Lec 24: Class PP and $\oplus$P; Valiant-Vazirani theorem

A couple of observations.

- **Obs 1:** 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 computation path of M' on i/p x has length <u>exactly</u> $T'(|x|)$.

- **Obs 2:** 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. $\Pr[M'(x)=1] = \Pr[M(x)=1]$ $\forall x \in \{0,1\}^*$, and every computation path of M' on i/p x has length <u>exactly</u> $T'(|x|)$.

Class PP (Probabilistic Polynomial Time)

- It is the decision version of the class #P.
- **Defn. 1:** A language L is in PP if there's a poly-time PTM M s.t. $x \in L \iff \Pr[M(x)=1] > \frac{1}{2}$.

Equivalent Definitions

- **Defn 2:** L is in PP if there's a poly-time NTM M s.t. $x \in L \iff$ majority (i.e, strictly $> \frac{1}{2}$) of the computation paths of M on i/p x are accepting.
- **Defn 3:** L is in PP if there's a poly-time DTM M and a polynomial function $p(\cdot)$ 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

- **Defn.:** A language $L \in PP$ is PP-complete if $L' \leq_p L$ for every $L' \in PP$.
- Let $\mathrm{MajSAT} := \{\text{Boolean ckt. } \varphi(x_1, \ldots, x_n) : \#\varphi > 2^{n-1}\}$.
- **Obs.:** MajSAT is PP-complete under poly-time (Karp) reduction.
- **Lemma:** $P^{\mathrm{MajSAT}} = P^{\#SAT}$ (i.e. $P^{PP} = P^{\#P}$).
- **Proof:** $\Rightarrow$ $\mathrm{MajSAT} \in P^{\#SAT}$ (easy).

  $\Leftarrow$ $\#SAT \in P^{\mathrm{MajSAT}}$

Notation. For an $\underline{x} \in \{0,1\}^*$, $\mathrm{Int}(\underline{x})$ will denote the integer corresponding to $\underline{x}$.

- Proof: (contd.) Let $\varphi(x_1, \ldots, x_n)$ be the i/p ckt. We wish to compute $\#\varphi$. Let $M(b_1, \ldots, b_n, x_1, \ldots, x_n)$ be a DTM that outputs 1 iff $\mathrm{Int}(\underline{x}) < \mathrm{Int}(\underline{b})$.

$$M(\underline{b}, \underline{x}) \xrightarrow[\text{by fixing } \underline{b}]{\text{Apply Cook-Levin}} \psi_{\underline{b}}(\underline{x}) \quad (\text{a Bool. ckt.}).$$

- Obs: $\#\psi_{\underline{b}}(\underline{x}) = \mathrm{Int}(\underline{b}) \in [0, 2^{n-1}]$.
- Define, $\Gamma_{\underline{b}}(z, \underline{x}) := (z \wedge \varphi(\underline{x})) \vee (\neg z \wedge \psi_{\underline{b}}(\underline{x}))$.

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

- <u>Proof (contd.)</u>. Query $\Gamma_{\underline{b}}(z,\underline{x})$ to the MajSAT oracle to check if $\#\Gamma_{\underline{b}}(\underline{z},\underline{x}) > \frac{1}{2}\cdot 2^{n+1} = 2^n$.
- Now use binary search on $\{0,1\}^n$ to find the smallest $\underline{b}$ s.t. $\#\varphi + \mathrm{Int}(\underline{b}) = 2^n \Rightarrow \#\varphi = 2^n - \mathrm{Int}(\underline{b})$.

$\blacksquare$

<u>Toda's theorem</u>: $PH \subseteq P^{\#SAT} = P^{MajSAT}$.

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 number of accepting paths of M on i/p x is odd.
- $\oplus SAT := \{\text{Boolean ckt. } \varphi : \#\varphi \text{ is odd}\}$.
- **Obs:** $\oplus SAT$ is $\oplus P$-complete under poly-time (Karp) reduction.
- **Obs:** $\text{co-}\oplus P = \oplus P$, i.e, $\oplus P$ is closed under complementation.

Proof: $\overline{\oplus SAT} := \{\text{Boolean ckt. } \varphi : \#\varphi \text{ is even}\}$ is co-$\oplus P$-complete.

- We wish to show that $\overline{\oplus SAT} \in \oplus P$.
- Let φ be the i/p formula. Define,

$$\psi(z, \underline{x}) := (z \wedge \varphi(\underline{x})) \vee (\neg z \wedge x_1 \wedge \cdots \wedge x_n).$$

$$\Rightarrow \# \psi(z, \underline{x}) = \# \varphi(\underline{x}) + 1 .$$ (Denote $\psi(z, \underline{x})$ as $\underline{\varphi + 1}$)

- 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, at first forms ψ and then guesses z and $\underline{x}$ and outputs $\psi(z, \underline{x})$. $\blacksquare$

The $\oplus$ quantifier

- We will treat $\oplus$ as a quantifier, just like $\exists$ & $\forall$.
- Defn: For a Boolean ckt. $\varphi(x_1, \dots, x_n)$, we say

$$\bigoplus_{\underline{x}} \varphi(\underline{x}) \text{ is } \underline{\text{true if } \#\varphi \text{ is odd}}.$$

- We can define the problem $\oplus$SAT, equivalently, as the set of all <u>true</u> quantified Boolean ckt. of the form $\bigoplus_{\underline{x}} \varphi(\underline{x})$.

