ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Exercise Set VII, Computational Complexity 2018

These exercises are for your own benefit. Feel free to collaborate and share your answers with other students. Solve as many problems as you can and ask for help if you get stuck for too long. Problems marked * are more difficult but also more fun :).

These problems are taken from various sources at EPFL and on the Internet, too numerous to cite individually.

1 Consider the problem MAX k-FUNCTION SAT:

- Given n Boolean variables $x_1, \ldots, x_n$ and m functions $f_1, \ldots, f_m$, each of which is a function of k (a constant) of the Boolean variables,
- Find a truth assignment to $x_1, \ldots, x_n$ that maximizes the number of functions satisfied.

1a Show that for a fixed k there is a constant-factor approximation algorithm for the MAX k-FUNCTION SAT. (The approximation guarantee will depend on k).

1b Show that, for every constant s, there is a k such that it is NP-hard to approximate MAX k-FUNCTION SAT within a factor s.

2 *(Exercise 11.6 in textbook)* Prove that $\mathbf{PCP}(0, \log n) = \mathbf{P}$. Prove that $\mathbf{PCP}(0, \mathrm{poly}(n)) = \mathbf{NP}$.

3 *(Exercise 9.3 in textbook)* Prove that in one-time pad encryption, no eavesdropper can guess any bit of the plaintext with probability better than $1/2$. That is, prove that for every function A, if (E, D) denotes the one-time pad encryption then

$$\Pr_{k \in \{0,1\}^n, x \in \{0,1\}^n} [A(\mathsf{E}_k(x)) = (i, b) \text{ s.t } x_i = b] \leq 1/2 \,.$$

4 *(Exercise 9.5 in textbook)* Show that if $\mathbf{P} = \mathbf{NP}$, then one-way functions do not exist.

5 Show that there is no polynomial-time (in the output length) computable pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ that has exponential stretch $\ell(n) = 2^n$ and is secure as defined in Lecture 14.