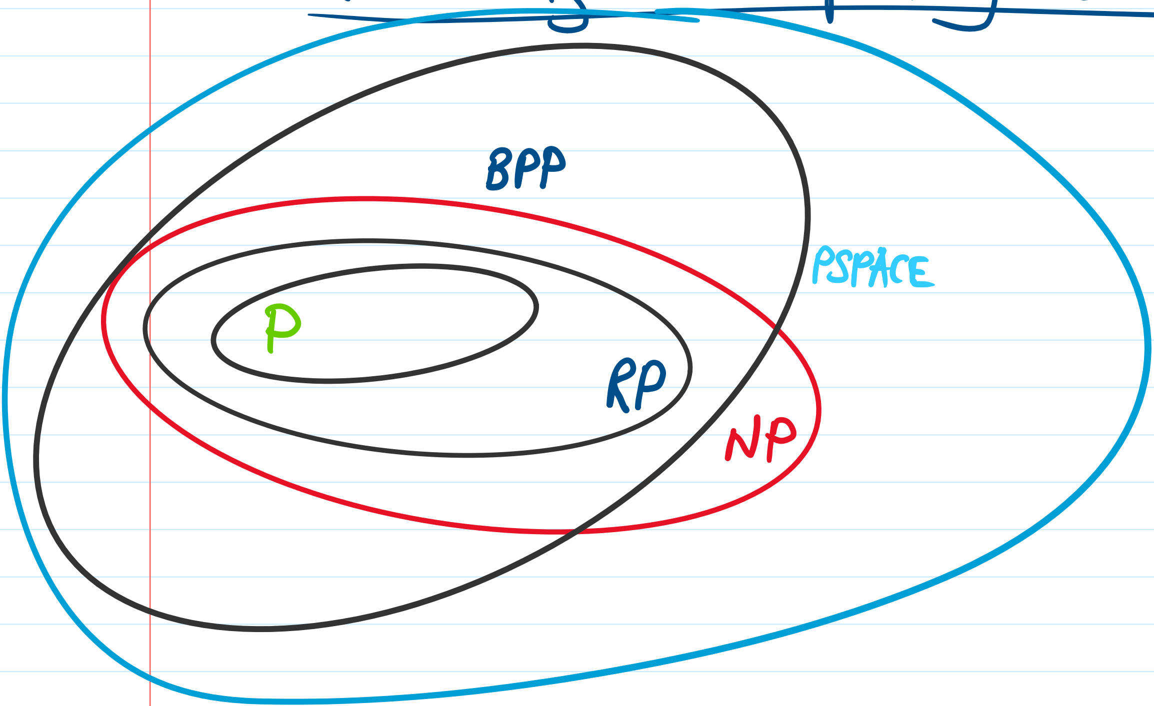
Lecture 27

Friday, July 26, 2019 11:24 AM

Randomized Complexity Classes



$$P \subseteq RP \subseteq NP \subseteq PSPACE$$

$$RP \subseteq BPP$$

__Def:__ $L \in RP$ if there is a polytime deterministic TM $M(x, y)$, $|y| \le poly(|x|)$

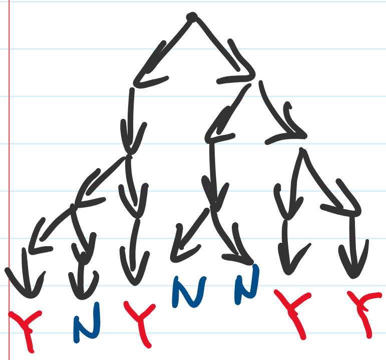
input: x ; random string: y

s.t. $\forall x \in \{0,1\}^n$,

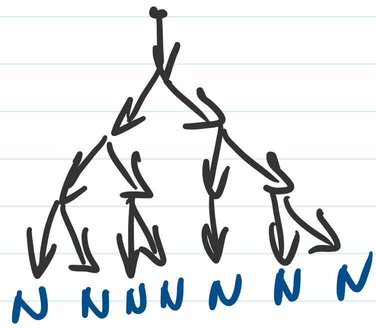
(1) $x \in L \Rightarrow \Pr_y[M(x,y) \text{ accepts}] \geq \frac{1}{2}$

(2) $x \notin L \Rightarrow \Pr_y[M(x,y) \text{ accepts}] = 0$

On input $x \in L$, On input $x \notin L$, On input $x \in L$, M's computation



On input $x \notin L$,



An RP-algorithm is always correct on $x \notin L$, (no false positives) & may be wrong (with prob. $\leq \frac{1}{2}$) on $x \in L$. (may give false negatives)

One-sided error algorithm.

__Def:__ $L \in BPP$ if there is a polytime det. TM $M(x,y)$, $|y| \leq poly(|x|)$ s.t. $\forall x \in \{0,1\}^n$,

(1) $x \in L \Rightarrow \Pr_y [M(x,y) \text{ accepts}] \geq \frac{2}{3}$

(2) $x \notin L \Rightarrow \Pr_y [M(x,y) \text{ accepts}] \leq \frac{1}{3}$

may have both false positives and false negatives.

Two-sided error algorithm.

