16/11/21

Last class : $BPP \subseteq P/poly$

Thm :- $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$

BPP is closed under complementation.

$BPP = coBPP$

$\Rightarrow$ it suffices to show that $BPP \subseteq \Sigma_2^P$

Let $L \in BPP$. need to show that $L \in \Sigma_2^P$

$L \in BPP$. $\exists$ a det. TM M and a polynomial $q(\cdot)$ s.t.

$$x \in L \Rightarrow \Pr_{r \in \{0,1\}^{q(|x|)}}[M(x,r)=1] \geq 2/3 \geq 1 - \frac{1}{2^{|x|^d}}$$

$$x \notin L \Rightarrow \Pr_r[M(x,r)=1] \leq \frac{1}{3} \leq \frac{1}{2^{|x|^d}}$$

Define $|x| =: n$, $q(|x|) =: m$.

Choose $d=1$. In other words, the error prob. is $\leq \frac{1}{2^n}$

$$x \in L \Rightarrow \Pr_{r \in \{0,1\}^m}[M(x,r) = 1] \geq 1 - \frac{1}{2^n}$$

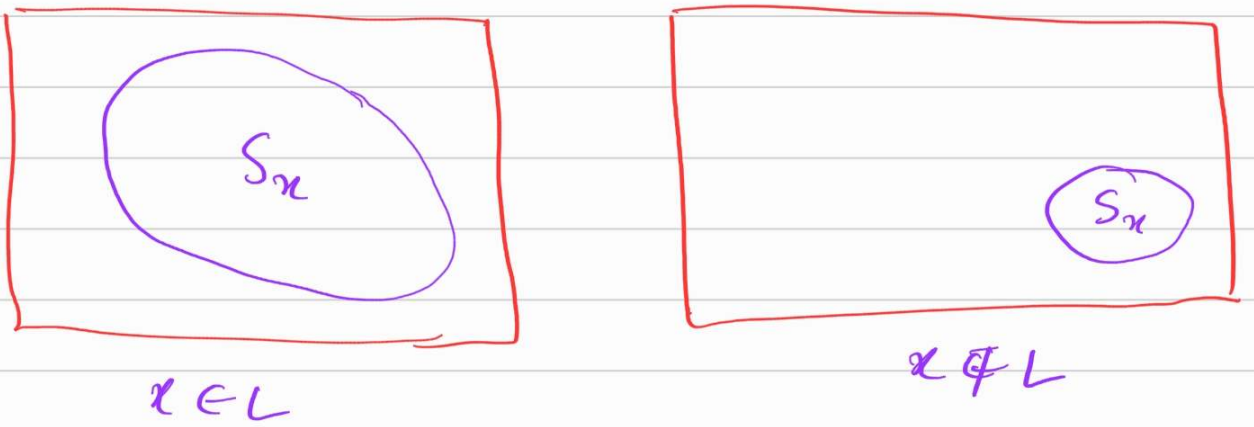
$$x \notin L \Rightarrow \Pr_r[M(x,r) = 1] \leq \frac{1}{2^n}$$

Consider the space of random strings $\{0,1\}^m$

$$S_x := \{ r \in \{0,1\}^m \mid M(x,r) = 1 \}$$

if $x \in L$ then $|S_x| \geq \left(1 - \frac{1}{2^n}\right) 2^m$

if $x \notin L$ then $|S_x| \leq 2^{m-n}$



Q. How many translations of S_x is required to cover all of $\{0,1\}^m$?

Define $k := \left\lceil \frac{m}{n} \right\rceil + 1$

Claim 1 :- $\exists\ u_1, \ldots, u_k \in \{0,1\}^m$ s.t.

$$\bigcup_{i=1}^{k} S_x + u_i = \{0,1\}^m$$

where $S_x + u_i = \{ y + u_i \in \{0,1\}^m \mid y \in S_x \}$

and $x \in L$

↑ bit wise XOR

Proof: $\Pr_{u_1,\ldots,u_k}\left[\bigcup_{i=1}^{k} S_x + u_i = \{0,1\}^m \right] > 0$

(Probabilistic Method)

Pick $u_1, \ldots, u_k$ uniformly at random from $\{0,1\}^m$ independently and

Fix $r \in \{0,1\}^m$.

