Lec 27 : Deterministic reduction from PH to #SAT

Recap

Theorem 1 : (Randomized reduction from Σ_c-SAT to $\oplus$SAT)

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 circuit $g(\varphi)$ 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. This is fine as $c = O(1)$.

- Obs: A randomized reduction can be viewed as a deterministic reduction that additionally takes a random string as input.
- Set $p = 2$ in Theorem 1.
- Corollary *: There is a deterministic reduction g that given a QBF φ with c levels of alternations and a random string $r \in \{0,1\}^R$, where $R = |\varphi|^{O(1)}$, runs in time $\text{poly}(|\varphi|)$ and outputs a ckt. $g(\varphi, r)$ s.t.

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

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

Viewing the reduction g as a DTM

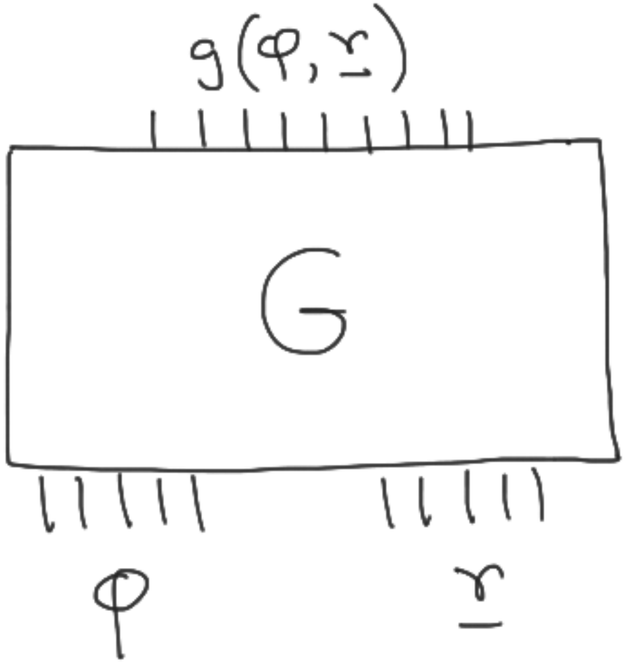


Fig 1: DTM G corresponding to the reduction g.

- Recall Step 2 of the proof of Toda's theorem.

  Step 2 : (Derandomization of Step 1). Give a deterministic poly-time reduction from PH to #SAT.

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

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

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

  — $|\varphi_1 \cdot \varphi_2 \cdot \cdots \cdot \varphi_m| = |\varphi_1| + \cdots + |\varphi_m| + m$.

  — $\#(\varphi_1 \cdot \varphi_2 \cdot \cdots \cdot \varphi_m) = \#\varphi_1 \cdot \#\varphi_2 \cdot \cdots \cdot \#\varphi_m$.

(b) Let $\varphi_1(x_1, \dots, x_{n_1})$ and $\varphi_2(x_1, \dots, x_{n_2})$ be ckts and $n_2 \geq n_1$.

Define,

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

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

$$- \#(\varphi_1 + \varphi_2) = \#\varphi_1 + \#\varphi_2 .$$

(c) For $c \in \mathbb{Z}_{>0}$,

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

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

— (2)

Proof of Step 2

- **Lemma *:** There is a deterministic poly-time reduction that given a parameter $\ell \in \mathbb{Z}_{>0}$ and a ckt. ψ, runs in time $\text{poly}(|\psi|, \ell)$ and outputs a ckt. τ s.t.

$$\oplus\psi \text{ is true} \implies \#\tau = -1 \bmod 2^{\ell+1}$$

$$\oplus\psi \text{ is false} \implies \#\tau = 0 \bmod 2^{\ell+1}.$$

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

$$\#\psi_i = -1 \bmod 2^{2^i} \implies \#\psi_{i+1} = -1 \bmod 2^{2^{i+1}}$$

$$\#\psi_i = 0 \bmod 2^{2^i} \implies \#\psi_{i+1} = 0 \bmod 2^{2^{i+1}}. \quad \text{— (1)}$$

- Finally, set $\psi_0 = \psi$ and $\tau = \psi_{\lceil \log(\ell+1) \rceil}$.
- Let us focus on the construction of ψ_{i+1} from ψ_i. Let $\#\psi_i = t$. We will construct a polynomial $p(t)$ with positive integer coefficients such that

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

- Note: If $t = 0 \mod 2^{2^i}$, then $t^2 = 0 \mod 2^{2^{i+1}}$ and so, $t^2 p(t) = 0 \mod 2^{2^{i+1}}$. Hence, if we define

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

The interpretation of this ckt is given by Eqn(0).

