Lec 18

Recap:

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 $\text{poly}(|\varphi|, p)$ & o/p's a ckt $g(\varphi)$ s.t.

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

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

Note: $|g(\varphi)|$ is exponential in c, but this is fine as c is a const.

Set $p = 2$. Also, a rand. red. can be viewed as a det. red. that additionally takes a "rand." string as i/p.

Cor *: There's a det. red. g that given a QBF φ with c levels of alternation and a string $\underline{r} \in \{0,1\}^R$, where $R = |\varphi|^{O(1)}$, runs in time $\text{poly}(|\varphi|)$ & $\forall p$'s a det $g(\varphi, \underline{r})$ s.t.

$$\varphi \text{ is true} \Rightarrow \Pr_{\underline{r} \in \{0,1\}^R} [\oplus\, g(\varphi, \underline{r}) \text{ is true}] \geq \frac{3}{4}$$

$$\varphi \text{ is false} \Rightarrow \Pr_{\underline{r} \in \{0,1\}^R} [\text{" " " " false}] \geq \frac{3}{4}.$$

Viewing the reduction g as a DTM.

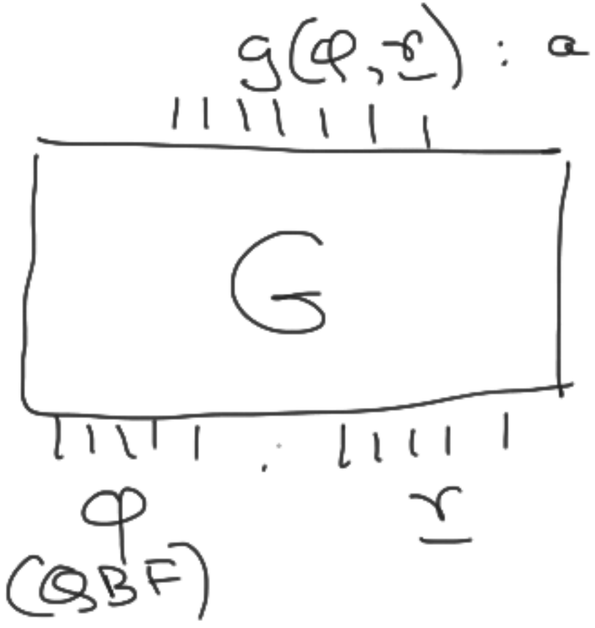


Fig 1: G is the DTM corr. to the det. red. g.

Recall, Step 2 in the pf. sketch of Toda's thm.

Step 2: (Derandomizing Step 1 by strengthening the oracle)
Give a det. poly time red. from PH to #SAT.

Remarks: It would follow from the pf. of Step 2 that only one query to the #SAT oracle is sufficient.

Notations: ▷ (Recap) Let $\varphi_1(\underline{x}_1), \cdots, \varphi_m(\underline{x}_m)$ be clets. on disjoint sets of var. Define

$$(\varphi_1 \varphi_2 \cdots \varphi_m)(\tilde{x}) = \varphi_1(\underline{x}_1) \wedge \cdots \wedge \varphi_m(\underline{x}_m)$$

- $|\varphi_1 \cdots \varphi_m| = |\varphi_1| + \cdots + |\varphi_m| + m$
- $\#(\varphi_1 \cdots \varphi_m) = \#\varphi_1 \cdots \#\varphi_m$

▷ Let $\varphi_1(x_1, \cdots, x_{n_1})$ & $\varphi_2(x_1, \cdots, x_{n_2})$ be defn & $n_2 \geq n_1$. Define

$$(\varphi_1 + \varphi_2)(z, x_1, \cdots, x_{n_2}) := \Big(z \wedge \varphi_2(x_1, \cdots, x_{n_2})\Big) \vee \Big(\neg z \wedge x_{n_1+1} \wedge \cdots \wedge x_{n_2} \wedge \varphi_1(x_1, \cdots, x_{n_1})\Big)$$

- $\#(\varphi_1 + \varphi_2) = \#\varphi_1 + \#\varphi_2$
- $|\varphi_1 + \varphi_2| = |\varphi_1| + |\varphi_2| + O(n_2)$.

