

Recall from last class:

$L \in \oplus P$ means $\exists x \in L \Leftrightarrow \#\{y \mid R(x,y)\} \text{ is odd for some polynomial decidable } R$
 pronounced "parity-P"
 $|y| \leq |x|^c$

Valiant-Vazirani implies $NP \subseteq RP \oplus P[1]$ (s.t. call to the oracle is easy, a SAT oracle)
 The W proof gave us a reduction $NP \mapsto \oplus, \text{ s.t.}$

$\exists x \varphi(x) \Rightarrow \mathbb{P}\{\exists! x, y \mid \Theta(x,y)\} \geq 1/8n$
 $\neg \exists x \varphi(x) \Rightarrow \mathbb{P}\{\exists x, y \mid \Theta(x,y)\} = 0$
 and so this implies

$\exists x \varphi(x) \Rightarrow \mathbb{P}\{\oplus(x,y) \mid \Theta(x,y)\} \geq 1/8n$
 $\neg \exists x \varphi(x) \Rightarrow \mathbb{P}\{\oplus(x,y) \mid \Theta(x,y)\} = 0$
 recall this is the parity guessifier:

$\oplus x \psi(x)$ means "there are an odd # of x s.t. $\psi(x)$ "
 We can amplify this probability by taking lots of copies:

$\mathbb{P}\{\bigvee_{i=1}^t \oplus(x, y_i) \mid \Theta(x, y_i)\} \geq 1/10$ if $t \geq 100n$ is large enough.

The reason we passed to $\oplus$ is because this turns out to again be a parity formula (via closure properties of $\oplus$ from last time).

This gives us a reduction $\varphi \mapsto \mathbb{I}$ s.t.
 $\exists x \varphi(x) \Rightarrow \mathbb{P}\{\oplus \mathbb{I}(x)\} \geq 1/2$
 $\neg \exists x \varphi(x) \Rightarrow \mathbb{P}\{\oplus \mathbb{I}(x)\} = 0$

We will use this to prove:

Thm (Today)
 ① $PH \subseteq BPP \oplus P[1]$ ($\subseteq BPP \oplus P$)
 ② $PH \subseteq P \oplus P$

But first we need to define $\#P$ (pronounced "counting-P", "sharp-P", or "number-P")
DEF A function $f: \Sigma^* \rightarrow \mathbb{N}$ is in $\#P$ if $\exists$ a polynomial relation $R(x,y)$ s.t. $\forall x, f(x) = |\{y \mid R(x,y)\}|$.
 (if y is poly-time computable)

EXAMPLES: $\#SAT: f(\varphi) = \#\text{satisfying assignments of } \varphi$.

$\#CIRCUIT-SAT: f(C) = \#\text{satisfying assignments to circuit } C$.

$\#3-COLOR: f(G) = \#\text{valid 3-colorings of } G$.

In general, take your favorite NP problem, and count the # of witnesses. But this makes sense for things in P too eg $\#2-SAT$, and $\#2-SAT$ might be fixed even though $2-SAT$ is easy.

$\#P$ -completeness: we need a notion of reduction. There are a few problems:

1. PARSIMONIOUS REDUCTION:

" $f \leq$ parsimonious g " if $\exists$ polynomial reduction F s.t. $\forall x, f(x) = g(F(x))$.

$\hookrightarrow$ non-standard notion.
 This preserves the # of solutions, and $[f \leq g] \Rightarrow [f \in P] \Leftrightarrow [g \in P]$ (here, $\#P$ is just you can compute in polynomial, so this would work for ~~some~~ defining $\#P$ -completeness.

But this turns out not to be a good idea.

CLAIM: $\forall f \in \#P, f \leq \text{CIRCUIT-SAT}$

PF: Circuit-levin reduction.

It's too restrictive: there are problems in P whose counting version are hard (like $2-SAT$), and we can never have a parsimonious reduction to $2-SAT$.

Back to the proof of Toda's Thm.

SEPTEMBER 24 (5)

First: going from $PH \subseteq BPP \oplus P^{17}$ to $PH \subseteq P^{#P}$.

Given $L \in PH$, we'll show $\rightarrow$ via a reduction as follows:

$x \mapsto \varphi_1, \varphi_2, \dots, \varphi_R$
and where R is the # of random bits

$x \in L \Rightarrow$ at least $\frac{3}{4}$ of the φ_i 's are in $\oplus SAT$ this BPP language was.

