Computational Complexity – Lecture 19.

Agenda: Toda's Theorem.

Recap: – $\#P = \{ f : \Sigma^* \to \mathbb{N} ; f(x) = \#\text{acc. witnesses for } M \text{ on } x \}$.

– #SAT, Perm are #P-complete.

Some arithmetic with #SAT.

Say $\#SAT(\varphi) = m$ & $\#SAT(\varphi') = m'$.

▷ Can we build a formula with $m.m'$ sat. assignments.

$$\text{“}\varphi \times \varphi'\text{”} = \varphi(x) \wedge \varphi'(y)$$

▷ What about a formula with $m+m'$ assignments?

$$\text{“}\varphi + \varphi'\text{”} = [(z=0) \wedge \varphi(x)] \vee [(z=1) \wedge \varphi'(x)]$$

▷ What about $m + c$ for a constant c?

$$\text{“}\varphi + c\text{”} = [(z=0) \wedge \varphi(x)] \vee [(z=1) \wedge (x < c)]$$

How powerful is #P.?

$\#P = FP \Rightarrow PH = P$.

A finer question: What can you do in $P^{\#P}$?

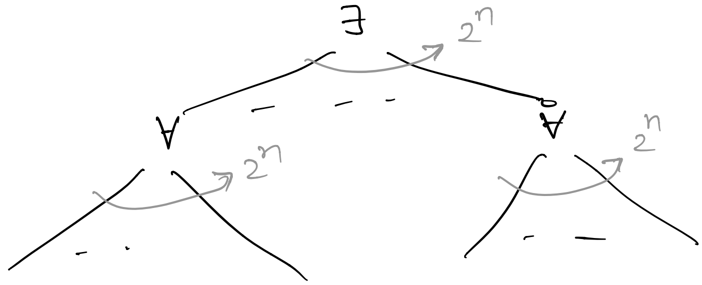
(Recall: $P = NP \Rightarrow PH = P$ but $P^{NP} \subseteq \Sigma_2^P$ and not PH).

Thm [Toda]: $PH \subseteq P^{\#P}$

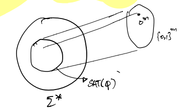
In fact, only one query is made to the #P oracle.

↳ Agenda for this class

$\exists x.\ \forall y\ \ \varphi(x,y).$



Valiant-Vazirani Lemma:
There is a randomised algo that, on input 1^n, returns a formula $\tau(x_1,..,x_n)$ such that for every $\varphi(x_1,..,x_n)$



$$\varphi \in SAT \Rightarrow \Pr[\#SAT(\varphi \wedge \tau) = 1] \geq 1/8n$$
$$\varphi \in \overline{SAT} \Rightarrow \Pr[\#SAT(\varphi \wedge \tau) = 0] = 1.$$

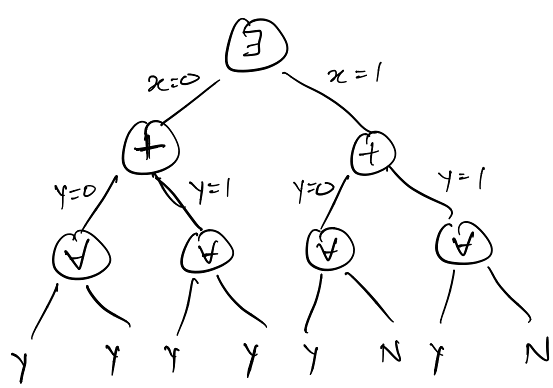
(τ doesn't care about what φ was: $\tau(x) = (h(x) = \bar{0}\ )$)

Issue: $1/8n$ is way too small a probability... can we amplify it somehow?

