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

Spring Semester 2013
Problem Set 11
July 9, 2013

Complexity Theory

Due date: July 16, 2013 **before** *class!*

Problem 1 (10 Points)

Let $\mathbf{IP}'$ denote the class obtained by allowing the prover to be probabilistic in the definition of **IP**, i.e. the prover's strategy can be chosen at random from some distribution of functions. Prove that $\mathbf{IP}' = \mathbf{IP}$.

Problem 2 (10 Points)

Show that $\mathcal{NP}$ and **BPP** are contained in **MA** and in **AM**.

Problem 3 (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.

Problem 4 (10 Points)

Describe the arithmetization of boolean formulae when implementing

(i) false with the value 0 and true with -1.

(ii) false with the value -1 and true with 1.

(In the lecture you have seen the arithmetization for the case that false $\mapsto$ 0 and true $\mapsto$ 1.)