Christian Schindelhauer

Freiburg, the January 12, 2014
Discussion January 15, 2014

Exercise for the lecture

Computational Complexity

Winter 2014/15

Sheet 6

EXERCISE 1:
Show that every interactive proof system that convinces the verifiers with probability of at least $2/3$ can be modified to an interactive proof system that convinces the verifier with probability $99/100$ (Hint: Chernoff inequality).

EXERCISE 2:
Present an polynomial time bounded interactive proof system, where the prover convinces the verifier that

1. a given graph has a Hamiltonian cycle,
2. he can factorize a given number,
3. he can invert a given injective honest function f, which can be computed in polynomial time, i.e. given y, find x with $f(x) = y$. An honest function f has the property: $|f(x)| \geq |x|^c$, for some constant c and all $x \in \Sigma^*$.
4. Does this result generalize to non-honest invertible polynomial time computable functions?

EXERCISE 3:
Prove that an interactive proof system exists for the finding the worst case input (regarding runtime) of a given polynomial time bounded deterministic Turing machine an input length n, i.e. given DTM M and n, find x such that $\text{time}_M(x)$ is maximal for $x \in \Sigma^n$.
(Hint: Characterize the complexity of this problem).