Idea: Move from none vs one to even vs odd!

$$\bigoplus x : \varphi(x) = \begin{cases} \text{True} & \text{if } \varphi(x) \text{ is true for odd number of } x\text{'s} \\ \text{False} & \text{if } \varphi(x) \text{ is true for even number of } x\text{'s} \end{cases}$$

$\exists x\ \bigoplus y\ \forall z\ \ \varphi(x,y,z).$



Rem: $\neg \bigoplus z : \varphi(z) = \bigoplus z :$ " $\varphi(z)+1$ "

Amplifying VV:

$\exists y : \varphi(y) \implies \Pr_A\left[\bigoplus y : \varphi \wedge \tau \text{ is true}\right] \geq 1/8n$

$\neg \exists y : \varphi(y) \implies \Pr_A\left[\bigoplus y : \varphi \wedge \tau \text{ is true}\right] = 0.$

$$\varphi \wedge \tau^{(1)}, \quad \varphi \wedge \tau^{(2)}, \ldots, \quad \varphi \wedge \tau^{(k)}$$

$$\text{Amp-VV}(\varphi, \tau^{(1)}, \ldots, \tau^{(k)}) = \bigvee_{i=1}^{k} \left(\bigoplus(\varphi \wedge \tau^{(i)})\right)$$

$$= \bigoplus z : \text{"}((\varphi \wedge \tau^{(1)}) + 1) \cdots ((\varphi \wedge \tau^{(k)}) + 1) + 1\text{"}.$$

$$= \bigoplus z.\ \Gamma(z).$$

set $k = 8nt$

$\therefore$ φ satisfiable $\implies \Pr_\tau\left[\bigoplus z : \Gamma(z) = 1\right] \geq 1 - (1 - 1/8n)^k \geq 1 - \frac{1}{2^t}$

φ-unsatisfiable $\implies \Pr_\tau\left[\bigoplus z\ \Gamma(z) = 1\right] = 0.$

Can make as small as we want.

Step 1 of Toda's thm:

$$\Sigma_k\text{-SAT} \xrightarrow{BPP} \bigoplus \text{SAT}.$$

It will be useful to instead prove a stronger claim.

Lemma: (Relativised Toda-Step 1) There is a randomised algorithm that takes a quantified formula $\Phi(x) = \exists y^{(1)} \forall y^{(2)} \ldots Q y^{(c)} \varphi(x, y)$. and returns a formula $\Gamma(x, z)$ s.t $\Phi(x) \equiv \bigoplus z.\ \Gamma(x, z)$ w.h.p.
That is,

$$\Pr_A\left[\forall a \in \{0,1\}^n : \Phi(a) = 1 \iff \bigoplus z.\ \Gamma(a, z) = 1\right] \geq 1 - 1/2^t.$$

Can make as small as we want.

Pf: Induction on # quantifier alternations.

Base case: $i=1$. $\Phi(x) = \exists y : \varphi(x,y)$.

Let $\Gamma(x,z) = \text{Amp-VV}(\varphi(x,y), \tau^{(1)}, \ldots, \tau^{(k)})$

$$= \text{“} (\varphi(x,y) \wedge \tau^{(1)}(y) + 1) \cdots (\varphi(x,y) \wedge \tau^{(k)}(y) + 1) + 1 \text{”}$$

For any $a \in \{0,1\}^n$, we know that

$$\Pr\left[\exists y : \varphi(a,y) \not\Leftrightarrow \bigoplus z.\ \Gamma(a,z) = 1\right] \leq 1/2^t$$

$$\Rightarrow \Pr\left[\begin{array}{l}\text{For some}\\ a \in \{0,1\}^n\end{array} \exists y : \varphi(a,y) \not\Leftrightarrow \bigoplus z\ \Gamma(a,z) = 1\right] \leq 1/2^{t-n}.$$

$$\therefore \Pr\left[\Phi(x) = \exists y\ \varphi(x,y) \equiv \bigoplus z : \Gamma(x,z)\right] \geq 1 - 1/2^{t'}$$

Inductive step:

Say $\Phi(x) = \exists w : \psi(x,w)$

where ψ is a formula with $c-1$ alternations.

By induction, we have some $\alpha(x,w,z)$ such that

$$\psi(x,w) \equiv \underbrace{\bigoplus z : \alpha(x,w,z)}_{\beta(x,w)}. \quad \text{with prob} \geq 1 - 1/2^{t_1}.$$

(t_1 can be chosen by us).

Consider $\Phi'(x) = \exists w : \beta(x,w)$.

