Lec 16

Simple observations.

Obs: If there's a NTM M that decides L in time $T(n)$, then there's a NTM M' that decides L in time $T'(n) = O(T(n))$ and every comp. path of M' on i/p x has length **exactly** $T'(|x|)$. Moreover, we can also ensure the following:

(a) More than $1/2$ the comp. paths of M on i/p x are accepting

$\Leftrightarrow$ " " " " " " " M' " " " " "

(b) Parity of the no. of acc. paths of M on i/p x =

" " " " " " " M' " " " .

Obs: If there's a PTM M that has run-time $T(n)$, then there's a PTM M' that has run-time $T'(n) = O(T(n))$ s.t. $\Pr(M'(x)=1) = \Pr(M(x)=1) \quad \forall x \in \{0,1\}^*$, & every comp. path of M' on i/p x has length exactly $T'(|x|)$.

Class PP (Prob. Poly-time) [Decision version of class #P]

Defn: A lang. L is in PP if there's a poly-time PTM M s.t.

$$x \in L \iff \Pr\{M(x)=1\} > \frac{1}{2}.$$

$$\updownarrow$$

Defn: L is in PP if there's a poly-time NTM M s.t.

$x \in L \iff$ majority (strictly $> \frac{1}{2}$) of the comp. paths of M on i/p x are accepting.

$$\Updownarrow$$

Defn: L is in PP if there's a poly-time DTM M & a poly func. $P(\cdot)$ s.t.

$$x \in L \iff \left| \left\{ u \in \{0,1\}^{P(|x|)} : M(x,u) = 1 \right\} \right| > \frac{1}{2} \cdot 2^{P(|x|)}.$$

PP-completeness

Let $\text{MajSAT} := \{\text{Bool. ckts } \varphi(x_1, \ldots, x_n) : \#\varphi > 2^{n-1}\}$.

Obs: MajSAT is PP-complete under poly-time Karp reduction.

Lemma: $P^{\text{MajSAT}} = P^{\#\text{SAT}}$ $\quad (P^{PP} = P^{\#P})$

Pf: $\Rightarrow$ $\text{MajSAT} \in P^{\#\text{SAT}}$ (easy).

$\Leftarrow$ $\#\text{SAT} \in P^{\text{MajSAT}}$.

Let $\varphi(x_1, \ldots, x_n)$ be the i/p ~~formula~~/ckt. We wish to compute $\#\varphi$. Let $M(b_1, \ldots, b_n, x_1, \ldots, x_n)$ be a DTM that o/p's 1 iff $\text{Int}(\underline{x}) < \text{Int}(\underline{b})$.

$$M(\underline{b}, \underline{x}) \xrightarrow[\text{fixing } \underline{b}]{\text{Cook-Levin}} \psi_{\underline{b}}(\underline{x})$$

$\underline{\text{Obs:}}$ $\#\psi_{\underline{b}}(\underline{x}) = \text{Int}(\underline{b}) \in [0, 2^{n} - 1]$

$$\Gamma_{\underline{b}}(z, \underline{x}) = (z \wedge \varphi(\underline{x})) \vee (\neg z \wedge \psi_{\underline{b}}(\underline{x}))$$

$$\therefore \boxed{\#\Gamma_{\underline{b}}(z, \underline{x}) = \#\varphi + \text{Int}(\underline{b})}$$

Query $\Gamma_{\underline{b}}(z, \underline{x})$ to MajSAT oracle & check if

$$\#\Gamma_{b}(z, \underline{x}) > \frac{1}{2} \cdot 2^{n+1} = 2^{n}.$$

Now use binary search to find the smallest $\underline{b}$ s.t.

$$\#\varphi + \mathrm{Int}(\underline{b}) = 2^n \Rightarrow \#\varphi = 2^n - \mathrm{Int}(\underline{b}).$$

$\square$

Toda's thm: $PH \subseteq P^{\#SAT} = P^{MajSAT}$.

