ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Exercise Set V, 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 Let $\mathbf{IP}'$ denote the class that has the same definition as $\mathbf{IP}$ except that perfect completeness is enforced. Show that $\mathbf{IP} = \mathbf{IP}'$.

2 In this exercise, we are going to study an interactive proof protocol for the language

$$\text{3COL} = \{G : G \text{ is a 3-colorable graph}\}.$$

Our interactive proof is very similar to that seen in Lecture 10. Let $G = (V, E)$ be a graph and suppose the prover has a 3-coloring $\gamma : V \to \{R, Y, B\}$. The protocol then proceeds as follows:

P: Prover selects a uniformly random permutation π of $\{R, Y, B\}$, commits to $\pi(\gamma(v))$ for all $v \in V$, and sends those commitments to the verifier (using crypto).

V: Verifier selects $\{u, v\} \in E$ uniformly at random and sends edge to prover.

P: Prover reveals the commitments $a = \pi(\gamma(u))$ and $b = \pi(\gamma(v))$.

V: The verifier accepts iff $a, b \in \{R, Y, B\}$ and $a \neq b$.

The above protocol is the same as that seen in class *except* that the prover in the last step does not check that $\{u, v\}$, sent by the verifier, is indeed an edge. This omission does not affect completeness or soundness. However, it does ruin the computational zero-knowledge guarantee of the protocol (assuming $\mathbf{RP} \neq \mathbf{NP}$).

To see this, consider a graph G with a *unique* 3-coloring up to permutations of the color labels. For this graph, use the protocol a polynomial number of times with a malicious verifier to find a 3-coloring of G.

3 *(*, Exercise 8.6 from textbook)* Prove that for every $\mathbf{AM}[2]$ protocol for a language L, if the prover and the verifier repeat the protocol k times *in parallel* (i.e., sends all messages together in one round) and the verifier accepts only if all k copies accept, then the probability that the verifier accepts $x \notin L$ is at most $(1/3)^k$. Note that you *cannot* assume (without any arguments) that the prover answers the queries independently.

4 *(*)* In the previous problem we have shown that parallel repetition decreases the soundness as well as sequential repetition in **AM**. In other interactive proof models, the situation is more complex. In this problem, we are going to study one such example:

> There are two provers P and P', and a verifier V. The provers have unbounded power and can communicate before the interaction with V starts (but not after). The verifier is a restricted to be a probabilistic polynomial-time TM as usual.

The protocol that we study (by Uri Feige) is as follows:

V: Verifier chooses two independent random bits $b, b' \in \{0,1\}$, and sends b to P and b' to P'.

P and P': P and P' give answers q and q' in $\{1,2\} \times \{0,1\}$, respectively.

V: Verifier accepts if both answers $q = q' = (1, b)$ or if both answers $q = q' = (2, b')$.

It is quite easy to see that there is no strategy of P and P' that makes V accept with probability more than $1/2$. This is since P is unaware of the value of b' and P' is unaware of the value b. We now wish to use parallel repetition to decrease this soundness of $1/2$. So consider when running the above protocol two times in parallel:

V: Verifier chooses four independent random bits $b_1, b_2, b'_1, b'_2 \in \{0,1\}$, and sends b_1, b_2 to P and b'_1, b'_2 to P'.

P and P': P and P' give answers q_1, q_2 and q'_1, q'_2, respectively, from the set $\{1,2\} \times \{0,1\}$.

V: Verifier accepts if each of the q_i and q'_i satisfy the original criteria, i.e., if

$$q_1 = q'_1 \in \{(1, b_1), (2, b'_1)\} \qquad \textbf{and} \qquad q_2 = q'_2 \in \{(1, b_2), (2, b'_2)\}\,.$$

We would perhaps expect that the soundness of the above protocol is at most $1/4$ (which would be the case with sequential repetition). However, it is not! Indeed, give a strategy of P and P' that makes V accept with probability $1/2$.

We remark that it is however true that if we do ℓ parallel repetitions the soundness will go down exponentially fast in ℓ but not as fast as sequential repetition. This was first proved by Raz (in a general 2-prover 1-round of questions setting) and is called the Parallel Repetition Theorem.