Once again, using VV, we have that if

$$\exists w : \beta(x,w) \underset{\text{w.h.p}}{\equiv} \bigvee_{i=1}^{k_2} \left[\bigoplus w : \beta(x,w) \wedge \tau^{(i)}(w)\right]$$

$$\text{RHS} = \bigvee_{i=1}^{k_2} \left[\bigoplus w.\ \bigoplus z : \alpha(x,w,z) \wedge \tau^{(i)}(w)\right]$$

$$= \bigvee_{i=1}^{k_2} \left[\bigoplus w, z : \alpha(x, w, z) \wedge \tau^{(i)}(w) \right]$$

$$= \bigoplus \tilde{w}, \tilde{z} : \text{"}(\alpha(x,w,z) \wedge \tau^{(1)}(w) + 1) \cdots (\alpha(x,w,z) \wedge \tau^{(k_2)}(w) + 1) + 1\text{"}$$

$$\therefore \Phi(x) = \exists w : \psi(x,w) \underset{whp}{\equiv} \exists w : \beta(x,w)$$

$$\qquad\qquad\qquad\qquad \big|\big|\big| \text{ w.h.p}$$

$$\qquad\qquad\qquad\qquad \bigoplus \tilde{w} \tilde{z} : \Gamma(x, \tilde{w}, \tilde{z}) \qquad \square.$$

A super succinct version of writing this : (Disclaimer: I hate this...)

$$\exists \cdot BP \cdot \oplus P \subseteq BP \cdot \oplus P$$

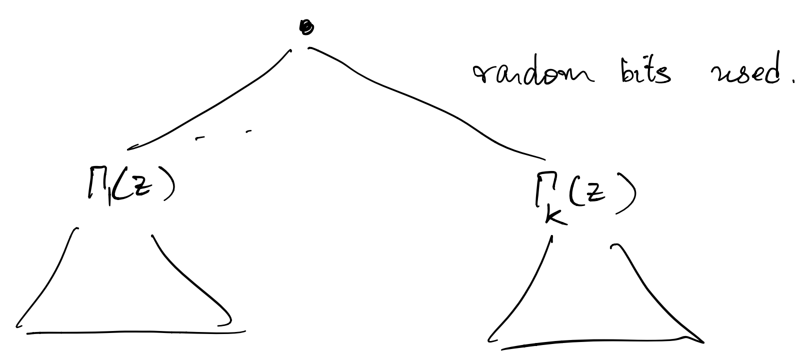
$NP \subseteq BP \cdot \oplus P$

$NP^{NP} \subseteq BP \cdot \oplus P^{NP} \subseteq BP \cdot \oplus P^{\oplus P} = BP \cdot \oplus P.$

(ugh!)

Step 2 of Toda's Thm:

$$\Phi = \exists x \, \forall y \, \exists z \cdots \varphi(x, y, z, \ldots) \xrightarrow{\text{w.h.p}} \bigoplus z : \Gamma(z)$$



Odd vs even is too razor-thin... can we amplify this gap?

Lemma: (Modulus Amplification) There is a deterministic polytime algo $A(1^m, \varphi)$ that transforms φ to ψ s.t

$$\oplus x: \varphi(x) = 1 \Rightarrow \#SAT(\psi) = -1 \bmod 2^m$$
$$\oplus x: \varphi(x) = 0 \Rightarrow \#SAT(\psi) = 0 \bmod 2^m.$$

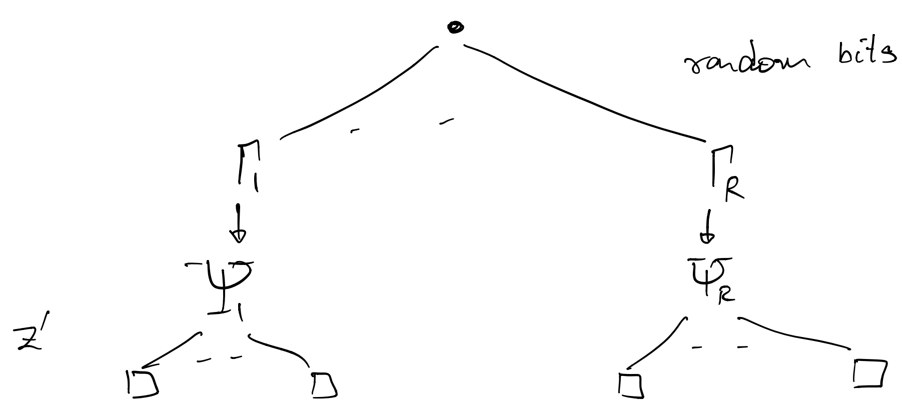
Let's finish the pf of Toda's thm from this.

