LECTURE 12

Note Title

TODAY:

- [VALIANT - VAZIRANI]: SAT $\leq$ Unique-SAT
- [TODA'S THEOREM]: $\underbrace{PH \subseteq BP^{\oplus P}} \subseteq P^{\#P}$

—— × ——

Recall from Last time:

Defn: Unique-SAT = (U_{YES}, U_{NO})

$U_{YES} = \{ \phi \mid \phi$ has 1 sat. assgnmt. $\}$

$U_{NO} = \{ \phi \mid \phi$ has 0 sat. " $\}$.

—— × ——

Defn: (Randomized "BP" reduction)

$\Pi \leq_R \Gamma$ if $\exists$ randomized alg. f s.t.

$x \in \Pi_{YES} \Rightarrow f(x) \in \Gamma_{YES}$ w.p. $\geq s(n) + \frac{1}{p(n)}$

$x \in \Pi_{NO} \Rightarrow f(x) \notin \Gamma_{NO}$ w.p. $\leq s(n)$

$s(n) = 0 \rightarrow$ "RP" reduction.

[Valiant - Vazirani] Theorem:

$$\text{SAT} \leq_{RP} \text{Unique-SAT}$$

Proof (Idea):

Given ϕ:

- Pick m, $h: \{0,1\}^n \rightarrow \{0,1\}^m$ at "random"
- Output $\psi(x) = \phi(x) \wedge [h(x) = \bar{0}]$.

formula if

To formalize idea, need:

- Small set $\mathcal{H}$ of functions
  $$\{h : \{0,1\}^n \to \{0,1\}^m\}$$
- Every $h \in \mathcal{H}$ should be polytime computable (have small formula).
- $\forall\ S \subseteq \{0,1\}^n \quad 2^{m-2} \leq |S| \leq 2^{m-1}$
  $$\Pr[\exists!\ x \in S \text{ s.t. } h(x) = \bar{0}] \geq \Omega(1)$$

How to get such family.

"6.046" ⇒ "Pairwise Independent Hashing"

aka "Universal Hashing".

Defn: $\mathcal{H}$ is pairwise independent if

$\forall\ x \neq y \in \{0,1\}^n \ ; \ \forall a, b \in \{0,1\}^m$

$$\Pr_{h \in \mathcal{H}} \left[h(x) = a \ ; \ h(y) = b \right] = \frac{1}{4^m} .$$

Lemma 1: If $\mathcal{H}$ is p.w.i. then $\forall S \subseteq \{0,1\}^n$

$2^{m-2} \leq |S| \leq 2^{m-1}$,

$$\Pr_{h \in \mathcal{H}} \left[\exists!\ x \in S ,\ h(x) = \bar{0} \right] \geq \frac{1}{8}$$

Lemma 2: $\exists\ \mathcal{H}$ s.t. $\mathcal{H}$ is easy to sample & every $h \in \mathcal{H}$ is polytime computable.

Proof of Lemma 1:

- Fix $x \neq y \in S$

$$\Pr\left[h(x) = 0 \ \wedge \ h(y) = 0 \right] = \frac{1}{4^m}$$

- Fix $x \in S$

$$\Pr\left[h(x)=0 \ \wedge \ \left(\forall y \in S - \{x\} \ \ h(y) \neq 0 \right) \right]$$

$$= \Pr\left[h(x) = 0 \right]$$

$$- \sum_{y \in S - \{x\}} \Pr\left[h(x) = 0 = h(y) \right]$$

$$= \frac{1}{2^m} - \frac{|S|-1}{4^m} \geq \frac{1}{2^{m+1}} \qquad \left[|S| \leq 2^{m-1} \right]$$

- $\Pr\left[\exists\, x \in S \ \text{ s.t. } \left(h(x)=0 \right) \wedge \left(\forall y \in S - \{x\} \ \ h(y) \neq 0 \right) \right]$

$$= \sum_{x \in S} \Pr\left[\qquad \right] \geq \frac{|S|}{2^{m+1}} \geq \frac{1}{8}$$

$(|S| \geq 2^{m-2})$.

$\boxtimes$

Proof of Lemma 2:

(Many constructions are known)

$$\mathcal{H} = \left\{ h_{A,b}(x) = Ax + b \;\middle|\; \begin{array}{l} A \in \{0,1\}^{m \times n} \\ b \in \{0,1\}^m \end{array} \right\}$$

$$\Pr_{A,b}\left[Ax+b = \alpha \;\;\&\;\; Ay + b = \beta\right]$$

$$= \Pr\left[A(x-y) = \alpha - \beta \;\;\&\;\; b = \alpha - Ax\right]$$

$$= \Pr\left[A(x-y) = \alpha - \beta\right] \cdot \frac{1}{2^m}$$

$$= \Pr\left[i^{th} \text{ column of } A = \ldots\right] \cdot \frac{1}{2^m} = \frac{1}{4^m}$$

(where $(x-y)_i = 1$

$\boxtimes$

[TODA]'s THEOREM:

$$PH \subseteq P^{\#P}$$

Notes:

1. $P^{\#P}$ equals problems solvable with oracle to #SAT.

   In our case will consider languages of the form

$$L = \{(M, n, a, b) \mid M \text{ polytime } \& \ \#\{y \mid M(x,y) \text{ accepts}\} \leq a \pmod b\}$$

2. Theorem doesn't mention randomness.

Crucial Intermediate Concepts

- For class $\mathcal{C}$ can consider

$$\oplus \cdot \mathcal{C} = \{ \oplus \cdot L \, , \; L \in \mathcal{C} \}$$

where $\oplus L = \{ x \mid \# y$ s.t. $\{(x,y) \in L\}$ is even$\}$.