Error Probability Reduction

Thm: Let $M(x,y)$ be an RP-algo for a language L.
Then L can be decided by another RP algo. $M'(x,y')$ s.t. $\forall x \in \{0,1\}^n$

(1) $x \in L \Rightarrow \Pr_{y'}[M'(x,y') \text{ accepts}] \geq 1-2^{-k}$

(2) $x \notin L \Rightarrow \Pr_{y'}[M'(x,y') \text{ accepts}] = 0.$

Proof:
Define M' as follows:
" On input $x \in \{0,1\}^n$,
run $M(x,y_1)$, $M(x,y_2), \dots, M(x,y_k)$
for independent random y_i's.
If at least one $M(x,y_i)$ accepts,
then accept; otherwise reject. "

The run time of M' is k times

The runtime of M': $k \cdot \text{time}_M$

(polynomial if k is)

The error probability analysis:

- if $x \notin L$, then each $M(x, y_i)$ rejects and hence $M'(x, y')$ also rejects.
- if $x \in L$, then each $M(x, y_i)$ accepts with prob. $\geq \frac{1}{2}$ (by def. of RP)

$$\Pr_{y_1,\dots,y_k}\left[\bigwedge_{i=1}^{k}\left(M(x, y_i) \text{ rejects}\right)\right] \leq \left(\frac{1}{2}\right)^k$$

So, $\Pr_{y'}\left[M'(x, y') \text{ accepts}\right] \geq 1 - \left(\frac{1}{2}\right)^k.$

$\square$

<u>Thm:</u> Let $M(x,y)$ be a BPP-algo. for a language L. Then L can be decided by another BPP-algorithm $M'(x,y')$, with error probability $\leq 2^{-k}$.

<u>Proof:</u> Define M' as follows:

"On input $x \in \{0,1\}^n$,

run $M(x, y_1)$ $M(x, y_2)$ $M(x, y_k)$

run $M(x,y_1), M(x,y_2), \ldots, M(x,y_t)$
for independent random y_i's
(where $t = O(k)$).
Accept iff the Majority of the runs accept."

The runtime of M': $t \cdot \text{time}_M$

The error probability analysis:

Say, $x \in L$ (the other case is analogous):

$M(x,y_1)$ $M(x,y_2)$ ... $M(x,y_t)$

1 (accept)   0 (reject)   1 with prob. p ($p \geq \frac{2}{3}$)

- each $M(x,y_i) = \begin{cases} 1 & \text{w. prob.} \geq \frac{2}{3} \\ 0 & \text{w. prob.} \leq \frac{1}{3} \end{cases}$

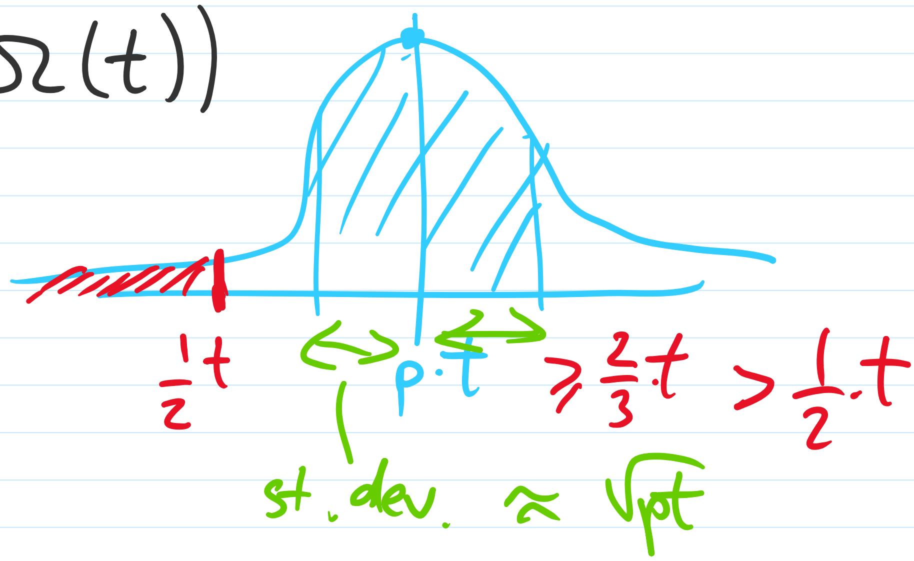
  by def. of BPP

- the expected number of 1's in these t experiments is $p \cdot t \geq \frac{2}{3} \cdot t$

- by the Law of Large Numbers,

$$\Pr_{y_1,\ldots,y_t}\left[\text{the number of accepts} < \frac{1}{2}t\right]$$

$$\leq \exp(-\Omega(t))$$



Chernoff bound:

$X_1, \ldots, X_t \in \{0,1\}$ indep. r.v. (identically distr.)

$$\Pr\left[\,\left|\sum X_i - \mathrm{Exp}\left[\sum X_i\right]\right| > \text{"large"}\right]$$

$$\leq \exp(-\Omega(t))$$

Poly Identity Testing

$$p(x) = 3 \cdot x^2 + 5 \cdot x - 13$$

$$p(x_1, x_2, \ldots, x_n) = \underline{\hspace{4cm}}$$

algo to compute p on any given input

$$\det \begin{vmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ & \ddots & & \\ & & \ddots & \\ x_{n,1} & \cdots & & x_{n,n} \end{vmatrix}$$

$$\det \begin{pmatrix} 1 & \cdots & & 1 \\ x_1 & \cdots & & x_n \\ x_1^2 & \cdots & & x_n^2 \\ \vdots & & & \vdots \\ x_1^{n-1} & \cdots & & x_n^{n-1} \end{pmatrix} = \prod_{j>i} (x_j - x_i)$$