Randomized Complexity Classes

Lemma (Markov) If X is non-negative random variable then $\Pr[X > \ell\, \mathbb{E}[X]] < 1/\ell$.

Thm: Let $X_1, \dots, X_n$ be independent bits with $\mathbb{E}[X_i] \leq p \to \Pr[X_i = 1] \leq p$

Then $\Pr\left[\sum_{i=1}^{n} X_i \geq pn(1+\varepsilon)\right] \leq 2^{-\frac{\varepsilon^2 np}{4}}$.

$$\boxed{\mathbb{E}\left[\sum_{i=1}^{n} X_i\right] \leq pn}$$

FACT: Suppose you toss a coin which gives heads w.p P.

Let T = # tosses to see first heads

$$\mathbb{E}[T] = p \cdot 1 + (1-p)(\mathbb{E}[T]+1)$$

$$\Rightarrow \mathbb{E}[T] = 1/p.$$

Randomized T.M

- End of each line of code randomly jump to one of two lines of code.

$\underset{\text{coBPP}}{\overset{}{}}$ coBPP
||
BPP: Bounded-error prob. poly. time

$f : \{0,1\}^* \to \{0,1\} \in BPP$ if $\exists$ poly time machine $M(x, r)$ ← random choices of machine

$\forall x \quad \Pr_r[M(x,r) = f(x)] \geq 2/3$. → this number does not matter as long as $> 1/2$.

$\geq 2^{-n}$

RP: Randomized poly time

$f \in RP$ if $\exists$ poly time $M(x,r)$

$\forall x$

- $f(x) = 0 \Rightarrow \Pr_r[M(x,r)=0] = 1$
- $f(x) = 1 \Rightarrow \Pr_r[M(x,r)=1] \geq 2/3$.

this number does not matter as long as > 0

$$ZPP \subseteq RP \subseteq BPP$$

$$RP \subseteq NP$$

$coRP \overset{?}{=} RP$

ZPP: Zero error prob. polytime

$f \in ZPP$ if $\exists$ machine $M(x,r)$

$\Pr_r[M(x,r) = f(x)] = 1$

$\mathbb{E}[\text{running time of } M(x,r)] \leq poly(n)$.

Thm: Suppose $\exists$ a prob poly time machine M computing f s.t. $\Pr_r[M(x,r) = f(x)] \geq \frac{1}{2} + n^{-c}$. The for every constant d, there is a prob. poly time M' computing f

$$\Pr_r[M'(x,r) = f(x)] \geq 1 - 2^{-n^d}.$$

Pf: M': · For some k run $M(x,r)$ n^k times.

· Output the majority outcome.

$X_1, \ldots, X_{n^k}$ $\qquad X_i = \begin{cases} 1 & \text{if } i^{th} \text{ run is an error} \\ 0 & \text{o.w.} \end{cases}$

$$\Pr_r[M'(x,r) \neq f(x)]$$

$$= \Pr\left[\sum_i X_i \geq \frac{n^k}{2}\right]$$

$$= \Pr\left[\sum_i X_i \geq n^k(\tfrac{1}{2} - n^{-c}) \cdot \frac{\tfrac{1}{2}}{(\tfrac{1}{2} - n^{-c})}\right]$$

$\frac{1}{1-2n^{-c}}$

$\frac{1}{1-\varepsilon} > 1+\varepsilon$

$$\leq \Pr\left[\sum_i X_i \geq n^k(\tfrac{1}{2} - n^{-c})(1 + 2n^{-c})\right]$$

$$\leq 2^{-\frac{(2n^{-c})^2 n^k (\frac{1}{2} - n^{-c})}{4}}$$

$$\leq 2^{-n^d} \quad \text{(choose } k \text{ large enough)}.$$

Thm: $BPP \subseteq EXP$

$RP \subseteq NP \subseteq EXP$

Thm: $ZPP = RP \cap coRP$.

Pf: Suppose $f \in ZPP$ via $M(x,r)$ $\mathbb{E}[\text{running time}] \le t(n)$

Claim: $f \in RP$. $f \in coRP$

Run algorithm $M(x,r)$ for $10 \cdot t(n)$ steps.

If alg. halts: output what it outputs

If alg does not halt: output 0. $\Downarrow$ 1

Suppose $f \in RP \cap coRP$ — RP via $M_1(x,r)$, $coRP$ via $M_2(x,r)$

Claim: $f \in ZPP$

M'

1. Simulate $M_1(x,r)$ if output 1, output 1.
2. " $M_2(x,r)$ " " 0, output 0.
3. Goto step 1.

$\mathbb{E}[\#\text{ rounds}] \le 3/2$.

Open: $BPP \stackrel{?}{=} P$

Thm: If $\exists f \in EXP$ s.t. $\exists \varepsilon > 0$ f cannot be computed by circuits of size $2^{\varepsilon n}$ then $BPP = P$.

Thm: Every $f \in BPP$ has poly sized circuits.

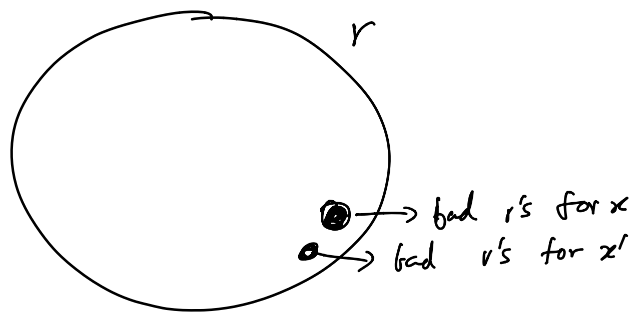
$M(x,r)$

Pf:

Make $M'(x,r)$

$$\Pr_r[\, M'(x,r) \neq f(x) \,] \leq 2^{-2n}.$$

For any input length n, $x \in \{0,1\}^n$ ↳ 2^n potential inputs.



$$\Pr_r\Big[\, \exists x \in \{0,1\}^n \text{ s.t. } M'(x,r) \neq f(x) \,\Big] \leq 2^{-2n} \cdot 2^n < 1$$

$$\Rightarrow \exists\, r \text{ s.t. } \underbrace{M'(x,r)}_{\text{Convert to a circuit.}} = f(x) \quad \forall x \in \{0,1\}^n.$$

Thm: $BPP \in NP^{3SAT}$.