Prof. Dr. Susanne Albers
Dr. Dimitrios Letsios
Lehrstuhl Theoretische Informatik
Fakultät für Informatik
Technische Universität München

Fall Semester
October 27, 2014

Randomized Algorithms

Exercise Sheet 3

Due: November 03, 2014

Exercise 1 (10 points)
In class, we presented a randomized algorithm for verifying modulo 2 matrix multiplications. Generalize the algorithm for verifying modulo k matrix multiplications, where $k > 2$. What are the differences if we analyze the generalized algorithm along the same lines with the analysis that we saw in class?

Exercise 2 (10 points)
Consider the randomized selection algorithm presented in class for finding the k-th smallest element in an array with n distinct elements. At each step, the algorithm goes from a sub-problem of size m to a sub-problem of size $m - X$, where X is a random variable.

- Show that $E[X] \geq g(m)$, where $g(m) = \frac{m}{4}$.
- In class, we showed that the expected number of recursive calls performed by the algorithm is at most $4 \ln n$. Show that its expected running time is $O(n)$.

Exercise 3 (10 points)
Show that **ZPP** = **RP** $\cap$ co-**RP**.

Exercise 4 (10 points)
Show that **P** $\subseteq$ **RP** $\subseteq$ **NP**.

Recall that the complexity class **NP** contains the languages that can be verified by a polynomial-time algorithm. Specifically, **NP** consists of every language L which has a polynomial-time verification algorithm A such that for every string x

- $x \in L \Rightarrow \exists$ certificate y such that $A(x, y)$ accepts
- $x \notin L \Rightarrow \forall$ certificate y, $A(x, y)$ rejects