Today

Interactive Proofs (Part II)

- $P^{\#P} \subseteq IP$
- $IP \subseteq PSPACE$

CS5.203.1 Computational Complexity

- Lecture # 23 (10 May 21)

Instructor: Prahladh Harsha

Recap from last time

Public-coins IP/AM protocol for computing the permanent

$A = (a_{ij})_{i=1, j=1}^{n}$ $\quad a_{ij} \in \mathbb{F}$ - finite field

$|\mathbb{F}| > 2n^3$.

(field is large enough)

$\text{Perm} = \{ (\mathbb{F}, n, A, \alpha) \mid \mathbb{F}$ - finite field. A - $n \times n$ matrix $A \in \mathbb{F}^{n \times n}$ $\text{perm}(A) = \alpha \}$.

$$\text{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

$$= \sum_{i=1}^{n} a_{1,i} \, \mathrm{Perm}(A_{1,i})$$

where $A_{1,i}$ – refer to the $(n-1) \times (n-1)$ matrix obtained by removing the 1^{st} row & i^{th} column.

Candidate IP-protocol:

$$(A, \alpha)$$

$$V \qquad\qquad\qquad P$$

$$V \xleftarrow{\alpha_1, \ldots \alpha_n} P$$

P: $\alpha_1, \ldots \alpha_n$

$\alpha_i = \mathrm{Perm}(A_{1,i})$

1. Checks if $\alpha = \sum_{i=1}^{n} a_{1,i} \cdot \alpha_i$

$i \in_R [n]$

$$V \xrightarrow{i} P$$

$$(A_{1,i}, \alpha_i)$$

Reduced the problem to a $(n-1) \times (n-1)$ setting to check if $\mathrm{perm}(A_{1,i}) = \alpha_i$

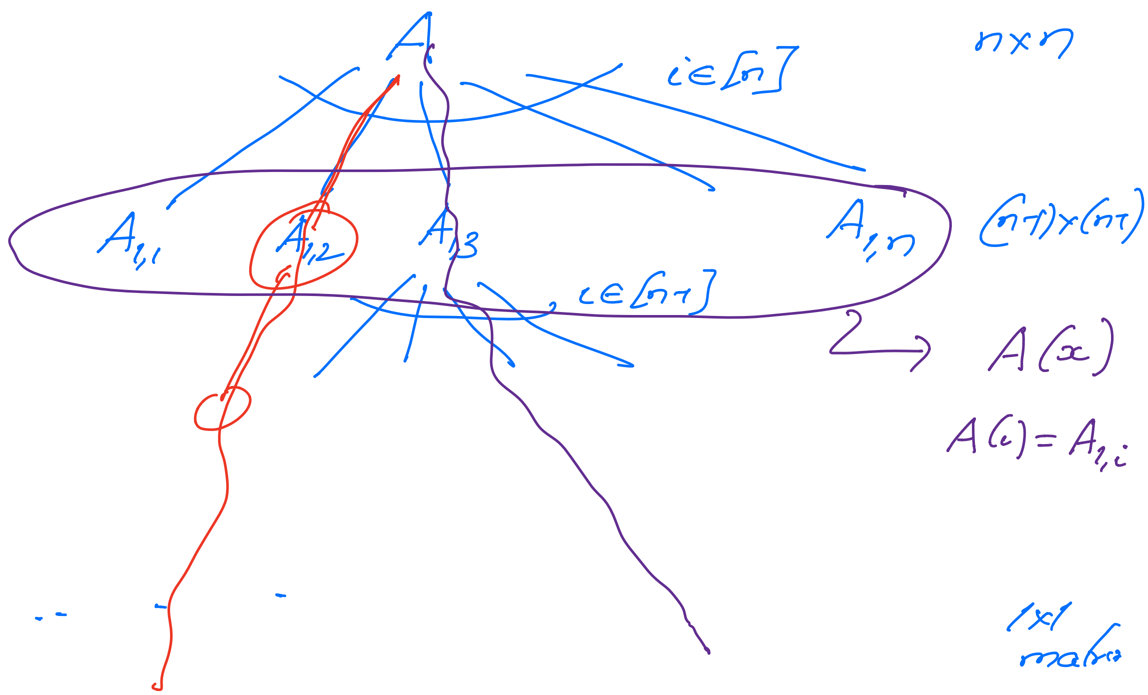
Qn: Is this a valid IP-protocol?

Efficiency ✓

Completeness ✓

Soundness: ???

Suppose $perm(A) \neq \alpha$.



Prover could cheat on just one of the paths.

Prob that the verifier catches the cheating prover $= \frac{1}{n!}$

Protocol is not sound.

