Randomized reductions (to NP & $\oplus$L)

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

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

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

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

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

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

- For space-bounded classes, we have:

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

- $L \in \underline{RL}$ if $\exists$ $O(\log n)$-space PTM M s.t. $\forall x$,

$x \in L \Rightarrow Pr[M(x)=1] \geq 2/3$,

$x \notin L \Rightarrow Pr[M(x)=1] = 0$.

▷ $\mathbb{L} \subseteq RL \subseteq BPL \subseteq P$ [Sketch: Compute a product of matrices of probabilities.]

– Examples:

- Uconn has a simple RL algorithm.
- We will show $GI \in BP.coNP$!

[Babai'15] put GI in $QuasiP = \bigcup_{c>0} Dtime(2^{\log^c n})$.

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

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

Proposition: (i) $GI \in NP$.

(ii) $GNI \in coNP$.

OPEN: $GI \in^? coNP$, $GNI \in^? NP$?

– Now, we put GNI in BP.NP. This is also a one-round Merlin-Arthur interactive protocol with public-coins !

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

Pf:

- **Idea:** For graphs G_1, G_2, the number of H s.t. $(H \cong G_1 \vee H \cong G_2)$ is **more** 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):

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

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

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

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

$= 2 \cdot (n!)$.

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

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

- Let $\underline{h_{B,b}} : \{0,1\}^m \longrightarrow \{0,1\}^k$
$u \mapsto Bu + b$
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. $2^{k-2} \leq 2 \cdot n! \leq 2^{k-1}$.

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

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

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

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

- 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.

Exercise: Chernoff bound yields probs. $\leq \frac{1}{3}$ resp. $\geq \frac{2}{3}$.

- Since, testing "$(H, \pi_0) \in S$" is in NP, we get a rand. poly-time reduction from GNI to NP. □

Corollary: $GNI \in BP \cdot NP \cap coNP$.

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

Pf sketch:

- 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 four steps.

(1) Convert $\forall y \, \phi$ to a GNI instance $g(x)$.

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

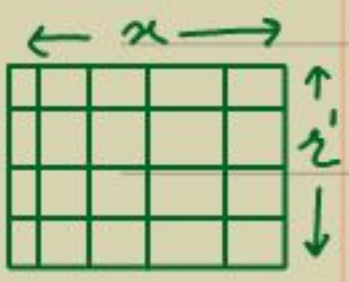
$M r, \exists a, [T(x,r,a)=1]$,

where M denotes "most", i.e.

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

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

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



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

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

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

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

□

Can SAT have small "circuits"?

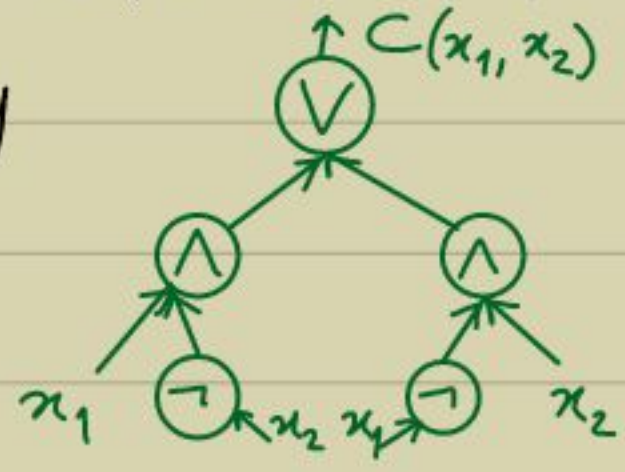
- TMs capture problems that can be solved by one algorithm.

  What if we allow different algorithms for different input lengths n?

- There is an elegant way to model this type of computation; inspired by the practical "silicon circuits".

Defn: • A boolean circuit $C(x_1, \dots, x_n)$ is a rooted tree with boolean input $x_1, \dots, x_n$ at the leaves; OR $\vee$, AND $\wedge$, NOT $\sim$ gates in the internal nodes & output C at the root.

Eg. $XOR(x_1, x_2) = (x_1 \wedge \bar{x}_2) \vee (\bar{x}_1 \vee x_2)$ is:



• Circuit may have many outputs / roots.

- Fanin is the number of inputs to a gate. Fanout that of the outputs.
- Size is the #vertices + #edges of the graph.
- Depth is the length of a path from the leaf to the root.

▷ $\forall f_n : \{0,1\}^n \to \{0,1\}$, $size(f_n) = O(2^n \cdot n)$.

OPEN: Can you think of an explicit family $\{f_n\}_{n \geq 1}$ s.t. $size(f_n) = \theta(2^n)$?

Defn: • $Size(s(n)) := \{\{f_n\}_{n\geq 1} \mid size(f_n) = O(s)\}$

$\{f_n\}_{n\geq 1}$: a boolean fn. $: \{0,1\}^* \to \{0,1\}$.

• $P/poly := \bigcup_{c \geq 0} Size(n^c)$.

Proposition: i) $P \subseteq P/poly$.

ii) $P/poly$ has uncomputable problems.

Sketch: i) Simulate TM steps by gates.

ii) Every unary language is in $P/poly$!

- Potentially, SAT may not have an efficient algorithm but it may have "small" circuits.

Theorem [Karp-Lipton '82]: $SAT \in P/poly \Rightarrow PH = \Sigma_2$.

Proof:

- Assuming $SAT \in P/poly$, we will show that $\Pi_2 Sat$ is in Σ_2. This will suffice.

- Consider a $\Pi_2 Sat$ instance:

$$\forall u, \exists v, \phi(u,v) \quad ---(1)$$

($u \in \{0,1\}^n$, ϕ has size $= m$)

- If SAT has small circuits, then there is a size-m^e circuit family $\{C_m\}_{m \geq 1}$ s.t. $C_m(\phi, u) = 1$ iff $\exists v, \phi(u,v)$.

- Using <u>self-reducibility</u> of SAT, we can turn C_m to a small circuit C'_m s.t. $C'_m(\phi, u)$ gives us the assignment v of $\phi(u,v)$.

$\Rightarrow$ If $\exists v\ \phi(u,v)$ then $\phi(u, C'_m(\phi,u)) = 1$.

- In other words, the qbf (1) is the same as:
  $\exists C'_m, \forall u,\ \phi(u, C'_m(\phi,u))$.

$\Rightarrow \Pi_2 Sat \in \Sigma_2$

$\Rightarrow \quad \Pi_2 = \Sigma_2 \quad \Rightarrow PH = \Sigma_2$. □

▷ $NP \not\subseteq P/poly \Rightarrow NP \neq P$.

- Thus, studying SAT via boolean circuits will give us stronger properties (wrt hardness).