ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Exercise Set VI, 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 [Easy direction of PCP Theorem] Prove that $\mathbf{PCP}(\log(n), 1) \subseteq \mathbf{NP}$.

2 [Taken from David Steurer's course] We motivated the use of error correcting codes for the proof of the PCP theorem by the claim that query efficient verifiers cannot reliably distinguish between proofs that are close in Hamming distance. In this exercise, you will show this claim.

Let V be a randomized algorithm (verifier) that given oracle access to a string π (the proof) makes at most q queries to it.

Let $x, \pi \in \{0,1\}^*$ be arbitrary bit strings. Let π' be a bit string obtained by flipping every entry of π with probability ϵ. Show that

$$\Pr[V^{\pi}(x) = 1] \geq \mathbb{E}_{\pi'} \Pr[V^{\pi'}(x) = 1] - q \cdot \varepsilon.$$

3 Prove that any language L that has a PCP-verifier using r coins and q adaptive queries also has a standard (i.e., nonadaptive) verifier using r coins and 2^q queries.

An adaptive verifier only decides where to make its j:th query to the proof after seeing the outcome of the first $j-1$ queries. In contrast a nonadaptive verifier (as seen in class) decides where to make all queries to the proof before seeing any results of the queries.

4 Let p be a prime number and consider the finite field $\mathbb{F}_p$ consisting of p elements. Let $f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i$ be a linear function over this field with coefficients $a_1, \ldots, a_n \in \mathbb{F}_p$. Prove the following statement:

If at least one coefficient is nonzero, then $\Pr_{x \in \mathbb{F}_p}[f(x) = b] = 1/p$ for every $b \in \mathbb{F}_p$.

5 Given a $\mathbf{PCP}(\log(n), 1)$ verifier V for SAT, and an input φ, one can wonder which proof has a maximal probability of being accepted by V along with input φ. Show that this problem is $\mathbf{NP}$-hard to approximate within a factor $1/2$.

6 *(*)* Show that

$$\text{GAP 3-SAT is } \mathbf{NP}\text{-complete} \iff \mathbf{NP} = \mathbf{PCP}(\log n, 1)\,.$$

GAP 3-SAT instances are 3-SAT instances with the constraint that either they are satisfiable or no more than $1-\epsilon$ of the clauses can be satisfied simultaneously. Deciding whether a GAP 3-SAT instance is satisfiable is in some sense easier than deciding if a general 3-SAT instance is satisfiable due to the ϵ-gap separating the satisfiable instances from the non-satisfiable ones.