Complexity Theory

Homework Sheet 2

Hand in before the lecture of Tuesday 21 Feb.

Preferably by email to bannink@cwi.nl

14 February 2017

Exercise 1. A coloring of a graph with c colors is an assignment of a number from $1, 2, \ldots, c$ to each vertex such that no adjacent vertices get the same number.

(a) Show that the following problem is in **P**.

Two-coloring: 2COL $= \{G : \text{graph } G \text{ has a coloring with two colors}\}$

(b) Contrary to the two-color version, the three-coloring problem is known to be **NP**-complete. (You don't have to prove this.)

Three-coloring: 3COL $= \{G : \text{graph } G \text{ has a coloring with three colors}\}$

Consider the following scenario: A mysterious (but trustworthy) wizard gives you a graph, and promises you that it is colorable with three colors.

Assuming $\mathbf{P} \neq \mathbf{NP}$, does there exist an efficient algorithm that finds a three-coloring of a graph, if you already know that such a coloring exists?

(c) Now consider a similar scenario: The trustworthy wizard gives you a graph, and promises you that it is colorable with three colors. Furthermore, it now tells you the color of three vertices, i.e. it gives three different vertices and three colors that belong to them. You are promised that there is a coloring where those three vertices have these colors.

Again assuming $\mathbf{P} \neq \mathbf{NP}$, does there exist an efficient algorithm that finds a three-coloring of a graph, given the information from the wizard?

Exercise 2. Let A be an **NP**-complete language. Let p be a polynomial and M_A a polytime TM such that

$$x \in A \iff \exists\, u \in \{0,1\}^{p(|x|)} : M_A(x,u) = 1.$$

(a) Define the set $B = \{\langle x, z\rangle \mid \exists\, z' \text{ such that } |zz'| \leq p(|x|) \text{ and } M_A(x, zz') = 1\}$. Show that B is in **NP**.

(b) Assume that we have access to A as an oracle. Basically this means that we have a subroutine which, given a string y, tells in a single step whether $y \in A$. (See Def. 3.4 in the book.) Construct a polytime TM M_{search} that finds a certificate as follows: On input $x \in \{0,1\}^*$, if $x \in A$ then M_{search} outputs a string u such that $M_A(x,u) = 1$; and if $x \notin A$ then M_{search} outputs 0. Use **(a)**.

Exercise 3. Let A be a language. When a TM M has access to the oracle A, we write M^A. We say A is *auto-reducible* if there is a polytime TM M such that

$$x \in A \iff M^A(x) = 1$$

with the special requirement that on input x the TM M is not allowed to query the oracle A for x.

Suppose A is **NP**-complete. Show that A is auto-reducible. Use **Exercise 2**.

Exercise 4.

(a) Show that there is no maximum set for $\leq_m^p$ reductions, i.e., that for any set A there is a set $B \not\leq_m^p A$ (Hint: is there an enumeration of all possible $\leq_m^p$-reductions?).

(b) Show that there is no maximal set, i.e., that for any set A there is a set B such that $A \leq_m^p B$ and $B \not\leq_m^p A$.