EO 224: Computational complexity theory - Assignment 1

Due date: September 12, 2014

General instructions:

- Write your solutions by furnishing all relevant details (you may assume the results already covered in the class).
- You are strongly urged to solve the problems by yourself.
- If you discuss with someone else or refer to any material (other than the class notes) then please put a reference in your answer script stating clearly whom or what you have consulted with and how it has benifited you. We would appreciate your honesty.
- If you need any clarification, please contact the instructor.

Total: 50 points

1. (**3 points**) [Excercise-2.16 from Arora-Barak's book] Suppose $L_1, L_2 \in \mathsf{NP}$. Then is $L_1 \cup L_2$ in NP? What about $L_1 \cap L_2$?

2. (**4 points**) [Excercise-2.29 from Arora-Barak's book] Suppose $L_1, L_2 \in \mathsf{NP} \cap \mathsf{coNP}$. Then show that $L_1 \oplus L_2$ is in $\mathsf{NP} \cap \mathsf{coNP}$, where $L_1 \oplus L_2 = \{x : x \text{ is in exactly one of } L_1, L_2\}$.

3. (**4 points**) [Excercise-2.19 from Arora-Barak's book] 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 $\sum_{i,j \in [n]} a_{i,j} u_i u_j = b$) where addition is modulo 2. Show that QUADEQ is NP-complete.

4. (**7 points**) [Excercise-2.16 from Arora-Barak's book] In the MAXCUT problem, we are given an undirected graph G and an integer k and have to decide whether there is a subset of vertices S such that there are at least k edges that have one endpoint in S and one endpoint in $\bar{S}$. Prove that this problem is NP-complete.

5. (**6 points**) [Excercise-2.34 from Arora-Barak's book] Suppose that you are given a graph G and a number k and are told that either (i) the smallest vertex cover of G is of size k or (ii) it is of size at least $3k$. Show a polynomial-time algorithm that can distinguish between these two cases. Can you do it with a smaller constant than 3? Since VERTEX COVER problem is NP-hard, why does this algorithm not show that $\mathsf{P} = \mathsf{NP}$?

6. (**6 points**) [Excercise-3.1 from Arora-Barak's book] Show that the following language is undecidable:

$$\{\underline{M} : M \text{is a machine that runs in } O(n^2) \text{ time}\}.$$

Here $\underline{M}$ is the Turing machine M's representation as a binary string.

7. (**8 points**) [Excercise-2.3 from Arora-Barak's book] Let LINEQ denote the set of satisfiable rational linear equations. That is, LINEQ consists of the set of all pairs $< A, \mathbf{b} >$ where A is an $m \times n$ rational matrix and $\mathbf{b}$ is an m dimensional rational vector, such that $A\mathbf{x} = \mathbf{b}$ for some n-dimensional vector $\mathbf{x}$. Prove that LINEQ is in NP (the key is to prove that if there exists such a vector x, then there exists an $\mathbf{x}$ whose coefficients can be represented using a number of bits that is polynomial in the representation of $A, \mathbf{b}$). (Note that LINEQ is actually in P: Can you show this?)

8. (**8 points**) [Excercise-2.5 from Arora-Barak's book] Let PRIMES $= \{n : n \text{ is a prime }\}$. Show that PRIMES $\in \mathsf{NP}$. You can use the following fact: A number n is prime iff for every prime factor q of $n-1$, there exists a number $a \in \{2, \ldots, n-1\}$ satisfying $a^{n-1} = 1 \mod n$ but $a^{(n-1)/q} \neq 1 \mod n$.

9. (**4 points**) [Excercise-3.6 (a) from Arora-Barak's book] Prove that the function $H(n)$ defined in the proof of Ladner's theorem is computable in time polynomial in n.