$$B_r := \left[r \notin \bigcup_{i=1}^{k} S_x + u_i \right]$$

$$\Pr_{u_1,\ldots,u_k}[B_r \text{ happens}]$$

$$= \Pr_{u_1,\ldots,u_k}\left[(r \notin S_x + u_1) \wedge (r \notin S_x + u_2) \cdots \wedge (r \notin S_x + u_k) \right]$$

$$= \prod_{i=1}^{k} \Pr_{u_i}[r \notin S_x + u_i]$$

$$= \prod_{i=1}^{k} \Pr_{u_i}[r + u_i \notin S_x] \quad \text{---------- } (*)$$

$$\Pr_{u_i}[r + u_i \notin S_x] \leq 2^{-n}$$

$$\Pr_{u_i}\left[u_i \notin S_x\right] \le \frac{2^m - |S_x|}{2^m} \le \frac{2^{m-n}}{2^m}$$

$$\le 2^{-n}$$

if u_i is chosen uniformly at random

then $r + u_i$ is also a random vector in $\{0,1\}^m$

from, (*)

$$\le \left(2^{-n}\right)^k$$

$$\Pr_{u_1,\ldots,u_k}\left[B_r \text{ happens}\right] \le 2^{-n\cdot k}$$

$$\Pr_{u_1,\ldots,u_k}\left[\bigcup_{i=1}^{k} S_x + u_i = \{0,1\}^m\right]$$

$$= 1 - \Pr_{u_1,\ldots,u_k}\left[\bigcup_{i=1}^{k} S_x + u_i \neq \{0,1\}^m\right]$$

$$\le \sum_{r\in\{0,1\}^m} \Pr_{u_1,\ldots,u_k}\left[B_r \text{ happens}\right]$$

$$\ge 1 - \sum_{r\in\{0,1\}^n} \Pr_{u_1,\ldots,u_k}\left[B_r \text{ happens}\right]$$

$$\geq 1 - 2^m \cdot 2^{-n \cdot k} \underbrace{>}_{\text{goal.}} 0$$

Therefore choose $k := \lceil \frac{m}{n} \rceil + 1$

just need $2^{m-nk} < 1 \Rightarrow m - nk < 0$

$$\Rightarrow k > \frac{m}{n}$$

Claim 2: when $x \notin L$, $\forall u_1, \ldots, u_k \in \{0,1\}^m$

$$\left| \bigcup_{i=1}^{k} S_x + u_i \right| \leq \sum_{i=1}^{k} |S_x + u_i|$$

$$= k \cdot |S_x| \leq k \cdot 2^{m-n}$$

$$\leq 2^{m - n + \log(\lceil \frac{m}{n} \rceil + 1)}$$

By choice of k,

Then for sufficiently large n, $-n + \log(\lceil \frac{m}{n} \rceil + 1) < 0$

$$\Rightarrow \left| \bigcup_{i=1}^{k} S_x + u_i \right| < 2^m$$

$x \in L \Rightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m$

$$\text{s.t.} \left[\bigcup_{i=1}^{k} S_x + u_i = \{0,1\}^m \right]$$

$x \notin L \Rightarrow \forall u_1, \ldots, u_k \in \{0,1\}^m$

$$\left[\bigcup_{i=1}^{k} S_x + u_i \neq \{0,1\}^m \right]$$

$x \in L \Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m$ s.t.

$$\left[\bigcup_{i=1}^{k} S_x + u_i = \{0,1\}^m \right]$$

$\Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \quad \forall r \in \{0,1\}^m$

$$\underbrace{\left[r \in \bigcup_{i=1}^{k} S_x + u_i \right]}_{\text{Poly-time check!}}$$

$\Leftrightarrow \exists u_1, \ldots, u_k \in \{0,1\}^m \quad \forall r \in \{0,1\}^m$

$$\underbrace{\left[r + u_i \in \bigcup_{i=1}^{k} S_x \right]}_{\bigvee_{i=1}^{k} M(x, r+u_i)}$$

This gives a Σ_2^P characterization.

[for some $i \in \{1, .., k\}$
$M(x, r+u_i)$ accepts]

$BPP \subseteq P/poly$.

