Computational Complexity

Homework Sheet 6

Hand in before March 21, 23:59

Preferably by email to `J.M.Czajkowski@cwi.nl`

Exercise 1 (4pt)**.** Consider the following polynomial-time reduction f from 3SAT to 3SAT. Let φ be a 3CNF formula with clauses $c_1, \dots, c_m$ and containing the variables $x_1, \dots, x_n$. Then $f(\varphi)$ is defined as the following 3CNF formula:

$$f(\varphi) = \varphi \wedge \left(\bigwedge_{j=1}^{m} y_j \right) \wedge \left(\bigwedge_{j=1}^{m} \bigwedge_{j'=1}^{m} (y_j \vee y_{j'}) \right),$$

where each of the variables y_j is a fresh variable that does not occur in φ. (Note: here we define a 3CNF formula as a CNF formula where each clause contains **at most** 3 literals. Note also: φ can be encoded by a string of size $O(m \log n)$.)

Let F be the following set of 3CNF formulas:

$$F = \{ \ f(\varphi) \mid \varphi \text{ is a 3CNF formula } \},$$

and let FUNNY-3SAT be the following decision problem:

$$\text{FUNNY-3SAT} = F \cap \text{3SAT}.$$

(a) Show that FUNNY-3SAT is solvable in time $2^{O(\sqrt{m})}$, where m denotes the number of clauses in the input formula.

(b) Show that FUNNY-3SAT is not solvable in time $2^{o(\sqrt{m})}$, where m denotes the number of clauses in the input formula, assuming that the ETH is true.

Exercise 2 (1pt)**.** Give an example of a decision problem that is not solvable in polynomial time (assuming P $\neq$ NP), yet that is solvable in time $2^{o(|x|)}$, where $|x|$ denotes the input size.

Exercise 3 (2pt)**.** Show that in interactive proof systems we gain nothing by allowing the prover to make use of randomness. That is, show that if we have a probabilistic prover P that convinces a verifier V to accept with probability p, where the probability is taken over the random coins of both P and V, then we have a deterministic prover P that convinces V to accept with probability $\geq p$, where the probability is now taken only over the random bits of V.

Exercise 4 (3pt)**.** Show that IP $\subseteq$ PSPACE.