Lec17

Recap: ▷ $\oplus$ quantifier: $\bigoplus_{\underline{x}} \varphi(\underline{x})$ is true $\iff$ $\varphi(\underline{x})$ has odd no. of sat. assgn.

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

$n = |\underline{x}|$.

▷ V-V thm: $\varphi(\underline{x}) \xrightarrow{f} \varphi(\underline{x}) \wedge \Psi_{k,h}(\underline{x})$

Bool. ckt.

1. Picks $k \in_r \{2, \cdots, n+1\}$
2. Picks $h \in_r \mathcal{H}_{n,k}$

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

$$\boxed{f(\varphi)(\underline{x}) = \varphi(\underline{x}) \wedge \Psi_{k,h}(\underline{x})} \quad (0)$$

$f(\varphi)$ is "syntactic"

Obs: $\Psi_{k,h}(\underline{x})$ doesn't depend on φ.

$|f(\varphi)| = poly(|\varphi|)$.

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

Obs *: (oblivious nature of the VV reduction)
If we define $f(\varphi)$, from φ, as in Eqn (0), then Eqn (1) holds for any Boolean function φ. But of course, the $|f(\varphi)|$ depends on ~~the~~ $|\varphi|$.

▷ For a Bool. ckt $\varphi(\underline{x})$, we've defined $(\varphi+1)(z, \underline{x})$ s.t. $\#(\varphi+1) = \#\varphi + 1$

Notation: Let $\varphi_1(\underline{x}_1), \cdots, \varphi_m(\underline{x}_m)$ be ckts on disjoint sets of variables.

Define
$$(\varphi_1 \cdot \varphi_2 \cdots \varphi_m)(\tilde{\underline{x}}) = \varphi_1(\underline{x}_1) \wedge \cdots \wedge \varphi_m(\underline{x}_m), \text{ where}$$
$$\tilde{\underline{x}} = \underline{x}_1 \uplus \cdots \uplus \underline{x}_m .$$

Obs: $\#(\varphi_1 \cdots \varphi_m) = \#\varphi_1 \, \#\varphi_2 \cdots \#\varphi_m$.

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

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

$$\iff \bigoplus_{\underline{\tilde{x}}} (\varphi_1 \cdots \varphi_m)(\underline{\tilde{x}})$$

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

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

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

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

Let $\Gamma := (\varphi_1+1)(\varphi_2+1)\cdots(\varphi_m+1)+1$

Then, $\#\Gamma = (\#\varphi_1+1)(\#\varphi_2+1)\cdots(\#\varphi_m+1)+1$, $|\Gamma| = \mathrm{poly}(|\varphi_1|,\ldots,|\varphi_m|)$.

(d) Let $\bigoplus_{\underline{y}} \varphi(\underline{x},\underline{y}) := \sum_{\underline{y}\in\{0,1\}^{|\underline{y}|}} \varphi(\underline{x},\underline{y}) \mod 2$ be a B. form on the $\underline{x}$-var.

Then, $\bigoplus_{\underline{x}} \bigoplus_{\underline{y}} \varphi(\underline{x},y) = \bigoplus_{\underline{x},\underline{y}} \varphi(\underline{x},\underline{y})$. (~~##~~ simple ex)

<u>Lemma 1</u> (Boosting the succ. prob in Thm $*$) There's a rand. red. g that given a para. p & a Bool. ckt φ, runs in time $\mathrm{poly}(|\varphi|, p)$ & o/p's a ckt $g(\varphi)(\underline{z},\underline{\tilde{x}})$ s.t.

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

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

__Pf:__ Run the V-V red. f independently m times.

Let the dp's be $f(\varphi)(\underline{x}_1), \ldots, f(\varphi)(\underline{x}_m)$

$$f(\varphi)(\underline{x}_1) = f(\varphi)_1, \quad \ldots, \quad f(\varphi)(\underline{x}_m) = f(\varphi)_m$$

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

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

From Eqn (2)$^{(c)}$, $g(\varphi)$ is easy to construct,

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

__Obs:__ If $\exists \underline{x}\, \varphi(\underline{x})$ is false then by Thm* $\bigoplus_{\underline{z}, \underline{\tilde{x}}} g(\varphi)(\underline{z}, \underline{\tilde{x}})$ is false w.p.1

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

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

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

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

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

Note: Lemma I gives a rand. poly-time red. from $\Sigma_1 SAT$ to $\oplus SAT$ w.h. succ. prob.

