Lecture 21

- Let $\widehat{IP} = IP$ except $\widehat{IP}[k]$ is all k-message protocols

- Then,

$$\widehat{IP}[k] \subseteq AM[k+2]$$

Proof idea

- GNI protocol in AM[2]
  - Proved LB on set

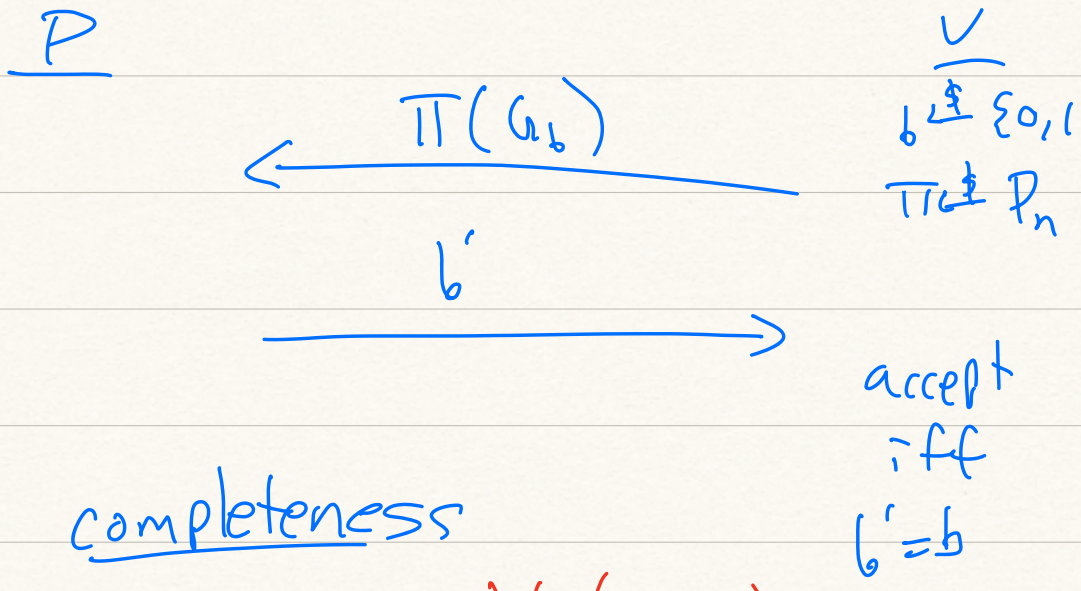
$$S = \{(H, \pi) : [H \cong G_0 \text{ or } H \cong G_1] \text{ and } \pi \in aut(H)\}$$

- Proved

$|S| \geq 2n!$ if $G_0 \not\cong G_1$

$|S| \leq n!$ if $G_0 \cong G_1$

Private-coin GNI



completeness

If $G_0 \not\cong G_1$, $\forall (b, \pi)$

prover can respond w/ $b' = b$.

$\Rightarrow$ all random choices of V lead to a accepting state

$\rightarrow R = \{(b, \pi) : b \in \{0,1\}, \pi \in P_n\}$

$\Rightarrow |R| = 2n!$

↳ accepting random strings for V

Soundness: If $G_0 \not\cong G_1$, then for every P^*

$$\Pr\left[(P^*, V)(G_0, G_1) = 1\right] = \frac{1}{2}$$

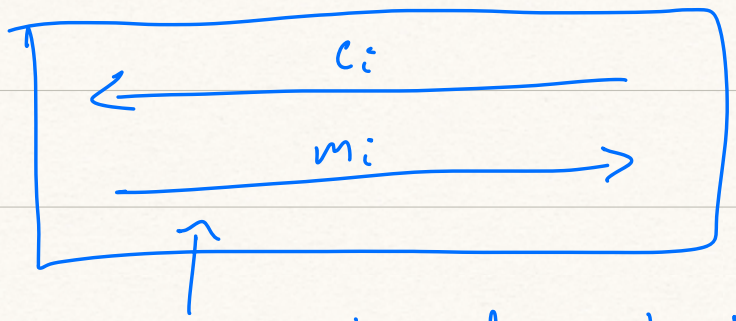
Prob. V accepts is at most $1/2$

$\Rightarrow |R| = n!$

- This is exactly the idea behind $IP[k] \subseteq AM[k+2]$
  $\rightsquigarrow \widetilde{IP}[n] \subseteq AM[n+2]$

- Let $L \in \widehat{IP}[k]$ w/ proof system (P, V)
- We design (P', V') as an $AM[k+2]$ protocol for L.

P' V'



Set lower bound protocol for proving to V' that

$|R_i| \geq k$, where

R_i is set of random private

strings that lead to

V in (P, V) to accept.

Can GI be NP-complete?

We don't think so

Theorem: If GI is NP-complete, then $\Sigma_2^P = \Pi_2^P$.

Proof: If GI is NP-complete, then GNI is coNP-complete.

