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

Summer Term 2015
Problem Set 12
July 6, 2015

Complexity Theory

Due date: July 13, 2015 **before** *class!*

Problem 1 (10 Points)

Show the following two claims:

1. *Perfect soundness* collapses the class **IP** to $\mathcal{NP}$, where perfect soundness means soundness with error probability 0.
2. *Perfect completeness* does not change the power of **IP**, where perfect completeness means completeness with error probability 0.

Problem 2 (10 Points)

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

Problem 3 (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. $a \equiv b^2 \mod p$.

1. Show that $\text{QR} := \{(a, p) \in \mathbb{Z}^2 : a \text{ is a quadratic residue modulo } p\}$ is in $\mathcal{NP}$.
2. Let $\text{QNR} := \{(a, p) \in \mathbb{Z}^2 : a \text{ is not a quadratic residue modulo } p\}$.
   Complete the following sketch of an interactive proof protocol for QNR and show its completeness and soundness:
   i.) Input: integer a and prime p.
   ii.) 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.
   iii.) ...

Problem 4 (10 Points)

A *zero-knowledge* proof system is an interactive proof system where the prover can convince the verifier that a given statement is true, without revealing any additional information about the statement apart from whether it is true or not. (For example, the protocol for Graph Nonisomorphism is zero-knowledge.)

Zero-knowledge proofs are highly important in Cryptography: for an authentication process one wants to convince the machine that indeed the password is correct, but without ever revealing it.

Describe a zero-knowledge interactive proof system for HamCycle, which contains all graphs which have a Hamiltonian cycle.