What abt. red. from Π_1-SAT to $\oplus$SAT?

<u>Lemma 2:</u> (rand. red. from Π_1-SAT to $\oplus$SAT). There's a rand. red. g that given a para p & a ckt φ, runs in time poly$(|\varphi|, p)$ & o/p's a ckt $g(\varphi)(\underline{z}, \underline{\tilde{x}})$ s.t.

$$\forall \underline{x}\ \varphi(\underline{x}) \text{ is true} \Rightarrow \Pr\Big[\bigoplus_{\underline{z},\underline{\tilde{x}}} g(\varphi)(\underline{z}, \underline{\tilde{x}}) \text{ is true}\Big] = 1$$

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

<u>Pf</u> (sketch): Take

$$\boxed{g(\varphi)(\underline{z}, \underline{\tilde{x}}) := \big(f(\neg\varphi)_1 + 1\big) \cdots \big(f(\neg\varphi)_m + 1\big)}$$ 4

, where $m = 10np$

<u>Obs:</u> $$\bigoplus_{\underline{z},\underline{\tilde{x}}} g(\varphi) \iff \neg\Big(\bigoplus_{\underline{x}_1} f(\neg\varphi)_1 \vee \cdots \vee \bigoplus_{\underline{x}_m} f(\neg\varphi)_m\Big)$$

<u>Cor 1</u> (from Lem 1 & 2): There's a rand. red. g that given a para. p & a QBF φ with 1 level of alternation runs in time poly$(|\varphi|, p)$ & o/p's a ckt $g(\varphi)$ s.t.

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

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

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

Cor 1 serves as the base case of the inductive proof of Step 1 of Toda's thm. The induction is on the no. of alternations.

Thm 1 (Rand. red. from Σ_c-SAT to $\oplus$SAT). There's a rand. red. g that given a para p & a QBF φ with c levels of alternations runs in time $\text{poly}(|\varphi|, p)$ & φ's a ckt $g(\varphi)$ s.t.

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

$$\varphi \text{ is false} \Rightarrow \Pr[\oplus g(\varphi) \text{ is false}] \geq \text{"} .$$

i.e., $\boxed{\varphi \Longleftrightarrow \oplus g(\varphi) \quad \text{w.p.} \geq 1 - \frac{1}{2^p}.}$ — (5)

We'll prove Thm-2 for $c=2$. The proof of the gen. case is similar. The idea is to apply VV thm for c times.

Rand. red. 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 $g(\varphi)$ that satisfies Eqn (5).
- Fix a $\underline{u}$ arbitrarily. Then, $\forall \underline{v} \varphi(\underline{u}, \underline{v})$ is a QBF (on the $\underline{v}$-vars) with 1 quantifier.
- Then by Lemma 2 & Cor 1, there's a poly$(|\varphi|, p')$ computable $g'(\varphi)$ s.t.

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

<u>Note</u>: $|g'(\varphi)| = \text{poly}(|\varphi|, p')$.

▷ Let's understand the structure of $g'(\varphi)$.

