Lecture 13

Note Title

Today

- Conclude Toda's Theorem:

$$\forall k \quad \Sigma_k^P \subseteq P^{\#P}$$

Recall last lecture: Operators on Complexity Classes

- $\exists \cdot L = \{ x \mid \exists y \ (x,y) \in L \}$

$\exists \cdot C = \{ \exists \cdot L \mid L \in C \}$

- $\forall \cdot L = \{ x \mid \forall y \ (x,y) \in L \}$

$\forall \cdot C = \{ \forall \cdot C \mid L \in C \}$

- $\oplus \cdot L = \{ x \mid \#\{ y \mid (x,y) \in L \} \text{ is even} \}$

$\oplus \cdot C = \{ \oplus \cdot L \mid L \in C \}$

- $BP_{q(n)} \cdot L = (\Pi_{YES}, \Pi_{NO})$

$$\Pi_{YES} = \{x \mid \Pr_y [(x,y) \in L] \geq 1 - 2^{-q(n)}\}$$

$$\Pi_{NO} = \{x \mid \Pr_y [(x,y) \in L] \leq 2^{-q(n)}\}$$

$$BP_{q(n)} \cdot C = \{BP_{q(n)} \cdot L \mid L \in C\}$$

$$BP \cdot C = \bigcap_{\text{Poly } q(n)} BP_{q(n)} \cdot C$$

Important Classes

- $\underbrace{\exists \cdot \forall \cdot \exists \cdot \forall \cdots \cdot}_{k} P = \Sigma_k^P$

- $BP \cdot P = BPP$

- $\oplus \cdot P = \oplus P \ni \oplus SAT$

- $BP \cdot \oplus \cdot P$
- $\exists \cdot BP \cdot \oplus \cdot P$; $\forall \cdot BP \cdot \oplus \cdot P$
- $BP \cdot \oplus \cdot BP \cdot \oplus \cdot P$

Elementary Properties

I. Complementation:

(a) "For most" C $\left[(BP \cdot \oplus)^i \cdot P \right]$

$\oplus \cdot C$ closed under complementation

(b) C closed under complementation

$\Rightarrow$ $BP \cdot C$ " .

(c) C closed under poly(n) - AND

$\Rightarrow$ $\oplus \cdot C$ closed under " ;

$BP \cdot C$ closed under " ;

Defn:

"k-AND" $\cdot L = \{(x_1 \ldots x_k) \mid$

$x_1 \in L$ AND

$x_2 \in L$ AND

$\vdots$

$x_k \in L \}$

Proof of (c):

$x_1, \ldots x_k \in \oplus \cdot L$

$\Leftrightarrow$ $\# y_1 \ldots y_k$ s.t.

$\{ (x_1, y_1) \in \omega\text{-}L$

AND $\vdots$

AND $(x_k, y_k) \in \omega\text{-}L \}$

is odd

$\longrightarrow \not$

$x_1 \ldots x_k \in BP \cdot L$

$\Leftrightarrow \Pr_{y_1 \ldots y_k}\Big[(x_1,y_1) \in L \text{ and } (x_2,y_2) \in L \text{ and } \vdots \Big] \geq 1 - k \cdot 2^{-\ell(n)}$

Lemma 1.1

$\exists \cdot \underbrace{BP \cdot \oplus \cdot P}_{\text{call this } C \text{ below}} \subseteq BP \cdot \oplus \cdot BP \cdot \oplus \cdot P$

Proof: Fix $L \in C$; By V-V $\exists \tilde{L} \in C$ s.t.

$\exists y$ s.t. $(x,y) \in L$

$\Leftrightarrow \Pr_z\Big[\#y \text{ s.t. } (x,y,z) \in \tilde{L} \text{ is even} \Big] \geq \frac{1}{p(n)}$

$(\forall y \ (x,y) \notin L \Rightarrow \Pr[\ \downarrow\ ] = 0)$

$$\tilde{L}^{(k)} = \left\{ (x, y_1 \ldots y_k \; z_1 \ldots z_\ell) \;\middle|\; (x, y_1, z_1) \in L \text{ and } \ldots (x, y_k, z_k) \in L \right\}$$

Since C is closed under poly-AND

$\Rightarrow \tilde{L} \in C$

$\exists\, y \quad (x, y) \in L$

$$\Rightarrow \Pr_{(z_1 \ldots z_k)} \left[\#(y_1 \ldots y_k) \text{ s.t. } (x, \bar{y}, \bar{z}) \in \tilde{L}^{(k)} \text{ is even} \right] \geq 1 - \left(1 - \frac{1}{p(n)}\right)^k$$

$$\in BP \cdot \oplus \cdot C$$

(Similarly: $\forall \cdot BP \cdot \oplus \cdot P \subseteq BP \cdot \oplus \cdot BP \cdot \oplus \cdot P$)

Lemma 1.2

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

Proof: Fix $L \in \oplus P$

$x \in \oplus \cdot BP \cdot L$ if

$$\#y \left\{ \Pr_z \left[(x,y,z) \in L \right] \geq 1 - \frac{1}{2^{q(n)}} \right\} \text{ is even.}$$

Define $L' = \left\{ (x,y) \mid \Pr_z \left[(x,y,z) \in L \right] \geq 1 - \frac{1}{2^{q(n)}} \right\}$