▷ For $c \in \mathbb{Z}_{>0}$,

$$c\varphi := \underbrace{\varphi + (\varphi + (\varphi \cdots + \varphi))\cdots}_{c\text{-times}}$$

$$\varphi^c := \underbrace{\varphi \cdot \varphi \cdot \cdots \cdot \varphi}_{c\text{-times}}$$

— (0)

Proof of Step 2

Lemma*: There's a det. poly-time red. that given a para $l \in \mathbb{Z}_{>0}$ and a ckt ψ, runs in time $\text{poly}(|\psi|, l)$ and qp's a ckt τ s.t.

- $\oplus\psi$ is true $\Rightarrow \#\tau = -1 \mod 2^{l+1}$.
- $\oplus\psi$ is false $\Rightarrow \#\tau = 0 \mod 2^{l+1}$.

Pf: The idea is to construct τ iteratively. At the $(i+1)$-th iteration, we construct ψ_{i+1} s.t.

$$\#\psi_i = -1 \mod 2^{2^i} \Rightarrow \#\psi_{i+1} = -1 \mod 2^{2^{i+1}}$$
$$\#\psi_i = 0 \mod 2^{2^i} \Rightarrow \#\psi_{i+1} = 0 \mod 2^{2^{i+1}}. \quad (1)$$

Finally, we set $\psi_0 = \psi$ & $\tau = \psi_{\log(\ell+1)}$.

Let's focus on the construction of ψ_{i+1} from ψ_i.

Let $\#\psi_i = t$. Think of defining a poly $p(t)$ with positive integer coeff. s.t

$$t = -1 \bmod 2^{2^i} \implies t^2 \cdot p(t) = -1 \bmod 2^{2^{i+1}}. \quad (2)$$

Note that if $t = 0 \bmod 2^{2^i}$, then $t^2 = 0 \bmod 2^{2^{i+1}}$ &

so $t^2 p(t) = 0 \bmod 2^{2^{i+1}}$ for any above mentioned kind of $p(t)$.

Hence, if we define

$$\psi_{i+1} := \underbrace{\psi_i^2 \cdot p(\psi_i)}$$ then Eqn (1) is satisfied.

the interpolation of this dat is given by Eqn (0).

Note, $\#\psi_{i+1} = (\#\psi_i)^2 \cdot \#(p(\psi_i))$

$= t^2 \cdot p(t)$.

Construction of $p(t)$: Suppose $t = k \cdot 2^{2^i} - 1$

If $p(t) = -(2k \cdot 2^{2^i} + 1) \bmod 2^{2^{i+1}}$, then we're done.

$t^2 = -2k \cdot 2^{2^i} + 1 \bmod 2^{2^{i+1}}$

$= -(2k \cdot 2^{2^i} - 1) \bmod 2^{2^{i+1}}$

$\Rightarrow t^2 p(t) = (2k \cdot 2^{2^i})^2 - 1 \bmod 2^{2^{i+1}}$

$= -1 \bmod 2^{2^{i+1}}$

$3t^2 + 4t = -6k \cdot 2^{2^i} + 3 + 4k \cdot 2^{2^i} - 4 \bmod 2^{2^{i+1}}$

$= -(2k \cdot 2^{2^i} + 1) \bmod 2^{2^{i+1}}$.

$\Rightarrow p(t) = 3t^2 + 4t$.

$$\therefore \psi_{i+1} := \psi_i^2 (3\psi_i^2 + 4\psi_i).$$

$$= 3\psi_i^4 + 4\psi_i^3.$$

Note, $|\psi_{i+1}| = |3\psi_i^4 + 4\psi_i^3| = \Theta(|\psi_i^4|) = \Theta(|\psi_i|)$.

$$\therefore |\tau| = |\psi_{\log(\ell+1)}| = \text{poly}(\ell, |\Phi|).$$ ∎

Let us denote the det. red. in Lemma * by h.

Think of composing h with the red. g in Cor *

by setting $\ell = R$. (where R is as in Cor *).

Let $v := h(g(\varphi, \underline{r}))$. Denote the var of v by $\underline{w}$.

