Technische Universität München (I7)
Prof. J. Křetínský / Dr. C.H. Broadbent

Summer term 2016
16. Juni 2016

Computational Complexity – Homework 10

Discussed on Monday 20.6.2016.

Exercise 10.1

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?

Exercise 10.2

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

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

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 $r \in \{0, 1, \ldots, p-1\}$ 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 10.3

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