Technische Universität München (I7) **Summer term 2019**
Prof. J. Křetínský / Dr. M.Raskin **22.05.2019**

Computational Complexity – Homework 8

Discussed on 24.05.2019.

Exercise 8.1

Give an interactive proof protocol for graph isomorphism and show that your protocol satisfies the completeness and soundness requirements.

Can you give a zero-knowledge one, too?

For this exercise, it is enough to use perfect zero knowledge: each execution of a protocol leaves a complete execution log; for a perfect zero-knowledge protocol there is a polynomial-time algorithm generatig logs with the exact same distribution.

Exercise 8.2

The class **IP** requires that for *some* prover probability of acceptance of a good word is at least 2/3 and for *all* provers probability of acceptance of a bad word is at most 1/3.

What class we get if we only require *existence* of a prover in both cases?

What class we get if we require the property of *all* provers in both cases?

What class we get if we swap the quantifiers?

Exercise 8.3

Let p be a prime number. An integer a is then a quadratic residue modulo p if there is some integer b s.t. $a \equiv b^2 \pmod{p}$.

(a) Show that $\mathrm{QR} := \{(a, p) \in \mathbb{Z}^2 \mid a$ is a quadratic residue modulo $p\}$ is in **NP**.

(b) Set $\mathrm{QNR} := \{(a, p) \in \mathbb{Z}^2 \mid a$ is not a quadratic residue modulo $p\}$.

Complete the following sketch to an interactive proof protocol for QNR and show its completeness and soundness:

i) Input: integer a and prime p.

ii) The verifier chooses $r \in \{0, 1, \dots, p-1\}$ and $b \in \{0, 1\}$ uniformly at random, keeping both secret.

i. If $b = 0$, the verifier sends $r^2 \mod p$ to the prover.

ii. If $b = 1$, the verifier sends $ar^2 \mod p$ to the prover.

iii) ...

Exercise 8.4

Is there an **IP** protocol consisting of $O(n)$ copies of some interaction, such that any constant number of rounds is not enough?

Exercise 8.5

Show that *perfect soundness* collapses the class **IP** to **NP**, where perfect soundness means soundness with error probability 0.