Randomized reductions, NP & $\mathbb{L}$

- A language A reduces to B in rand. poly-time, $A \leq_r B$, if $\exists$ poly-time PTM M s.t. $\forall x$,
$$\Pr[B(M(x)) = A(x)] \geq 2/3.$$

- Recall the reductions $PH \leq_r \oplus P$.

Defn: We define a rand. version of NP:
$BP \cdot NP := \{ L \mid L \leq_r SAT \}$.

Proposition: (i) $NP \subseteq BP \cdot NP$

(ii) $co\text{-}BP \cdot NP = BP \cdot coNP$.

In general, $BP \cdot \mathcal{C} := \{ L \mid L \leq_r \mathcal{C} \}$

- For space-bounded classes, we have:

Defn: • $L \in BPL$ if $\exists$ $O(\lg n)$-space PTM M s.t. $\forall x$, $\Pr[M(x) = L(x)] \geq 2/3$.

- $L \in \underline{RL}$ if $\exists\ O(\lg n)$-space PTM M s.t. $\forall x$,
  $x \in L \Rightarrow \Pr[M(x)=1] \geq 2/3$,
  $x \notin L \Rightarrow \Pr[M(x)=1] = 0$.

- <u>Examples</u>:
  - Uconn has a simple RL algorithm.
  - We will show $GI \in BP.coNP$!

<u>Defn</u>: · $\underline{GI} := \{(G_1, G_2) \mid$ finite graphs G_1, G_2 are isomorphic $\}$.

· $\underline{GNI} := \{(G_1, G_2) \mid G_1 \not\cong G_2\}$.

<u>Proposition</u>: (i) $GI \in NP$.

(ii) $GNI \in coNP$.

<u>OPEN</u>: $GI \in^? coNP$, $GNI \in^? NP$?

<u>Theorem</u> (Goldwasser - Sipser '86): GNI $\in$ BP.NP.

<u>Pf:</u>

- <u>Idea:</u> For graphs G_1, G_2, the number of H s.t. $(H \cong G_1 \vee H \cong G_2)$ is <u>more</u> when $G_1 \not\cong G_2$ than when $G_1 \cong G_2$!

  This "largeness" can be detected in BP.NP.

- Formally, consider the set S associated with the given graphs G_1, G_2 (on n vertices):

$$\underline{S} := \{ (H, \pi) \mid H \text{ has vertices } [n], \; H \cong G_1 \text{ or } H \cong G_2, \; \pi \in Aut(H) \}.$$

$\triangleright$ $G_1 \cong G_2 \Rightarrow \#S = \#\{H \mid H \cong G_1\} \times \#Aut(G_1)$

$$= \frac{n!}{\#Aut(H)} \times \#Aut(G_1) = n!$$

$\triangleright$ $G_1 \not\cong G_2 \Rightarrow \#S = \sum_{i=1}^{2} \#\{H \mid H \cong G_i\} \times \#Aut(G_i)$

$$= 2\cdot(n!) .$$

- Thus, S is <u>twice</u> larger when $(G_1, G_2) \in GNI$.

- We now give a general method to check this in BP.NP, using <u>hash</u> fns. (Recall $SAT \leq_R \oplus SAT$.)

- Let $\underline{h_{B,b}} : \{0,1\}^m \rightarrow \{0,1\}^k$
$$u \mapsto Bu+b$$
Where, $B \in \{0,1\}^{k\times m}$ & $b \in \{0,1\}^k$.

- We have from the hashing properties:
$$\Pr_{B,b}[\exists x \in S, h_{B,b}(x) = 0^k] \geq \frac{|S|}{2^k} - \frac{\binom{|S|}{2}}{2^{2k}}, \&$$
$$\leq |S|/2^k .$$

- We have $\underline{|S| = n!}$ or $2\cdot n!$. So, let us fix $\underline{k}$ s.t. $2^{k-2} \le 2\cdot n! \le 2^{k-1}$.

- $|S| = n! \Rightarrow \Pr_{B,b}[\exists x\in S, h_{B,b}(x) = 0^k]$

$$\le \frac{|S|}{2^k} = \frac{n!}{2^k} =: p .$$

- $|S| = 2\cdot n! \Rightarrow \Pr_{B,b}[\cdots] \geqslant \frac{|S|}{2^k} - \frac{\binom{|S|}{2}}{2^{2k}}$

$$\geqslant \frac{|S|}{2^k}\left(1 - \frac{|S|}{2^{k+1}}\right) \geqslant 2p\cdot\left(1-\frac{1}{4}\right) = \frac{3p}{2}.$$

- We now amplify these resp. probs. by picking $\underline{m} := 100/p^3$ many $h_{B,b}$ & checking that for $\underline{\text{at least}}$ $\frac{5p}{4}$ many hash fns. an "$x \in S$" exists.

$\underline{\text{Exercise:}}$ Chernoff bound yields probs. $\le \frac{1}{3}$ resp. $\geqslant \frac{2}{3}$.

- Since, testing "$(H, \pi) \in S$" is in NP, we get a <u>rand.</u> poly-time reduction from GNI to NP. $\Box$

<u>Corollary</u>: GNI $\in$ BP$\cdot$NP $\cap$ coNP.

<u>Theorem</u> (Schöning '87): GI is <u>NP-complete</u> $\Rightarrow$ $\Sigma_2 = \Pi_2 = PH$.

<u>Pf sketch</u>:

- Suppose GI is NP-complete. Then, GNI is coNP-complete.

- Let $\psi = \exists x \forall y \, \phi(x,y)$ be a Σ_2-Sat instance.
- We plan to convert it into an equivalent Π_2-Sat instance in <u>four</u> steps.

(1) Convert $\forall y \, \phi$ to a <u>GNI instance</u> $g(\underline{x})$.

(2) Using $GNI \in BP.NP$, convert $g(x)$ to a SAT instance (randomly):

$\mathcal{M}r, \exists a, [T(x,r,a)=1]$,

where $\mathcal{M}$ denotes "most", i.e.

$\Pr_r[\exists a, T(x,r,a)=1] \geq 2/3$.

- Now, we have ψ equivalent to $\exists x, \mathcal{M}r, \exists a, [T(x,r,a)=1]$.

(3) Use probability amplification to flip the first-two quantifiers, to get an equivalent formula:

$\mathcal{M}r', \exists x, \exists a', [T'(x,r',a')=1]$.

(4) Using $BPP \subseteq \Pi_2$, replace "$\mathcal{M}$" by $\forall\exists$:

$\forall s_1 \exists s_2 \exists x \exists a' [T''(s_1, s_2, x, a')=1]$.

$\Rightarrow \Sigma_2\text{-Sat} \in \Pi_2 \Rightarrow \Sigma_2 = \Pi_2 = PH$.

$\square$