Today

* IP = PSPACE
  - IP ⊆ PSPACE
  - #SAT ⊆ IP
  - TQBF ⊆ IP

Lecture 22
(Computational Complexity)
(23 Apr, 2020)
Instructor: Prahladh Harsha

Recall - IP formal definition
- GNI - 1 round private coins IP protocol
- Permanent - poly round public coins IP protocol.

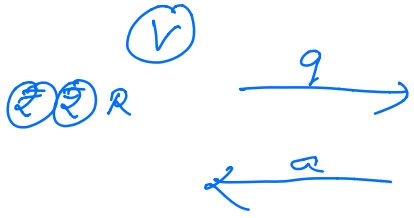
($P^{\#P} \subseteq IP$)

Today: Another proof of $P^{\#P} \subseteq IP$.

$IP \subseteq$??

Baby Case: 1 round IP protocols

$x \in L$



Prover wants to answer such that

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

Prover can figure out best a in poly space.

Conclusion: 1 round IP ⊆ PSPACE

Multiple Rounds:

- Same idea can be used recursively
- Prover can be computed in PSPACE

Cor: $IP \subseteq PSPACE$

Last time: Permanent $\in IP$

Today $\#SAT_D = \{(\varphi, k) \mid \#SAT(\varphi) = k\}$ (Decision version of #SAT)

Theorem: $\#SAT_D \in IP$

$\varphi(\quad) =$ 3CNF formula on n variable

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

Prover wants to convince Verifier that $(*)$ is true.

Vanilla Protocol.

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

$S() = k$

(V) $k = k_0 + k_1$, $b_1 \in_R \{0,1\}$, $k_{b_1} = k_{b_1,0} + k_{b_1,1}$

(P) Honest Prover: $k_0 = S(0)$, $k_1 = S(1)$; $k_{b_1,0} = S(b_1, 0)$, $k_{b_1,1} = S(b_1, 1)$

k_0, k_1

$S(b_1) = k_{b_1}$ →

← $k_{b_1,0}, k_{b_1,1}$

$b_2 \in_R \{0,1\}$ $\xrightarrow{b_2}$

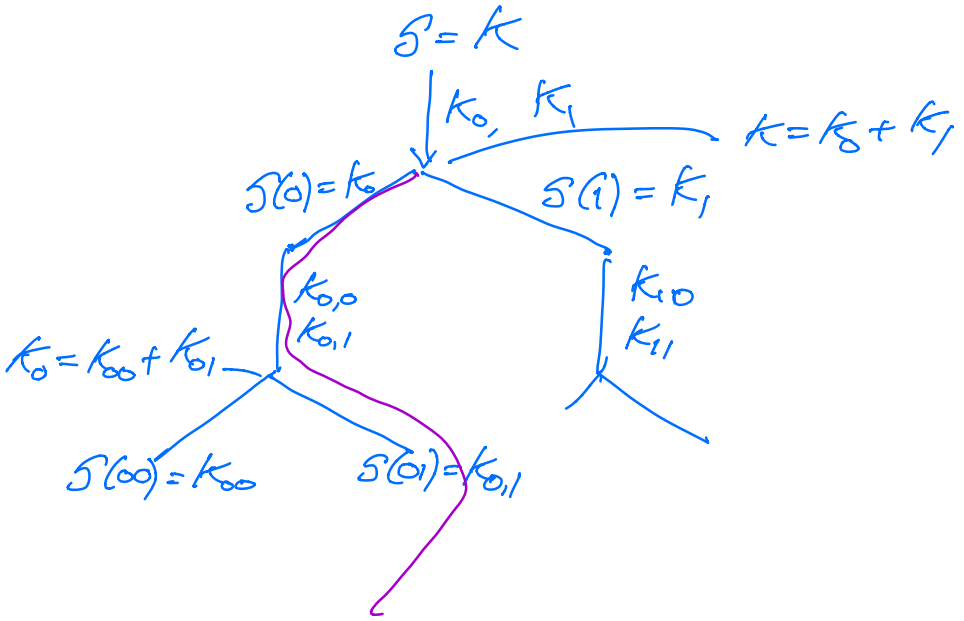
"$S(b_1, b_2) = k_{b_1,b_2}$" $\xleftarrow{}$

$\vdots$

Completeness: Honest Prover P

$(\varphi, k) \in \#SAT_D$; $\Pr_R[\langle (V \leftrightarrow P)(\varphi, k_1), R\rangle = acc] = 1$

What about soundness?



$S(0..0)$ $S(0110..1)$ $S(111)$

2^n leaves

There is a dishonest prover who can cheat on exactly one leaf & be caught

only w/ prob $1/2^n$

$\text{Prob}[\text{acc}] = 1 - \frac{1}{2^n}$. (too close to 1)

— Not a sound protocol.

Arithmetization:

$\varphi \longmapsto P_\varphi$

formula Polynomial

$\varphi(b_1 \ldots b_n) = P_\varphi(b_1 \ldots b_n) \quad \forall b_1 \ldots b_n \in \{0,1\}^n$

Inductively:

① φ = constant (rc, 0/1)
P_φ = constant

② $\varphi = x_i$ (variable)
$P_\varphi = x_i$.

