CS6840: Advanced Complexity Theory Feb 6, 2012

Lecture 17 : Reductions to $\oplus$-SAT: Amplified version

Lecturer: Jayalal Sarma *Scribe: Princy Lunawat*

The last few lectures focus on the Toda's theorem which states that $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$. The first half of the proof of the theorem shows a randomized reduction from PH to $\oplus\mathsf{SAT}$.

We proved the Valiant-Vazirani lemma which stated a randomized polynomial time algorithm that takes in a formula ϕ and produces a new formula ψ such that it gives a *weak form* of a randomized reduction from SAT to $U\mathsf{SAT}$. We have the following

$$\begin{aligned}\phi \in \mathsf{SAT} &\Rightarrow Pr\,(\psi \in \mathrm{U}\mathsf{SAT}) \geq \frac{1}{8n} \\ \phi \notin \mathsf{SAT} &\Rightarrow Pr\,(\psi \notin U\mathsf{SAT}) = 1\end{aligned}$$

We also concluded that this gives a weak[1] randomized reduction from NP to $\oplus\mathsf{SAT}$. Now we show how to amplify the success probability in the case of the reduction to $\oplus\mathsf{SAT}$. [2]

Indeed, something special about $\oplus$ is going to help us. In this lecture, we explore some properties of the $\oplus$ quantifier which are used to come up with a formula ϕ'' from a given formula $\phi \in \mathsf{SAT}$ such that $\phi'' \in \oplus\mathsf{SAT}$ with high probability. We thereby deduce that $\mathsf{NP} <_r^m \oplus\mathsf{SAT}$.

1 Parity Addition, Complementation and Multiplication

Given two boolean formulae, ϕ and ϕ', their parity can be added as follows:

$$\oplus(\phi + \phi')(\bar{z}) = \oplus(z_0 = 0 \wedge \phi) \vee \oplus(z_1 = 0 \wedge \phi')$$

Similarly, the parity can be complemented as:

$$(z = 0) \wedge (\sim x_1 \wedge \sim x_2 \wedge \ldots \wedge \sim x_n) \vee (\phi \wedge z = 1)$$

which is represented as $\phi + 1$. Multiplication of parity is obtained as:

$$\oplus\phi(\bar{z}) \times \oplus\phi'(\bar{z}) = \oplus(\phi(\bar{z}) \wedge \phi'(\bar{z}))$$

[1] The reduction is weak because the error probability$(1 - \frac{1}{8n})$ is much more than what is allowed in a randomized reduction $(\frac{1}{2})$

[2] Such an amplification is not known for the case of $U\mathsf{SAT}$.

2 Randomized Reduction

In our construction for the Valiant-Vazirani Lemma , we defined a formula $\psi_i = \phi \wedge (h_i(x) = 0^k)$ where x is an assignment of ϕ.Now consider a formula $\phi' = \overset{l-1}{\underset{i=0}{\wedge}} (\oplus \psi_i)$. if $\Pr[\psi_i \in \texttt{USAT}] \geq \frac{1}{8n}$, then $\Pr[\phi' \in \mathsf{SAT}] = 1 - \left(1 - \frac{1}{8n}\right)^l]$. We now come up with a formula ϕ'' equivalent to ϕ' such that the parity of ϕ'' is odd. that is, $\phi'' \in \oplus\mathsf{SAT}$ conditioned on the probability that atleast one $\psi_i \in \oplus\mathsf{SAT}$.
For simplicity, consider ψ_1 and ψ_2, one of which is in $\oplus\mathsf{SAT}$.We observe that both , $\psi_1 + 1$ and $\psi_2 + 1$ cannot have an odd parity. Therefore,we have,

$$\begin{aligned} \oplus(\psi_1 + 1).(\psi_2 + 1) &= 0 \\ \oplus((\psi_1 + 1).(\psi_2 + 1) + 1) &= 1 \end{aligned}$$

Hence, $((\psi_1 + 1).(\psi_2 + 1) + 1) \in \oplus\mathsf{SAT}$.In general , $\overset{l-1}{\underset{i=0}{\wedge}} ((\psi_i + 1) + 1) \in \oplus\mathsf{SAT}$ which is our new formula ϕ'' equivalent to ϕ. Hence , $\Pr[\phi'' \in \oplus\mathsf{SAT}]$ is the same as that of atleast one ψ_i having an odd parity.

$$\phi \in \mathsf{SAT} \Rightarrow Pr\left[\phi'' \in \oplus\mathsf{SAT}\right] = 1 - \left(1 - \frac{1}{8n}\right)^l$$

To amplify this probabilty to $1 - 2^{-m}$ we choose an appropriate value of l such that,

$$1 - \left(1 - \frac{1}{8n}\right)^l \geq 1 - 2^{-m}$$

Hence, we have

$$\begin{aligned} \phi \in \mathsf{SAT} &\Rightarrow Pr\left[\phi'' \in \oplus\mathsf{SAT}\right] \geq 1 - 2^{-m} \\ \phi \notin \mathsf{SAT} &\Rightarrow Pr\left[\phi'' \in \oplus\mathsf{SAT}\right] = 0 \end{aligned}$$

Hence, $\mathsf{NP} <_r^m \oplus\mathsf{SAT}$.