ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Homework III, Computational Complexity 2018

Due on Friday December 7 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 *(35 pts)* Håstad proved that there is a particularly simple PCP verifier for SAT. For every $\epsilon > 0$ it uses the $O(\log n)$ random bits to compute three positions in the proof, say i, j, and k, and a bit b, and accepts iff

$$\pi(i) + \pi(j) + \pi(k) = b \pmod 2.$$

Here $\pi(i)$ is the i'th bit in the proof π. The verifier has completeness $1-\epsilon$ and soundness $1/2+\epsilon$. In other words,

- If φ is a satisfiable SAT instance then there is a proof π that makes the verifier accept with probability at least $1-\epsilon$.
- If φ is a not satisfiable SAT instance then for any proof the verifier accepts with probability at most $1/2+\epsilon$.

Your task in this problem is to use the above described verifier to prove the following statements:

1a *(15 pts)* For any $\epsilon > 0$, it is NP-hard to approximate MAX-3LIN within a factor of $1/2+\epsilon$.

MAX-3LIN is the problem where the input is a system of linear equations (modulo 2); each equation contains at most 3 variables; and we wish to find an assignment to the variables that satisfies the maximum number of equations.

1b *(20 pts)* For any $\epsilon > 0$, it is NP-hard to approximate MAX-3SAT within a factor $7/8+\epsilon$.

(*Hint: Do a reduction directly from MAX-3LIN.*)

1c *(optional problem and no points but fun to think about)* It is NP-hard to approximate the Vertex Cover problem within a factor of c, for some c that you wish to maximize.

Specifically, show that c can be chosen to be $7/6-\epsilon$ for any $\epsilon > 0$.

Recall that in the Vertex Cover problem we are given an undirected graph $G = (V, E)$ and we wish to find a subset $V' \subseteq V$ of minimum cardinality such that each edge is covered. An edge $\{u, v\} \in E$ is covered if $u \in V'$ or $v \in V'$.

2 *(30 pts, Problem 11.8 in the book of Arora & Barak)* Show that if SAT $\in \mathbf{PCP}(r(n), 1)$ for some $r(n) = o(\log n)$ then $\mathbf{P} = \mathbf{NP}$. This shows that the PCP theorem is probably optimal up to constants.

A proof for the case when the verifier reads at most $\log \log n$ random bits is rewarded with 20pts and is a good starting point.

(*Hint: What is the length of a proof for a* $\boldsymbol{PCP}(r(n), 1)$ *verifier? Recall that we assume that the proof only contains bits that are read with non-zero probability.*)

3 *(35 pts, Problem 9.2 in the book of Arora & Barak)* Let (E, D) be an encryption scheme satisfying $\mathsf{D}_k(\mathsf{E}_k(x)) = x$ for every key k and message x. If the message-size is m and the key-size is $n < m$, then prove that there exist two messages $x, x' \in \{0,1\}^m$ such that $\mathsf{E}_{U_n}(x)$ is not the same distribution as $\mathsf{E}_{U_n}(x')$.