

Lec 26: Randomized reduction from PH to $\oplus$ SAT

Recap

- The $\oplus$ quantifier: $|\underline{x}| = n$.

$\bigoplus_{\underline{x}} \varphi(\underline{x})$ is true $\iff \varphi(\underline{x})$ has odd no. of satisfying assignments

$$\iff \sum_{\underline{x} \in \{0,1\}^n} \varphi(\underline{x}) = 1 \pmod{2}$$

- The VV theorem *: There's a randomized reduction f s.t.

$$\exists \underline{x} \varphi(\underline{x}) \text{ is true} \Rightarrow \Pr \left[\bigoplus_{\underline{x}} f(\varphi)(\underline{x}) \text{ is true} \right] \geq \frac{1}{8n}$$

$$\exists \underline{x} \varphi(\underline{x}) \text{ is false} \Rightarrow \Pr \left[\bigoplus_{\underline{x}} f(\varphi)(\underline{x}) \text{ is false} \right] = 1$$

— (1)

Oblivious nature of the VV reduction

- Recall the proof of the VV theorem:

$$\begin{array}{ccc} \varphi(x) & \xrightarrow[\substack{1. \text{ Pick } k \in_r \{2, \dots, n+1\} \\ 2. \text{ Pick } h \in_r H_{n,k}}]{f} & \boxed{\varphi(x) \wedge \psi_{k,h}(x) =: f(\varphi)(x)} \quad - (0) \\ \uparrow & & \uparrow \\ \text{i/p. Bool. ckt.} & & \text{ckt. that captures the computation} \\ & & \text{of a DTM that ops 1 iff } h(x) = 0^k. \end{array}$$

- The reduction f is very "syntactic" — it doesn't look into φ .
- Obs*: If we define $f(\varphi)(x)$, from $\varphi(x)$, as in Eqn (0), then Eqn (1) holds for any Boolean function φ .
But of course, $|f(\varphi)|$ depends on $|\varphi|$.

- Recall, for a Boolean ckt $\varphi(\underline{x})$, we've defined $(\varphi+1)(\underline{z}, \underline{x})$ in such a way that $\#(\varphi+1) = \#\varphi + 1$.

- Notation: Let $\varphi_1(\underline{x}_1), \dots, \varphi_m(\underline{x}_m)$ be ckt's on disjoint sets of variables. Define,

$$(\varphi_1 \cdot \varphi_2 \cdot \dots \cdot \varphi_m)(\tilde{\underline{x}}) := \varphi_1(\underline{x}_1) \wedge \dots \wedge \varphi_m(\underline{x}_m), \text{ where}$$

$$\tilde{\underline{x}} = \underline{x}_1 \uplus \underline{x}_2 \uplus \dots \uplus \underline{x}_m.$$

- Obs: $\#(\varphi_1 \cdot \varphi_2 \cdot \dots \cdot \varphi_m) = \#\varphi_1 \cdot \#\varphi_2 \cdot \dots \cdot \#\varphi_m$, and

$$|\varphi_1 \cdot \varphi_2 \cdot \dots \cdot \varphi_m| = \text{poly}(|\varphi_1|, \dots, |\varphi_m|).$$

Useful properties of the $\oplus$ quantifier

• Obs 1: (a) $\left(\bigoplus_{\underline{x}_1} \varphi_1(\underline{x}_1) \right) \wedge \left(\bigoplus_{\underline{x}_2} \varphi_2(\underline{x}_2) \right) \wedge \dots \wedge \left(\bigoplus_{\underline{x}_m} \varphi_m(\underline{x}_m) \right)$

$$\Leftrightarrow \bigoplus_{\tilde{\underline{x}}} (\varphi_1 \cdot \varphi_2 \cdot \dots \cdot \varphi_m)(\tilde{\underline{x}})$$

(b) $\neg \bigoplus_{\underline{x}} \varphi(\underline{x}) \Leftrightarrow \bigoplus_{\underline{z}, \underline{x}} (\varphi + 1)(\underline{z}, \underline{x})$