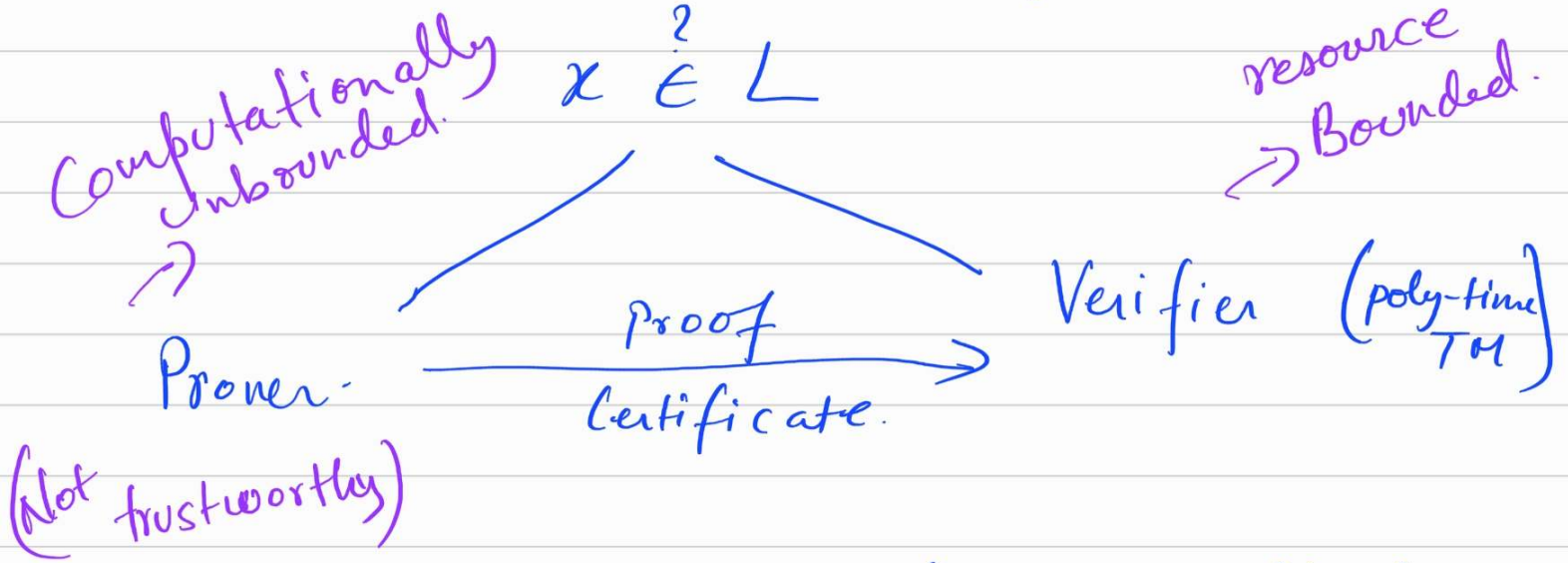
$BPP \subseteq NP$?

$NP \subseteq BPP$?

if $NP \subseteq BPP$.

$\Rightarrow$ $NP \subseteq P/poly \Rightarrow$ PH collapses.

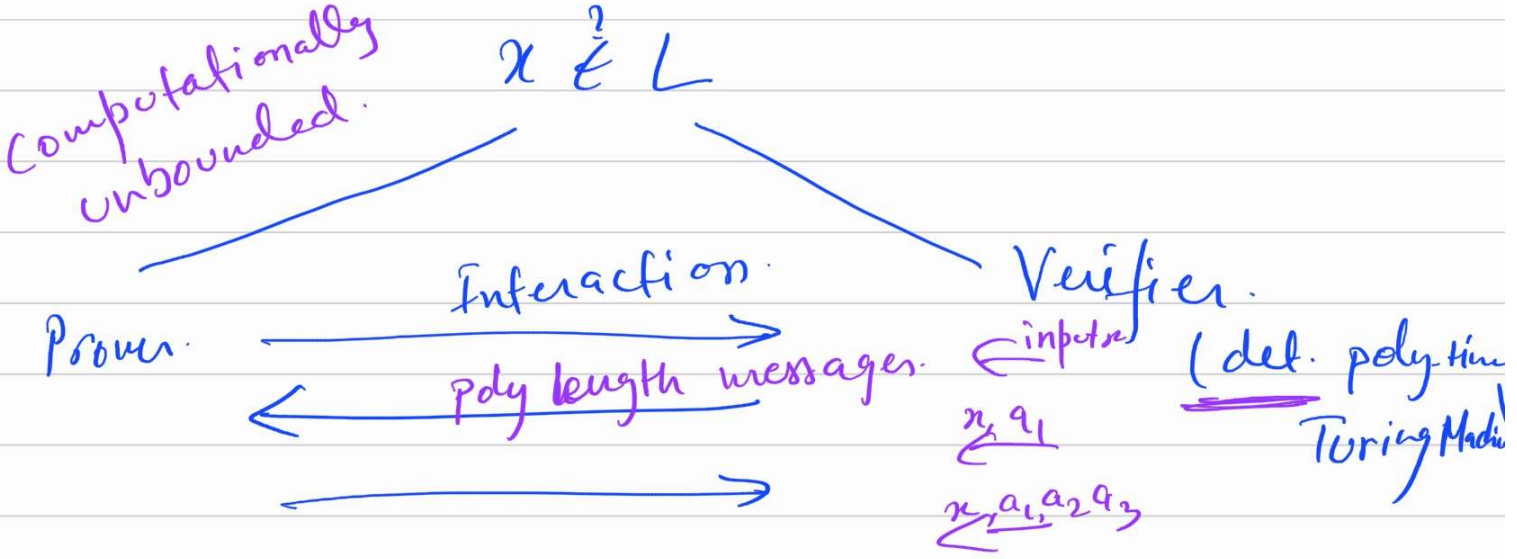
Interactive Proofs. (IP)



if $x \in L \Rightarrow \exists$ a proof s.t. Verifier accepts.