$x \notin L \Rightarrow$ at most $1/4$ of the φ_i 's are in $\oplus SAT$.

To get the ~~stronger~~ conclusion $PH \subseteq P^{#P}$, we'll derandomize this reduction via a trick:

Let τ be some formula. We'll have a map $\tau \mapsto \tau^*$ so that

$$\# \tau \equiv 1 \pmod{2} \Rightarrow \# \tau^* \equiv -1 \pmod{4}.$$

$$\# \tau \equiv 0 \pmod{2} \Rightarrow \# \tau^* \equiv 0 \pmod{4}.$$

Also, this preserves the (residue) mod (something big). If we repeat this,

$$\tau \mapsto \tau^* \mapsto \tau^{**} \mapsto \dots \mapsto \tau^{O(\log n \cdot \kappa)} = \tau_{\text{final}}$$

each time we ~~also decide the sign~~ will multiply the sign of the formula by a constant factor, and τ_{final} has poly sign.

Suppose we run this on the φ_i 's. Then we get

$$\geq \frac{3}{4} \text{ of the } \varphi_i \text{ finally have } \# \varphi_i^{\text{final}} \equiv -1 \pmod{2} \text{ (HUGE)}$$

$$\leq \frac{1}{4} \text{ " " " } \equiv 0 \pmod{2} \text{ (HUGE)}$$

Choose $HUGE \leq 2^{2^k}$. Thus,

$$\sum_i (\# \varphi_i^{\text{final}}) \text{ either } \begin{cases} \in [-2^k, -\frac{3}{4} \cdot 2^k] & \text{if } x \in L \\ \in [-\frac{1}{4} \cdot 2^k, \frac{1}{4} \cdot 2^k] & \text{if } x \notin L \end{cases}$$

And, we can compute this, if we had access to a $\#P$ oracle.

That is, we make a really big formula.

$$\psi(i, w) := \varphi_i(w). \quad \left\{ \begin{array}{l} \text{via some trick, we} \\ \text{can make } \psi \text{ poly sized} \end{array} \right\}$$

and then, with our $\#P$ -oracle, we can count the number of satisfying assignments to ψ , mod 2^{2^k} .

That's really negative $\Leftrightarrow x \in L$
that's close to 0 $\Leftrightarrow x \notin L$

So $L \in P^{#P}$.

Now all that's left (modulo trickiness above) is to ~~construct a formula~~ describe $\tau \mapsto \tau^*$

Trick: given a formula, ~~you can~~ make a formula w that satisfies assignments, you can make a formula w that satisfies assignments.

And, given two formulae w_1, w_2 sat. assn, can make a new formula w that sat. assn.

Thus, we can make τ^* w/

$$\# \tau^* = 4(\# \tau)^3 + 3(\# \tau)^4$$

and it turns out this has the desired properties.

That shows how to turn a proof $PH \subseteq BPP \oplus P^{17}$ ~~into a proof~~ $PH \subseteq P^{#P}$.
[See Adar-Barak or Googole around for more details].

Now: A few comments on $PH \subseteq BPP \oplus P^{17}$.

The idea is to eliminate quantifiers one at a time. It suffices to show

Thm $\forall k \geq 1, \exists$ polytime randomized reduction that takes a

$\oplus SAT$ formula Φ and outputs a $\oplus SAT$ formula Φ' s.t. Φ, Φ' have the same truth value with probability

at least $1 - 1/10 \cdot 2^{-k}$

SEPTEMBER 24 (6)

eg, for $k=2$,

Φ is of the form $\bigoplus x \exists y \forall z \psi(x,y,z)$

and Φ' would look like $\bigoplus y \forall z \psi'(y,z)$.

This is enough — we run this k times, and the failure probability is no more than $\sum_{i=1}^k \frac{1}{10 \cdot i^2} \leq \frac{1}{10}$.

The Π_{k-1} vs Σ_{k-1} doesn't matter, since

$$\bigoplus x \forall z \psi \iff \bigoplus x (\exists z (\neg \psi))$$

$$\iff \bigoplus x \exists z (\neg \psi),$$

since the parity of good assignments is the same as that of bad assignments (since they sum to 2^n , which is even).

Next time: finish up the details.