(c) $\left(\bigoplus_{\underline{x}_1} \varphi_1(\underline{x}_1) \right) \vee \left(\bigoplus_{\underline{x}_2} \varphi_2(\underline{x}_2) \right) \vee \dots \vee \left(\bigoplus_{\underline{x}_m} \varphi_m(\underline{x}_m) \right)$

$$\Leftrightarrow \neg \left[\left(\neg \bigoplus_{\underline{x}_1} \varphi_1(\underline{x}_1) \right) \wedge \left(\neg \bigoplus_{\underline{x}_2} \varphi_2(\underline{x}_2) \right) \wedge \dots \wedge \left(\neg \bigoplus_{\underline{x}_m} \varphi_m(\underline{x}_m) \right) \right]$$

$$\Leftrightarrow \bigoplus_{\underline{z}, \tilde{\underline{x}}} \left((\varphi_1 + 1) \cdot (\varphi_2 + 1) \cdot \dots \cdot (\varphi_m + 1) + 1 \right)(\underline{z}, \tilde{\underline{x}}) \quad \text{--- (2)}$$

where $|\underline{z}| = m+1$.

• Let $\Gamma := (\varphi_1 + 1) \cdot (\varphi_2 + 1) \cdot \dots \cdot (\varphi_m + 1) + 1$. Then,

$$\# \Gamma = (\# \varphi_1 + 1) (\# \varphi_2 + 1) \dots (\# \varphi_m + 1) + 1;$$

$$|\Gamma| = \text{poly}(|\varphi_1|, \dots, |\varphi_m|).$$

(d) Define $\bigoplus_{\underline{y}} \varphi(\underline{x}, \underline{y}) := \sum_{\underline{y} \in \{0,1\}^{|\underline{y}|}} \varphi(\underline{x}, \underline{y}) \pmod{2}$, which is a Boolean func. in the $\underline{x}$ vars. Then,

$$\bigoplus_{\underline{x}} \bigoplus_{\underline{y}} \varphi(\underline{x}, \underline{y}) = \bigoplus_{\underline{x}, \underline{y}} \varphi(\underline{x}, \underline{y}). \quad (\text{simple exercise})$$

Boosting the success prob. of the VV theorem*

- Lemma 1: There is a randomized reduction g that given a parameter p and a Boolean ckt. $\varphi(x)$, runs in time $\text{poly}(|\varphi|, p)$ and outputs a ckt. $g(\varphi)(x, \tilde{x})$ s.t.

$$\exists \underline{x} \varphi(\underline{x}) \text{ is true} \Rightarrow \Pr_{\substack{\underline{x}, \tilde{x}}} [\bigoplus g(\varphi)(\underline{x}, \tilde{x}) \text{ is true}] \geq 1 - \frac{1}{2^p}$$

$$\exists \underline{x} \varphi(\underline{x}) \text{ is false} \Rightarrow \Pr_{\substack{\underline{x}, \tilde{x}}} [\text{" is false}] = 1.$$

- Proof: Run the VV reduction independently m times.

Let the outputs be $f(\varphi)(x_1), \dots, f(\varphi)(x_m)$

$\downarrow$
 $f(\varphi)_1$

$\downarrow$
 $f(\varphi)_m$

- Proof (contd.) We wish to output a $g(\varphi)(\underline{z}, \underline{\tilde{x}})$ s.t.

$$\bigoplus_{\underline{z}, \underline{\tilde{x}}} g(\varphi)(\underline{z}, \underline{\tilde{x}}) \Leftrightarrow \left(\bigoplus_{\underline{z}_1} f(\varphi)_1 \right) \vee \dots \vee \left(\bigoplus_{\underline{x}_m} f(\varphi)_m \right) \quad \text{--- (3)}$$

- By Obs 1(c), $g(\varphi)$ is easy to construct.

$$g(\varphi)(\underline{z}, \underline{\tilde{x}}) := \left((f(\varphi)_1 + 1) \cdot (f(\varphi)_2 + 1) \cdot \dots \cdot (f(\varphi)_m + 1) + 1 \right) (\underline{z}, \underline{\tilde{x}})$$

- Obs: If $\exists \underline{x} \varphi(\underline{x})$ is false, then by $\vee\vee$ theorem*,

$$\bigoplus_{\underline{z}, \underline{\tilde{x}}} g(\varphi)(\underline{z}, \underline{\tilde{x}}) \text{ is false with probability } 1.$$

