CS221 LECTURE 9

2/20/2018

TODAY: $BPP \subseteq P/_{poly}$

$BPP \subseteq PH$

+ other stuff.

Last time

Definition of $BPP_{c,s}$

$L \in BPP_{c,s}$ if $\exists$ poly time $M(\cdot,\cdot)$ s.t.

$\forall x$

$x \in L \Rightarrow \Pr_y[M(x,y)=1] \geq c$

$x \notin L \Rightarrow \Pr_y[M(x,y)=1] \leq s$

Regular BPP $c = 2/3, \quad s = 1/3$

Weak BPP $c - s = \frac{1}{poly(n)}$

Strong BPP $c = 1 - \exp(-poly(n)), \quad s = \exp(-poly(n))$

Amplification Thm: Strong BPP = Weak BPP

Application (1): $BPP \subseteq P/poly$.

Proof: Idea: Want to show $\exists$ single y for which

$$M(x,y) = L(x) \quad \forall x \in \{0,1\}^n.$$

Idea: Work with "Strong BPP"

$$c = 1 - \frac{1}{2^{n+1}} \; ; \quad s = \frac{1}{2^{n+1}}$$

$\forall x \in \{0,1\}^n$

$$\Pr_y \left[M(x,y) \neq L(x) \right] \leq \frac{1}{2^{n+1}} \triangleq \delta$$

$$\Pr_y \left[\exists x \;\; M(x,y) \neq L(x) \right] \leq \underbrace{2^n \cdot \delta}_{\text{Union Bound}} \leq \frac{1}{2}$$

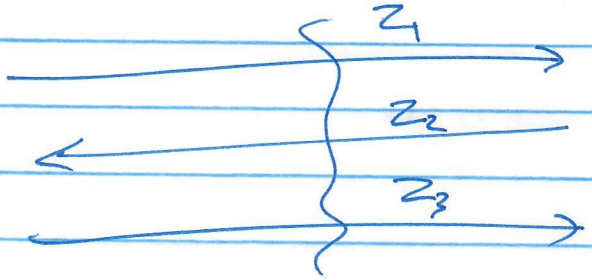
$\Rightarrow \exists y$ s.t. $\forall x \;\; M(x,y) = L(x)$.

Use y as advice !!

Application 2: BPP ⊆ PH

Recall PH = Debate

Alice "$x \in L$" Bob "$x \notin L$"



$V(x, z_1, z_2, z_3) = 1 \iff x \in L$.

Ideas that don't work

Alice → Bob "y" s.t. $M(x,y)=1$

(exists $\forall x$)

Bob → Alice "y" s.t. $M(x,y)=0$.

(also exists $\forall x$)

Really need to utilize/prove "many" such y's exist.

Idea of Proof

- if $S \subseteq \{0,1\}^m$ $\quad [m = |y|]$

  & $|S|$ large, then random shifts of S cover $\{0,1\}^m$

- if $|S|$ small, random shifts leave most of $\{0,1\}^m$ uncovered.

Verifying Idea: random shift = permutations $\pi_1 : \{0,1\}^m \to \{0,1\}^m$

$\vdots$ "

π_m "

π_{m+1}

① Assume $|S| \geq \frac{1}{2} \cdot 2^m$

if $\pi_1 \ldots \pi_{m+1}$ are random permutations, fix $y \in \{0,1\}^m$

$$\Pr_{\pi_1 \ldots \pi_{m+1}}\left[\exists i \text{ s.t. } M(x, \pi_i(y)) = 1\right] = 1 - \frac{1}{2^{m+1}}$$

$$\Pr\left[\forall i \quad M(x, \pi_i(y)) = 0\right] \leq 2^{-(m+1)}$$

$$\Pr\left[\exists y \ \forall i \quad M(x, \pi_i(y)) = 0\right] \leq 2^m \cdot 2^{-(m+1)}$$

$$\leq \frac{1}{2}$$

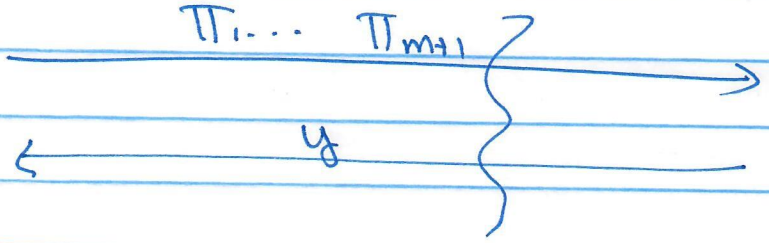
$\Rightarrow \exists \pi_1 \ldots \pi_{m+1} \ \forall y \ \exists i \quad M(x, \pi_i(y)) = 1$.

