Computational Complexity

Mohammad Mahmoody

Session 21
April 2014

Complexity Class **BPP**

Definition 7.3 *(**BPP**, alternative definition)* A language L is in **BPP** if there exists a polynomial-time TM M and a polynomial $p : \mathbb{N} \to \mathbb{N}$ such that for every $x \in \{0, 1\}^*$, $\Pr_{r \in_R \{0,1\}^{p(|x|)}}[M(x, r) = L(x)] \geq 2/3$.

How to decrease the error for **BPP**

- Suppose $\begin{array}{l} x \in L \Rightarrow \Pr[M(x) = 1] \overset{=}{\geq} 1/2 + \varepsilon \\ x \notin L \Rightarrow \Pr[M(x) = 0] \geq 1/2 + \varepsilon \end{array}$

$\frac{1}{n}$

k : odd

M_k : run $M(x)$ k times using independent randomness.

we get back $a_1, a_2, \dots, a_k$ and output : majority.

→ the expected # of "correct" answers is $\geq \left(\frac{1}{2}+\varepsilon\right) \cdot k$

define : c_i = boolean random variable $\begin{cases} 1 & \text{if } M(x) \text{ answer correctly} \\ 0 & \text{if } M(x) \text{ — wrong.} \end{cases}$

$\Pr[c_i = 1] \geq \frac{1}{2} + \varepsilon$: $\mathrm{Exp}[c_i] \geq \frac{1}{2} + \varepsilon$

$E\left[\sum c_i\right] \geq \sum E[c_i] \geq k\left(\frac{1}{2} + \varepsilon\right)$

linearity of exp.

Big Q: $\Pr\left[\underbrace{\sum c_i}_{k} > \frac{1}{2}\right] \overset{?}{=}$

Chernoff-Hoeffding Bound

Concentration Bound:

- Theorem: Suppose $a_1, \dots a_{\cancel{n}\,k}$ are independent Boolean random variables such that $\mathrm{Ex}[a_i] = \Pr[a_i = 1] = \beta$ and let $a = \frac{\Sigma_i a_i}{\cancel{n}\,k}$ then and $\underbrace{\Pr[a \geq \beta + \varepsilon]}_{\text{bad 1}}$ and $\underbrace{\Pr[a \leq \beta - \varepsilon]}_{\text{bad 2}}$ are both $< 2^{-\cancel{n}k\varepsilon^2}$

if we run M_k: what is prob. of getting wrong answer?

recall: $\Pr[c_i : i^{th}$ exec. being correct$] \geq \frac{1}{2} + \varepsilon$ β

$\boxed{2^{-k\varepsilon^2}}$

$\underbrace{\text{if alg } M_n \text{ fails}}_{E_1} \Longrightarrow$ fraction of correct answer $\leq \frac{1}{2}$

$\Rightarrow \frac{\Sigma c_i}{k} \leq 1/2$

$\Rightarrow \beta - \Sigma c_i/k \geq \varepsilon \Leftarrow E_2$

$\Pr[E_1] \leq \Pr[E_2] \leq$

Randomness for **other complexity classes**

- BP.L (and R.L)
- BP.NP (and R.NP?)
- BP.P/poly?

Turing Machine

randomness

input

memory

output

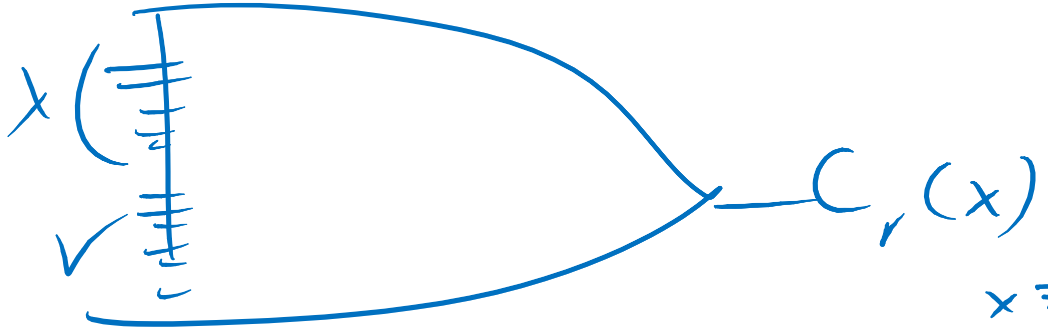
$\Pr[\text{Correct}] \geq \frac{2}{3}$

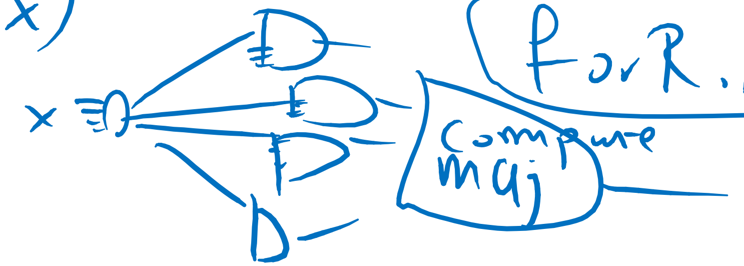
$\geq \frac{1}{2} + \frac{1}{10}$

$= NP$

$L \in BP.NP$ iff

$\exists$ randomize $M(\cdot)$ s.t. $\begin{cases} x \in L \Rightarrow \exists w.\ \Pr[M(x,w)=1] \geq \frac{2}{3} \\ x \notin L \Rightarrow \forall w\ \Pr[M(x,w)=0] \geq \frac{2}{3} \end{cases}$





for R.NP = 1

if $L \in BPP$ (or BP. P/poly) and $\Pr\{\text{error for input lgy } n\} < 2^{-n}$

$\Longrightarrow$ $\exists$ sequence $\{r_1, r_2 \ldots r_n \ldots\}$

$\Longrightarrow$ if we use r_n for <u>any</u> input $x \in \{0,1\}^n$

we get correct answer.

(★) $\Pr\{\text{output } \underline{\text{wrong}}\} < 2^{-n}$ $\quad |x| = n$

claim : $\exists\, r : \forall x \quad M(r, x)$ is correct

(★)$_2$ Suppose: $\forall r \ \exists x$ st.. $M(x, r) = \text{wrong} \Longrightarrow P_{x,r}[\text{wrong}] \geq 2^{-n}$

pretend r is chosen first

$\Longrightarrow$ we get bad x prob $\geq 2^{-n}$

(★)$_1$ $\longrightarrow$ $P_{r,x}[\text{wrong}] < 2^{-n}$