ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Exercise Set VIII, 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 random variables $Z_1, \ldots, Z_n \in \{0,1\}$. Let $Z = \sum_{i=1}^n Z_i$. Show that $\mathrm{Var}[Z] = \sum_{i=1}^n \mathrm{Var}[Z_i]$ if $Z_1, \ldots, Z_n$ are pairwise independent. Also give an example of random variables that are not pairwise independent and satisfy $\mathrm{Var}[Z] \neq \sum_{i=1}^n \mathrm{Var}[Z_i]$.

2 Let $m = 2^k - 1$ and recall the definition of the random vectors $r^1, \ldots, r^m \in \{0,1\}^n$ seen in Lecture 15:

- Choose k strings $s^1 \ldots, s^k$ independently at random from $\{0,1\}^n$.
- For every $j \in [m]$, we associate a unique nonempty set $T_j \subseteq [k]$ with j in some canonical fashion and define $r^j = \sum_{t \in T_j} s^t \mod 2$. That is, r^j is the bitwise XOR of all the strings among $s^1, \ldots, s^k$ that belong to the jth set.

Show that the vectors $r^1, \ldots, r^m$ are pairwise independent, i.e., if you only consider two vectors r^i and r^j with $i \neq j$ then they look as two independent random vectors.

3 Show that no classic (deterministic or probabilistic) strategy used by Alice and Bob can cause them to win the Parity Game (considered in Lecture 16) with probability strictly more than 3/4.

4 What state do you get if you start with the basic state $|0^m\rangle$ and then apply the Hadamard gate to very qubit?

5 Why can't OR and AND simply be implemented as quantum operations?

6 Show that OR and AND can be implemented as quantum operations if we store the result in a 3rd qubit (that is initialized to $|0\rangle$).

The NOT gate is easy to implement and thus we can simulate any classic circuit (and hence any TM) with elementary quantum operations. This gives that $\mathbf{BPP} \subseteq \mathbf{BQP}$.

7 How can you make a classic TM reversible? Why does an efficient reversible TM for computing $f(x)$ given x *not* imply that we can efficiently find x given $f(x)$? (In particular, why doesn't it imply that we can invert one-way functions?)