KTH Computer Science
and Communication

Homework V, Complexity Theory Fall 2011

Due on October 7 at 14.15, i.e. at the beginning of the lecture. The general rules on homework solutions available at the course home-page apply. In particular, discussions of ideas in groups of up to at most two people are allowed but solutions should be written down individually.

Some of the problems below are “classical” and hence their solutions is probably posted on the Internet. It is not allowed to use such solutions in any way. The order of the problems is “random” and hence do not expect that the lowest numbered problems are the easiest.

Any corrections or clarifications on this problem set will be posted under “homework” on the course home-page http://www.csc.kth.se/utbildning/kth/kurser/DD2446/kplx11/uppgifter.

1 (20p) Nondeterminism can in many circumstances be thought of as an existential quantifier. Some languages A can be characterized by a language of pairs $B \in$ P and a constant k such that

$$x \in A \Leftrightarrow \exists y(|y| \leq |x|^k) \wedge (x, y) \in B. \tag{1}$$

1a (5p) Prove that such a characterization is possible iff $A \in$ NP.

If we instead have k alternating quantifiers (i.e. every other is $\exists$ and every other is $\forall$), each quantifying over a polynomial number of bits we get a class called Σ_k (thus in particular Σ_1 is just a different name for NP). If we have k quantifies with the first being a $\forall$ the class is called Π_k. Another name for Π_1 is co-NP.

1b (3p) Show that this is a well deserved name in that if we have $A \in$ NP and B is in the complement of A (i.e. $x \in B$ iff $x \notin A$) then $B \in$ co-NP.

The union of Σ_k for all natural numbers k is called the *polynomial time hierarchy* often abbreviated as PH.

1c (1p) Show that $PH = \cup_{k=1}^{\infty} \Pi_k$ and that PH is closed under complementatin and thus the definition is symmetric.

1d (5p) Show that for any k, $\Sigma_k \subseteq PSPACE$. Conclude that TQBF belongs to PSPACE.

1e (3p) Show that if for some k we have $\Sigma_{k+1} = \Sigma_k$ then for any $m \geq k$ we can conclude that $\Sigma_m = \Sigma_k$.

1f (3p) Let us consider the problem of unique satisfiability, i.e. the set of Boolean formulas with exactly one satisfying assignment. Can you place this problem in any of the above defined classes?

2 (16p) Show by an explicit program that multiplication belongs to L. You need not design a Turing machine but can describe a high level algorithm but you should keep careful count of the working space it uses.

2a (10p) Show that this is true when bits are output in the natural order with least significant bit first.

2b (5p) Show that this is true when bits are output in the natural order with most significant bit first.

2c (1p) Is the above fact true for any function in L? In other words is it always true that if outputting the answer in one order is in L so is outputting the answer in the reverse order?