Lec 25: 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.

$$\boxed{\begin{array}{l} \exists \underline{x}\ \varphi(\underline{x}) \text{ is true} \Rightarrow \Pr\left[\bigoplus_{\underline{x}} f(\varphi)(\underline{x}) \text{ is true}\right] \geq \frac{1}{8n} \\ \nexists \underline{x}\ \varphi(\underline{x}) \text{ is false} \Rightarrow \Pr\left[\bigoplus_{\underline{x}} f(\varphi)(\underline{x}) \text{ is false}\right] = 1 \end{array}} \quad \text{--- (1)}$$

Oblivious nature of the VV reduction

- Recall the proof of the VV theorem:

$$\varphi(\underline{x}) \xrightarrow[\substack{1.\ \text{Pick } k \in_r \{2, \cdots, n+1\} \\ 2.\ \text{Pick } h \in_r \mathcal{H}_{n,k}}]{f} \boxed{\varphi(\underline{x}) \wedge \psi_{k,h}(\underline{x}) =: f(\varphi)(\underline{x})} \quad -(0)$$

i/p. Bool. ckt.

ckt. that captures the computation of a DTM that o/ps 1 iff $h(\underline{x}) = 0^k$.

- The reduction f is very "syntactic" — it doesn't look into φ.

- Obs*: If we define $f(\varphi)(\underline{x})$, from $\varphi(\underline{x})$, 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 $(\varphi+1)(z,\underline{x})$ in such a way that $\#(\varphi+1) = \#\varphi + 1$.
- Notation: Let $\varphi_1(\underline{x}_1), \cdots, \varphi_m(\underline{x}_m)$ be ckts. on disjoint sets of variables. Define,

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

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

- Obs: $\#\left(\varphi_1 \cdot \varphi_2 \cdot \cdots \cdot \varphi_m\right) = \#\varphi_1 \cdot \#\varphi_2 \cdots \#\varphi_m$, and

$$\left|\varphi_1 \cdot \varphi_2 \cdot \cdots \cdot \varphi_m\right| = \mathrm{poly}\left(|\varphi_1|, \cdots, |\varphi_m|\right).$$

Useful properties of the $\oplus$ quantifier

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

$$\iff \bigoplus_{\underline{\tilde{x}}} \left(\varphi_1 \cdot \varphi_2 \cdot \cdots \cdot \varphi_m\right)(\underline{\tilde{x}})$$

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

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

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

$$\iff \bigoplus_{\underline{z}, \underline{\tilde{x}}} \left((\varphi_1 + 1) \cdot (\varphi_2 + 1) \cdot \cdots \cdot (\varphi_m + 1) + 1\right)(\underline{z}, \underline{\tilde{x}}) \quad \text{—— } (2)$$

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

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

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

$$|\Gamma| = \mathrm{poly}(|\varphi_1|, \ldots, |\varphi_m|).$$

(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,

$$\bigoplus_{\underline{x}} \bigoplus_{\underline{y}} \varphi(\underline{x},\underline{y}) = \bigoplus_{\underline{x},\underline{y}} \varphi(\underline{x},\underline{y}).$$ (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. $\varphi(\underline{x})$, runs in time $\mathrm{poly}(|\varphi|, p)$ and outputs a ckt. $g(\varphi)(\underline{z}, \underline{\tilde{x}})$ s.t.

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

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

- **Proof:** Run the VV reduction independently m times. Let the outputs be $f(\varphi)(\underline{x}_1), \ldots, f(\varphi)(\underline{x}_m)$

$$f(\varphi)(\underline{x}_1) \downarrow f(\varphi)_1 \qquad f(\varphi)(\underline{x}_m) \downarrow f(\varphi)_m$$

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

$$\boxed{\bigoplus_{\underline{z}, \underline{\tilde{x}}} g(\varphi)(\underline{z}, \underline{\tilde{x}}) \Longleftrightarrow \left(\bigoplus_{\underline{x}_1} f(\varphi)_1\right) \vee \cdots \vee \left(\bigoplus_{\underline{x}_m} f(\varphi)_m\right)} \quad \text{— (3)}$$

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

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

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

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

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

$$\Pr\left[\bigoplus_{\underline{z},\underline{\tilde{x}}} g(\varphi)(\underline{z},\underline{\tilde{x}}) \text{ is false}\right]$$

$$= \Pr\left[\bigoplus_{\underline{x}_1} f(\varphi)_1 \text{ is false}\right] \cdot \ldots \cdot \Pr\left[\bigoplus_{\underline{x}_m} f(\varphi)_m \text{ is false}\right]$$

$$\leq \left(1-\frac{1}{8n}\right)^m \leq \frac{1}{2^p} \quad \text{if } m = 10np, \text{ where } |\underline{x}| = |\underline{x}_i| = n.$$

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

Lemma 1 gives a randomized poly-time reduction from Σ_iSAT to $\oplus$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 ckt. $\varphi(\underline{x})$ runs in time poly$(|\varphi|, p)$ and outputs a ckt $g(\varphi)(\underline{z}, \underline{\tilde{x}})$ 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.

