ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Homework II, Topics in Theoretical Computer Science 2016

Due on Monday April 11 at 9:00 (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 *(25 pts)* In these two subproblems, we shall study circuits of bounded depth. The *depth* of a circuit is the length of the longest directed path from an input to the output gate.

1a *(10 pts)* Show that any language L can be decided by a circuit family $\{C_n\}_{n\in\mathbb{N}}$ where C_n has constant depth but is allowed to have unbounded fan-in and exponential size. More specifically, C_n can be constructed using three layers: the first layer consists of (potential) NOT gates of the input bits, the second of AND gates (of unbounded fan-in), and the last layer is a single OR gate (of unbounded fan-in).

1b *(15 pts)* Let PARITY $= \{x \in \{0,1\}^* : \oplus_{i\in|x|} x_i = 1 \pmod 2\}$ be the language consisting of strings of odd parity. Show that PARITY cannot be decided by a circuit family $\{C_n\}_{n\in\mathbb{N}}$ where C_n has depth $o(\log n)$ and the maximum fan-in of any gate is two.

(As a side remark, we note the following much stronger result by Håstad: PARITY cannot be decided by circuits that have depth $o(\log n/\log\log n)$, unbounded fan-in, and are of polynomial size.)

2 *(27 pts, Exercise* 5.10 *from the textbook)* Suppose A is some language such that $\mathbf{P}^A = \mathbf{NP}^A$. Then show that $\mathbf{PH}^A \subseteq \mathbf{P}^A$.

Hint: First study the proof of "$\mathbf{P} = \mathbf{NP}$ *implies* $\mathbf{PH} = \mathbf{P}$*" (Theorem* 5.4 *in the textbook). Then show that this proof relativizes, i.e., holds with respect to any oracle.*

3 *(48 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

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

3a *(22 pts)* Prove that it follows that $\mathbf{P} = \mathbf{BPP}$.

3b *(26 pts)* 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 $1/\epsilon$ 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.