ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Homework I, Topics in Theoretical Computer Science 2016

Due on Tuesday March 22 at 12:00 (send an email to ola.svensson@epfl.ch). Solutions to many homework problems, including problems on this set, are available on the Internet, either in exactly the same formulation or with some minor perturbation. It is *not acceptable* to copy such solutions. It is hard to make strict rules on what information from the Internet you may use and hence whenever in doubt contact Ola Svensson. You are, however, allowed to discuss problems in groups with up to three students.

1 *(15 pts, Exercise* 2.14 *from the textbook)* Cook used a somewhat different notion of reduction (than Karp reductions): A language L is *polynomial-time Cook-reducible* to a language L' if there is a polynomial time TM M that given an *oracle* for deciding L' can decide L. Show that 3SAT is Cook-reducible to TAUTOLOGY.

(Recall that TAUTOLOGY is the language of Boolean formulas that are satisfied by all assignments and 3SAT is the language of 3CNF Boolean formulas that have a satisfying assignment.)

2 *(30 pts, Exercise* 2.19 *from the textbook)* Let QUADEQ be the language of all satisfiable sets of quadratic equations over 0/1 variables (a quadratic equation over $u_1, \ldots, u_n$ has the form $\sum_{i,j\in[n]} a_{i,j}u_iu_j = b$) where addition is modulo 2. Show that QUADEQ is **NP**-complete.

3 *(25 pts, Exercise* 6.8 *from the textbook)* A language $L \subseteq \{0,1\}^*$ is sparse if there is a polynomial p such that $|L \cap \{0,1\}^n| \leq p(n)$ for every $n \in \mathbb{N}$. Show that every sparse language is in $\mathbf{P}_{/\mathbf{poly}}$.

4 *(30 pts, Exercise* 3.7 *from the textbook)* Show that there is an oracle A and a language $L \in \mathbf{NP}^A$ such that L is not polynomial time reducible to 3SAT even when the machine computing the reduction is allowed access to A.

Hint: use a similar oracle as used for proving $P^O \neq NP^O$.