

CSE200: Computability and Complexity

Fall 2008, Homework 7

Instructor: Daniele Micciancio
Due Wednesday November 26, 2008

Problem 1: NP, RP and BPP

- (a) Show that if $\mathcal{L}_1, \mathcal{L}_2 \in RP$ (resp. BPP) then $\mathcal{L}_1 \cup \mathcal{L}_2 \in RP$ and $\mathcal{L}_1 \cap \mathcal{L}_2 \in RP$ (resp. BPP).
- (b) In class, we defined the class $ZPP = RP \cap coRP$. Show that if $coNP \subseteq RP$ then $NP = ZPP$.

Problem 2: More on NP, RP and BPP

(a) In class we defined class BPP as follows: BPP is the class of all languages \mathcal{L} for which there exists a probabilistic polynomial-time TM M , such that:

$$\begin{aligned}x \in \mathcal{L} &\Rightarrow Pr_r[M(x, r) = 1] \geq 1 - \epsilon \\x \notin \mathcal{L} &\Rightarrow Pr_r[M(x, r) = 1] \leq \epsilon\end{aligned}$$

where the error probability is $\epsilon = 1/3$. We also observed that the error probability can be reduced to $1/2^n$ using standard repetition techniques. (Formally, we proved the result for RP . You can read the details of a similar proof for BPP from the textbook.) In other words, the class BPP remains the same even if we replace the $\epsilon = 1/3$ in the above definition with $\epsilon = 1/2^n$.

- Show that if \mathcal{L} is NP -complete and $\mathcal{L} \in RP$, then $NP \subseteq RP$.
- Show that if $NP \subseteq BPP$ then $NP = RP$.

(b) Let $BPP^{BPP} = \bigcup_{\mathcal{L} \in BPP} BPP^{\mathcal{L}}$ (the exponent \mathcal{L} denotes oracle access to a language $\mathcal{L} \in BPP$). Show that $BPP^{BPP} = BPP$.

Can you prove the same result for RP ?