Homework I, Computational Complexity 2018

Due on Friday October 26 at 17:00 (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 *(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.

2 *(35 pts, from course by Luca Trevisan)* Prove that $\mathbf{NP} \neq \mathbf{E}$.

Recall that $\mathbf{E} := \mathbf{DTIME}(2^{O(n)})$ is the class of languages decidable by deterministic TM in time $2^{O(n)}$. Also recall that a language A has a many-to-one polynomial time reduction (aka Karp reduction) to a language B, written $\leq_p$, if there is a polynmomial time computable function $f(\cdot)$ such that for every instance $x \in \{0,1\}^*$ we have $x \in A \Leftrightarrow f(x) \in B$. In your proof show that **NP** is *closed* under polynomial many-to-one reductions, that is $A \leq_p B$ and $B \in \mathbf{NP}$ implies $A \in \mathbf{NP}$, and that if **E** were closed under many-to-one reductions, we would have a contradiction to the time hierarchy theorem.

3 *(35 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 (many-to-one) reducible to 3SAT even when the machine computing the reduction is allowed access to A.

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