- For class $\mathcal{C}$ can consider

$$\text{(strong) } BP \cdot \mathcal{C} = \bigcap_{\text{poly } q(n)} \left\{ \bigcup_{L \in \mathcal{C}} \left(BP_{q(n)} \cdot L \right) \right\}$$

$$\left(BP_{q(n)} \cdot L \right)_{YES} = \left\{ x \;\middle|\; \Pr_y \left[(x,y) \in L \right] \geq 1 - \frac{1}{2^{q(n)}} \right\}.$$

$$\left(BP_{q(n)} \cdot L \right)_{NO} = \left\{ x \;\middle|\; \Pr_y \left[(x,y) \in L \right] \leq \frac{1}{2^{q(n)}} \right\}.$$

Central Class

$BP \cdot \oplus \cdot P$

L given by polytime machine $M(\cdot,\cdot,\cdot)$

s.t.

$$L = \left\{ x \;\middle|\; \Pr_y \left[\#\{z \text{ s.t. } M(x,y,z) \text{ accepts}\} = \text{even} \right] \geq 1 - 2^{-q(n)} \right\}.$$

1. Not an "intuitive class".
2. Clearly solvable in PSPACE;
   also in $P^{\#P(P^{\#P})}$
   2 levels of counting.
3. Surprising results of [TODA].

Lemma 1: $PH \subseteq BP \cdot \oplus \cdot P$

(Proved as in Valiant-Vazirani + some nice calculus)

Lemma 2: $BP \cdot \oplus \cdot P \subseteq P^{\#P}$

(Quite surprising, but not too hard)

Today: Start proof of Lemma 1.

Main Ideas :

1. [Valiant-Vazirani]

$$NP \subseteq \text{weak-}BP \cdot \underbrace{\overline{\oplus}}_{} \cdot P$$

Good case 1 sat. assignmt.

Bad case 0 " .

2. So hopefully

$$NP \subseteq (\text{strong})\ BP \oplus P$$
$$coNP \subseteq BP \oplus P$$

3. By induction/extension

$$\Sigma_{k-1}^{P}, \Pi_{k-1}^{P} \subseteq BP \cdot \oplus \cdot P$$

$$\Rightarrow \Sigma_{k}^{P}, \Pi_{k}^{P} \subseteq BP \cdot \oplus \cdot BP \cdot \oplus \cdot P$$

4. For reasonable class $\mathcal{C}$ [in our case $\oplus P$]

$$\oplus \cdot BP \cdot \mathcal{C} \subseteq BP \cdot \oplus \cdot \mathcal{C}$$

[holds only for strong BP]

5. For reasonable class $\mathcal{C}$ [again $\oplus \cdot P$]

$$BP \cdot BP \cdot \mathcal{C} \subseteq BP \cdot \mathcal{C}$$

[holds only for strong BP]

6. For reasonable class $\mathcal{C}$ [this time P]

$$\oplus \cdot \oplus \cdot \mathcal{C} \subseteq \oplus \cdot \mathcal{C}$$

7. Using 3, 4, 5, 6 get

$$\Sigma_k^P \subseteq BP \cdot \oplus \cdot P$$

Lets start with (2)

Lemma 1.1 $NP \subseteq BP \oplus P$

Proof: Fix $L \in NP$ given by M

By VV $\exists$ M' s.t.

$$\exists y \; M(x,y) \text{ accepts}$$

$$\Leftrightarrow \Pr_h \left[\exists!\, y \; M'(x,h,y) \text{ accepts} \right] \geq \frac{1}{p(n)}$$

$$\downarrow$$

(else $= 0$)

Let $M''(x,h,1y) = 1$ if $M'(x,h,y) = 1$

& $M''(x,h,\bar{0}) = 1$

Thus $x \in L \Rightarrow \Pr_h \left[\#\{y \mid M''(x,h,y)\} \text{ even} \right] \geq \frac{1}{p(n)}$.

$x \notin L' \Rightarrow$ " $= 0$.

$$M^{(3)}\left(x,\ \begin{matrix} h_1 \dots h_k \\ y_1 \dots y_k \end{matrix}\right) \quad \text{accepts}$$

$$\text{if} \quad M''(x, h_1, y_1) \ \text{accepts}$$

$$\underline{\text{and}} \quad M''(x, h_2, y_2) \ \text{accept}$$

$$\vdots$$

$$\underline{\text{and}} \quad M''(x, h_k, y_k) \ \text{accepts.}$$

<u>Claim</u>

$$\Pr_{h_1 \dots h_n}\left[\#\left\{ \begin{matrix} (y_1 \dots y_n) \ \text{s.t.} \\ M^{(3)}(x, h_1 \dots h_k, y_1 \dots y_n) \ \text{accepts} \end{matrix} \right\} \text{even} \right]$$

$$= \Pr_{h_1 \dots h_n}\left[\exists i \ \text{s.t.} \ \#\{ y_i : M''(x, h_i, y_i) \ \text{accepts} \} \ \text{even} \right]$$

$$\geq 1 - \left(1 - \frac{1}{P(n)}\right)^k = 1 - 2^{-q(n)} \quad \text{if}$$

k suff. large.

Abstracting / Extending (2).

Proof needs two elements

- $\mathcal{C}$ closed under complementing
  [to construct M'' from M']
- $\mathcal{C}$ closed under AND
  [to construct $M^{(3)}$ from M'']

Claim: $BP \oplus P$ closed under complementation, and.

(Proof omitted)

Lemma 1.2: $\exists \cdot BP \oplus P \subseteq BP \oplus BP \oplus P$

$\forall \cdot BP \oplus P \subseteq$ " .