Toda's theorem: Proof outline

- **Step 1:** Give a randomized poly-time reduction from PH to $\oplus$SAT.
- **Step 2:** (Derandomization of Step 1) Give a deterministic poly-time reduction from PH to #SAT.
- **Open:** $\boxed{\text{Is } NP \subseteq P^{\oplus SAT} \text{ ?}}$
- Proof of Step 1 uses the Valiant-Vazirani theorem.

Valiant-Vazirani theorem

- USAT := $\{$Boolean ckt φ : $\#\varphi = 1\}$

  $\uparrow$
  unique

- Obs: USAT $\subseteq \oplus$SAT.

- Theorem (VV'86): there is a randomized poly-time reduction f s.t. for every n-variate Boolean ckt. φ, the following holds:

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

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

- **Corollary 1:** There is a randomized poly-time reduction from SAT to $\oplus$SAT with success probability $\geq \frac{1}{8n}$.

  ↳ This success prob. can be boosted. We'll see how later.

- **VV Lemma:** Let $\mathcal{H}_{n,k}$ be a family of pairwise independent hash fns. from $\{0,1\}^n$ to $\{0,1\}^k$, and $S \subseteq \{0,1\}^n$ be such that $2^{k-2} \leq |S| \leq 2^{k-1}$. Then,

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

Proof of the Valiant-Vazirani Lemma

- For every $\underline{x}, \underline{x}' \in S$, $\underline{x} \neq \underline{x}'$,
  - $\Pr_h[h(\underline{x}) = 0^k] = \Pr_h[h(\underline{x}') = 0^k] = \frac{1}{2^k}$.
  - $\Pr_h[h(\underline{x}) = 0^k \wedge h(\underline{x}') = 0^k] = \frac{1}{2^{2k}}$.
- Let $N :=$ No. of $\underline{x} \in S$ s.t. $h(\underline{x}) = 0^k$. We would like to lower bound $\Pr_h[N = 1]$.
- For the rest of the proof, we'll denote $\Pr_h$ as $\Pr$.

- Proof (contd.): Observe that

$$\Pr[N=1] + \Pr[N \geq 2] = \Pr[N \geq 1]$$

$$\Rightarrow \Pr[N=1] = \Pr[N \geq 1] - \Pr[N \geq 2]$$

Need to lower bound (for $\Pr[N \geq 1]$)

Need to upper bound (for $\Pr[N \geq 2]$)

- $\Pr[N \geq 2] \leq \binom{|S|}{2} \cdot \frac{1}{2^{2k}}$ (by union bound).
- $\Pr[N \geq 1] \geq |S| \cdot \frac{1}{2^k} - \binom{|S|}{2} \cdot \frac{1}{2^{2k}}$

(by inclusion - exclusion principle)

- Therefore,

$$\Pr[N=1] \geqslant |S| \cdot \frac{1}{2^k} - 2 \cdot \binom{|S|}{2} \cdot \frac{1}{2^{2k}}$$

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

$$\geqslant \frac{1}{8}.$$

- As $2^{k-2} \leq |S| \leq 2^{k-1}$, $\quad \frac{1}{4} \leq \frac{|S|}{2^k} \leq \frac{1}{2}$.

$\blacksquare$

Proof of the Valiant-Vazirani theorem

- Let M be a DTM that takes i/p: $k \in \mathbb{N}$, $h \in \mathcal{H}_{n,k}$, $\underline{x} \in \{0,1\}^n$ and outputs 1 iff $h(\underline{x}) = 0^k$.

$$M(k, h, \underline{x}) \xrightarrow[\text{by fixing } k, h]{\text{Cook-Levin reduction}} \psi_{k,h}(\underline{x}) \quad \text{(Bool. ckt)}$$

- Consider the following randomized reduction f.

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

Proof of the Valiant-Vazirani theorem (contd.)

- **Obs:** If $\varphi \notin SAT$ then $f(\varphi) \notin SAT$.
- **Obs:** If $\varphi \in SAT$ then $f(\varphi) \in USAT$ w.p. $\geq \frac{1}{8n}$.

Proof: Let S be the set of satisfying assignments of φ. Observe,

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

- With prob. $\frac{1}{n}$, the reduction function f chooses the "right" k, i.e., the chosen k satisfies

$$2^{k-2} \leq |S| \leq 2^{k-1}.$$

- Therefore, conditional on the "right" choice of k,

$$\Pr_h\left[\text{there's a unique } \underline{x} \in S \text{ s.t. } h(\underline{x}) = 0^k\right] \geq \frac{1}{8}$$

(by the Valiant-Vazirani lemma)

- $$\Pr_{k,h}\left[f(\varphi) \in USAT\right] \geq \frac{1}{8n}.$$

$\blacksquare$