6.841 Advanced Complexity Theory March 19, 2007

Lecture 12

Lecturer: Madhu Sudan *Scribe: Suho Oh, Jose Soto*

1 Overview

- Randomized Reductions. Valiant-Vazirani: $SAT \leq_{RP} Unique\text{-}SAT$.
- Toda's Theorem: $PH \subseteq P^{\#P}$.

2 The Theorem of Valiant-Vazirani.

To state this theorem we will need some definitions first:

Definition 1 (*Unique-SAT* promise problem) .

$$\begin{aligned} Unique\text{-}SAT &= (U_{YES}, U_{NO}). \\ U_{YES} &= \{\varphi \,|\, \varphi \textit{ has 1 satisfying assignment}\}. \\ U_{NO} &= \{\varphi \,|\, \varphi \textit{ has 0 satisfying assignment}\}. \end{aligned}$$

Definition 2 (Randomized Reductions) *Given two promise problems $\Pi = (\Pi_{YES}, \Pi_{NO})$ and $\Gamma = (\Gamma_{YES}, \Gamma_{NO})$. We say that Π reduces to Γ under a BP randomized reduction "$\Pi \leq_{BP} \Gamma$" if there exists a probabilistic polynomial time algorithm A, a polynomial $p(n)$ and a polynomial time computable function $s(n)$ such that:*

$$\begin{aligned} x \in \Pi_{YES} \Longrightarrow \quad & A(x) \in \Gamma_{YES} \quad && w.p. \;\geq s(n) + \frac{1}{p(n)}. \\ x \in \Pi_{NO} \Longrightarrow \quad & A(x) \notin \Gamma_{NO} \quad && w.p. \;\leq s(n). \\ & [\Longleftrightarrow A(x) \in \Gamma_{NO} \quad && w.p. \;\geq 1 - s(n)]. \end{aligned}$$

When $s(n) = 0$ we say that it is a RP randomized reduction and we denote it by "$\Pi \leq_{RP} \Gamma$".

Using the previous definition we can state the theorem as follows:

Theorem 1 (Valiant-Vazirani)

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

To find an RP reduction a natural idea is to map an instance $\varphi(x)$ of SAT into a new formula $\psi(x) = \varphi(x) \wedge f(x)$, where $f(x)$ is a sufficiently "nice" formula. In that way if $\varphi(x) \in SAT_{NO}$ then we would know that $\psi(x)$ has no satisfying assignment, and so $\psi(x) \in U_{NO}$. The problem is to determine a nice $f(x)$ such that if $\varphi \in SAT_{YES}$, then $\psi(x)$ has exactly one satisfying assignment with enough probability.

How can we find such a formula?

One idea is to pick some $m \leq n$, and some $h : \{0,1\}^n \to \{0,1\}^m$ "at random", and output the formula $\psi(x) = \varphi(x) \wedge [h(x) = \overline{0}]$ so that if $\varphi \in SAT_{YES}$ then hopefully $\psi \in U_{YES}$.

Let us formalize the idea a little bit:

Define for a fixed φ, the set S of satifying assignment of φ, $S = \{x \,|\, \varphi(x) = 1\}$. Clearly there exist an $m \in \{2, \ldots, n+1\}$ such that $2^{m-2} \leq |S| \leq 2^{m-1}$. Using that m we can pick a function $h : \{0,1\}^n \to \{0,1\}^m$ and use it to output ψ.

How can we find the right m? We just guess it, since we are picking it at random from the set $\{2, \ldots, n+1\}$, we are right with probability $1/n$.

How can we pick h? We can not pick it at random since h would not be efficiently computable. What do we mean/want?

We need a set $\mathcal{H} \subseteq \{h : \{0,1\}^n \to \{0,1\}^m\}$ such that:

1. $\mathcal{H}$ is not too big. Precisely we need $|\mathcal{H}| \le 2^{poly(n)}$ so that we are able to pick an element from it using with only $poly(n)$ random bits.
2. Every $h \in \mathcal{H}$ should be computable in polynomial time (i.e. it should have a small formula)
3. A typical $h \in \mathcal{H}$ should be sufficiently random. More precisely, for any set $S \subseteq \{0,1\}^n$ with $2^{m-2} \le |S| \le 2^{m-1}$,
$$Pr[\exists! x \in S \text{ s.t. } h(x) = \overline{0}] \ge \Omega(1).$$

How can we get such family? We can use a "Pairwise Independent hash family".