- **Choice of $p(t)$:** Set $\boxed{p(t) = 3t^2 + 4t}$.
- **Obs:** $t = -1 \bmod 2^{2^i} \Rightarrow t^2 \cdot p(t) = -1 \bmod 2^{2^{i+1}}$.

Proof: Let $t = k \cdot 2^{2^i} - 1$ for $k \in \mathbb{Z}$.

$$\Rightarrow t^2 = -(2k2^{2^i} - 1) \bmod 2^{2^{i+1}}.$$

$$\Rightarrow 3t^2 + 4t = -6k2^{2^i} + 3 + 4k \cdot 2^{2^i} - 4 \bmod 2^{2^{i+1}}.$$

$$= -(2k2^{2^i} + 1) \bmod 2^{2^{i+1}}.$$

$$\Rightarrow t^2 \cdot p(t) = (2k2^{2^i} - 1)(2k2^{2^i} + 1) \bmod 2^{2^{i+1}},$$

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

∎

- Therefore, $\psi_{i+1} = \psi_i^2 \cdot p(\psi_i) = \psi_i^2 \cdot (3\psi_i^2 + 4\psi_i)$

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

- Note: $|\psi_{i+1}| = |3\psi_i^4 + 4\psi_i^3| = \theta(|\psi_i^4|) = \theta(|\psi_i|)$.

$\therefore |\tau| = |\psi_{\lceil \log(\ell+1) \rceil}| = \text{poly}(\ell, |\psi|)$. ■ Lemma *

- Let us denote the deterministic reduction in Lemma* by h.
- Now think of composing h with the reduction g in Corollary * by setting $\ell = R$ (where R is as in Cor*).
- Let $\gamma := h(g(\varphi, \underline{r}))$. Denote the vars. of γ by $\underline{w}$.

