CS 221 LECTURE 16

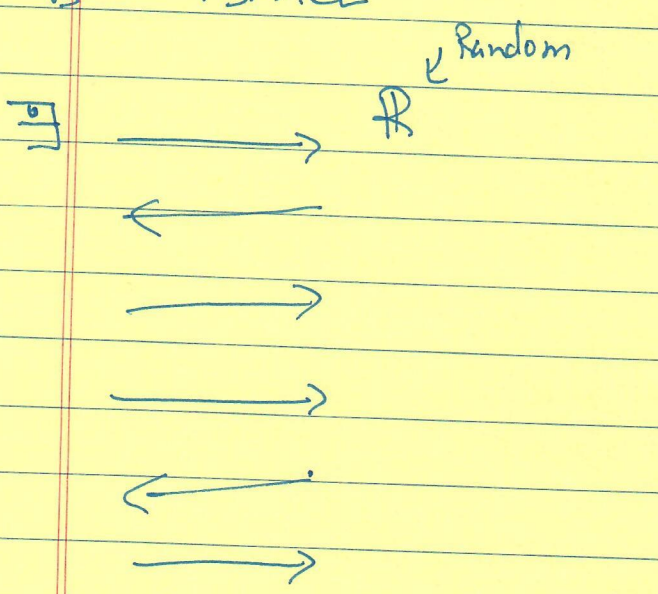
3/22/2018

TODAY : IP = PSPACE

Recall : $L \in IP$ if $\exists$ prob. poly time verifier V s.t. the following hold $\forall x \in \{0,1\}^*$

- $x \in L \Rightarrow \exists$ Prover P s.t. $(P \leftrightarrow V)(x)$ accepts w.p. $\geq \frac{2}{3}$
- $x \notin L \Rightarrow \forall$ provers P $(P \leftrightarrow V)(x)$ accepts w.p. $\leq \frac{1}{2}$.

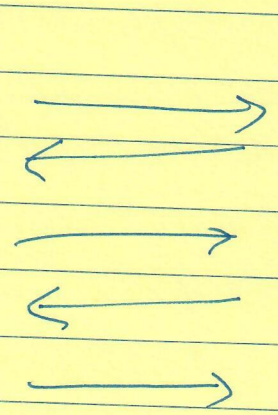
IP vs. PSPACE



$V(x, q_1 .. q_k, a_1 .. a_k)$
other player

↑ powerful player with random

Observer ≡ random player



$V(x, q_1 .. q_k, a_1 .. a_k)$

↑

2 powerful players with polytime observer

- PSPACE = Games (like GO ...)
- IP = Games (like Solitaire ...)

Moral of IP = PSPACE: We should watch "masters" playing Solitaire (if we watch chess grandmasters).

(1) IP ⊆ PSPACE

Idea: Given ~~V_1~~ $V(x, q_1 \dots q_i, a_1 \dots a_{i-1})$

Can compute $\max_{a_i \dots a_k} \Pr_{q_{i+1} \dots q_k} [\, V(x, q_1 \dots q_i, a_1 \dots a_{i-1}, q_{i+1} \dots q_k, a_i \dots a_k) = \text{accept} \,]$

in PSPACE

---

(2) $\#P \subseteq IP$ [Lund, Fortnow, Karloff, Nisan]

Key idea: Arithmetization.

SAT ∈ LOGIC vs. SAT ∈ Algebra

$x_i \in \{0,1\}$ → $x_i \in \{0,1\} \subseteq \mathbb{Q}$

$\neg x_i$ → $1 - x_i$

Clause $C_j = X_1 \vee X_2 \vee \neg X_3 \Rightarrow P_j(X_1, X_2, X_3)$

$= 1 - (1-X_1)(1-X_2)(X_3)$

$C_j = \{$ Sat. $\Leftrightarrow P_j(\ ) = 1$

$\phi = \bigwedge_{j=1}^{m} C_j$

$P(X=x_n)$

$\Rightarrow = \prod_{j=1}^{m} P_j(\bar{x})$.

$\# \phi \Rightarrow \sum_{x \in \{0,1\}^n} P_j(\bar{x})$

What meaning does $P(5, -1, 3, 2, 4, 6, 2/3, \ldots)$ have?

Answer: Nothing, but it exists! it is a number ...