Say $\Phi = \exists x \forall y \exists z \dots \varphi(x, y, z, \dots)$ is the quantified formula with $O(1)$-alternations.

Step 1 can be thought of as the output of a det algo $A(\Phi, r_1, \dots, r_m)$ where $r_1, \dots, r_m$ are the random bits.

Consider the following machine:

- Guess $r_1, \dots, r_m$
- Compute $\Gamma(z) = A(\Phi, r_1, \dots, r_m)$.
- Apply modulus amp. to $\Gamma(z)$ to get $\Psi(z')$ such that
  $$\oplus z: \Gamma(z) = 1 \Rightarrow \#SAT(\Psi(z)) = -1 \bmod 2^m$$
  $$\oplus z: \Gamma(z) = 0 \Rightarrow \#SAT(\Psi(z)) = 0 \bmod 2^m$$
- Guess z' and accept if $\Psi(z') = 1$.



If Φ was false, then $\bigoplus z.\ \Gamma_i(z) = 0$ for all i.

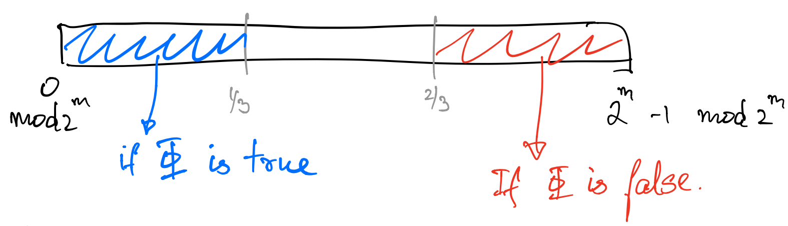
$\Rightarrow$ $\#SAT(\varphi_i(z')) = 0 \bmod 2^m$ for all i

$\Rightarrow$ # acc. runs of M = $0 \bmod 2^m$.

If Φ is true, then $\bigoplus z: \Gamma_i(z) = -1 \bmod 2^m$ for $\geq 2/3$ of i's
$\bigoplus z: \Gamma_i(z) = 0 \bmod 2^m$ for $\leq 1/3$ of i's.

If Φ is false, then $\bigoplus z: \Gamma_i(z) = -1 \bmod 2^m$ for $\leq 1/3$ of i's
$\bigoplus z: \Gamma_i(z) = 0 \bmod 2^m$ for $\geq 2/3$ of i's.

$\therefore$ #acc. paths of M mod 2^m is



The $P^{\#P}$ algo:

- Build the above machine M.
- Ask the #P oracle the number of acc. paths of M. (Or, conv. M to a formula using Cook-Levin and ask #P oracle for #SAT).
- Compute the residue modulo 2^m.
  If residue is "small" return True
  Else return False.

$\square$.

How do you amplify modulus?

$$a \rightsquigarrow f(a)$$

$$0 \bmod k \rightsquigarrow 0 \bmod k^2$$

$$-1 \bmod k \rightsquigarrow -1 \bmod k^2.$$

What about a^3? $\quad a = -1 + rk \Rightarrow a^3 = -1 + 3rk \bmod k^2$

$$a^3(a^3+2) = (3rk-1)(3rk+1) \bmod k^2$$

$$= -1 \bmod k^2.$$

$$f(\varphi) = \varphi^6 + 2\varphi^3.$$

How large is $f(\varphi)$? $\quad \leq 20|\varphi|.$

$\therefore$ To go from $0/{-1} \bmod 2 \rightsquigarrow 0/{-1} \bmod 2^n$,
size becomes $\mathrm{poly}(n) \cdot |\varphi|$. $\square$.