Definition 3 (Pairwise independent) $\mathcal{H} \subseteq \{h : \{0,1\}^n \to \{0,1\}^m\}$ *is a pairwise independent family if* $\forall x \neq y \in \{0,1\}^n, \forall \alpha, \beta \in \{0,1\}^m$,

$$\Pr_{h \in \mathcal{H}}[h(x) = \alpha, h(y) = \beta] = \frac{1}{4^m}.$$

Lemma 1 *There exists a pairwise independent hash family $\mathcal{H}$ such that it is easy to sample and $\forall h \in \mathcal{H}$, formula-size$(h)$ is $poly(n)$.*

Proof Define
$$\mathcal{H} = \{h_{A,b}(x) = Ax + b \pmod 2 \,|\, A \in \{0,1\}^{m \times n}, b \in \{0,1\}^m\}.$$

It is clear that $h_{A,b}$ has small formula size and for any $x \neq y, \alpha, \beta$:

$$\Pr_{A,b}[Ax + b = \alpha, Ay + b = \beta] = \frac{1}{4^m}.$$

■

Lemma 2 $\forall S \subseteq \{0,1\}^n$, $2^{m-2} \le |S| \le 2^{m-1}$,

$$\Pr_{h \in \mathcal{H}}[\exists! x \in S, h(x) = \overline{0}] \ge \frac{1}{8}.$$

Proof Fix $x \in S$, then:
$$\Pr_{h \in \mathcal{H}}[h(x) = 0] = \frac{1}{2^m}.$$

Fix $x \neq y \in S$, then:
$$\Pr_{h \in \mathcal{H}}[h(x) = 0 \wedge h(y) = 0] = \frac{1}{4^m}.$$

Then:

$$\begin{aligned}\Pr_{h \in \mathcal{H}}[h(x) = 0 \wedge \forall y \in S \setminus \{x\}, (h(y) \neq 0)] &\ge \Pr_{h \in \mathcal{H}}[h(x) = 0] - \sum_{y \in S \setminus \{x\}} \Pr_{h \in \mathcal{H}}[h(x) = 0 = h(y)] \\ &\ge \frac{1}{2^m} - \frac{|S|}{4^m} \ge \frac{1}{2^{m+1}},\end{aligned}$$

where the last inequality holds since $|S| \le 2^{m-1}$.

Hence,

$$\begin{aligned}\Pr_{h \in \mathcal{H}}[\exists x \in S \text{ s.t. } h(x) = 0 \wedge \forall y \in S \setminus \{x\}, (h(y) \neq 0)] &= \sum_{x \in S} \Pr_{h \in \mathcal{H}}[h(x) = 0 \wedge \forall y \in S \setminus \{x\}, (h(y) \neq 0)] \\ &\ge \frac{|S|}{2^{m-1}} \ge \frac{1}{8},\end{aligned}$$

where the first equality holds by independence of the events inside the probability, and the last equality holds since $|S| \geq 2^{m-2}$. ■

Using both lemmas we can prove Valiant-Vazirani's theorem. Given an instance φ for SAT, the polynomial time algorithm A does the following:

1. It picks at random $m \in \{2, \ldots, n+1\}$.
2. It picks at random a hash function from the hash family $\mathcal{H}$ given by Lemma 1.
3. It outputs the formula $\psi(x) = \varphi(x) \wedge [h(x) = 0]$.

If $\varphi(x) \in SAT_{YES}$, then with probability $1/n$, A picks the right m. Using Lemma 2 for S the set of satisfying assignments of φ, we know that A picks a hash function from $\mathcal{H}$, such that $h(x) = 0$ for an unique $x \in S$. It follows that with probability $1/(8n)$ the algorithm outputs a formula with only one satisfying assignment, i.e. a formula in U_{YES}.

On the other hand, if $\varphi(x) \in SAT_{NO}$, then A will output $\psi(x)$ that has no satisfying assignment. Hence A is an RP reduction from SAT to *Unique-SAT*.

