Technische Universität München
Fakultät für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr
Chris Pinkau

Spring Semester 2013
Problem Set 10
July 2, 2013

Complexity Theory

Due date: July 9, 2013 **before** *class!*

Problem 1 (10 Points)

Show the following two claims:

(i) *Perfect soundness* collapses the class **IP** to $\mathcal{NP}$, where perfect soundness means soundness with error probability 0.

(ii) *Perfect completeness* does not change the power of **IP**, where perfect completeness means completeness with error probability 0.

Problem 2 (10 Points)

Show that $\mathbf{IP} \subseteq \mathbf{PSPACE}$.

Problem 3 (10 Points)

Give an interactive protocol to show that Graph Isomorphism $\in$ **IP**.

Problem 4 (10 Points)

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

(i) Show that $\text{Qr} := \{(a, p) \in \mathbb{Z}^2 : a \text{ is a quadratic residue modulo } p\}$ is in $\mathcal{NP}$.

(ii) Set $\text{Qnr} := \{(a, p) \in \mathbb{Z}^2 : a \text{ is not a quadratic residue modulo } p\}$.
Complete the following sketch of an interactive proof protocol for Qnr and show its completeness and soundness:

1.) Input: integer a and prime p.

2.) V chooses $r \in \{0, \ldots, p-1\}$ and $b \in \{0, 1\}$ uniformly at random, keeping both secret.
If $b = 0$, V sends $r^2 \mod p$ to P.
If $b = 1$, V sends $ar^2 \mod p$ to P.

3.) ...