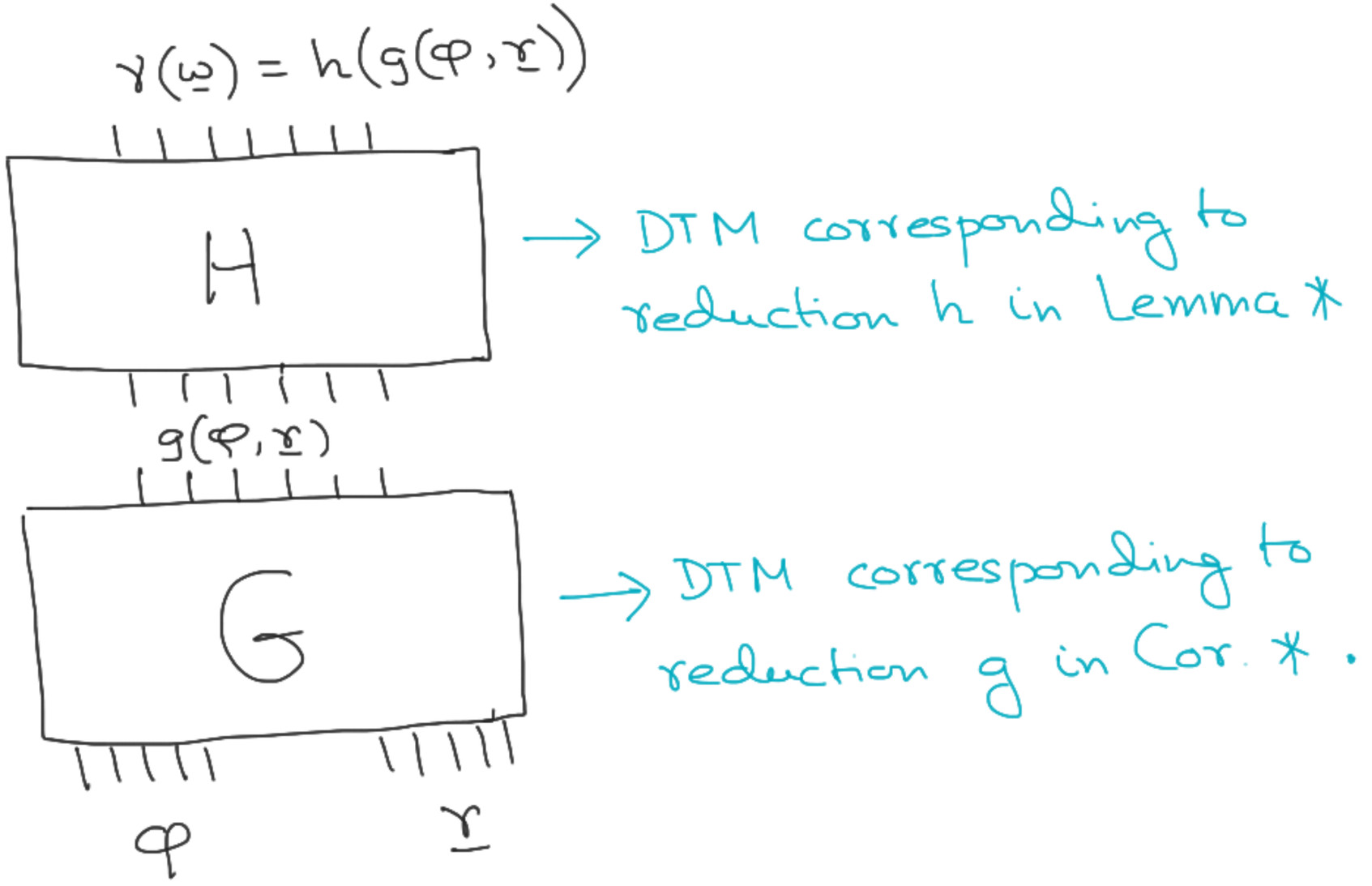


Fig 2: Composing the two reductions g and h

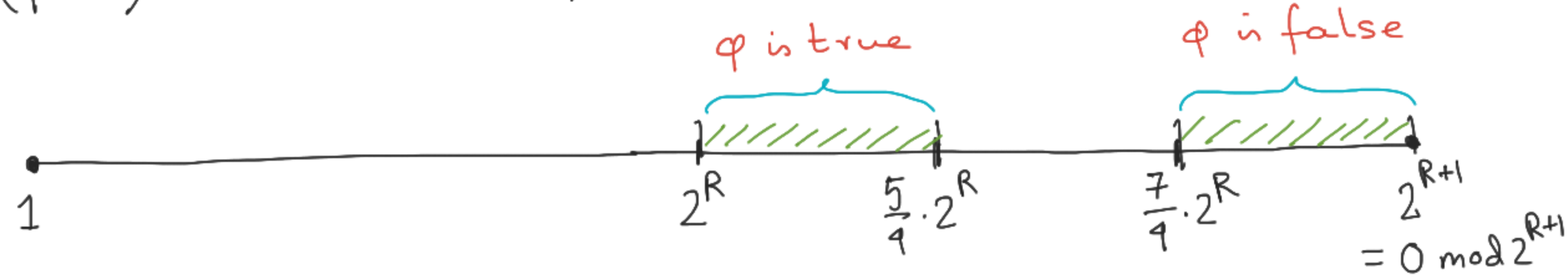
- Consider the following sum

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

- Obs: (a) If Φ is true, then at least $\frac{3}{4}$ of the summands are $-1 \bmod 2^{R+1}$, and the remaining are $0 \bmod 2^{R+1}$. Hence, in this case, the above sum lies between -2^R and $-\left(\frac{3}{4} \cdot 2^R\right)$ modulo 2^{R+1}.
- (b) If Φ is false, then at most $\frac{1}{4}$ of the summands are $-1 \bmod 2^{R+1}$, and the remaining are $0 \bmod 2^{R+1}$. Hence, in this case, the sum lies between $-\left(\frac{1}{4} \cdot 2^R\right)$ and 0 modulo 2^{R+1}.

- **Note:** ▷ $-2^R = 2^R \mod 2^{R+1}$; $-\left(\frac{3}{4}\cdot 2^R\right) = 2^{R+1} - \frac{3}{4}\cdot 2^R = \frac{5}{4}\cdot 2^R \mod 2^{R+1}$.