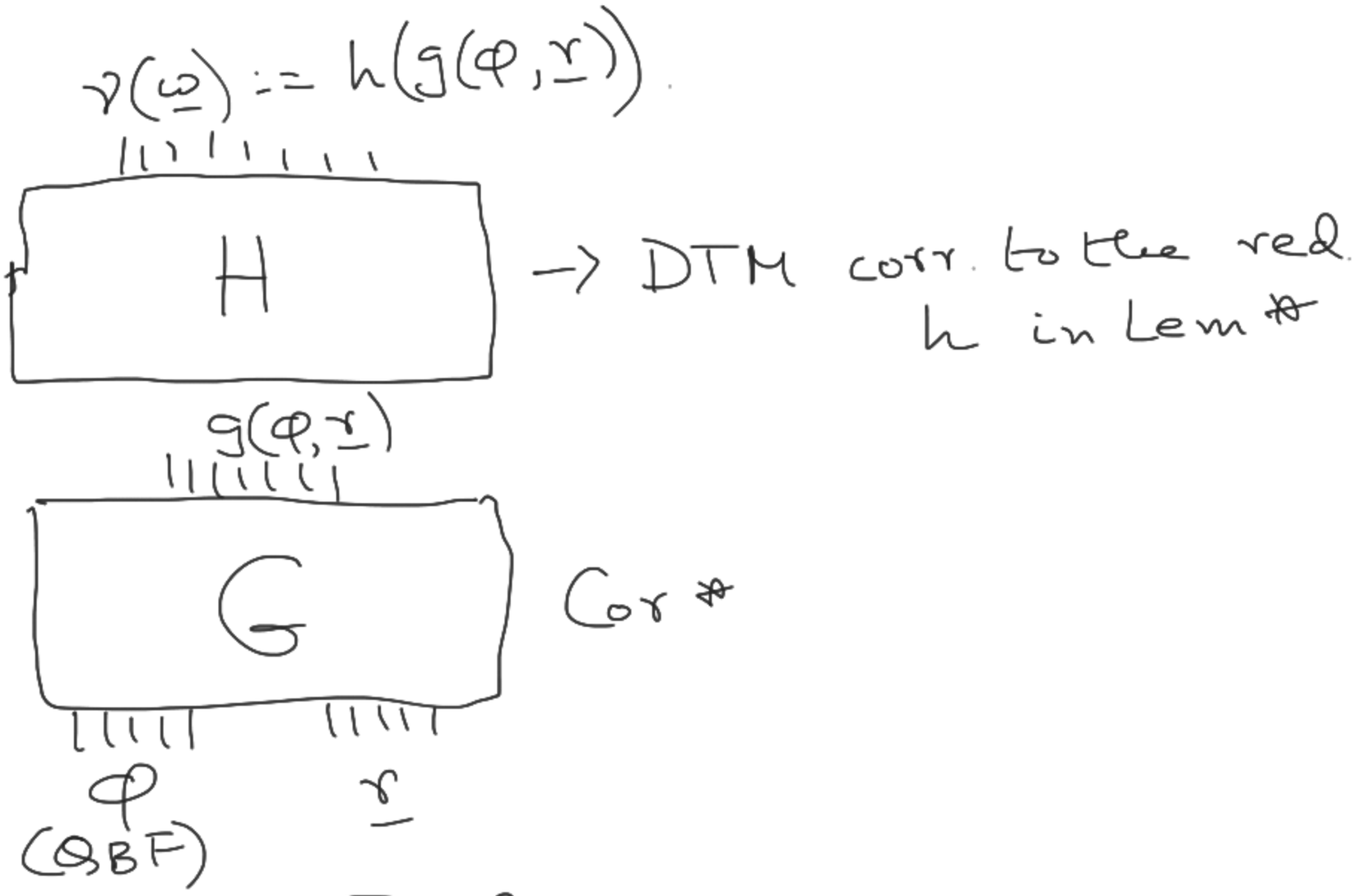

$r(\omega) := h(g(\varphi, \underline{r}))$
H
→ DTM corr. to the red h in Lem *
$g(\varphi, \underline{r})$
G
Cor *
φ
(QBF)
$\underline{r}$

Fig 2:

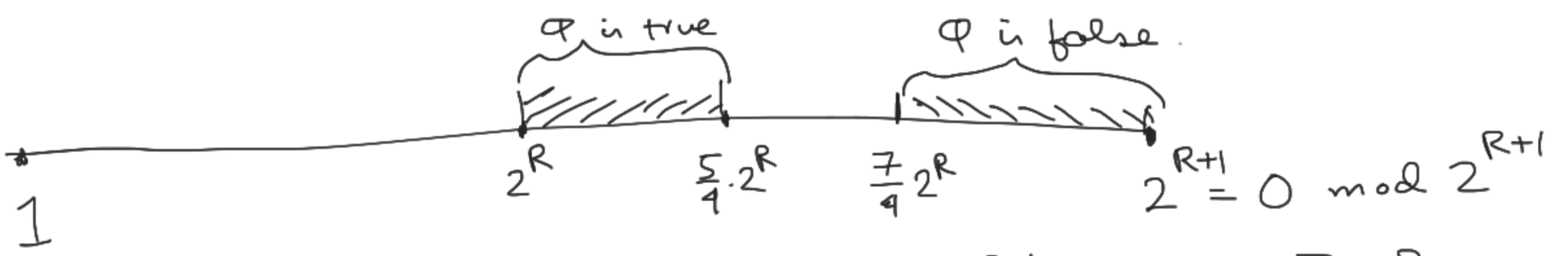
Consider the sum

$$S := \sum_{\underline{r} \in \{0,1\}^R} \#\left(h(g(\varphi, \underline{r}))\right) \qquad \text{— (3)}$$

▷ If φ is true, then at least $\frac{3}{4}$ of the summands are $-1 \bmod 2^{R+1}$ & the remaining are $0 \bmod 2^{R+1}$.
Hence, in this case, the above sum lies between

$$-2^R \quad \text{and} \quad -\left(\tfrac{3}{4} \cdot 2^R\right) \quad \bmod 2^{R+1}.$$

▷ If φ is false, then at most $\frac{1}{4}$ of the summands are $-1 \bmod 2^{R+1}$, & the rem. are $0 \bmod 2^{R+1}$. Hence, the sum lies between $-\left(\frac{1}{4} \times 2^R\right)$ & $0 \bmod 2^{R+1}$.



- $-2^R = 2^R \mod 2^{R+1}$; $-\left(\frac{3}{4}\times 2^R\right) = 2^{R+1} - \frac{3}{4}2^R = \frac{5}{4}\cdot 2^R \mod 2^{R+1}$.
- $-\left(-\frac{1}{4}\cdot 2^R\right) = 2^{R+1} - \frac{1}{4}2^R = \frac{7}{4}\cdot 2^R \mod 2^{R+1}$.

So, if we know the sum S (given in Eqn (3)), then we can find out if φ is true or false simply by checking if $S \mod 2^{R+1} \in \left[2^R, \frac{5}{4}2^R\right]$ or $\in \left[\frac{7}{4}2^R, 2^{R+1}\right]$.

Note,

$$S = \sum_{\underline{r} \in \{0,1\}^R} \#\left(h(g(\varphi, \underline{r}))\right)$$

$$= \sum_{\underline{r} \in \{0,1\}^R} \sum_{\underline{\omega} \in \{0,1\}^{|\underline{\omega}|}} h\left(g(\varphi, \underline{r})\right)(\underline{\omega}) \qquad \text{—— (4)}$$