(2) Now if $|S| \leq \frac{1}{2(m+1)} \cdot 2^m$

then $\begin{cases} \text{fix } \Pi_1 \ldots \Pi_{m+1} \\ \Pr_y [\exists i \text{ s.t. } m(x, \Pi_i(y)) = 1] \leq \frac{1}{2} \end{cases}$

$\Rightarrow \forall \Pi_1 \ldots \Pi_{m+1} \; \exists y$ s.t. $\forall i \; m(x, \Pi_i(y)) = 0$.

Put Together



$\exists i$ s.t. $m(x, \Pi_i(y)) = 1$?

Almost works: Problem = ?

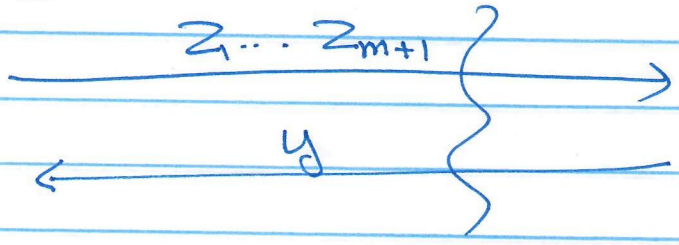
Π_i "too random" ; need $m \cdot 2^m$ bits to describe ...

Simpler $\Pi_i \longrightarrow$ Pick $z_i \in \{0,1\}^m$ at random

$\Pi_i(y) = z_i \oplus y$ [bitwise XOR]

Has all randomness properties for above analysis ☒.

Resulting Protocol



V: Accept if $\exists i$ s.t. $M(x, z_i \oplus y) = 1$.

Neat aspect of proof: Neither Alice / Bob need to be "superpowerful" to play their part whp.

Crucial Role of Amplification:

$BPP_{\frac{1}{2}, \frac{1}{2(m+1)}}$ where m = # random bits. (not length input).

Why is this ok?

Neat aspect of proof: Neither Alice nor Bob need to be "superpowerful" to play their part whp.

Alice can pick $z_1 \ldots z_{m+1}$ purely at random

Bob can pick y " "

- "Effectivity used by "Goldwasser-Sipser" to ~~prove~~ give a counting proof" ... will see later in course.

- [For now]: ~~Promise-BPP~~

$P = $ Promise-RP $\Rightarrow$ $P = $ Promise-BPP.

- Proof:

~~$L = \{(x, z_1 .. z_{m+1}) \mid \Pr_y [\exists i \; M(x, y+z_i) = 1] \geq \frac{1}{2}\}$~~

$M'((x, z_1 .. z_{m+1}); y) = 1$ if ~~$\forall$~~ $\exists i$ ~~s.t.~~ $M(x, y+z_i) = 0$.

~~$x \in L \Rightarrow \Pr[M']$~~

$L'_Y = \{(x, z_1 .. z_{m+1}) \mid \Pr_y [M'(\;\; ; y) = 1] \geq \frac{1}{2}\}$

$L'_N = \{(x, z_1 .. z_{m+1}) \mid \Pr_y [\;\;\;\;\;\; = 1] \leq 0\}$

$\Rightarrow L' \in$ Promise-RP $\Rightarrow L' \in P$

Now consider $M''(x; z_1 .. z_{m+1}) = 1$ if $(x, z_1 .. z_{m+1}) \in L'$

$= 0$ o.w.

~~if $x \in L \Rightarrow \Pr_{z_1 .. z_{m+1}} [M''(x, z_1 .. z_{m+1})]$~~

$L''_Y = \{x \mid \Pr_{z_1 .. z_{m+1}} [(x, z_1 .. z_{m+1}) \in L'] \geq \frac{1}{2}\}$ $L''_N = [\;\;\;\;] \leq 0.$

$L'' \in$ Promise-RP $\Rightarrow L'' \in P$. ∎.

Aside:

Randomized Log Space

RL → One-sided error
BPL → two sided error.

} Need to insist
run time = Poly(n).
+ space = O(log n).

Famous RL problem: Undirected s-t conn.

- Graph G undirected, (s,t) vertices in G
- Question: ∃ path from s to t in G
- in RL: take a random walk
- Alas also in L [Reingold '04]: take all of CS221 + lot more...

- $RL \subseteq NL \subseteq L^2$
  $BPL \subseteq L^2$ [Savitch?]
  State of Art $BPL \subseteq L^{3/2}$!