Complexity Theory

Homework Sheet 1

Turn in before the lecture of Tuesday 8 Sep.

1 September 2015

Exercise 1. Which relations $f \in \bullet(g)$ hold for $\bullet \in \{\mathcal{O}, o, \Omega, \omega, \Theta\}$ for the following pairs of functions? Prove which relations hold and which relations do not hold.

1. $f(n) = n^{\log n}$ $\quad g(n) = 2^{(\log n)^3}$.
2. $f(n) = n!$ $\quad g(n) = 2^n$.
3. $f(n) = \log n$ $\quad g(n) = n$.
4. $f(n) = n^5$ $\quad g(n) = 100n^5$.

Exercise 2. By the fundamental theorem of arithmetic, any natural number x can be uniquely written as a product

$$x = p_1 \cdot p_2 \cdots p_k$$

with $p_1, \dots, p_k$ prime numbers such that $p_i \leq p_j$ if $i < j$. This yields a function

$$f : \mathbb{N} \to \{0,1\}^* : x \mapsto \langle p_1, p_2, \dots, p_k \rangle,$$

which maps a natural number x to a binary encoding of the prime factorization of x.

(a) Using the fact that there is a polynomial-time algorithm for testing primality,[1] show that deciding whether $z = f(x)$, when given x and z as input, can be done in polynomial time.

(b) Show that the set

$$\text{FACTORIZATION} = \{\langle x, i \rangle \mid \text{the } i\text{-th bit of } f(x) \text{ is } 1\}$$

is in NP.

[1] Which has been an open problem for a very long time, but solved in 2002 by Agrawal, Kayal and Saxena, see `http://en.wikipedia.org/wiki/AKS_primality_test`.

(c) Show: if FACTORIZATION is NP-complete, then NP = coNP.

(d) Define

$$\text{COMPOSITE} = \{\langle x \rangle \mid x \in \mathbb{N} \text{ has at least two prime factors}\}.$$

Show: COMPOSITE is NP-complete if and only if P = NP.

Exercise 3. Show that NP $\subseteq$ EXP.

Hint. Answers will be graded with two criteria: they should be correct and intelligent, but also concise and to the point.