Complexity Theory

Homework Sheet 1

(Turn in before the lecture of Monday 7 Apr.)

31 March, 2014

Exercise 1. Prove or disprove the following: If $f(n) = O(n)$ and $g(n) = \Theta(n)$, then

1. $f(n) + g(n) = O(n)$.
2. $f(n) - g(n) = O(1)$.
3. $f(n)g(n) = O(n^2)$.
4. $\frac{f(n)}{g(n)} = O(1)$.

Exercise 2. By the fundamental theorem of arithmetic, any given natural number x can be uniquely expressed as the product of prime numbers $x = p_1 p_2 \dots p_k$, where p_i is any prime, not necessarily the i-th prime, also allowing for repeated primes. Thus there is a well-defined one-to-one function $f(x) = \langle p_1, p_2, \dots, p_k \rangle \in \{0,1\}^*$, $p_i \leq p_j$ if $i < j$, which gives (a binary encoding of) the 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

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

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`.

Exercise 3. A given function $f : \{0,1\}^* \to \{0,1\}^*$ is called *honest* if there is some real constant $c \geq 0$ such that $|f(x)|^c > |x|$ for all x.

(a) Show that if P = NP then every honest, polynomial-time computable function has its inverse also polynomial-time computable.

(b) Prove the converse of the previous statement, i.e., show that if every honest, polynomial-time computable function has a polynomial-time computable inverse, then P = NP. Hint: Which function would you have to invert to find the witness you are searching for?

Together, the result is sometimes known as the cryptographic theorem:

Theorem 1. P = NP *if and only if every honest, polynomial-time computable function has a polynomial-time computable inverse.*

Exercise 4. 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.