• Suppose $\exists \underline{x} \varphi(\underline{x})$ is true. Then,

$$\Pr \left[\bigoplus_{\underline{z}, \tilde{\underline{x}}} g(\varphi)(\underline{z}, \tilde{\underline{x}}) \text{ is false} \right]$$
$$= \Pr \left[\bigoplus_{\underline{z}_1} f(\varphi)_1 \text{ is false} \right] \cdot \dots \cdot \Pr \left[\bigoplus_{\underline{z}_m} f(\varphi)_m \text{ is false} \right]$$
$$\leq \left(1 - \frac{1}{8n}\right)^m \leq \frac{1}{2^p} \text{ if } m = 10np, \text{ where } |\underline{x}| = |\underline{x}_i| = n.$$

$$\therefore \Pr \left[\bigoplus_{\underline{z}, \tilde{\underline{x}}} g(\varphi)(\underline{z}, \tilde{\underline{x}}) \text{ is true} \right] \geq 1 - \frac{1}{2^p}.$$

Lemma 1 gives a randomized poly-time reduction from $\Sigma_1\text{SAT}$ to $\oplus\text{SAT}$ with high success probability.

Reduction from Π_1 -SAT to $\oplus$ SAT

- Lemma 2: There is a randomized reduction g that given a parameter p and a det. $\varphi(\underline{x})$ runs in time $\text{poly}(|\varphi|, p)$ and outputs a cht. $g(\varphi)(\underline{z}, \underline{\tilde{x}})$ s.t.

$$\forall \underline{x} \varphi(\underline{x}) \text{ is true} \Rightarrow \Pr_{\underline{z}, \underline{\tilde{x}}} \left[\bigoplus g(\varphi)(\underline{z}, \underline{\tilde{x}}) \text{ is true} \right] = 1,$$

$$\forall \underline{x} \varphi(\underline{x}) \text{ is false} \Rightarrow \Pr_{\underline{z}, \underline{\tilde{x}}} \left[\bigoplus g(\varphi)(\underline{z}, \underline{\tilde{x}}) \text{ is false} \right] \geq 1 - \frac{1}{2^p}.$$

- Proof: We wish to construct a $g(\varphi)(\underline{z}, \underline{\tilde{x}})$ s.t.

$$\bigoplus_{\underline{z}, \underline{\tilde{x}}} g(\varphi)(\underline{z}, \underline{\tilde{x}}) \Leftrightarrow \neg \left(\bigoplus_{\underline{x}_1} f(\neg \varphi)_1 \vee \dots \vee \bigoplus_{\underline{x}_m} f(\neg \varphi)_m \right)$$

By Obs 1(c),

$$g(\varphi)(\underline{z}, \underline{\tilde{x}}) := (f(\neg \varphi)_1 + 1) \cdot \dots \cdot (f(\neg \varphi)_m + 1), \text{ where } m = |\text{Onp}|. \quad (4)$$

Today's theorem: Step 1 (base case)

- Corollary 1: (follows from Lemma 1 & 2). There is a rand. reduction g that given a parameter p and a QBF φ with one level of alternation, runs in time $\text{poly}(|\varphi|, p)$ and outputs a ckt. $g(\varphi)$ s.t.

$$\varphi \text{ is true} \Rightarrow \Pr [\oplus g(\varphi) \text{ is true}] \geq 1 - \frac{1}{2^p},$$

$$\varphi \text{ is false} \Rightarrow \Pr [\oplus g(\varphi) \text{ is false}] \geq 1 - \frac{1}{2^p},$$

$$\text{i.e., } \varphi \Leftrightarrow \oplus g(\varphi) \text{ w.p. } \geq 1 - \frac{1}{2^p}.$$

- The above corollary serves as the base case of the inductive proof of Step 1 of Today's theorem. The induction is on the no. of alternations.

Randomized reduction from Σ_c -SAT to $\oplus$ SAT

Theorem 1: There is a randomized reduction g that given a parameter p and a QBF φ with c levels of alternations, runs in time $\text{poly}(|\varphi|, p)$ and outputs a ckt. $g(\varphi)$ s.t.

$$\varphi \text{ is true} \Rightarrow \Pr[\oplus g(\varphi) \text{ is true}] \geq 1 - \frac{1}{2^p},$$

$$\varphi \text{ is false} \Rightarrow \Pr[\oplus g(\varphi) \text{ is false}] \geq 1 - \frac{1}{2^p},$$

i.e. $\varphi \iff \oplus g(\varphi)$ with prob. $\geq 1 - \frac{1}{2^p}$. — (5)

Proof: We will prove the theorem for $c=2$. The proof of the general case is similar. The idea is to apply the VV theorem c times.

