Complexity Theory

Homework Sheet 6

(Turn in before the exercise session of Thursday 15 October.)

8 October 2014

Definition 1. Define RP to be the class of languages A for which there is a polytime machine M, and some constant c, such that for all $x \in \{0,1\}^*$,

$$x \in A \implies \Pr_r[M(x,r) = 1] \geq 2/3,$$

$$x \notin A \implies \Pr_r[M(x,r) = 0] = 1,$$

where r is drawn from the uniform distribution over $\{0,1\}^{n^c}$.

Define the complexity class ZPP to be the class of languages A for which there is a polytime machine M which ouputs either 0, 1 or ?, and some constant c, such that for all $x \in \{0,1\}^*$,

$$\Pr_r[M(x,r) = ?] \leq 1/2,$$
$$\text{if } M(x,r) = 1, \text{ then } x \in A,$$
$$\text{if } M(x,r) = 0, \text{ then } x \notin A,$$

where r is drawn from the uniform distribution over $\{0,1\}^{n^c}$.

Exercise 1. Prove the following statements.

(a) $\text{ZPP} = \text{RP} \cap \text{coRP}$

(b) $\text{RP} \subseteq \text{NP}$,

(c) $\text{RP}^{\text{RP}} \subseteq \text{BPP}$.

Exercise 2. Define BPP/*poly*. Show that BPP/*poly* = P/*poly*.

Exercise 3. Show that in interactive proof systems we gain nothing by allowing the prover to make use of randomness. That is, show that if we have a probabilistic prover P that convinces a verifier V to accept with probability p, where the probability is taken over the random coins of both P and V, then we have a deterministic prover P that convinces V to accept with probability $\geq p$, where the probability is now taken only over the random bits of V.