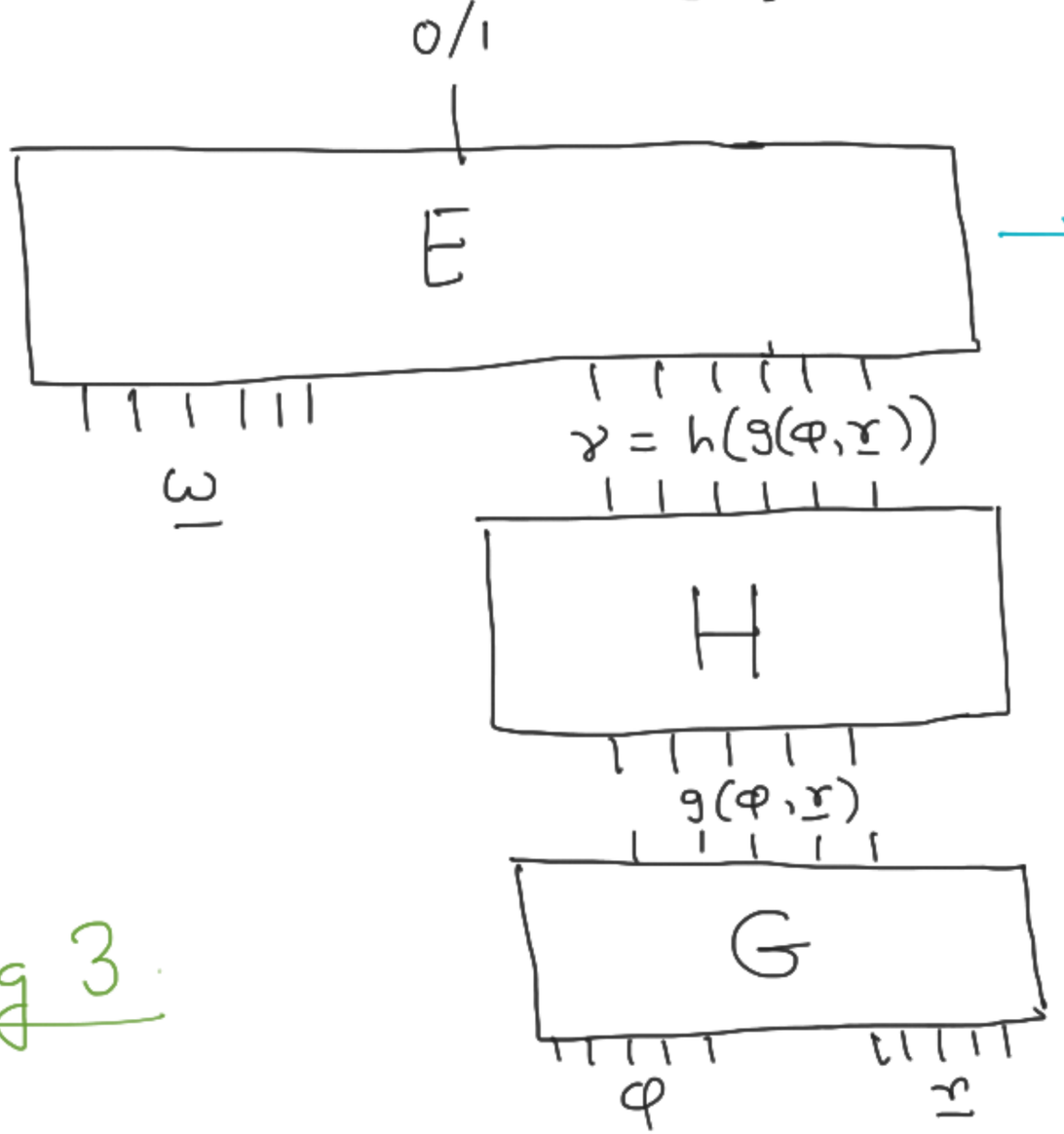
  ▷ $-\left(\frac{1}{4}\cdot 2^R\right) = 2^{R+1} - \frac{1}{4}2^R = \frac{7}{4}\cdot 2^R \mod 2^{R+1}$.



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

$$S \bmod 2^{R+1} \in \left[\frac{7}{4}2^R, 2^{R+1}\right].$$

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



→ DTM that evaluates γ at $\underline{\omega}$.

Lemma *

Corollary *

Fig 3

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

$$\Gamma_\varphi(\underline{r}, \underline{\omega}) = M_\varphi(\underline{r}, \underline{\omega}) \quad \forall\ \underline{r}, \underline{\omega}\ .$$

- Remark: Γ_φ is poly-time computable from φ.

- From 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 can find out if φ is true/false. $\Rightarrow$ PH $\subseteq$ $P^{\#SAT}$.
- Only <u>one</u> query to the #SAT oracle is required.