CS221 LECTURE 13

3/6/2018

TODAY

TODA'S THEOREM

① $\forall i.\ \Sigma_i^P \subseteq BP \cdot \oplus \cdot P$

② $BP \cdot \oplus \cdot P \subseteq P^{\#P}$

Recall operators

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

  $\exists \cdot L = \{x \mid \exists y \text{ s.t. } (x,y) \in L\}$

  $\left.\begin{array}{l}\forall \cdot \mathcal{C} \\ \text{similar} \\ \oplus \cdot \mathcal{C}\end{array}\right]$

- $BP \cdot \mathcal{C} = \bigcap_{\text{poly } p} \{BP_p \cdot L \mid L \in \mathcal{C}\}$

  $(BP_p \cdot L)_Y = \{x \mid \Pr_y[(x,y) \in L] \geq 1 - 2^{-p(n)}\}$

  $(BP_p \cdot L)_N = \{x \mid \Pr_y[(x,y) \in L] \leq 2^{-p(n)}\}$.

First Key Lemma $\exists \cdot \mathcal{C} \subseteq BP \cdot \oplus \cdot \mathcal{C}$

Proof:

- Simpler Case $\mathcal{C} = P$; so $\exists \cdot \mathcal{C} = NP$

Want a tranformation

$$\phi \longrightarrow \psi$$

$\Rightarrow$ if ϕ satisfiable then $\Pr_r \left[\psi(r, \cdot) \text{ has odd } \# \text{ sat. assigns} \right] \geq \ldots$

$\Rightarrow$ if ϕ not sat. then $\Pr_r \left[\psi(r, \cdot) \text{ has even } \# \right] \geq \ldots$

[Two lemmas that have this feature: (1) Razborov-Smolensky (2) Valiant-Vazirani (unique SAT).]
↑ uniform! so we will use this.

Given $\phi \rightarrow \psi$ s.t.

$\phi \in SAT \Rightarrow \Pr[\psi \text{ has odd}] \geq \frac{1}{4n}$

$\phi \notin SAT \Rightarrow \Pr[\psi \text{ has odd}] = 0$.

But not "very high" prob. which is what we're promised.

Amplification for BP.⊕.P (for this reduction)

(1) Can flip odd ≠ even to get.

$$\phi \in SAT \Rightarrow \Pr[\psi \text{ has even}] \geq \frac{1}{4n}$$

$$\phi \notin SAT \Rightarrow \Pr[\psi \text{ has even}] = 0$$

(2) Boost by product

$$\phi \in SAT \Rightarrow \Pr_{r_1 \ldots r_t}\left[\bigwedge_{i=1}^{t} \psi(r_i, z_i) \text{ has even}\right] \geq 1-\left(1-\frac{1}{4n}\right)^t$$

(var.)

$$\Pr_{\ldots}[\quad \text{has even}] = 0.$$

What changes for general C_0 ?

$\exists . C_0 \longrightarrow BP.\oplus . C_0$

Need to ensure that if

$$L = \{(x,y,z) | \ldots\} \in C_0$$

then so is

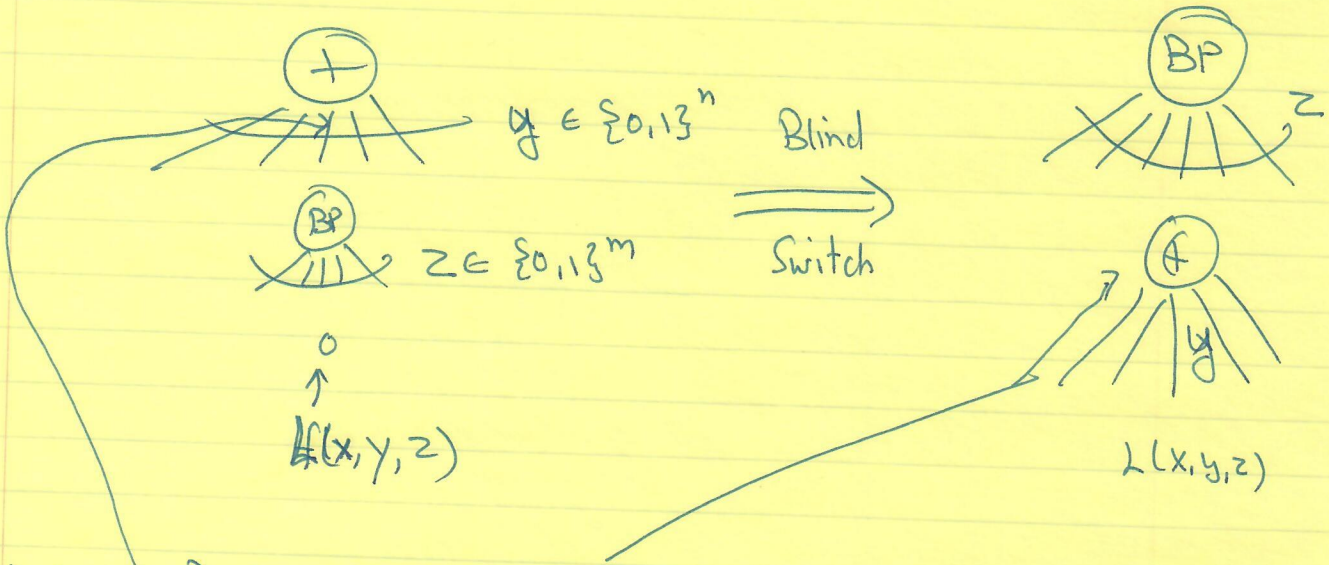
$$L_t = \left\{ (x, y_1, y_2 .. y_t, z_1 .. z_t) \;\middle|\; \#_{(x,y_i,z_i)\in L}\, \forall i \right\}$$