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

By Obs 1(c),

$$\boxed{g(\varphi)(\underline{z}, \underline{\tilde{x}}) := \left(f(\neg\varphi)_1 + 1\right) \cdot \cdots \cdot \left(f(\neg\varphi)_m + 1\right)}, \text{ where } m = 10np. \quad (4)$$

Toda'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 <u>one</u> level of alternation, runs in time $\mathrm{poly}(|\varphi|, p)$ and outputs a ckt. $g(\varphi)$ s.t.

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

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

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

- The above corollary serves as the base case of the inductive proof of Step 1 of Toda'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. $\boxed{\varphi \Leftrightarrow \oplus g(\varphi) \text{ with prob. } \geq 1 - \frac{1}{2^p}.}$ —— (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 poly$(|\varphi|, p')$ computable ckt. $g'(\varphi)$ s.t.

VV thm.

$$\forall \underline{v}\, \varphi(\underline{u}, \underline{v}) \Longleftrightarrow \oplus g'(\varphi) \quad \text{w.p.} \geq 1 - \frac{1}{2^{p'}}.$$

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,

$$g'(\varphi)(\underline{u}, \underline{z}', \underline{\tilde{v}}) = \left(f(\neg\varphi)_1 + 1\right) \cdot \dots \cdot \left(f(\neg\varphi)_{m'} + 1\right),$$ where $m' = 10 \cdot |\underline{v}| \cdot p'$ 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, $f(\neg\varphi)_i + 1 = \left(f(\neg\varphi)_i + 1\right)(\underline{u}, z_i', \underline{v}_i)$.
- The expression for $g'(\varphi)$ above is <u>very "syntactic" with regard to the $\underline{u}$-vars.</u> It does not "touch" the $\underline{u}$-vars.

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

$$\forall \underline{v}\ \varphi(\underline{u},\underline{v}) \Longleftrightarrow \bigoplus_{\underline{z}',\tilde{\underline{v}}} g'(\varphi)(\underline{u},\underline{z}',\tilde{\underline{v}}) \text{ with prob. } \geq 1-\frac{1}{2^{p}}.$$

- By union bound,

$$\boxed{\forall \underline{v}\ \varphi(\underline{u},\underline{v}) \Longleftrightarrow \bigoplus_{\underline{z}',\tilde{\underline{v}}} g'(\varphi)(\underline{u},\underline{z}',\tilde{\underline{v}}) \text{ with prob. } \geq 1-\frac{1}{2^{p'-|\underline{u}|}},}$$

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

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

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

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

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

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

  ↳ VV thm.

$$\boxed{\exists u\, \tau(u) \Leftrightarrow \oplus g(\tau) \quad \text{w.h.p}} \quad \text{—— (8)}$$

- 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.

$$\boxed{\oplus g(\tau) \Longleftrightarrow \left(\bigoplus_{\underline{u}_1} f(\tau)_1\right) \vee \cdots \vee \left(\bigoplus_{\underline{u}_m} f(\tau)_m\right)} \qquad (9)$$

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

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

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

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

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

- Note that $\boxed{|h(\varphi)_i| = \mathrm{poly}(|\varphi|, p').}$

- From Eqn(9), we want a $g(\tau)$ s.t.

$$\boxed{\oplus g(\tau) \Longleftrightarrow \left(\bigoplus_{\underline{u}_1, \underline{z}'_1, \tilde{\underline{v}}_1} h(\varphi)_1\right) \vee \cdots \vee \left(\bigoplus_{\underline{u}_m, \underline{z}'_m, \tilde{\underline{v}}_m} h(\varphi)_m\right)} \quad -(10)$$

- Set $m = 10 \cdot |\underline{u} \uplus \underline{z}' \uplus \tilde{\underline{v}}| \cdot p$, so that the above equivalence happens w.p. $\geq 1 - \frac{1}{2^p}$.

- Finally, $\exists \underline{u} \forall \underline{v}\ \varphi(\underline{u}, \underline{v}) \Longleftrightarrow \exists \underline{u}\ \tau(\underline{u})$ w.p $\geq 1 - \frac{1}{2^{p'-|\underline{u}|}}$ [by Eqn(7)]

$\Longleftrightarrow \oplus g(\tau)$ w.p $\geq 1 - \frac{1}{2^p}$, [by Eqn(8)]

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