Randomized reduction from Σ_2 -SAT to $\oplus$ SAT

- Let $\exists \underline{u} \forall \underline{v} \varphi(\underline{u}, \underline{v})$ be the i/p QBF. We wish to construct a $g(\varphi)$ that satisfies Eqn. (5).
- Fix a $\underline{u}$ arbitrarily. Then, $\forall \underline{v} \varphi(\underline{u}, \underline{v})$ is a QBF in the $\underline{v}$ variables with one quantifier.
- By Lemma 2 and Corollary 1, there is a $\text{poly}(|\varphi|, p')$ computable ckt. $g'(\varphi)$ s.t.
 $\forall \underline{v} \varphi(\underline{u}, \underline{v}) \Leftrightarrow \oplus g'(\varphi) \quad \omega.p. \geq 1 - \frac{1}{2^{p'}}.$

Note: $|g'(\varphi)| = \text{poly}(|\varphi|, p')$. We'll fix p' later in the analysis.

- Let us understand the structure of $g'(\varphi)$.

- By Eqn. (4) in the proof of Lemma 2,

$$g'(\varphi)(\underline{u}, \underline{z}', \underline{\tilde{v}}) = (f(\neg\varphi)_1 + 1) \cdot \dots \cdot (f(\neg\varphi)_{m'} + 1), \text{ where } m' = 10 \cdot |\underline{v}| \cdot p' \text{ and}$$

$$f(\neg\varphi)_i = f(\neg\varphi)(\underline{u}, \underline{v}_i) = \neg\varphi(\underline{u}, \underline{v}_i) \wedge \psi_{k'_i, h'_i}(\underline{v}_i).$$

- So, $f(\neg\varphi)_i + 1 = (f(\neg\varphi)_i + 1)(\underline{u}, \underline{z}'_i, \underline{v}_i)$.

- The expression for $g'(\varphi)$ above is very "syntactic" with regard to the $\underline{u}$ -vars. It does not "touch" the $\underline{u}$ -vars.

- For an arbitrarily fixed $\underline{u}$, we have

$$\forall \underline{v} \quad \phi(\underline{u}, \underline{v}) \iff \bigoplus_{\underline{z}', \underline{\tilde{v}}} g'(\phi)(\underline{u}, \underline{z}', \underline{\tilde{v}}) \quad \text{with prob.} \geq 1 - \frac{1}{2^P}.$$

- By union bound,

$$\forall \underline{v} \quad \phi(\underline{u}, \underline{v}) \iff \bigoplus_{\underline{z}', \underline{\tilde{v}}} g'(\phi)(\underline{u}, \underline{z}', \underline{\tilde{v}}) \quad \text{with prob.} \geq 1 - \frac{1}{2^{P'-|\underline{u}|}},$$

irrespective of $\underline{u}$. Hence,

- $\exists \underline{u} \forall \underline{v} \quad \phi(\underline{u}, \underline{v}) \iff \exists \underline{u} \bigoplus_{\underline{z}', \underline{\tilde{v}}} g'(\phi)(\underline{u}, \underline{z}', \underline{\tilde{v}}) \quad \text{w.p.} \geq 1 - \frac{1}{2^{P'-|\underline{u}|}}.$

- Let $\tau(\underline{u}) := \bigoplus_{\underline{z}', \underline{v}} g'(\varphi)(\underline{u}, \underline{z}', \underline{v})$. — (6)

- $\tau(\underline{u})$ is a Boolean function in the $\underline{u}$ -vars, but it may not have a $\text{poly}(|\varphi|)$ size circuit.

