Technische Universität München (I7) **Summer term 2019**
Prof. J. Křetínský / Dr. M.Raskin **14.05.2019**

Computational Complexity – Homework 6

Discussed on 17.05.2019.

Recall that $L \in \mathbf{RP}$ if there exists a polynomial p and a polynomial-time TM $M(x;u)$ using certificates u of length $p(|x|)$ such that for every $x \in \{0,1\}^*$

$$x \in L \Rightarrow Pr[A_{M;x} \geq 3/4 \text{ and } x \notin L \Rightarrow Pr[A_{M;x}] = 0$$

Further $\mathbf{co} - \mathbf{RP} = \{\bar{L} \mid L \in \mathbf{RP}\}$ and $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{co} - \mathbf{RP}$.

Exercise 6.1

(a) Show that **RP** does not change if we replace in the definition $\geq 3/4$ by $\geq n^{-k}$ or $\geq 1 - 2^{-n^k}$ (with $k > 0$).

(b) Let $L \in \mathbf{NP}$ be decided by a poly-time TM $M(x,u)$ with certificates u of length $p(|x|)$.

Prove or disprove that $x \in L \Rightarrow \Pr[A_{M,x}] \geq n^{-k}$ needs to hold for some $k > 0$ if a polynomial number $r(|x|)$ of reruns should suffice to reduce the probability of false negatives below any given bound $c \in (0,1)$.

Remark: Use that $(1 - 1/k)^k \approx e^{-1}$ for large k.

Exercise 6.2

A cut in a connected non-oriented graph is a set of edges such that their removal makes the graph disconnected.

Consider the following problem: given a graph G and an integer k determine whether the graph G has a cut of size at most k.

Prove that this problem is in **RP**.

Exercise 6.3

Prove that verifying matrix multiplication (given matrices A, B, C check $AB = C$) is in **coRP**. Show that the verifying algorithm can be made quadratic (for a constant error probability).

Exercise 6.4

Show that $L \in \mathbf{ZPP}$ if and only if L is decided by some PTM in expected polynomial time.

Exercise 6.5

For a given $c > 0$ let a language L be in $\mathbf{PP}_{\geq c}$ if $x \in L \Leftrightarrow \Pr[A_{M,x}] \geq c$. Similarly, the class $\mathbf{PP}_{>c}$ is defined.

Show that

(a) $\mathbf{PP}_{>1/2} = \mathbf{PP}_{\geq 1/2}$.

(b) $\mathbf{PP}_{>1/2}$ is closed under complement and symmetric difference.

Remark: The symmetric difference $A\Delta B$ of two sets A, B is defined by $A\Delta B := (A \setminus B) \cup (B \setminus A)$.

(c) MajSat is $\mathbf{PP}_{>1/2}$-complete.

Remark: MajSat is the following problem: Given a Boolean expression with n variables, is it true that the majority of the 2^n truth assignments to its variables, i.e., at least $2^{n-1} + 1$ of them, satisfy it?

*(d) $\mathbf{PP}_{\geq 3/4} = \mathbf{PP}_{\geq 1/2}$.