<u>Lemma 2:</u> Let ψ be a boolean formula & $m \in \mathbb{N}$. Then, there is a poly-time TM T s.t. $\varphi = T(\psi, 1^m)$ is a boolean formula satisfying:

$$\#\psi \equiv 1 \pmod 2 \Rightarrow \#\varphi \equiv -1 \pmod{2^{m+1}}$$

& $$\#\psi \equiv 0 \pmod 2 \Rightarrow \#\varphi \equiv 0 \pmod{2^{m+1}}.$$

<u>Proof:</u> • We build φ iteratively using new operations '$+$' & '$*$'.

• For formulas $F(\bar{x})$ & $G(\bar{y})$ define new formulas,

$$(F+G)(\bar{x}, u) := (u=0 \wedge F(\bar{x})) \vee (u=1 \wedge G(\bar{x})).$$

& $$(F*G)(\bar{x}, \bar{y}) := F(\bar{x}) \wedge G(\bar{y}).$$

▷ $\#(F+G) = (\#F) + (\#G)$, &

$\#(FG) = (\#F) \cdot (\#G)$.

• Start with $\varphi_0 := \psi$.

- Define $\varphi_{i+1} := 4\varphi_i^3 + 3\varphi_i^4$.

<u>Claim:</u> $\#\varphi_i \equiv -1 \pmod{2^{2^i}}$
$\Rightarrow \#\varphi_{i+1} \equiv -1 \pmod{2^{2^{i+1}}}$, &

$\#\varphi_i \equiv 0 \pmod{2^{2^i}}$
$\Rightarrow \#\varphi_{i+1} \equiv 0 \pmod{2^{2^{i+1}}}$.

<u>Proof:</u>

- Observe that $4(-1+2^j.q)^3 + 3(-1+2^jq)^4$
$\equiv 4.(-1+3.2^jq) + 3(1-4.2^jq)$
$\equiv -1 \pmod{2^{2j}}$.

- Also, $4.(2^jq)^3 + 3.(2^jq)^4$
$\equiv 0 \pmod{2^{2j}}$. $\square$

- By induction, we deduce that φ_i for $i = O(\lg m)$, will have the properties that we wanted in φ.

(No. of vars. in φ grow by a $\lg m$ factor) $\square$

Proof of Toda's thm.:

- Let $L \in PH$. Let x be a string.
- By Lemmas 1 & 2, we get a poly-time NDTM M & $m = poly(|x|)$ s.t.

$$x \in L \Rightarrow \Pr_{r \in \{0,1\}^m}\left[\#\text{acc.path } M(x,r) \equiv -1 \bmod 2^{m+1}\right] \geq 2/3, \&$$

$$x \notin L \Rightarrow \Pr_r [\cdots] < 1/3.$$

- Further, $\forall x, \forall r$, $\#\text{acc.path } M(x,r) \equiv 0 \text{ or } -1 \bmod 2^{m+1}$.

replace random bits by non-det. ones

- Let us define an NDTM M' that on input x, guesses $r \in \{0,1\}^m$ & accepts iff M accepts (x,r).

$$\Rightarrow \#\text{acc.path } M'(x) = \sum_r \#\text{acc.path } M(x,r)$$

0 or 1

- Its value modulo 2^{m+1} is:

$$\begin{cases} \text{between } -\frac{2}{3}\cdot 2^m \;\&\; -2^m, & \text{if } x \in L. \\ \text{between } -\frac{1}{3}\cdot 2^m \;\&\; 0, & \text{if } x \notin L. \end{cases}$$

$\Rightarrow$ Computing #acc. path $M'(x)$ is enough to solve L.

$\Rightarrow$ $PH \subseteq P^{\#P}$ $\square$

notice how the proof used the intermediate class $\oplus P$

- Randomization was a simplifying tool/notion in the above proof, though the theorem statement did not call for randomness at all!

- We will now use randomization to compute.

Probabilistic TM (PTM)

- Defn: • We call M a PTM if it has two transition fns. δ_0, δ_1 and in each transition step M randomly follows δ_i with prob. $= 1/2$.

• We say M decides L if $x \in L$ iff $\Pr_{\text{steps}}[M \text{ accepts } x] \geq 2/3$.

- Naturally, we can now talk about "efficient" PTMs.

Defn: • For a $T: \mathbb{N} \to \mathbb{N}$ a PTM M decides L in $T(n)$ time if M halts on every $x \in \{0,1\}^*$ in $\leq T(|x|)$ steps, regardless of its random choices, and decides $x \in ? L$.

- $\underline{\text{BPtime}(T(n))} := \{L \subseteq \{0,1\}^* \mid$ a PTM M decides L in time $O(T(n))\}$.

- $\underline{\text{BPP}} := \bigcup_{c \in \mathbb{N}} \text{BPtime}(n^c)$.

(bounded prob. poly-time)
(unlike, prob. poly-time PP !)

Proposition: (i) $P \subseteq BPP \subseteq EXP$.

(ii) Alternatively, $L \in \underline{BPP}$ if $\exists$ det. poly-time TM M & $c>0$ s.t. $\forall x \in \{0,1\}^*$, $x \in L$ iff $\Pr_{r \in \{0,1\}^{|x|^c}}[M(x,r)=1] \geq \frac{2}{3}$.

- This is closer to our notion of a "randomized poly-time" algorithm M solving a problem L.