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

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

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,

$$(f(\neg\varphi)_i + 1) = (f(\neg\varphi)_i + 1)(\underline{u}, z_i', \underline{v}_i)$$

$$= (z_i' \wedge f(\neg\varphi)(\underline{u}, \underline{v}_i)) \vee (\neg z_i' \wedge \underbrace{v_1 \wedge \cdots \wedge v_{n_2}}_{\underline{v}_i\text{-vars.}})$$

Obs: The expression for $g'(\varphi)$ is very syntactic with regard to the $\underline{u}$-vars. [It doesn't quite "touch" $\underline{u}$-vars]

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

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

▷ If we choose $p' \geq |\underline{u}|^2$, then by union bound,

for all $\underline{u}$,

$$\forall \underline{v}\ \varphi(\underline{u},\underline{v}) \iff \bigoplus_{\underline{z}',\underline{\tilde{v}}} g'(\varphi)(\underline{u},\underline{z}',\underline{\tilde{v}}) \quad \text{w.h.p.}$$

Hence,

$$\exists \underline{u}\, \forall \underline{v}\, \varphi(\underline{u}, v) \iff \exists \underline{u} \bigoplus_{\underline{z}', \underline{\tilde{v}}} g'(\varphi)(\underline{u}, \underline{z}', \underline{\tilde{v}}) \quad \text{w.h.p.}$$

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

$\tau(\underline{u})$ is a B. func. in the $\underline{u}$-vars, but it may not have a poly$(|\varphi|)$ ckt.

<u>By defn</u>:

$$\tau(\underline{u}) = \sum_{\underline{z}', \underline{\tilde{v}}} g'(\varphi)(\underline{u}, \underline{z}', \underline{\tilde{v}}) \mod 2. \quad \left(\text{recall Obs 1 (d)}\right)$$

Then

$$\boxed{\exists \underline{u}\, \forall \underline{v}\, \varphi(\underline{u}, \underline{v}) \iff \exists \underline{u}\, \tau(\underline{u}) \quad \text{w.h.p.}}$$ — (7)

Recall from Obs * that if we define $f(\tau)$, from τ, as in Eqn (0), then Eqn (1) holds for any B.f τ.
So, if we replace ϕ by τ in Lemma 1 & construct $g(\tau)$ as in Eqn (3) then

$$\boxed{\exists \underline{u}\, \tau(\underline{u}) \iff \bigoplus g(\tau) \quad \text{w.h.p}} \rightarrow (8)$$

But, we ~~xx~~ need to worry abt the ckt-complexity of $g(\tau)$. So, lets understand the structure of $g(\tau)$ carefully (from Eqn(3)). We want a $g(\tau)$ s.t.

$$\boxed{\bigoplus g(\tau) \iff \left(\bigoplus_{\underline{u}_1} f(\tau)_1\right) \vee \cdots \vee \left(\bigoplus_{\underline{u}_m} f(\tau)_m\right)} \rightarrow (9)$$

, where

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

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

(by Eqn (6))

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

The $\underline{z}'$, $\underline{\tilde{v}}$ vars are bounded by the $\bigoplus$ quantifier. So, we can as well assume that they are fresh sets of vars. $\underline{z}'_i$ & $\underline{\tilde{v}}_i$.

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

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

(by Obs 1(d))

<u>Note:</u> $|h(\varphi)_i| = \mathrm{poly}(|\varphi|, p')$.

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

$\therefore$ from Eqn (9), we want a $g(\tau)$ s.t.

$$\bigoplus_{\underline{z}, \tilde{\underline{u}}, \tilde{\underline{z}}', \tilde{\tilde{\underline{v}}}} g(\tau)(\underline{z}, \tilde{\underline{u}}, \tilde{\underline{z}}', \tilde{\tilde{\underline{v}}}) \iff \left(\bigoplus_{\underline{u}_1, \underline{z}'_1, \tilde{\underline{v}}_1} h(\varphi)_1 \right) \vee \cdots \vee \left(\bigoplus_{\underline{u}_m, \underline{z}'_m, \tilde{\underline{v}}_m} h(\varphi)_m \right)$$

$\hookrightarrow$ Eqn (10)

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

Finally,

$$\exists \underline{u} \forall \underline{v}\, \varphi(\underline{u}, \underline{v}) \iff \exists \underline{u}\, \tau(\underline{u}) \quad \text{w.h.p} \quad (\text{Eqn}(7))$$

$$\iff \bigoplus g(\tau) \quad \text{''} \quad (\text{Eqn}(8)), \text{ where}$$

$g(\tau)$ is as in Eqn (10). $\blacksquare$