

# Lecture 16 - Randomized Complexity Classes

Lance Fortnow (notes for 02/18/08 scribed by Sanchit Misra)

February 22, 2008

- $L \in RP$  if there is a probabilistic polytime TM  $M$  s.t.  $\forall x \in \Sigma^*$   
 $x \in L \Rightarrow Pr(M(x) \text{ accepts}) \geq \frac{1}{2}$   
 $x \notin L \Rightarrow Pr(M(x) \text{ accepts}) = 0$   
which means no matter what coin we toss, we will never accept  $x$  by mistake.
- $RP \subseteq NP$  (nondeterministically guess the flip of coins)
- $Composite \in RP$   
 $Prime \in Co-RP$
- The constant value  $1/2$  doesn't matter. Infact following are two equivalent ways of writing  $RP$ :  
 $\forall$  polynomials  $q$   
 $x \in L \Rightarrow Pr(M(x) \text{ acc}) \geq 1 - 2^{-q(|x|)}$   
or  
 $\exists$  polynomial  $p$   
 $x \in L \Rightarrow Pr(M(x) \text{ acc}) \geq \frac{1}{p(|x|)}$

Proof: Define  $M, p$  s.t.

$$x \in L \Rightarrow Pr(M(x) \text{ acc}) \geq \frac{1}{p(|x|)}$$

$$x \notin L \Rightarrow Pr(M(x) \text{ acc}) = 0$$

Define  $M'$  s.t.

$$x \in L \Rightarrow Pr(M'(x) \text{ acc}) \geq 1 - 2^{-q(|x|)}$$

$$x \notin L \Rightarrow Pr(M'(x) \text{ acc}) = 0$$

$M'(x)$  : run  $M(x)$  for  $k$  times with independent coin tosses. Accept if any run accepts. Hence,

$$\begin{aligned}
x \notin L &\Rightarrow Pr(M(x) \text{ acc}) = 0 \Rightarrow Pr(M'(x) \text{ acc}) = 0 \\
x \in L &\Rightarrow Pr(M(x) \text{ acc}) \geq \frac{1}{p(|x|)} \\
&\Rightarrow Pr(M(x) \text{ rej}) \leq 1 - \frac{1}{p(|x|)} \Rightarrow Pr(M'(x) \text{ rej}) \leq (1 - \frac{1}{p(|x|)})^k \\
(1 + a)^b &\sim e^{ab} \text{ (if } ab \rightarrow \infty \text{ or } -\infty) \\
&\Rightarrow Pr(M'(x) \text{ rej}) \leq e^{\frac{-k}{p(|x|)}} \leq 2^{\frac{-k}{p(|x|)}} \leq 2^{-q(|x|)} \\
Pr(M'(x) \text{ acc}) &\geq 1 - 2^{-q(|x|)}, k = p(|x|)q(|x|)
\end{aligned}$$

- PP : Probabilistic polynomial time  
 $x \in L \Rightarrow Pr(M(x) \text{ accepts}) > \frac{1}{2}$   
 $x \notin L \Rightarrow Pr(M(x) \text{ accepts}) \leq \frac{1}{2}$
- $L \in BPP$  if there is a probabilistic polytime TM  $M$  s.t.  $\forall x \in \Sigma^*$   
 $x \in L \Rightarrow Pr(M(x) \text{ accepts}) \geq \frac{2}{3}$  or  $\frac{1}{2} + \frac{1}{p(|x|)}$  or  $1 - 2^{-q(|x|)}$   
 $x \notin L \Rightarrow Pr(M(x) \text{ accepts}) \leq \frac{1}{3}$  or  $\frac{1}{2} - \frac{1}{p(|x|)}$  or  $2^{-q(|x|)}$   
 BPP: Bounded error probabilistic polynomial time. All three above definitions are equivalent.  
 Define  $M$  s.t.  
 $x \in L \Rightarrow Pr(M(x) \text{ accepts}) \geq \frac{2}{3}$   
 $x \notin L \Rightarrow Pr(M(x) \text{ accepts}) \leq \frac{1}{3}$   
 Define  $M'$  s.t.  
 $M'$  runs  $M(x)$   $k$  times independently. If  $M(x)$  accepts atleast  $\geq \frac{k}{2}$  times then accept, else reject

Let  $p = Pr(M(x) \text{ accepts}) \geq \frac{2}{3}$

If  $x \in L \Rightarrow Pr(M'(x) \text{ rej}) = \sum_{i=0}^{\frac{k}{2}} \binom{k}{i} p^i (1-p)^{k-i} \leq \sum_{i=0}^{\frac{k}{2}} \binom{k}{i} (\frac{2}{3})^i (\frac{1}{3})^{k-i} \leq$

$$\sum_{i=0}^{\frac{k}{2}} \binom{k}{i} (\frac{2}{3})^{\frac{k}{2}} (\frac{1}{3})^{\frac{k}{2}}$$

(maximizes at  $k/2$ )

$$(\frac{2}{3})^{\frac{k}{2}} (\frac{1}{3})^{\frac{k}{2}} \sum_{i=0}^{\frac{k}{2}} \binom{k}{i} \leq (\frac{2}{9})^{\frac{k}{2}} \sum_{i=0}^k \binom{k}{i} \leq (\sqrt{4.5})^{-k} \cdot 2^k \sim 2^{-0.084k}$$

$$k = \frac{q(|x|)}{0.084} = 15q(|x|)$$

- We don't know the relation between BPP and NP.

- ZPP : Zero-Error PP  
 $x \in L \Rightarrow Pr(M(x) \text{ accepts}) = 1$   
 $x \notin L \Rightarrow Pr(M(x) \text{ accepts}) = 0$  and  
 The expected running time of M is polynomial; i.e.;  
 $\exists$  poly  $q$   
 $\sum_{i \geq 0} i Pr(M(x) \text{ acc in } i \text{ steps}) \leq q(|x|)$
- Theorem:  $ZPP = RP \cap \text{Co-RP}$   
 Run the machines corresponding to RP and Co-RP, say  $M_{RP}$  and  $M_{\text{Co-RP}}$ . If  $M_{RP}$  accepts, we halt and accept. If  $M_{\text{Co-RP}}$  accepts, we halt and reject.
- Theorem : If  $DTIME(2^n) \not\subseteq DSPACE(2^{\epsilon n})$  for some  $\epsilon > 0$ , then  $P = ZPP = RP = \text{Co-RP} = \text{BPP}$   
 We don't know how to make the condition true. But, we believe that it is true.