Say z bad for y if

$$L(x,y,z) \neq L'(x,y)$$

$$\Pr_z \left[z \text{ bad for } y \right] \leq 2^{-q(n)}$$

$$\Pr_z[\exists y \text{ s.t. } z \text{ bad for } y] \leq \underbrace{2^m \cdot 2^{-q(n)}}$$

Can make this as small as we want!

if z s.t. $\forall y$ z good for y

then $L'(x,y) = L(x,y,z) \quad \forall y.$

$$\Rightarrow \Pr_z\left[\#y \text{ s.t. } (x,y,z) \in L \text{ is even}\right]$$

$$\leq \Pr_z[\exists y \text{ bad for } z]$$

$$\leq \underbrace{2^m \cdot 2^{-q(n)}}_{\times}$$

Lemma 1.3

$$\oplus \cdot \oplus \cdot P = \oplus \cdot P$$

Proof: $x \in \oplus \cdot \oplus \cdot L$

if $\#\, y_1$ s.t.

$(x, y_1) \in \oplus \cdot L$ is odd

$$\Leftrightarrow \sum_{y_1} \oplus L(x, y_1) = 1 \pmod 2$$

$$\Leftrightarrow \sum_{y_1} \sum_{y_2} L(x, y_1, y_2) = 1 \pmod 2$$

$\Leftrightarrow$ x $\#\,(y_1, y_2)$ s.t. $L(x, y_1, y_2) = 1$ is odd.

Lemma 1.4

$$BP \cdot BP \cdot \mathcal{C} \subseteq BP \cdot \mathcal{C}$$

Proof:

$$\Pr_{y_1}\left[\Pr_{y_2}\left[(x, y_1, y_2) \in L\right] \geq 1 - \frac{1}{2^{q(n)}}\right] \geq 1 - \frac{1}{2^{q_2(n)}}$$

$$\Rightarrow \Pr_{y_1 y_2}\left[(x, y_1 y_2) \in L\right] \geq 1 - \frac{1}{2^{q_1(n)}} - \frac{1}{2^{q_2(n)}}$$

$\square$

Putting it together:

Theorem 9: $\Sigma_k^P \subseteq BP \cdot \oplus \cdot P$

Proof: By induction (base case $k=0$)

$\Pi_{k-1}^P, \Sigma_{k-1}^P \subseteq BP \cdot \oplus \cdot P$

$\Sigma_k^P = \exists \cdot \Pi_{k-1}^P$

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

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

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

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

$\square$

Theorem 2: $BP \oplus P \subseteq P^{\#P}$

Proof:

Fix $L \in P$ & corresponding $L' \in BP \oplus P$

(So $x \in L' \Rightarrow \Pr_y \left[\#z \{(x,y,z) \in L\} \text{ is odd} \right] \geq 1 - \frac{1}{2^{q(n)}}$)

Say # y's $= 2^k$

Idea: Consider "good y"

$x \in L' \Rightarrow \#z \{(x,y,z) \in L\} = 1 \pmod 2$

$x \notin L' \Rightarrow$ " $= 0 \pmod 2$

Wouldn't it be nice if 2 could be replaced by 2^m for large m?

Then would have

$$x \in L' \Rightarrow \#(y,z) \text{ s.t. } \{(x,y,z) \in L\}$$

$$\in \left[2^k\left(1 - \frac{1}{2^{-q(n)}}\right), 2^k\right] \bmod 2^m$$

$$x \notin L' \Rightarrow \#(y,z) \text{ s.t. } \{(x,y,z) \in L\}$$

$$\in \left[0, 2^k \cdot \frac{1}{2^{-q(n)}}\right] \bmod 2^m$$

if $k \leq m$ then we're done.

But how to make "dream" come true:

Can we try to boost the modulus?

Say have

$x \in L \Rightarrow \#y\{M(x,y) \text{ accepts}\} = 1 \pmod{2^k}$

$x \notin L \Rightarrow$ " $= 0$ " .

Can we boost?

Some "counting magic"

Can add # accepting paths.
multiply " .

Say $M_1(x,y)$ accepts N_1 y's

& $M_2(x,y)$ accepts N_2 y's

then can create $M_+(x,y)$ accepts $N_1 + N_2$ y's

2 $M_*(x,y)$ accepts $N_1 \cdot N_2$ y's

Can use this to create M_p accepting $p(N)$ y's if M accepts N y's for any positive integer polynomials!

—— ∞ ——

Example: Can create Machine M' that has $2N^2 + 3N + 1$ y's if M accepts in N ways!

Unfortunately: Doesn't help .....

However, slight twist works

Suppose M is polytime m/c accepting

$x \in L \Rightarrow \#y$ s.t. $M(x,y)$ accepts $= -1 \pmod{2^k}$

$x \notin L \Rightarrow$ " $= 0$ ".

Let $\tilde{M}$ accepts $3N^4 + 4N^3$ y's if M accepts N y's.

then

$x \in L \Rightarrow \#y$ s.t. $M(x,y)$ accepts $= -1 \bmod 2^{2k}$

$x \notin L \Rightarrow$ " $= 0$ ".

Do this $\log m$ times .... & we're set.

Conclude $BP\cdot\oplus\cdot P \subseteq P^{\#P}$ ☒