Lecture 15

Zero-Sided Error

- BPP = Languages L decidable in <u>strict</u> polynomial time by PTM M

$$\underbrace{\Pr[M(x) = L(x)]}_{\text{strict poly time}} \geq 2/3$$

RP : same thing but

$$x \in L \Rightarrow \Pr[M(x) = 1] \geq 2/3$$

$$x \notin L \Rightarrow \Pr[M(x) = 0] = 1$$

coRP :

$$x \in L \Rightarrow \Pr[M(x) = 1] = 1$$

$$x \notin L \Rightarrow \Pr[M(x) = 0] \geq 2/3$$

ZPP: Languages decidable by a PTM in expected polynomial time:

$\forall x$,

$$\Pr[M(x) = L(x)] = 1$$

but M runs in expected poly-time.

- If $T_{M,x}$ is random variable for runtime of $M(x)$.

$$\Rightarrow \mathbb{E}[T_{M,x}] = p(|x|)$$

$$\mathbb{E}[T_{M,x}] =$$

$$\sum_{i=1}^{\infty} i \cdot \Pr[T_{M,x} = i]$$

$$ZPP = \bigcup_{c} ZTIME(n^c)$$

$ZTIME(T) =$

all languages decided by PTM M in expected time $O(T)$

→ If $M(x)$ halts, then $M(x) = L(x)$ w.p. 1

$$L(x) = \begin{cases} 1 & \text{if } x \in L \\ 0 & \text{if } x \notin L \end{cases}$$

Thm: ZPP = RP $\cap$ coRP.

Proof.

$RP \cap coRP \subseteq ZPP$

- Let $L \in RP \cap coRP$
- Let A_L be the RP machine
  B_L be the coRP machine

$x \in L \Rightarrow$ $\Pr[A_L(x) = 1] \geq 2/3$
$\Pr[B_L(x) = 1] = 1$

$x \notin L \Rightarrow$ $\Pr[A_L(x) = 0] = 1$
$\Pr[B_L(x) = 0] \geq 2/3$

D(x):
- while true:

- Run $A_L(x)$ and $B_L(x)$.
- If they both accept, accept.
- If they both reject, reject.

① If $D(x)$ halts, then $D(x) = L(x)$.

- $D(x)$ always halts.
  - $x \in L \Rightarrow$
    - $\Pr[B_L(x)=1] = 1$
    - $\Pr[A_L(x)=1] \geq 2/3$

    $\Rightarrow$ outputs 1
  - $x \notin L \Rightarrow$

- $\Pr[A_L(x)=0] = 1$
- $\Pr[B_L(x)=0] \geq 2/3$

$\Rightarrow$ outputs 0

- Let $p(n)$ be the runtime of A_L, B_L on inputs of length n. (p is polynomial)

$$\mathbb{E}[\underbrace{T_{D,x}}_{\text{runtime of } D \text{ on input } x}] = \sum_{i=1}^{\infty} 2i \cdot p(n) \cdot \Pr[T_{D,x} = 2i\, p(n)]$$

i = # of loops that D runs (running $A_L(x)$, $B_L(x)$ to completion).

$$= 2p(n) \sum_{i=1}^{\infty} \underline{i} \underbrace{\Pr[T_{D,x} = 2ip(n)]}$$

$$\parallel$$

$$= \Pr[D(x) \text{ halts at } i \text{ loops}]$$

<u>$i=1$</u>

$$\Pr[D(x) \text{ hats at } i=1 \text{ loops}]$$

$D(x)$ halts iff

$$x \in L \Rightarrow \underbrace{A_L(x) = B_L(x) = 1}_{} \quad 2/3$$

or w.p.

$$x \notin L \Rightarrow \overbrace{A_L(x) = B_L(x) = 0}^{}$$

Pr[D(x) halts at i=1 loops]

$\underline{i=2}$

Pr[D(x) halts at i=2 loops]

$\Leftrightarrow$ $\boxed{A_i(x) \neq B_i(x) \text{ for first}}$
loop

and $\boxed{A_i(x) = B_i(x) \text{ for second loop}}$

Pr[·] = 1/3

Pr[/] = 2/3

$$= 2p(n) \sum_{i=1}^{\infty} \underline{i} \Pr[T_{D,x} = 2ip(n)]$$

$$= 2p(n) \cdot \sum_{i=1}^{\infty} i \cdot \left(\frac{1}{3}\right)^{i-1} \left(\frac{2}{3}\right)$$

$$= 4p(n) \cdot \underbrace{\sum_{i=1}^{\infty} i \cdot \left(\frac{1}{3}\right)^{i}}$$

$$= 4p(n) \cdot \frac{3}{4} = 3p(n). \checkmark$$

D runs in expected polynomial time!

$L \in ZPP$.

$ZPP \subseteq RP \cap coRP$

Markov's Inequality

If X is non-neg. random variable

$$\Pr[X \geq a] \leq \frac{\mathbb{E}[X]}{a}$$

$L \in ZPP \Rightarrow$

$\exists$ PTM D_L running in ~~exp~~ polynomial time $q(n)$.

$D_L(x) = L(x) \quad \forall x$

- Define machine A

  $A(x)$:

  - Compute $T = 3q(|x|)$
  - Run $D_L(x)$ for at most T steps
    - If $D_L(x)$ halts, output same thing
  - Output 0. — output 1

    $\underbrace{\text{output 1}}_{\text{coRP}}$

<u>Need to show:</u>

$x \in L \Rightarrow \Pr[A(x)=1] \geq 2/3$

$x \notin L \Rightarrow \Pr[A(x)=0] = 1$

- $x \notin L$

  ① $D_L(x)$ halts within T steps

  $\Rightarrow D_L(x) = 0$ ✓

  ② $D_L(x)$ doesn't halt

  $\Rightarrow$ machine outputs 0 ✓

$x \notin L \Rightarrow \Pr[A(x) = 0] = 1$

$x \in L \Rightarrow \Pr[A(x) = 1] \geq 2/3$

$A(x) = 1$ iff

$D_L(x) = 1$ within

$T = 3q(|x|)$ steps.

$$\Pr[T_{D_L,x} \geq a] \leq \underbrace{\frac{\mathbb{E}[T_{D_L,x}]}{a}}_{= \frac{1}{3}}$$

$$\mathbb{E}[T_{D_L,x}] = q(|x|)$$

$$a = 3\,\mathbb{E}[T_{D_L,x}]$$
$$= 3q(|x|) = T$$

$$\Pr[T_{D_L,x} \geq T] \leq \frac{1}{3}$$

$$\Rightarrow \Pr[A_L(x) = 1] \geq 2/3$$

$\Rightarrow$ LGRP

$\boxed{15}$