Define

$P^{(n)}(x), P^{(n-1)}(x), \ldots P^{(0)}(x)$ as follows

$P^{(0)}(x) = P(x)$

$P^{(1)}(x) = \sum_{x_1 \in \{0,1\}} P^{(0)}(x)$

$$P^{(i)}(X) = \sum_{X_i \in \{0,1\}} P^{(i-1)}(X)$$

$$P^{(n)}(X) = \sum_{X_n} P^{(n-1)}(X) = \sum_{X \in \{0,1\}^n} P(X)$$

Key features

(1) $P^{(0)}$ easy to compute (in P)

(2) $P^{(i)}$ easy to compute with oracle for $P^{(i-1)}$. [using two queries to $P^{(i-1)}$]

(3) $P^{(i)}$ low-degree polynomial.

(4) final goal: of form $\boxed{\text{Check } P^{(n)}(0) = N}$

* IP: Stages $n, n-1, \ldots 1, 0$.

- at i^{th} stage will have determined $a_i \in \mathbb{Z}^n$ & $N_i \in \mathbb{Z}$ s.t. goal: $P^{(i)}(a_i) = N_i$
- To compute $P^{(i)}(a_i)$ need $P^{(i-1)}(b_i^0)$ & $P^{(i-1)}(b_i^1)$

Ask prover to give

$$g_i(t) \triangleq P^{(i-1)}\left(b_i^0 + t \cdot (b_i^1 - b_i^0)\right) \quad \left[\begin{array}{l} t=0 \Rightarrow b_i^0 \\ t=1 \Rightarrow b_i^1 \end{array}\right]$$

[$g(t)$ = univ. poly of deg $\leq \deg(P^{(i-1)})$]

Prover replies with $\hat{g}(t)$.

Verifier: (i) Verify $N_i = \hat{g}_i(0) + \hat{g}_i(1)$ → if false reject

(ii) - Pick θ_i randomly from $[1 \ldots n^2 m]$

- Let $a_{i-1} = b_i^0 + \theta_i (b_i^1 - b_i^0)$

- $N_{i-1} = \hat{g}_i(\theta_i)$

Induction: Verify $P^{(i-1)}(a_{i-1}) = N_{i-1}$

Key Claim: if $P^{(i)}(a_i) \neq N_i$

then $\Pr_{\theta_i}\left[\left(P^{(i-1)}(a_{i-1}) = N_{i-1}\right)\right] \leq \frac{1}{n^2}$. (Not reject &)

Proof: Both g_i & $\hat{g}_i$ are deg $\leq m$ poly.

① if $g_i = \hat{g}_i$ then $P^{(i-1)}(b_i^0) = \hat{g}_i(0) + \hat{g}_i(1)$

$= P^{i-1}(b_i^0) + P^{i-1}(b_i^1)$

$= P^{(i)}(a_i) \neq N_i$

(so will reject)

② if $g_i \neq \hat{g}_i$ then

$\Pr_{\theta_i}\left[g_i(\theta_i) = \hat{g}_i(\theta_i) \right] \leq \frac{\deg}{n^2 m} = \frac{1}{n^2}$

$P^{(i-1)}(b_i^0 + \theta_i(b_i^1 - b_i^0))$ = N_{i-1}

PSPACE ⊆ IP [Shamir]

(1) Protocol Same ;

(2) Just need to arithmetize PSPACE via "polynomial evolution rules".

↑ Get this from Savitch.

Details

- $P^{(i)}(X_1 \ldots X_n, Y_1 \ldots Y_n) = 1$ if alg. goes from state $(X_1 \ldots X_n) \to (Y_1 \ldots Y_n)$ in 2^i steps.

  $= 0$ if $X_1 \ldots X_n, Y_1 \ldots Y_n \in \{0,1\}^n$ (otherwise)

Goal:

- ~~Challenge~~ $P^{(n)}(X_1 \ldots X_n, Y_1 \ldots Y_n) = 1$?

  ($X_1 \ldots X_n$: initial; $Y_1 \ldots Y_n$: accepting.)

- $P^{(i)}(X_1 \ldots X_n\, Y_1 \ldots Y_n) = \sum_{Z_1 \ldots Z_n} P^{(i-1)}(X_1 \ldots X_n\, Z_1 \ldots Z_n) \cdot P^{(i-1)}(Z_1 \ldots Z_n\, Y_1 \ldots Y_n)$

further details omitted ☒