

# CSL857: Randomized Algorithms

Ragesh Jaiswal  
CSE, IIT Delhi

# Complexity Classes

---

RP, BPP, ZPP etc.

# Complexity Classes

- Randomized complexity class **BPP**:

- A language  $L \subseteq \{0,1\}^*$  is said to be in the class **BPP** if there is a randomized Turing machine  $M$  such that

$$\forall x \in L, \Pr[M(x, R) \text{ accepts}] \geq 3/4, \text{ and}$$

$$\forall x \notin L, \Pr[M(x, R) \text{ accepts}] < 1/4.$$

Moreover  $M$  runs in time  $p(|x|)$  for some polynomial function  $p(\cdot)$ .

- Let us define a class high-**BPP**:

- A language  $L \subseteq \{0,1\}^*$  is said to be in the class high-**BPP** if there is a randomized Turing machine  $M$  such that

$$\forall x \in L, \Pr[M(x, R) \text{ accepts}] \geq 1 - 2^{-k}, \text{ and}$$

$$\forall x \notin L, \Pr[M(x, R) \text{ accepts}] < 2^{-k}.$$

Moreover  $M$  runs in time  $p(|x|)$  for some polynomial function  $p(\cdot)$  and  $k$  is any large fixed constant (say  $k = 100$ ).

- Claim: **BPP** = high-**BPP**

# Complexity Classes

- Theorem (Chernoff bound): Let  $n \geq 1$  be an integer and let  $X_1, X_2, \dots, X_n$  be  $n$  independent 0/1 valued random variables. Let  $X = X_1 + X_2 + \dots + X_n$  and let  $a > 0$  be any real number. Then

$$\Pr[X \geq E[X] + an] \leq e^{-\frac{a^2 n}{2+a}}$$

$$\Pr[X \leq E[X] - an] \leq e^{-\frac{a^2 n}{2}}$$

# Complexity Classes

- Claim:  $BPP \subseteq \text{high} - BPP$ .
  - Proof: Consider the BPP machine  $M$  for any language  $L \in BPP$ . Construct the following machine  $M'$ :
    - $M'$  runs  $n$  independent copies of  $M$  and then returns the *majority* answer.
    - $\forall x \in L, \Pr[M'(x, R) \text{ accepts}] \geq 1 - 2^{-k}$   
 $\forall x \notin L, \Pr[M'(x, R) \text{ accepts}] \leq 2^{-k}$
    - What is the value of  $n$  for which the above two inequalities are true?

# Complexity Classes

- RP: The class of decision languages that have Monte Carlo algorithms that runs in polynomial time (worst-case) and have a one sided error of at most  $\frac{1}{2}$ . The algorithms commits error when  $x \in L$ .
- Co-RP: The class of decision languages that have Monte Carlo algorithms that runs in polynomial time (worst-case) and have a one sided error of at most  $\frac{1}{2}$ . The algorithms commits error when  $x \notin L$ .
- ZPP: The class of decision languages that have a Las-Vegas algorithm that runs in expected polynomial time.
- Claim:  $ZPP = RP \cap \text{co-RP}$ .

# Chernoff Bounds

Theorem (Chernoff bound): Let  $n \geq 1$  be an integer and let  $X_1, X_2, \dots, X_n$  be  $n$  independent 0/1 valued random variables. Let  $X = X_1 + X_2 + \dots + X_n$  and let  $a > 0$  be any real number. Then

$$\Pr[X \geq E[X] + an] \leq e^{-\frac{a^2 n}{2+a}}$$

$$\Pr[X \leq E[X] - an] \leq e^{-\frac{a^2 n}{2}}$$

# Chernoff Bounds

- Theorem: Let  $X_1, \dots, X_n$  be independent, 0/1 random variables, and let  $p_i = E[X_i]$  for all  $i = 1, \dots, n$ . Let  $X = X_1 + X_2 + \dots + X_n$  and let  $\mu = E[X]$ . Let  $\delta > 0$  be any real number. Then

$$\Pr[X > (1 + \delta) \cdot \mu] \leq \left[ \frac{e^\delta}{(1 + \delta)^{(1+\delta)}} \right]^\mu.$$

- Corollary: Let  $X_1, \dots, X_n$  be independent, 0/1 random variables, and let  $p_i = E[X_i]$  for all  $i = 1, \dots, n$ . Let  $X = X_1 + X_2 + \dots + X_n$  and let  $\mu = E[X]$ . Let  $0 < \delta \leq 1$  be any real number. Then

$$\Pr[X > (1 + \delta) \cdot \mu] \leq e^{-\frac{\delta^2 \mu}{3}}.$$

# Chernoff Bounds

- Theorem: Let  $X_1, \dots, X_n$  be independent, 0/1 random variables, and let  $p_i = E[X_i]$  for all  $i = 1, \dots, n$ . Let  $X = X_1 + X_2 + \dots + X_n$  and let  $\mu = E[X]$ . Let  $\delta > 0$  be any real number. Then

$$\Pr[X > (1 - \delta) \cdot \mu] \leq \left[ \frac{e^{-\delta}}{(1 - \delta)^{(1-\delta)}} \right]^\mu.$$

- Corollary: Let  $X_1, \dots, X_n$  be independent, 0/1 random variables, and let  $p_i = E[X_i]$  for all  $i = 1, \dots, n$ . Let  $X = X_1 + X_2 + \dots + X_n$  and let  $\mu = E[X]$ . Let  $0 < \delta \leq 1$  be any real number. Then

$$\Pr[X > (1 - \delta) \cdot \mu] \leq e^{-\frac{\delta^2 \mu}{2}}.$$

End

---