if $x \notin L \Rightarrow \forall$ proofs Verifier rejects.

This gave us the Class NP.



if $x \in L \Rightarrow \exists$ a sequence of messages that makes Verifier accepts.

if $x \notin L \Rightarrow \forall$ sequence of messages Verifier rejects.

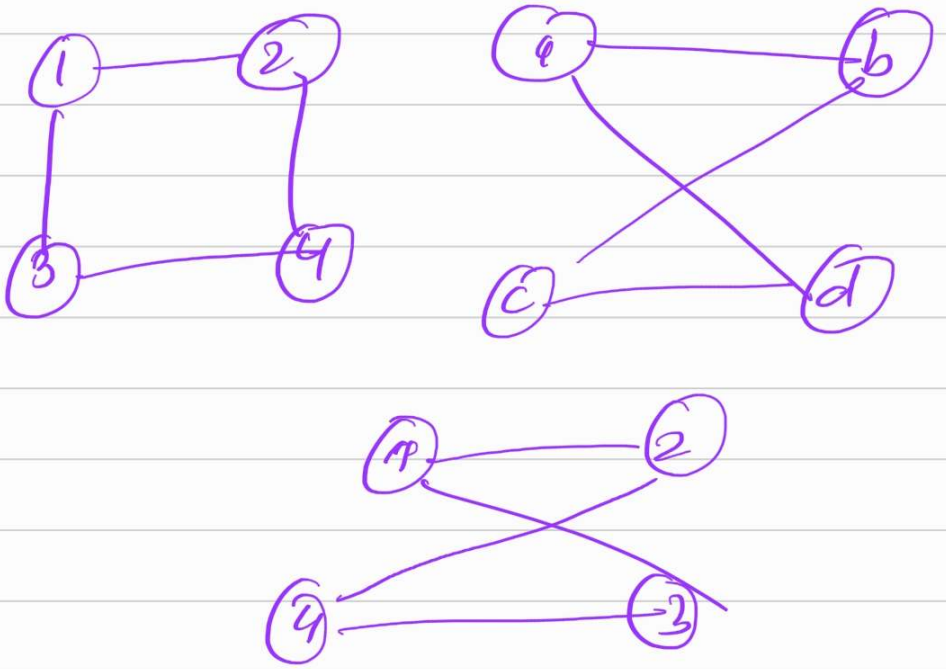
With interactions ^ but det. Verifier. you still get the class NP!

Now suppose the Verifier is probabilistic. (toss random private coins)
i.e. Accept/reject with prob $\geq 2/3$.

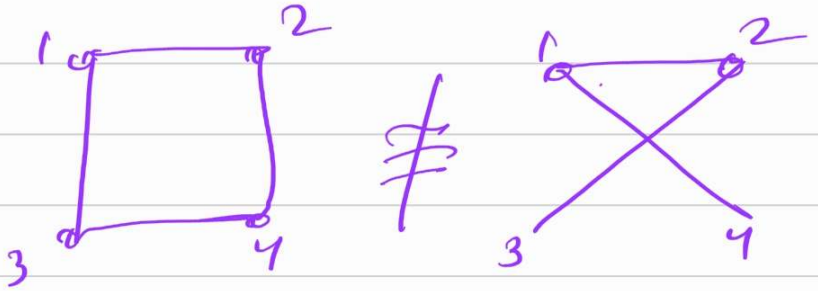
Do you get something NEW ?!

Graph-Isomorphism (GI)

$GI := \{ (G_1, G_2) \mid G_1 \text{ is isomorphic to } G_2 \}$.



$G_1 \cong G_2$ if $\exists$ a permutation of vertices of G_1 s.t. you get G_2.



$GI \in NP$.

$\overline{GI}$:= Graph non-isomorphism

$= \{ (G_1, G_2) \mid G_1$ is non-isomorphic to $G_2 \}$

$2^{poly(\log n)}$ – best known algo. for GI (Babai)