# Probabilistic Reduction from PH to $\oplus$P

This material was presented in class on April 14, 2016. We wish to prove

**Arora-Barak's Lemma 17.17**: For any constants $c$ and $m$ in $\mathcal{N}$, there exists a probabilistic polynomial-time algorithm $f$ such that, for any $\sum_c$SAT instance $\psi$,

$$\begin{aligned} \psi \text{ is true } &\longrightarrow \; Pr[f(\psi) \in \oplus SAT] \geq 1 - 2^{-m} \\ \psi \text{ is false } &\longrightarrow \; Pr[f(\psi) \in \oplus SAT] \leq 2^{-m} \end{aligned}$$

The $\oplus$SAT version of the Valiant-Vazirani lemma, which was presented in the previous lecture, gives us this result for $c = 1$. We will prove by induction on $c$ that the result holds not only for $\Sigma_c$SAT instances but also for $\Pi_c$SAT instances.

From the algorithm $f$ that reduces SAT to $\oplus$SAT with correctness probability $1 - 2^{-m}$, we can easily construct an algorithm $f'$ that reduces coSAT to $\oplus$SAT with the same correctness probability: Just let $f'(\psi) = f(\psi) + 1$, where addition of formulas and the formula "1" are as defined in Chapter 17 (and in class during the previous lecture). So the base case ($c = 1$ for both $\Sigma$ and $\Pi$) of what we're trying to prove is true. Our inductive hypothesis is that it is true for $c - 1$. In particular, it holds for instances $\psi$ of $\Pi_{c-1}$SAT. We will use this to prove that it holds for instances $\phi$ of $\Sigma_c$SAT. Any such $\phi$ is of the form

$$\phi(x_1, x_2, \ldots, x_c) = \exists x_1 \forall x_2 \cdots Q_c x_c \phi'(x_1, x_2, \ldots, x_c),$$

where each of the $x_i$'s is a *string* of boolean variables, and $Q_c$ is $\exists$ if $c$ is odd and $\forall$ if $c$ is even. Note that $\phi$ is of the form $\exists x_1 \psi(x_1)$, where $\psi(x_1)$ is an instance of $\Pi_{c-1}$SAT. By our inductive hypothesis, for any $m \in \mathcal{N}$, there is a probabilistic, polynomial-time algorithm $f$ such that $\rho(z, x_1) = (f(\psi(x_1)))(z)$, $\beta(x_1) = \oplus_z \rho(z, x_1)$, and, with probability at least $1 - 2^{-(m+1)}$, $\beta(x_1) = \psi(x_1)$. In particular, with probability at least $1 - 2^{-(m+1)}$, $\exists x_1 \beta(x_1)$ if and only if $\exists x_1 \psi(x_1)$.

We now examine the proof of the (USAT version of the) Valiant-Vazirani lemma and note that it is *oblivious* in the sense that it does not use the structure of the formula $\phi$ when producing the formula $\tau(\cdot, \cdot)$. Obliviousness implies that, for any boolean function $\beta$ on a string $x_1$ of $n$ boolean variables, the input $1^n$ is sufficient for the Valiant-Vazirani reduction to produce a boolean formula $\tau(w, q)$, where $|w| = n$ and $|q| = \text{poly}(n)$, such that, with probably at least $\frac{1}{8n}$, $\tau$ has a unique satisfying assignment. Note that, if $\tau$ has a unique satisfying assignment, then it is in $\oplus$P. So, for any boolean function $\beta$, we have

$$\begin{aligned} \exists x_1 \beta(x_1) &\longrightarrow \; Prob[(\oplus_{w,q} \tau(w, q)) \wedge (\beta(x_1) = 1)] \geq \frac{1}{8n} \\ \neg \exists x_1 \beta(x_1) &\longrightarrow \; Prob[(\oplus_{w,q}(\tau(w, q)) \wedge (\beta(x_1) = 1)] = 0. \end{aligned}$$

In our inductive proof, $\beta(x_1) = \oplus_z \rho(z, x_1)$, and $\rho$ is a formula of size polynomial in the size of our original $\Sigma_c$SAT instance $\phi$. Thus, we have

$$\begin{aligned} \exists x_1 \beta(x_1) &\longrightarrow Prob[(\oplus_{w,q} \tau(w,q)) \wedge (\oplus_z \rho(z, x_1))] \geq \frac{1}{8n} \\ \neg \exists x_1 \beta(x_1) &\longrightarrow Prob[(\oplus_{w,q} \tau(w,q)) \wedge (\oplus_z \rho(z, x_1))] = 0. \end{aligned}$$

Applying the definition of multiplication of formulas from our previous lecture, we get

$$\begin{aligned} \exists x_1 \beta(x_1) &\longrightarrow Prob[\oplus_{w,q,z} (\tau \cdot \rho)(w, q, z, x_1)] \geq \frac{1}{8n} \\ \neg \exists x_1 \beta(x_1) &\longrightarrow Prob[\oplus_{w,q,z} (\tau \cdot \rho)(w, q, z, x_1)] = 0. \end{aligned}$$

We can use the same procedure as we used to convert the USAT version of Valiant-Vazirani to the $\oplus$SAT version of Valiant-Vazirani in order to produce a formula $\alpha$ that, with probability $1 - 2^{-(m+1)}$, is in $\oplus$SAT if and only if $\exists x_1 \beta(x_1)$.

Finally, we compose these two reductions to transform our original instance $\phi$ of $\Sigma_c$SAT to a $\oplus$SAT instance $\alpha$ such that, with probability at least $1 - 2^{-m}$, $\phi \in \Sigma_c$SAT if and only if $\alpha \in \oplus$SAT. The error probability is at most $2^{-m}$, because an error occurs if and only if there is disagreement between $\phi = \exists x_1 \psi(x_1)$ and $\exists x_1 \beta(x_1)$ (which occurs with probability at most $2^{-(m+1)}$) or there is disagreement between $\exists x_1 \beta(x_1)$ and $\alpha \in \oplus$SAT (which also occurs with probability at most $2^{-(m+1)}$). We use the same "add 1" trick as we used for SAT and coSAT to conclude that the result holds for $\Pi_c$SAT if is hold for $\Sigma_c$SAT.