Idea: Interpolate the n $(n-1)\times(n-1)$ matrices $A_{1,i}$'s to obtain a single matrix $A(x)$

s.t. $A(i) = A_{1,i}\ \forall i \in [n]$

& ask prover to provide $\mathrm{perm}(A(x))$

$$\underbrace{\begin{bmatrix} & & \\ & i,j & \\ & & \end{bmatrix}}_{A_{1,1}} \quad \underbrace{\begin{bmatrix} & \cdot\ \cdot & \\ & i,j & \\ & & \end{bmatrix}}_{A_{1,2}} \quad \cdots \quad \underbrace{\begin{bmatrix} & & \\ & i,j & \\ & & \end{bmatrix}}_{A_{1,n}}$$

$A^{(i,j)}(x) \leftarrow$ Unique poly of deg $\leq n$

s.t. $A^{(i,j)}(k) = A_{1,k}^{(i,j)}$

$A(x) = \left[A^{(i,j)}(x)\right]_{i,j=1}^{n-1,\,n-1} \rightsquigarrow$ polynomial entries of deg at most n each

$p(x) = \mathrm{perm}(A(x))$ ① univariate poly of deg $< n(n-1)$

② $p(i) = \mathrm{perm}(A(i)) = \mathrm{perm}(A_{1,i})$

Modified IP-protocol for permanent

(A, α)

V $\qquad\qquad\qquad\qquad$ P

Construct $A(x)$

s.t (1) deg $< n$

(2) $A(i) = A_{1,i}$ $\forall i \in [n]$

(3) Compute $p(x) = \text{perm}(A(x))$

$$V \xleftarrow{\;p(x)\;} P$$

(ie, $n(n-1)$ field elements)

If $n > 1$

(1) Checks

$$\alpha = \sum_{i=1}^{n} a_{1,i} \cdot p(i)$$

$\beta \in_R \mathbb{F}$

$$V \xrightarrow{\;\beta\;} P$$

Reduced to $\underbrace{(A(\beta), p(\beta))} \in$ Perm

Efficient ✓

Completeness:

If $\text{Perm}(A) = \alpha$, then there exists an honest prover P s.t

$$\Pr_{\beta_1 \dots \beta_n}\left[(V_\alpha \leftrightarrow P)(A, \alpha; \bar{\beta}) = acc\right] = 1$$

Soundness:

Suppose $Perm(A) \neq \alpha$

We need to show for all provers P^*

$$\Pr_{\beta_1 \dots \beta_n}\left[(V_\alpha \leftrightarrow P^*)(A, \alpha; \bar{\beta}) = acc\right] \leq \frac{1}{2}.$$

Fix a prover P^*, and the first message of P^* (i.e. uni poly p).

Case (i) $p(x) \equiv perm(A(x))$

Case (ii) $p(x) \not\equiv perm(A(x))$ }.

<u>Case (i)</u> $\alpha \neq \sum a_{1,i} \cdot perm(A_{1,i})$

$$= \sum a_{1,i} \cdot perm(A(i))$$

$$= \sum a_{1,i} \cdot p(i)$$ / Verifier rejects.

Case (ii) $p(x) \not\equiv perm(A(x))$

$$\Pr_{\beta}\left[p(\beta) = \mathrm{perm}(A(\beta))\right] \leq \frac{\deg}{|\mathbb{F}|}$$

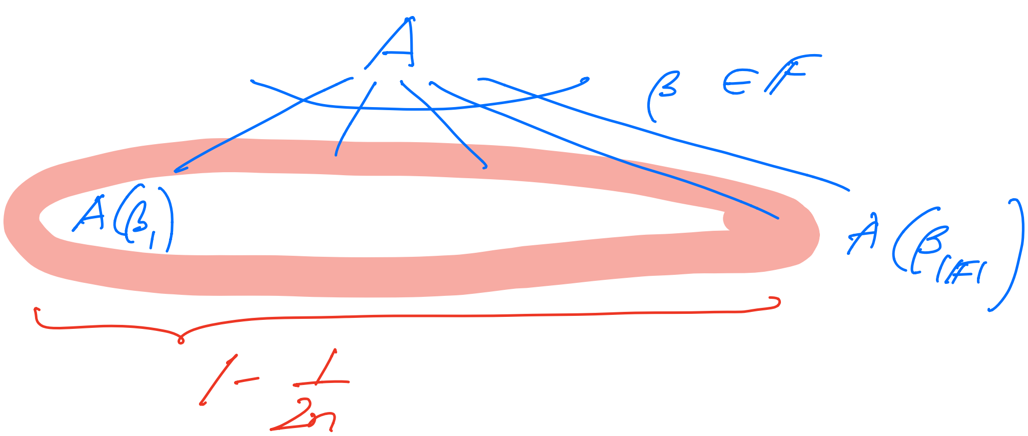
$$\leq \frac{1}{2n} \quad \text{if } |\mathbb{F}| \geq 2n^3$$

$$\Pr\left[\text{Prover is not caught}\right] \leq \frac{1}{2n} + \frac{1}{2n} + \dots + \frac{1}{2n}$$

$$\leq \frac{1}{2}. \qquad \boxtimes$$

Conclusion:

$PH \subseteq P^{\#P} \subseteq IP$

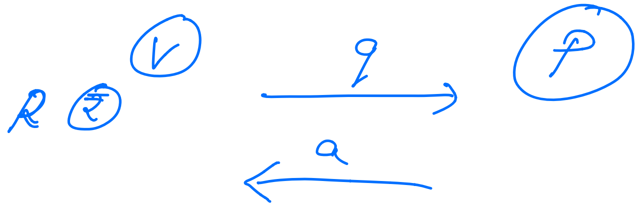


Upper Bound for IP.

$IP \subseteq ???$

Baby Case:

$x \overset{?}{\in} L$



$V(x, R, a) =$ acc/rej

Prover wants to answer s.t.

$\Pr_R[(V \leftrightarrow P)(x;R) = acc]$

is maximized.

Prover can (in PSPACE) find for every qn q, the ans a that causes the verifier to accept.

Concl: 1-round $IP \subseteq PSPACE$

$>$ 1-round, can run over all possible transcripts & det acc prob.

↪ PSPACE

$IP \subseteq PSPACE$

In fact, $PSPACE \subseteq IP$

Last 2 this lecture: $P^{\#P} \subseteq IP$

(by giving an IP-protocol for permanent)

Will give an alternate proof of $P^{\#P} \subseteq IP$

(by giving an IP-protocol for #SAT)

[And then extend this IP-protocol to TQBF]

$\#SAT_D = \{(\varphi, k) \mid \#SAT(\varphi) = k\}$

$\hookrightarrow \varphi$ - 3CNF formula.

Theorem: $\#SAT_D \in IP$

$\varphi = C_1 \wedge C_2 \ldots \wedge C_m$

Conjunction of m clauses w/ 3 literals each.

$$S_0(\cdot) = \sum_{x_1 \in \{0,1\}} \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \varphi(x_1 \ldots x_n) = k \quad \ldots (*)$$

Partial Summation

$$S_i(x_1 \ldots x_i) = \sum_{x_{i+1} \in \{0,1\}} \sum_{x_{i+2} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \varphi(x_1 \ldots x_n)$$

$\forall i:$

$$S_i(x_1 \ldots x_i) = S_{i+1}(x_1 \ldots x_i, 0) + S_{i+1}(x_1 \ldots x_i, 1)$$

$$S_n(x_1 \ldots x_n) = \varphi(x_1 \ldots x_n)$$

(φ, k)

"$S_0(\cdot) = k$"

V $\qquad\qquad$ P

$$V \xleftarrow{k_0,\, k_1} P$$

$S_1(0) = k_0$, $S_1(1) = k_1$

Checks $k = k_0 + k_1$

$b \in_R \{0,1\}$

$$V \xrightarrow{b} P$$

"$S_1(b) = k_b$"

(Reduces # var by 1
recurse).

There is a cheating prover that can cause the verifier to accept w/ probability $\geq \frac{1}{2^n}$

$$\varphi \xrightarrow{\text{Arithmetization}} P_\varphi$$

formula   polynomial

$$\{0,1\} \subseteq \mathbb{F}$$

s.t $\forall (b_1 \ldots b_n) \in \{0,1\}^n$

$$P_\varphi(b_1 \ldots b_n) = \varphi(b_1 \ldots b_n).$$

Arithmetization

(Define Inductively).

① $\varphi =$ constant $0/1$

$$P_\varphi = \text{constant } 0/1$$

② $\varphi = x_i$ (variable)

$$P_\varphi = x_i$$

③ $\varphi = \neg \psi$ (negation)

$$P_\varphi = 1 - P_\psi$$

(4) $\varphi = \psi_1 \wedge \psi_2$ (conjunction)

$P_\varphi = P_{\psi_1} \cdot P_{\psi_2}$ (poly multiplication)

(5) $\varphi = \psi_1 \vee \psi_2$ (disjunction)

$= \overline{\overline{\psi_1} \wedge \overline{\psi_2}}$

$= 1 - (1 - P_{\psi_1}) \cdot (1 - P_{\psi_2})$

φ – 3CNF formula

P_φ

$\deg(P_\varphi) =$

$\deg(\text{clause}) \leq 3$

$\deg(P_\varphi) \leq 3m$

Arithmetization of φ : P_φ

(1) $\deg(P_\varphi) \leq 3m$

(2) $\forall b_1 \ldots b_n \in \{0,1\}^n$

$P_\varphi(b_1 \ldots b_n) = \varphi(b_1 \ldots b_n)$

Next lecture: Use above arithmetization to show $\#SAT_D \in IP$