- $\forall L \in coNP,\ L \leq_p GNI$

  $\forall x$

  $x \in L \leftrightarrow f(x) \in GNI$

- $TAUT \leq_p GNI$

- $\phi \in TAUT \leftrightarrow \forall y\ \phi(y) = 1$

  $\forall y\ \phi(y)$

- $\phi \in TAUT \iff f(\phi) \in GNI$
- Recall $\Sigma_2 SAT$

  $\psi \in \Sigma_2 SAT$ iff

  $\exists x \forall y \phi(x,y)$

  $|x| = |y| = n$
- $\psi \in \Sigma_2 SAT$ iff

  $\exists x \forall y\ g(x) \in GNI$

  $g(x) = f(\phi(x,\cdot))$

- $GNI \in AM[2]$

  WLOG: (P,V) for GNI

  is $AM[2]$ protocol with

  * Perfect completeness

* Soundness $< 2^{-n}$

$m = \text{poly}(n)$

$m' = \text{poly}(n)$

P — V

$r \xleftarrow{\$} \{0,1\}^m$

$a \in \{0,1\}^{m'}$

$x \notin GNI$ iff

$\forall r \; \exists a \; V(x, r, a) = 1$

- Claim $\varphi = \exists x \forall y \; \phi(x,y) = 1$

$\longleftrightarrow \forall r \; \exists x, a \; V(g(x), r, a) = 1$

+ransforms

$\phi(x, \cdot)$ into

GNI instance

iff TAUT

If $q = [\exists x \forall y \phi(x,y)] = 1$

$\Rightarrow \exists x$ s.t. $\phi(x,\cdot)$ is a TAUT

$\Rightarrow f(\phi(x,\cdot)) = g(x) \in GNI$

$\Rightarrow \forall r \exists x, a \; V(g(x), r, a) = 1$

Suppose $q = [\exists x \forall y \phi(x,y)] = 0$

$\Rightarrow \bar{q} = 1 = [\forall x \exists y \overline{\phi(x,y)}]$

$\Rightarrow \forall x \exists y \; \phi(x,y) = 0$

$\Rightarrow g(x) \notin GNI$

$\Rightarrow GI$

$\Rightarrow \Pr[(P^*, V)(g(x)) = 1] < 2^{-n}$

$\Rightarrow \Pr[(P^*, V)(g(x)) = 0] > 1 - 2^{-n}$

$\Rightarrow$ $g(x) \in GNI$

P $g(x)$ q ... V

$\xleftarrow{r}$

$\xrightarrow{a^*}$

$$Pr_r[V(g(x), r, a^*) = 1] < 2^{-n}$$

$$\Leftrightarrow Pr_r[V(g(x), r, a^*) = 0] > 1 - 2^{-n}$$

very large

$\rightarrow$

$$\exists r^* \; \forall x, a^* \; V(g(x), r^*, a^*) = 0$$

↳ negation of what we had before

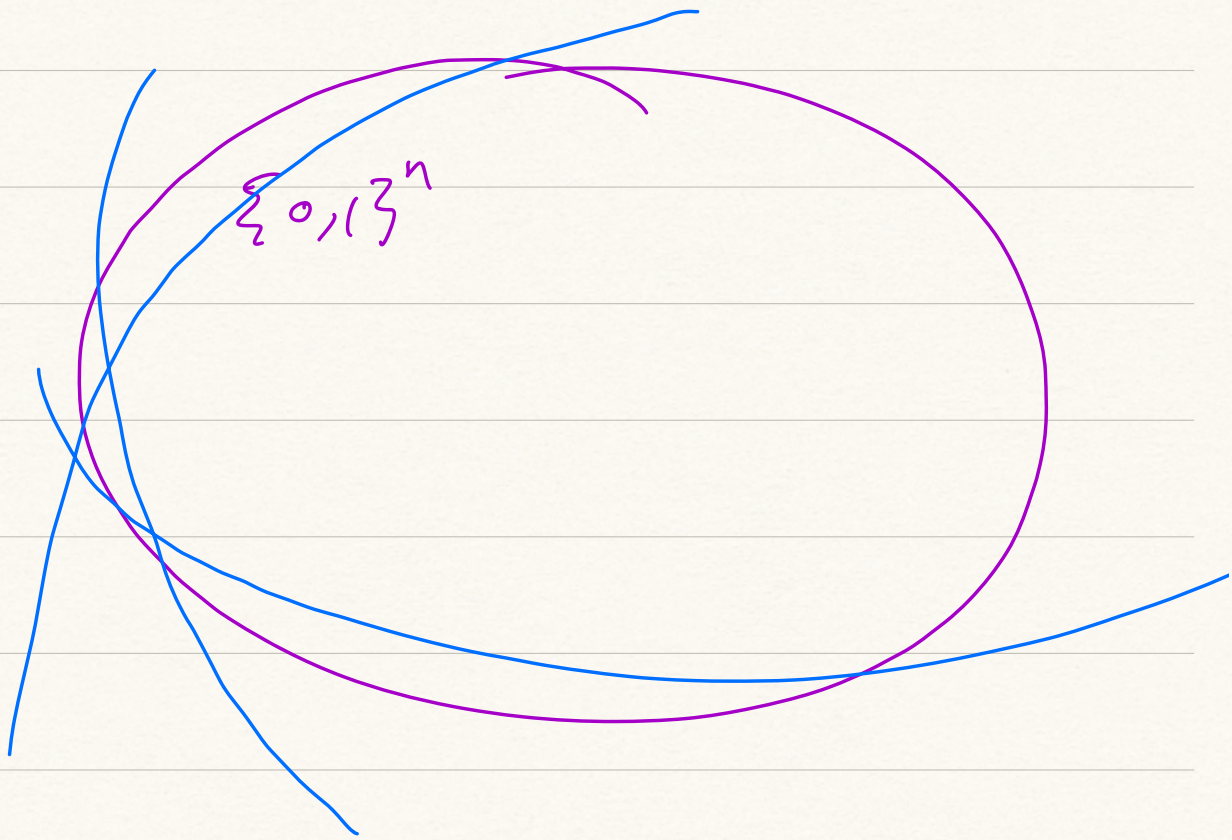
$Q \in \Sigma_2 SAT$

$\updownarrow$

$\forall r \; \exists x, a \; V(q(x), r, q) = 1$

$\in \Pi_2 SAT$

$\Rightarrow \Sigma_2^P \subseteq \Pi_2^P$ $\quad \blacksquare$



IP = PSPACE

- $NP \subseteq IP \subseteq PSPACE$

believe $NP \neq IP$

many believed $IP \neq PSPACE$

- why?
  - Interaction alone doesn't give us anything
    - I.e., $IP = NP$
  - Many people believe $BPP = P$

- More evidence of $IP \neq PSPACE$

- $\forall\ k = o(1)$,

  $IP[k] \subseteq AM[k+2] = AM[2]$