Clearly, $NP, co\text{-}NP \subseteq P^{\#SAT}$.

Class $\oplus P$ (Parity P)

Defn: A language L is in $\oplus P$ if there's a NTM M s.t. $x \in L$ iff the no. of acc. paths of M on i/p x is **odd**.

$\oplus SAT := \{$ Bool. ckt. φ : $\#\varphi$ is odd $\}$.

<u>Obs:</u> $\oplus SAT$ is $\oplus P$-complete under poly-time Karp reduction.

<u>Obs:</u> co-$\oplus P = \oplus P$, i.e., $\oplus P$ is closed under complementation.

<u>Pf. sketch:</u> $\overline{\oplus SAT} = \{$ Bool. ckt. φ : $\#\varphi$ is even $\}$ is co-$\oplus P$ complete.

$$\psi(z, \underline{x}) := (z \land \varphi(\underline{x})) \lor (\neg z \land x_1 \land x_2 \land \dots \land x_n)$$

$\Rightarrow \#\psi(z, \underline{x}) = \#\varphi(\underline{x}) + 1$; We'll denote $\psi(z, \underline{x})$ as $\varphi + 1$.

$\therefore \varphi(\underline{x}) \in \overline{\oplus SAT} \iff \psi(z, \underline{x}) \in \oplus SAT$

Think of a NTM that on i/p φ, forms $\psi(z, \underline{x})$, guesses z & $\underline{x}$ & o/p's $\psi(z, \underline{x})$. $\square$ (fill in proof)

Treating $\oplus$ as a quantifier (just like $\exists$ & $\forall$)

Defn: For a Bool. ckt $\varphi(x_1, \dots, x_n)$, we say $\bigoplus_{\underline{x}} \varphi(\underline{x})$ is true if $\#\varphi$ is odd.

We could have defined $\oplus$SAT as the set of all true quantified Bool. ckts of the form $\bigoplus_{\underline{x}} \varphi(\underline{x})$.

Toda's thm: Proof sketch.

Step 1: Give a rand. poly-time reduction from PH to $\oplus$SAT.

<u>Step 2</u>: (derandomization of Step 1) Give a det. poly-time reduction from PH to #SAT.

<u>Open</u>: It is not known if $NP \subseteq P^{\oplus SAT}$.

Proof of Step 1 uses the Valiant-Vazirani thm.

USAT := {Bool. det φ : $\#\varphi = 1$}.

unique.

<u>Obs</u>: $USAT \subseteq \oplus SAT$.

Theorem: (Valiant-Vaz '86): There's a randomized poly-time reduction f s.t. for every n-variate B.ckt φ, the following holds:

$$\varphi \in SAT \Rightarrow \Pr[f(\varphi) \in USAT] \geq \frac{1}{8n}$$

$$\varphi \notin SAT \Rightarrow \Pr[f(\varphi) \notin SAT] = 1$$

$\boxed{\text{Cor 1:}}$ We get a rand. poly-time red. from SAT to $\oplus$SAT with succ. prob. $\geq \frac{1}{8n}$

(we'll boost this prob.).

Pf. of the V-V thm.

Lemma: (VV'86) Let $\mathcal{H}_{n,k}$ be a family of pairwise-ind. hash func. from $\{0,1\}^n \to \{0,1\}^k$, and $S \subseteq \{0,1\}^n$ s.t. $2^{k-2} \leq |S| \leq 2^{k-1}$. Then,

$$\Pr_{h \in_r \mathcal{H}_{n,k}} \{\text{there's a unique } \underline{x} \in S \text{ s.t. } h(\underline{x}) = 0^k\} \geq \frac{1}{8}.$$

Pf: For every $\underline{x}, \underline{x}' \in S$, $\underline{x} \neq \underline{x}'$,

$\triangleright$ $\Pr\{h(\underline{x}) = 0^k\} = \Pr\{h(\underline{x}') = 0^k\} = \frac{1}{2^k}$.