Exercise: verify for $C = BP.\oplus.P$. ☒ concludes Key Lemma

Half-Key Lemma: ~~$BP \cdot \oplus \cdot C \subseteq$~~

$$\oplus \cdot BP \cdot C \subseteq BP \cdot \oplus \cdot C$$

Pool: Say $L \in \oplus \cdot BP \cdot C$



- Index Parity gates on right by z.
- Denote y^{th} wire by $f(x,y)$
- z^{th} gate wrong (for fixed x) if

$$\exists y \text{ s.t. } L(x,y,z) \neq f(x,y)$$

$$\Pr_z[z^{th} \text{ gate wrong}] \leq 2^n \cdot \Pr_{z,y}[L(x,y,z) \neq f(x,y)]$$

$$\leq 2^n \cdot \max_y \Pr_y[L(x,y,z) \neq f(x,y)]$$

$$\leq 2^n \cdot 2^{-p(n)} \leq 2^{-(p(n)-n)}$$

$\blacksquare$

Conclusion:

$$\Sigma_p^i \subseteq \exists \cdot \Sigma_p^{i-1}$$

$$\subseteq \exists \cdot BP \cdot \oplus \cdot P \qquad [\text{Induction on } i]$$

$$\subseteq BP \cdot \oplus \cdot BP \cdot \oplus \cdot P \qquad [\text{Key Lemma}]$$

$$\subseteq BP \cdot BP \cdot \oplus \cdot \oplus \cdot P \qquad [\text{Halt-Key}]$$

$$= BP \cdot \oplus \cdot P \qquad \boxtimes$$

Part II: $BP \cdot \oplus \cdot P \subseteq P^{\#P}$

(Not as surprising, but clever + nice insight into #P).

Main Idea: Have M s.t.

$$x \in L \iff \Pr_{y \in \{0,1\}^n}\left[\#\{z \mid M(x,y,z)=1\} = \text{odd}\right] \geq \frac{1}{2}$$

[don't even need the B in BPP for this part]

Can we just count $\#\{(y,z) \text{ s.t. } M(x,y,z)=1\}$?

[No use ...]

But suppose we had

$$\Pr_y\left[\#\{z \mid M(x,y,z)=1\} = 1 \mod 2^{n+1}\right] \geq \frac{1}{2}$$

Then $\#\{(y,z) \text{ s.t. } M(x,y,z)=1\} \mod 2^{n+1} \geq 2^{n-1}$

$\Leftrightarrow \quad x \in L.$

Want a transformation $M(x,y,z) \Rightarrow N(x,y,w)$

s.t.

- $\#\{z \text{ s.t. } M(x,y,z)=1\} = 0 \mod 2 \Rightarrow \#\{w \mid N(x,y,w)=1\}$
  $= 0 \mod 2^k$
- $= 1 \quad \Rightarrow$
  $= 1 \ldots$

Can we do this.

Transformations / Closure of #P

Recall: $f: \{0,1\}^* \to \mathbb{Z}^{\geq 0}$ in #P if $\exists$ M s.t. $f(x) = \#_y |M(x,y)$

Claim: $f_1, f_2 \in \#P \Rightarrow f_1 + f_2,\ f_1 \cdot f_2 \in \#P$.

(Exercise)

In fact for every nice positive poly $g(x)$ of deg $\leq$ poly(n) & positive integer coeff.

$f \in \#P \Rightarrow g \circ f \in \#P$.

positive

Question: Given k, can we get, poly g of deg poly(k) s.t.

if $f(x) = 0 \mod 2 \Rightarrow g(f(x)) = 0 \mod 2^k$

$f(x) = 1 \mod 2 \Rightarrow g(f(x)) = 1 \mod 2^k$

Answer: NO

$\boxtimes$

However if we ask:

$f(x) = 0 \bmod 2 \Rightarrow g(\ ) = 0 \bmod 2^k$

$f(x) = -1 \bmod 2 \Rightarrow g(\ ) = -1 \bmod 2^k$

Then we can get!

~~$\exists$~~ $\exists m$ of deg 4

Fact: if $x = 0 \bmod 2^\ell \Rightarrow m(x) = 0 \bmod 2^{\ell+1}$

$x = -1 \bmod 2^\ell \Rightarrow m(x) = -1 \bmod 2^{\ell+1}$

Proof: Really want. $x^2 \mid m(x)$

$\Leftarrow (x^2+1)^2 \mid m(x)+1$

$m(x)+1 = (x^2+1)^2(x-1)^2 + 2x^2(x+1)^2$

$= 4x^3 + 3x^4 + 1$ ☒

Let $m_k(x) = m(m_{k-1}(x))$

deg $m_k = 4^k$; $f(x) = 0 \bmod 2 \Rightarrow m(f(x)) = 0 \bmod 2^k$

$f(x) = -1 \bmod 2 \Rightarrow m(f(x)) = -1 \bmod 2^k$.

m_{n^2} = positive poly

☒

(of TODA's Thm.)