so $h(0) = \text{Perm}(M)$

Conclude: Answer correct w.p. $1 - (n+1)\delta$.

(for every M)

History: From Average-case hardness to IP = PSPACE

① [Lipton '89] Permanent is random self-reducible

② [Blum, Luby, Rubinfeld '90] If a function f is random-self-reducible & downward self-reducible, then correctness of "program" P (= oracle P) computing f can be checked

③ [Nisan '90 (email)] Permanent is checkable ($\Rightarrow$ has 2-prover IP).

④ With much more work [Lund, Fortnow, Karloff, Nisan] $\#P \subseteq IP$

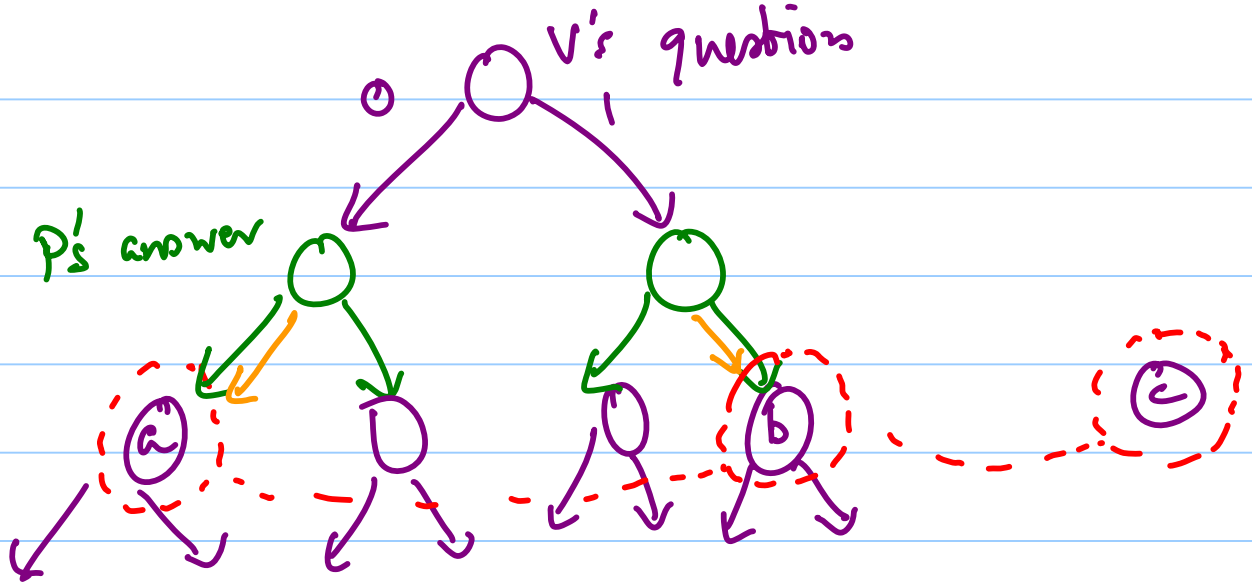
⑤ [Shamir '90]: IP = PSPACE

#P ⊆ IP

- Given what we know, should already be able to show [Nisan '90]'s result above.

- To do better:
  - Need a way of "combining" queries
  - Currently, reduce one worst-case instance to n random instances.
  - for IP need to reduce n (or at least 2) worst-case instances to 1 (not necessarily random) instance

(see picture on next page)



V would like to know both questions would lead to accepting answers;

& would be nice to combine the two purple children ^{a,b} into new "purple" child c that would (w.h.p.) reject if either a or b reject.

Key insight: This combining can be done for algebraic problems!

Combining w questions

Given: f degree d, n variate poly over $\mathbb{Z}_p$

& $x_1, x_2, \ldots x_w \in \mathbb{Z}_p^n$

& $a_1, a_2 \ldots a_w \in \mathbb{Z}_p$

Verifier's task:

Verify that $\left(f(x_1) = a_1\right)$ AND

$\left(f(x_2) = a_2\right)$ AND

$\vdots$

$\left(f(x_w) = a_w\right)$

Protocol: To reduce to one question of the form y, b

"Is $f(y) = b$?"

(will solve this using curves)

Curves in n-dimensional space

Curve $C : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p^n$

$= C^{(1)} \dots C^{(n)} : \mathbb{Z}_p \to \mathbb{Z}_p$

$C(t) = \langle C^{(1)}(t), \dots C^{(n)}(t) \rangle$

Degree of Curve:

$$= \max_i \{ \deg C^{(i)} \}$$

Curve C **passes through** $x \in \mathbb{Z}_p^n$ if

$\exists\, t \in \mathbb{Z}_p$ s.t. $x = C(t)$.

Interpolation: $\exists$ deg w curve C passing through $x_1 \dots x_w$

Protocol:

- Pick (any) degree w curve C passing through $x_1 \dots x_w$
- Ask prover for $f \circ C$ (poly of degree $d \cdot w$) say prover replies with h
- ① for every t, i s.t. $C(t) = x_i$ verify $h(t) = a_i$
- ② Pick $\alpha \in \mathbb{Z}_p$ at random & let $C(\alpha) = y$, $h(\alpha) = b$

Analysis - if $f(x_i) = a_i \quad \forall i$,

prover should respond with $h = f \circ C$.

- if $\exists i$ s.t. $f(x_i) \neq a_i$:

- Case 1: $h = f \circ C$

then for some t [the one for which $C(t) = x_i$]

$$h(t) = f \circ C(t) = f(x_i) \neq a_i$$

so verifier rejects.

- Case 2: $h \neq f \circ C$

for random α $\left[\text{w.p.} \geq 1 - \frac{d \cdot w}{p}\right]$

$$h(\alpha) \neq f \circ C(\alpha)$$

$$\Leftrightarrow \quad b \neq f(y)$$

#P ⊆ PSPACE

- Let $P_n(x_{11} \dots x_{nn})$ denote $n \times n$ perm.
- Given: M, a protocol to verify "$P_n(M) = a$"

- **Verifier**: Let $M_1, M_2, \dots M_n$ denote $(n-1) \times (n-1)$ minors of M so that

$$P_n(M) = \sum_{i=1}^{n} m_{1i} \cdot P_{n-1}(M_i)$$

- Viewing $M_1 \dots M_n \in \mathbb{Z}_p^{(n-1)^2}$ pick C of deg n passing through $M_1 \dots M_n$
- Ask prover for $P_{n-1} \circ C$; say response $= h$

- ① Let t_i be such that $C(t_i) = M_i$

  Verify $a = \sum M_{ii}\, h(t_i)$;

② Pick $\alpha \in \mathbb{Z}_p$ at random ;

let $N = C(\alpha)$;

& $b = h(\alpha)$;

Verify (recursively)

"$P_{n-1}(N) = b$"

Analysis: Easy given the rest ;

PSPACE? Idea develop sequence concept

$P_1, P_2, \ldots P_{n-1}, P_n$ so as to apply to PSPACE also.

Key elements: P_i low-degree & easy to compute from P_{i-1}.