- Then, $\exists \underline{u} \forall \underline{v} \varphi(\underline{u}, \underline{v}) \Leftrightarrow \exists \underline{u} \tau(\underline{u})$ w.p. $\geq 1 - \frac{1}{2^{P' - |\underline{u}|}}$. — (7)

- From Obs *, if we replace φ by τ in Lemma 1 and construct $g(\tau)$ as in Eqn (3), then $\hookrightarrow$ v v thm.

$$\exists \underline{u} \tau(\underline{u}) \Leftrightarrow \bigoplus g(\tau) \quad \underline{\text{w.h.p.}} \quad \text{--- (8)}$$

- But, we need to think about the circuit complexity of $g(\tau)$. So, let us scrutinize the structure of $g(\tau)$ using Eqn (3). We want a $g(\tau)$ s.t.

$$\bigoplus g(\tau) \iff \left(\bigoplus_{\underline{u}_1} f(\tau)_1 \right) \vee \dots \vee \left(\bigoplus_{\underline{u}_m} f(\tau)_m \right) \quad \text{--- (9)}$$

where $f(\tau)_i = f(\tau)(\underline{u}_i) = \tau(\underline{u}_i) \vee \psi_{k_i, h_i}(\underline{u}_i)$

$$= \bigoplus_{\underline{z}', \underline{\tilde{v}}} g'(\varphi)(\underline{u}_i, \underline{z}', \underline{\tilde{v}}) \vee \psi_{k_i, h_i}(\underline{u}_i) \quad [\text{by Eqn (6)}]$$

$$= \bigoplus_{\underline{z}', \underline{\tilde{v}}} \left(g'(\varphi)(\underline{u}_i, \underline{z}', \underline{\tilde{v}}) \vee \psi_{k_i, h_i}(\underline{u}_i) \right).$$

- In the above equation, the $\underline{z}', \underline{\tilde{v}}$ vars are bounded by the $\oplus$ quantifier. So, we can assume they are fresh sets of vars. $\underline{z}'_i, \underline{\tilde{v}}_i$.

Hence, $\bigoplus_{\underline{u}_i} f(\tau)_i = \bigoplus_{\underline{u}_i} \bigoplus_{\underline{z}'_i, \underline{\tilde{v}}_i} \left(g'(\varphi)(\underline{u}_i, \underline{z}'_i, \underline{\tilde{v}}_i) \vee \psi_{k_i, h_i}(\underline{u}_i) \right)$

[by Obs 1(d)] $= \bigoplus_{\underline{u}_i, \underline{z}'_i, \underline{\tilde{v}}_i} \underbrace{\left(g'(\varphi)(\underline{u}_i, \underline{z}'_i, \underline{\tilde{v}}_i) \vee \psi_{k_i, h_i}(\underline{u}_i) \right)}_{\text{Call this } h(\varphi)(\underline{u}_i, \underline{z}'_i, \underline{\tilde{v}}_i) =: h(\varphi)_i}$

$= \bigoplus_{\underline{u}_i, \underline{z}'_i, \underline{\tilde{v}}_i} h(\varphi)_i$

- Note that $|h(\varphi)_i| = \text{poly}(|\varphi|, P')$.

- From $\Sigma_{\text{eqn}}(9)$, we want a $g(\tau)$ s.t.

$$\bigoplus g(\tau) \Leftrightarrow \left(\bigoplus_{\underline{u}_1, \underline{z}'_1, \underline{\tilde{v}}_1} h(\varphi)_1 \right) \vee \dots \vee \left(\bigoplus_{\underline{u}_m, \underline{z}'_m, \underline{\tilde{v}}_m} h(\varphi)_m \right) \quad - (10)$$

- Set $m = 10 \cdot |\underline{u} \cup \underline{z}' \cup \underline{\tilde{v}}| \cdot p$, so that the above equivalence happens w.p. $\geq 1 - \frac{1}{2^p}$.
- Finally, $\exists \underline{u} \forall \underline{v} \varphi(\underline{u}, \underline{v}) \Leftrightarrow \exists \underline{u} \tau(\underline{u})$ w.p. $\geq 1 - \frac{1}{2^{p' - |\underline{u}|}}$ [by $\Sigma_{\text{eqn}}(7)$]
 $\Leftrightarrow \bigoplus g(\tau)$ w.p. $\geq 1 - \frac{1}{2^p}$, [by $\Sigma_{\text{eqn}}(8)$]

where $g(\tau)$ is as in $\Sigma_{\text{eqn}}(10)$. Total err. prob. $\leq \frac{1}{2^{p' - |\underline{u}|}} + \frac{1}{2^p}$.