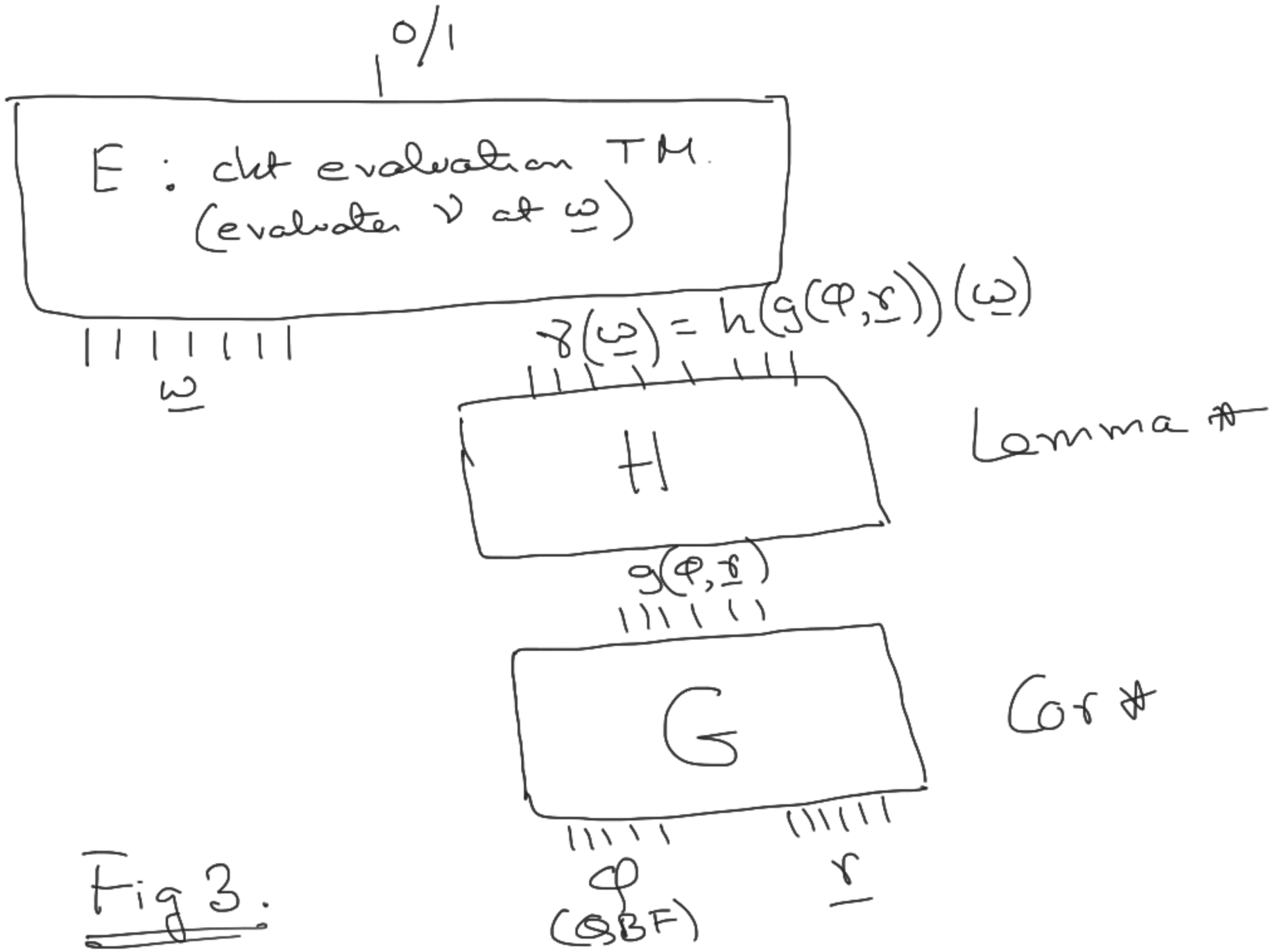

0/1
E : ckt evaluation TM.
(evaluates ν at ω)
ω
γ(ω) = h(g(φ, r))(ω)
H
Lemma *
g(φ, r)
G
Cor *
φ
(QBF)
r

Fig 3.

By fixing φ, we can view the above computation as a DTM M_φ on inputs $\underline{r}$ & $\underline{\omega}$. By Cook-Levin, there's a poly-size ckt. Γ_φ that captures the comput of M_φ, i.e. $M_\varphi(\underline{r}, \underline{\omega}) = \Gamma_\varphi(\underline{r}, \underline{\omega})$ for all $\underline{r}, \underline{\omega}$.

Imp note: Γ_φ is poly-time computable from φ as the DTMs G, H & E can be explicitly described.

By Eqn (4)

$$S = \sum_{\underline{r} \in \{0,1\}^R} \sum_{\underline{\omega} \in \{0,1\}^{|\underline{\omega}|}} M_\varphi(\underline{r}, \underline{\omega})$$

$$= \sum_{\underline{r}} \sum_{\underline{\omega}} \Gamma_\varphi(\underline{r}, \underline{\omega}) = \#\Gamma_\varphi(\underline{r}, \underline{\omega})$$

Therefore, by querying Γ_φ to the #SAT oracle, we know if φ is true/false.

$$\Rightarrow PH \subseteq P^{\#SAT}.$$

∎