$\triangleright$ $\Pr_h \{h(\underline{x}) = 0^k \wedge h(\underline{x}') = 0^k\} = \frac{1}{2^{2k}}$.

$N :=$ # of $\underline{x} \in S$ s.t. $h(\underline{x}) = 0^k$.

We would like to lower bound $\Pr\{N=1\}$.

Observe, $\Pr\{N=1\} + \Pr\{N \geq 2\} = \Pr\{N \geq 1\}$

$$\therefore \Pr\{N=1\} = \underbrace{\Pr\{N \geq 1\}}_{\text{need to l.b}} - \underbrace{\Pr\{N \geq 2\}}_{\text{need to u.b.}}$$

▷ $\Pr\{N \geq 2\} \leq \binom{|S|}{2} \cdot \frac{1}{2^{2k}}$ (U.B).

▷ $\Pr\{N \geq 1\} \geq |S| \cdot \frac{1}{2^k} - \binom{|S|}{2} \cdot \frac{1}{2^{2k}}$ (L.B)

by inclusion-exclusion.

$$\therefore \Pr\{N=1\} \geq |S| \cdot \frac{1}{2^k} - 2 \cdot \binom{|S|}{2} \cdot \frac{1}{2^{2k}}$$

$$\geq |S| \cdot \frac{1}{2^k} - |S|^2 \cdot \frac{1}{2^{2k}}$$

$$\geq \frac{1}{8} \quad \left(\because 2^{k-2} \leq |S| \leq 2^{k-1}\right).$$

$$\hookrightarrow \frac{1}{4} \leq |S| \cdot \frac{1}{2^k} \leq \frac{1}{2}.$$

$\blacksquare$

Let M be a DTM that takes inputs $k \in \mathbb{N}$, $h \in \mathcal{H}_{n,k}$ & $\underline{x} \in \{0,1\}^n$ & o/p's 1 iff $h(\underline{x}) = 0^k$. $\quad M(k, h, \underline{x}) \xrightarrow[\text{for fixed } k,h]{\text{Cook-Levin}} \psi_{k,h}(\underline{x})$

$\hookrightarrow$ Bool. ckt.

Now think of the following randomized red.

$$\varphi(\underline{x}) \xrightarrow[\substack{1.\ \text{Picks } k \in_r \{2,\cdots,n+1\}. \\ 2.\ \text{Picks } h \in_r \mathcal{H}_{n,k}.}]{f} \underbrace{\varphi(\underline{x}) \wedge \psi_{k,h}(\underline{x})}_{= f(\varphi)}.$$

Obs: If $\varphi(\underline{x}) \notin SAT$ then $f(\varphi) \notin SAT$.

Obs: If $\varphi(\underline{x}) \in SAT$, then $f(\varphi) \in USAT$ w.p. $\geq \frac{1}{8n}$.

Pf: Let $S :=$ set of satisfying assign. of φ.

$$2^0 \leq |S| \leq 2^n.$$

▷ With prob. $\frac{1}{n}$ the red. f chooses the "right" k, i.e, k satisfies, $2^{k-2} \leq |S| \leq 2^{k-1}$.

$\therefore$ conditional on the "right" choice of k,

$$\Pr_h\left[\exists \text{ unique } \underline{x} \in S \text{ s.t. } h(\underline{x}) = 0^k\right] \geq \frac{1}{8} \cdot \text{ (V.V. lemma)}$$

$$\varphi(\underline{x}) = 1 \qquad\qquad \psi_{k,h}(\underline{x}) = 1$$

$$\Rightarrow \quad \varphi(\underline{x}) \wedge \psi_{k,h}(\underline{x}) = 1$$

$$\Rightarrow \quad \Pr_{k,h}\left[f(\varphi) \text{ has a unique satisfying assignment}\right] \geq \frac{1}{n} \cdot \frac{1}{8} = \frac{1}{8n}$$

$\blacksquare$