Complexity Theory

Homework Sheet 7

(Turn in before the lecure of Monday 19 May.)

12 May, 2014

The date and location of the final exam have changed!
New information: Monday May 26 at D1.115.

Exercise 1. Show that NP $\subseteq$ BPP implies NP = RP.
Hint: Use self-reducibility.

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.

Exercise 4. Given three $n \times n$ matrices A, B, and C, consider the problem of checking whether the product of A and B equals C. That is, to check whether $C_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj}$, for all $i, j \in \{1, \ldots, n\}$. The naïve algorithm would just compute the product AB and compare this to C, but computing it entry by entry takes time $O(n^3)$, and even the fastest known algorithm for matrix multiplication takes $O(n^{2.3729})$ steps.[1] Give a randomized algorithm that solves this problem in time $O(n^2)$, with constant one-sided error.

Hint: Multiply both AB and C with a random 0/1-vector v. Show that having a wrong C_{ij} will be always be detected either by v, or by v with entry v_j negated.

[1] Finding the exact value of the exponent ω in the running time of the fastest matrix multiplication algorithm $O(n^\omega)$ is an open problem – it is only known that $2 \leq \omega < 2.3729$.