Complexity Theory

Homework Sheet 6

(Turn in before the lecure of Monday 12 May.)

5 May, 2014

Exercise 1. Show that, given a fair coin, you can simulate the roll of a dice. More precisely, describe an algorithm A which runs in $O(\log \frac{1}{\delta})$ steps and outputs a number of 1 to 6 or an auxiliary symbol **?**, in a way such that:

1. Conditioned on not outputting **?**, A outputs a number $1, \ldots, 6$, each with probability exactly $1/6$.
2. The probability that A outputs **?** is at most δ.

Definition 1. RP is the class of sets A for which there is a polytime machine M, and some constant c, such that

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

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

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

Exercise 2. Show that in the previous definition, we could have replaced $2/3$ with $1/n$ or with $1 - 2^{-n}$, and we would still get the same class. Please/Hint: Show it all in one go.

Definition 2. ZPP is the class of sets A for which there is a polytime machine M, which can output 0, 1 or **?**, and some constant c, such that

$$\forall x : \Pr_r[M(x,r) = \text{?}] \leq 1/2,$$

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

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

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

In other words, M is a probabilistic machine which is never wrong, but is allowed to answer 'do not know' with bounded probability.[2]

Exercise 3. (a) Show that ZPP $\subseteq$ RP $\cap$ coRP.

(b) Show that RP $\cap$ coRP $\subseteq$ ZPP.

[1] If you can't make heads or tails of that statement, don't hesitate to ask for help.

[2] This definition of ZPP is different from (but equivalent to) the one in the book, which uses the notion of expected running time.