## Randomization

**BPP:** Bounded error prob. poly time

$f \in BPP$ if $\exists$ randomized poly time machine $M$ s.t

$Pr[M(x) = f(x)] \geq 2/3$.

$RL \subseteq L^{3/2}$

BPL

- $RP \subseteq BPP$
- $coBPP = BPP$
- $coRP \stackrel{?}{=} RP$

**RP:**

$f \in RP$ if $\exists$ rad. poly time machine $M$ s.t

if $f(x)=1$, $Pr[M(x) = f(x)] \geq 2/3$ $\quad > 0$

if $f(x)=0$, $Pr[M(x) = f(x)] = 1$.

start

$M(x)=1$

**ZPP:** Zero-error prob. poly time

$f \in ZPP \Leftrightarrow \exists$ rad machine s.t $Pr[M(x) = f(x)] = 1$

$\mathbb{E}[$running time of $M(x)] = poly(n)$.

---

**Thm:** $ZPP = RP \cap coRP$.

**Pf:** $ZPP \subseteq RP$, $ZPP \subseteq coRP \Rightarrow ZPP \subseteq RP \cap coRP$

**Lemma:** If $T$ is a non-neg. random variable

$Pr[T \geq t] \leq \frac{\mathbb{E}[T]}{t}$.

Suppose $f \in ZPP$ via $M$.

Let $T$ be running time.

$\mathbb{E}[T] \leq r(n)$.

$M'(x)$

- Run $M(x)$ for $3 \cdot r(n)$ steps.
- If $M(x)$ halts output same output.
- Otherwise output 0.

$RP \cap coRP \subseteq ZPP$

Suppose $f \in RP$ via $M$, $f \in coRP$ via $M'$

$M''(x)$

If $M(x)=1$, output 1

If $M'(x)=0$, output 0

Goto

Suppose you have a coin that is heads with prob $p$.

$\mathbb{E}[$# tosses before first heads$] = \frac{1}{p}$.

$\mathbb{E}[X] = (1-p)(\mathbb{E}[X]+1) + p$ $\quad X$ = # tosses before first heads

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

$$P \subseteq ZPP \subseteq \begin{matrix} RP \\ \cap \\ coRP \end{matrix} \subseteq BPP \subseteq NP^{SAT}$$

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

---

**Chernoff** Suppose $X_1, \ldots, X_n \in \{0,1\}$ are independent, $\forall i \ \mathbb{E}[X_i] = p$.

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

**Consequence:** Suppose $f \in BPP$ via $M$.

$M'(w)$

Run $M(w)$ $t$ times.

Output majority outcome.

$$X_1, X_2, \ldots, X_t \quad X_i = \begin{cases} 1 & \text{iff } i^{th} \text{ round error} \\ 0 & \text{o.w.} \end{cases}$$

$$\mathbb{E}[X_i] \leq 1/3.$$

$$\Pr[\text{error}] \leq \Pr\left[\sum_i X_i \geq t/2\right] \leq 2^{-\Omega(t)}.$$

$$\Pr[f(w) = M'(w)] \geq 1 - 2^{-\Omega(t)}.$$

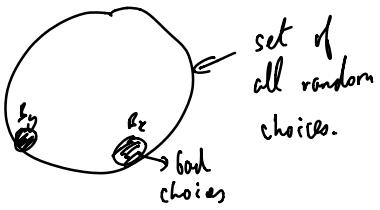
---

**Consequences of error reduction**

1. $BPP \subseteq SIZE(poly(n))$.

$f \in BPP$ via $M$ $\Rightarrow$ $\exists M'$ polytime, $\Pr[M'(x) = f(x)] > 1 - 2^{-n}$. $\forall n$

$\exists$ seq of choices $r$ s.t. $r \notin \bigcup_x B_x$




$\Rightarrow$ poly size circuit after fixing $r$.

2. If $P = NP$ then $P = BPP$.

Suppose $f \in BPP$ via $M$ (w.h.p. prob of error $< 2^{-n}$).

$$f(x) = 1 \iff \exists u \; \forall r \; \underbrace{C(x,u,r)}_{\text{poly sized circuit}}$$

$$\overset{\text{if } P=NP}{\iff} \exists u \; C'(x,u) \qquad \neg\exists r \; \neg C(x,u,r)$$

$$\overset{\text{if } P=NP}{\iff} C''(x)$$

$M(x, r)$ with $r \in \{0,1\}^m$ let $u_1, \ldots, u_k \in \{0,1\}^m$ $k > m/n$

Claim: If $f(x) = 0$