Today
- Interactive Proofs
  * - Formal defn & properties
  * $P^{\#P} \subseteq IP$.

Lecture 21
Computational Complexity
(17 Apr, 2020)
Instructor: Prahladh Harsha

Recall: Informal defn of Interactive Proofs & GNI $\in$ IP.

Formal Defn:

Recall defn NP:

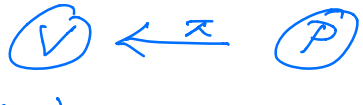
$L \in NP$ if $\exists$ efficient polynomial time verifier V s.t

(1) Efficiency:
V is poly in $|x|$

(2) Completeness:
$x \in L \Rightarrow \exists \pi, V(x,\pi)$ – acc

(3) Soundness:
$x \notin L \Rightarrow \forall \pi, V(x,\pi)$ – rej

$x \in L$



$V(x,\pi)$ = acc/rej

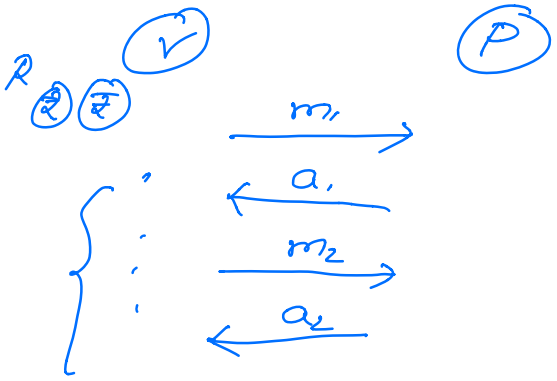
Extend this defn to Interactive Proofs.

- First define a Verifier & Proof

V: On input x & randomness R

Next message fn
$V(x, R, (i)\text{transcript}) \rightarrow$ next msg or acc/rej

$x \in L$



$V(x, R, \text{transcript}) = \text{acc/rej}$

Prover is a similar next message fn (but w/ no efficiency restrictions.
(Prover is deterministic)

$(V \leftrightarrow P)(x; R) = \text{acc/rej}$

$L \in IP$ if $\exists$ an efficient randomized verifier V & a def. prover P s.t

(1) Efficiency: V runs in time $\text{poly}(|x|)$

(2) Completeness:

$x \in L \Rightarrow \Pr_R[(V \leftrightarrow P)(x, R) = \text{acc}] \geq 2/3$

(3) Soundness

$x \notin L \Rightarrow \forall P^*$ (not necessarily the honest P)

$\Pr_R[(V \leftrightarrow P^*)(x, R) = \text{acc}] \leq 1/3$

Graph Non-Isomorphism:

$GNI = \{(G_0, G_1) \mid G_0 \not\cong G_1\}$

Obs: (i) $GNI \in coNP$ (Non-membership giving the iso.).

(ii) GI is not known to be either in P or NP-complete.

(G_0, G_1)

V P

If $|V(G_0)| \neq |V(G_1)|$
then rej
$n = |V(G_0)| = |V(G_1)|$

$b \in_R \{0,1\}$
$\sigma \in_R S_n$
$H \leftarrow \sigma(G_b)$ ——H——> Find G_c s.t $G_c \cong H$

<——c——

If $b = c$ - accept
else - rejects

[Private Coins Protocol]

Remarks:

(1.) The error can be reduced to any $\frac{1}{2^{O(n)}}$ by just repeating the protocol (in sequence) n times.

[An alternate repetition is doing them in parallel. Also works, but requires proof
(Round complexity is maintained if one repeats 1/ε).

(2) Prover can be probabilistic.
The prover can use its power to figure the best random coins.

(3) Private vs Public Coins:
Private: Verifier does not reveal randomness
Public: Verifier reveals random coins. (round by round)
Surprisingly for every private-coins protocol, there is an public-coins protocol.

(4) Perfect Completeness: YES, the prob is 1 & not 2/3.
(also true). [Surprising].

(5) Perfect Soundness: Can soundness error be reduced to 0? No
Prover can just send the random coins that cause V_c to accept

making the protocol deterministic

def-IP = NP

Parameters:

- Public vs. Private (Private coins — Interactive Proofs IP
- Public Coins — Arthur-Merlin proof systems AM
- Round Complexity
  eg: GNI — 1 round private coins protocol.
  - can be as large polynomial.
- Perfect Completeness

Public Coin Protocol for computing the Permanent

$A = (a_{ij})_{\substack{i=1 \\ j=1}}^{n}$ $\quad a_{ij} \in \mathbb{F}$ $\left(|\mathbb{F}| \geq \frac{1}{2n^3}\right)$

$\mathbb{F}$ - finite field.

$$Perm_{\mathbb{F}} = \{ (A, \alpha) \mid perm(A) = \alpha \}.$$

$A \in \mathbb{F}^{n \times n}, \alpha \in \mathbb{F}$

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

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

Candidate Protocol:

(V) $\xleftarrow{(A, \alpha)}$ (P)

