ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Homework II, Computational Complexity 2018

Due on Friday November 16 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 *(33 pts, Exercise from Luca Trevisan's course)* Suppose that there is a deterministic polynomial-time algorithm A that, on input (the description of) a circuit C, produces a number $A(C)$ such that

$$\Pr_x[C(x) = 1] - \frac{2}{5} \leq A(C) \leq \Pr_x[C(x) = 1] + \frac{2}{5}.$$

1a *(33 pts)* Prove that it follows that $\mathbf{P} = \mathbf{BPP}$.

1b *(optional problem and no points but fun to think about)* Prove that there exists a deterministic algorithm A' that, on input a circuit C and a parameter ϵ, runs in time polynomial in the size of C and in $2/\epsilon$ and produces a value $A'(C, \epsilon)$ such that

$$\Pr_x[C(x) = 1] - \epsilon \leq A'(C, \epsilon) \leq \Pr_x[C(x) = 1] + \epsilon.$$

Hint: The threshold function $f_t : \{0,1\}^n \to \{0,1\}$, where $t \in \{1, \cdots, n\}$, defined by

$$f(x) = 1 \Leftrightarrow \sum_i x_i \geq t$$

has a polynomial-sized (in n) circuit.

2 *(33 pts, Exercise 8.8(a) from textbook)* In this exercise we explore the trick used to prove $\mathbf{IP} \subseteq \mathbf{PSPACE}$. Let φ be QBF formula satisfying the following property:

If $x_1, \ldots, x_n$ are φ's variables sorted according to their order of (first) appearance, then for every variable x_i there is at most a single universal quantifier ($\forall$) involving x_j (for $j > i$) appearing before the last occurrence of x_i in φ.

Show that in this case, when we run the sumcheck protocol discussed in lecture (with the modification that we use the check $s(0) \cdot s(1) = K$ for product operations), the prover only needs to send polynomials of polynomial degree.

3 *(34 pts, slightly adapted Exercise* 8.5 *from the textbook)* In class we saw a (slightly) simplified version of Goldwasser-Sipser's **AM**[2] protocol for the set lower bound problem. However, the protocol did not have perfect completeness.

In this exercise, your goal is to give a **AM**[$O(1)$] protocol for the set lower bound problem with *perfect completeness.*

You may assume[1] the following: a random hash-function $h : X \to Y$ can efficiently be communicated. Note that, for every $y \in Y$, such a distribution of hash functions satisfies

$$\Pr_h[\exists x \in X : h(x) = y] \geq \frac{1}{2} \qquad \text{if } |X| \geq |Y|.$$

Hint: First note that in the current set lower bound protocol we can have the prover choose the hash function. Consider the easier case of constructing a protocol to distinguish between the case $|S| \geq K$ and $|S| \leq \frac{1}{c}K$ where $c \geq 2$ can even be a function of K (this can be achieved by taking the cartesian product of S a couple of times as done in the lecture). It c is large enough, we can allow the prover to use several hash functions $h_1, \ldots, h_i$, and you can prove that if i is large enough then we will have $\cup_i h_i(S) = Y$ in the case when $|S| \geq K$.

[1] For intuition of this assumption, please see the discussion about efficient pairwise independent hash functions in the textbook (Theorem 8.15 and Claim 8.16.1).