2.1 Consequences

Corollary 1 $SAT \leq_{RP} \bigoplus SAT$.
Where $\bigoplus SAT := \{\phi \mid \textit{Number of satisfying assignments of } \phi \textit{ is even } \}$

Proof
We reduce *Unique-SAT* to $\bigoplus SAT$ as following. For given $\psi(x) \in$ *Unique-SAT*,

$$\psi^{'}(bx) := \begin{cases} 1, & b = 0, x = \overline{0} \\ 1, & b = 1, \psi(x) = 1 \\ 0, & o.w. \end{cases}$$

Combining with $SAT \leq_{RP}$ *Unique-SAT*, the corollary follows! ■

Now we can use this reduction k times to get,

$$\begin{aligned} \psi \quad &\longrightarrow \quad \psi_1(x_1) \\ &\longrightarrow \quad \psi_2(x_2) \\ &\longrightarrow \quad \psi_3(x_3) \\ &\cdots \\ &\longrightarrow \quad \psi_k(x_k) \end{aligned}$$

Set $\hat{\psi}$ as,

$$\hat{\psi}(x_1, \cdots, x_k) = \bigwedge_{i=1}^{k} \psi_i(x_i)$$

Then, # of satisfying assignments of $\hat{\psi} = \prod$(#of satisfying assignments of ψ_i)
So if the # of satisfying assignments for some ψ_i is even, then # of satisfying assignments for $\hat{\psi}$ is even too! From this we get :

$$SAT \leq_{StrongBP} \bigoplus SAT$$

3 Toda's Theorem

Theorem 2 (Toda) $PH \subseteq P^{\#P}$

3.1 Operators

For a complexity class $\mathcal{C}$, define the following operators:

Parity Operator :

- $\bigoplus \mathcal{C} := \{\bigoplus L | L \in \mathcal{C}\}$
- $\bigoplus L := \{x | \#$ of y's satisfying $(x, y) \in L$ is even $\}$

BP Operator :

- $BP \cdot \mathcal{C} := \{BP \cdot L | L \in \mathcal{C}\}$
- $BP \cdot L := \{x | \ Pr_y[(x, y) \in L] \geq 1 - 2^{-q(n)}\}$
- i.e., if $x \notin BP \cdot L$, $Pr_y[(x, y) \in L] \leq 2^{-q(n)}$

$\exists$ Operator :

- $\exists \mathcal{C} := \{\exists L | L \in \mathcal{C}\}$
- $\exists L := \{x | \exists y$ such that $(x, y) \in L\}$.

3.2 Properties

Proofs will be shown on Wednesday.

1. $\bigoplus \cdot P \cdot \mathcal{C} \leq BP \cdot \bigoplus \mathcal{C}$.
2. $\bigoplus \cdot \bigoplus \cdot \mathcal{C} \leq \bigoplus \mathcal{C}$.
3. $BP \cdot BP \cdot \mathcal{C} \leq BP \cdot \mathcal{C}$.

3.3 Main Ideas

$SAT \leq_{StrongBP} \bigoplus SAT$ implies:

- $NP \subseteq BP \cdot \bigoplus \cdot P$.
- $Co\text{-}NP \subseteq BP \cdot \bigoplus \cdot P$, because $BP \cdot \bigoplus \cdot P$ is closed under complement.

$$\begin{aligned}\Sigma_2^P \subseteq \exists \cdot \forall \cdot P &\subseteq BP \cdot \bigoplus \cdot BP \cdot \bigoplus \cdot P \\ &\subseteq BP \cdot BP \cdot \bigoplus \cdot \bigoplus \cdot P \text{ (Using properties above)} \\ &\subseteq BP \cdot \bigoplus \cdot P.\end{aligned}$$

By induction, we can get

$$\Sigma_k^P \subseteq BP \cdot \bigoplus \cdot P.$$

which implies $PH \subseteq BP \cdot \bigoplus \cdot P$.

4 To show Next time

- $BP \cdot \bigoplus \cdot P \subseteq P^{\#P}$.
- $L := \{(M, x, a, b) | \# \ \{y | M(x, y) \text{ accepts }\} \leq a(mod\ b)\ \} \in P^{\#P}$.
- $\Sigma_k^P \subseteq \exists \cdot BP \cdot \bigoplus \cdot P$.