- Huh: $BP \cdot NP = AM = AM[2]$

  Don't think this is much different from NP

  * under "plausible" conjectures, $NP = AM$

- No simple proofs existed for $k = \omega(1)$, so $IP[poly(n)]$ did not seem more powerful than $IP[O(1)] = AM$.

Theorem: $IP = PSPACE$ [Shamir 90, LFKN 90?]

Proof: $IP \subseteq PSPACE$

Idea: $L \in IP$ w/ (P, V)

→ encode $(P, V)(x)$ interaction as TQBF instance

- $P(x)$ $\qquad\qquad$ $V(x)$

m_1 →

← c_2

m_3 →

← c_4

⋮

← α_k →

ℓ-message protocol

$$\alpha_i = \begin{cases} c_i & \text{if } \ell \text{ even} \\ m_i & \text{if } \ell \text{ odd} \end{cases}$$

- $x \in \{0,1\}^n$

(P, V) has perfect completeness

- $\Pr[(P,V)(x) = 1] = 1$: if $x \in L$

- $\Pr[(P^*, V)(x) = 1] \leq 2^{-n}$: if $x \notin L$

If $x \in L$:

$$\exists m_1 \forall c_2 \exists m_3 \cdots Q_\ell \alpha_\ell \quad V(x, m_1, c_2, \cdots, \alpha_\ell) = 1$$

$$Q_\ell = \begin{cases} \exists & \text{if } \ell \text{ is odd} \\ \forall & \text{if } \ell \text{ even} \end{cases}$$

exactly True TQBF

If $x \notin L$, what happens?

$\forall m_1 \forall c_2 \forall m_3 \forall c_4 \cdots \forall \alpha_2$

$$Pr[V(\cdots) = 0] \geq 1 - 2^{-n}$$

$\Rightarrow \forall m_1 \exists c_2^* \forall m_3 \exists c_4^* \cdots$

$$Pr[V(\cdots) = 0] = 1$$

$\Rightarrow V(\ldots) = 0$

$\rightarrow$ negated TQBF instance.

$\Rightarrow L \in PSPACE$

PSPACE $\subseteq$ IP non-trivial

We'll show

$TQBF \in IP$

First, Simpler Question

IP for $\overline{3SAT}$?

$\phi \in \overline{3SAT} \leftrightarrow \forall x\, Q(x) = 0$

Idea: Prove that

$|\{x : Q(x) = 1\}| = 0$

More General:

$\#SAT_k = \{(Q, K) \text{ s.t. } ?$

ϕ has exactly K satisfying assignments

Arithmitization:

- For n-variable ϕ, transform it into n-variable polynomial P_ϕ over $\mathbb{Z}_p$ for some large prime p.

$$\phi : \{0,1\}^n \to \{0,1\} \subseteq \mathbb{Z}_p$$

$$P_\phi : \mathbb{Z}_p^n \to \mathbb{Z}_p$$

$$P_\phi(x) = \phi(x) \quad \forall x \in \{0,1\}^n$$

How to encode ϕ?

- $x_i \wedge x_j = 1$ over $\{0,1\}$

$\Rightarrow x_i \cdot x_j = 1$ in $\mathbb{Z}_p$

- $\overline{x_i} \mapsto 1 - x_i$

$\overline{(\overline{x_j} \wedge \overline{x_i})} = x_i \vee x_j$

- $x_i \vee x_j \mapsto 1 - (1-x_i)(1-x_j)$

$\leadsto x_i + x_j - x_i \cdot x_j$

lecture 21