Checks if $\alpha = \sum a_{1,i} \cdot \alpha_i$

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

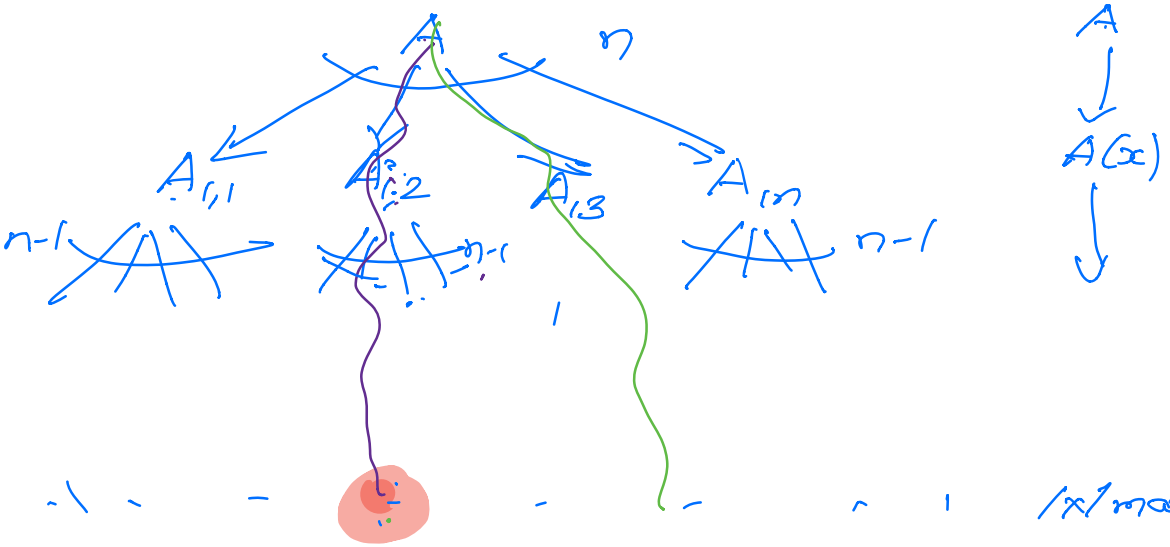
$\alpha_1, \ldots \alpha_n$

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

$i \in_R [n]$

$\xrightarrow{i}$

reduced the problem to check $(A_{1,i}, \alpha_i) \in Perm$



Prover could cheat on just one of the $n!$ paths $\Rightarrow$ the verifier will detect this only $\frac{1}{n!}$ of the time

$x \notin L \Rightarrow \Pr[(V \leftrightarrow P^*)(A, x; R) = \text{acc}] \leq 1 - \frac{1}{n!}$

very close to 1.

$A_{1,i}$ = matrix formed by removing 1st row & i^{th} column.

We will interpolate over the i's to come up with a matrix $A(x)$ — a $(n-1)\times(n-1)$ matrix of polynomial entries, s.t each entry has deg $< n$.

s.t

$A(i) = A_{1,i}$

$$\begin{bmatrix} \ddots \\ A_{1,1} \end{bmatrix} \quad \begin{bmatrix} \vdots \\ A_{1,2} \end{bmatrix} \quad \cdots \quad \begin{bmatrix} \vdots \\ A_{1,n} \end{bmatrix}$$

$A(x)$ entries are poly

$$\begin{bmatrix} \textcircled{\text{deg } n\text{ poly}} & \cdots \\ & A(x) \end{bmatrix}_{n-1 \times n-1}$$

$A(x)$ — $(n-1)\times(n-1)$ matrix of poly entries of deg $< n$. s.t

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

$P(x) = \underline{\text{perm}(A(x))}$ ① Univariate poly in x. of deg $\leq n(n-1)$.

② $p(i) = \text{perm}(A_{1,i})$, $i \in [n]$.

(A, α)

V

P

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

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

$\xleftarrow{p(x)}$ (i.e., $n(n-1)$ field elts)

V checks

$\alpha = \sum a_{1,i} \cdot p(i)$

$\beta \in_R \mathbb{F}$

$\xrightarrow{\beta}$

(Prove to $(A(\beta), p(\beta)) \in \text{Perm}_{\mathbb{F}}$

$(n-1) \times (n-1)$ matrix

$\in \mathbb{F}$

Efficient: ✓

Completeness: The honest prover P satisfies

$\forall (A, \alpha) \in \text{Perm}_{\mathbb{F}}$ (i.e., $\text{Perm}(A) = \alpha$) ✓

$\Pr_{\beta_1, \ldots \beta_n}[(V \leftrightarrow P)(A, \alpha; \beta) = \text{acc}] = 1$

(8)

Soundness: Suppose $Perm(A) \neq \alpha$.

- Case(i) $Perm(A(x)) \neq p(x)$
- Case(ii) $Perm(A(x)) = p(x)$

Case (ii): $\alpha \neq \sum a_{i,i} \cdot p(i)$ ✓

Case (i) $Perm(A(x)) \neq p(x)$.

$Q(x) = p(x) - Perm(A(x))$

$\deg Q < n(n-1)$. & $Q \not\equiv 0$

$$\Pr_{\beta \in F}[Q(\beta) = 0] \leq \frac{d(Q)}{|F|} \leq \frac{n(n-1)}{2n^3} \leq \frac{1}{2n}$$

Total error $\leq \frac{1}{2n} + \frac{1}{2n} + \ldots + \frac{1}{2n}$

$< \frac{1}{2}$.

Hence, Permanent has a public coin poly round AM protocol.

$PH \subseteq P^{\#P} \subseteq IP$ (Next time: $IP \subseteq PSPACE$, $PSPACE \subseteq IP$)

⊠