③ $\varphi = \neg\psi$ (negation)
$P_\varphi = 1 - P_\psi$

④ $\varphi = \psi_1 \wedge \psi_2$
$P_\varphi = P_{\psi_1} \cdot P_{\psi_2}$

Arithmetization ✓

φ - 3CNF formula
m clauses

$\deg(P_\varphi)$

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

$C = \bar{x}_1 \vee x_2 \vee x_3 = \overline{(x_1 \wedge \bar{x}_2 \wedge \bar{x}_3)}$

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

P_φ & φ agree on Boolean Values.

$$\sum_{x_1 \in \{0,1\}} \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} P_\varphi(x_1 \ldots x_n) = k$$

Work with some finite field $\mathbb{F}$.

$$S(\alpha_1 \ldots \alpha_i) = \sum_{a_{i+1} \in \{0,1\}} \cdots \sum_{a_n \in \{0,1\}} P_\varphi(\alpha_1 \ldots \alpha_i, a_{i+1} \ldots a_n)$$

"$S() = k$"

(V) (P)

$k = p_1(0) + p_1(1)$ ← $p_1(x)$ — coeffs of univ poly

$S(x)$ = univariate poly

$r_1 \in_R \mathbb{F}$ —r_1→ "$p_1(r_1) = S(r_1)$"

$p(r_1) := S(r_1)$

← $p_2(x_2)$

$p_1(r_1) = p_2(0) + p_2(1)$

$p(x_2) := S(r_1, x_2)$

$r_2 \in_R \mathbb{F}$ —r_2→

"$p(r_2) = S(r_1, r_2)$"

$\vdots$

$p(r_1 \dots r_n) = S(r_1 \dots r_n)$

Completeness:

Honest Prover P

$(\varphi, k) \in \#SAT_D$

$$\Pr_R\left[(V \leftrightarrow P)((\varphi, k), R) = acc\right] = 1$$

Soundness:

P^* - any prover $\quad (\varphi, k) \notin \#SAT_D$

$$\Pr_{r_1 \dots r_n}\left[(V \leftrightarrow P)((\varphi, k), R) = rej\right]$$

$$\geq \underbrace{\left(1 - \frac{d}{q}\right)\left(1 - \frac{d}{q}\right) \dots \left(1 - \frac{d}{q}\right)}_{n \text{ times}}$$

$$= \left(1 - \frac{d}{q}\right)^n \geq 1 - \frac{nd}{q} \geq \frac{99}{100}$$

As long as we choose $|F| > 100nd$

$= 300n^2$

$\#SAT_D \in IP.$ ☒

So far

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

Theorem [Lund-Fortnow-Karloff-Nisan, Shamir]

$IP = PSPACE$

Lemma: $TQBF \in IP$ (Cor. $PSPACE \subseteq IP$)

Pf: $\exists x_1 \forall x_2 \exists x_3 \ldots \underbrace{\varphi(x_1 \ldots x_n)}$

↓ Arithmetization

$P_\varphi(x_1 \ldots x_n)$

$\varphi = \forall x \; \psi(x_1 \ldots)$ $\qquad P_\varphi = P_\psi(0) \cdot P_\psi(1)$

$\psi \downarrow P_\psi$

$\varphi(x_1 \ldots x_n) \longrightarrow P_\varphi(x_1 \ldots x_n)$

$\psi(x_1 \ldots x_{n-1})$

$\forall x_n \varphi(x_1 \ldots x_n) \longrightarrow P_\varphi(x_1 \ldots x_{n-1}, 0) \cdot P(x_1 \ldots x_{n-1}, 1)$

$\psi(x_1 \ldots x_{n-1})$

$= \exists x_n \varphi(x_1 \ldots x_n) \longrightarrow P_\psi(x_1 \ldots x_{n-1})$

$= 1 - (1 - P_\varphi(x_1 \ldots x_{n-1}, 0))$

$(1 - P_\varphi(x_1 \ldots x_{n-1}, 1))$

Input $\psi = Q_1 x_1 \ldots Q_n x_n \; \varphi(x_1 \ldots x_n)$

"$P_\psi = 1$"

(V) ← $P_1(x_1)$ — (P)

$1 = P_1(0) \cdot P_1(1)$

$\psi = \forall x_1 \varphi(x_1)$

$P_1(x_1) := P_\psi(x_1)$

$r_1 \in_R \mathbb{F}$ → r_1

"$P_\psi(r_1) = P_1(r_1)$"

Completeness ✓

Soundness: $\left(1 - \frac{d}{q}\right)^n$ ✓

Efficiency:

$\deg(P_\varphi) = 3n$

But each quantifier doubles the degree

final degree can be as large as $3n \cdot 2^n$

too large. XX

Idea:

We care about value of poly at Boolean values.

Univariate $p(x)$ - possibly large degree

$q(x) := x \cdot p(1) + (1-x)\, p(0)$

$q(b) = p(b) \quad \forall b \in \{0,1\}, \quad \deg(q) \leq 1$

$p(x) \xrightarrow{L_x} x p(1) + (1-x) p(0)$

(Linearing Operator). $L_{x_i} \cdot p(x) =: q(x)$

Input $Q_1 x_1 \ldots Q_n x_n \; \varphi(x_1 \ldots x_n)$

$\downarrow$

$P_{Q_1 x_1} \quad P_{Q_1 x_1 Q_2 x_2} \quad P_{Q_1 x_1 \ldots} \; P_\varphi(x_1 \ldots x_n)$

$\ldots P_{Q_{n-1} x_{n-1}} L_{x_{n-1}} \ldots L_{x_1} P_{Q_1 x_1 \ldots Q_n x_n} \underbrace{L_{x_n} \cdot L_{x_2} L_{x_1} P_\varphi(x_1 \ldots x_n)}$

individual degree in each var is ≤ 1

Polynomial Operations $= n + n-1 + \ldots + 1$

$+ n$

$= O(n^2)$

$\mathcal{O} \qquad \mathcal{O}_{x_n} \mathcal{O}_{x_n} P_\varphi$

$\mathcal{O} = \begin{cases} L - \text{linearing operator} \\ \exists - \text{existential operator} \\ \forall - \text{universal operator.} \end{cases}$

(Contd in next lecture) ⊠