QUANTUM CRYPTOGRAPHY
Master of Logic, University of Amsterdam, 2017
TEACHERS: Jan Czajkowski, Yfke Dulek, and Christian Schaffner

Practice problem set 9

You do not have to hand in these exercises, they are for practicing only.

Problem 1: Fun with PR boxes (Homework Problems 1-5 of Chapter 9)

In this homework, we will investigate side stepping the impossibility proof in some fun other ways! Similar to the setting of the wizard who gave Alice and Bob special forms of randomness, we'll imagine that they are given some very special resources that they can use during their protocol. We start our investigations with Alice and Bob having access to a very special box - also known as a PR-box or non-local box - used in the study of quantum non-locality.

Imagine thus that Alice and Bob get access to a special box. This box takes two inputs: one input bit x from Alice, and one input bit y from Bob. Once any input is given, the box generates a random bit r with $P_R(0) = P_R(1) = 1/2$. The box then outputs $b = r + x \cdot y \mod 2$ to Bob and $a = r$ to Alice.

(a) Alice and Bob now want to find a protocol to solve the following task: Alice holds a database of two bits x_0 and x_1 and Bob holds some bit y. Bob would like to retrieve the bit x_y from Alice's database. To achieve this, they can use the box above and in addition Alice is allowed to send one bit to Bob. Bob is not allowed to send anything to Alice. How can they do this?

(b) How well can Alice and Bob play the CHSH game in case they have a single PR box at their disposal?

(c) Slightly shocked by this outcome, Alice and Bob begin to suspect that their box is cheating. Namely they suspect their box of actually violating the non-signaling condition (i.e. it somehow magically allows Alice and Bob to communicate when playing the CHSH game). Therefore they resolve to test what are called the *non-signaling conditions*.

The non-signaling conditions intuitively say that if Alice and Bob input something into the box and receive an output, Alice's output should not depend on Bob's input and Bob's output should not depend on Alice's input. Formally what they will do is the following: Alice generates a bit x at random such that $P_X(0) = P_X(1) = \frac{1}{2}$ and inputs it in the box on her side and Bob generates a bit y at random such that $P_Y(0) = P_Y(1) = \frac{1}{2}$ and inputs it on his side. Then they receive output bits a and b from the box (distributed as described above) which they will use to check the following conditions:

$$\forall a, x, y, \tilde{y} \in \{0,1\} : \sum_{b \in \{0,1\}} P(a, b|x, y) = \sum_{b \in \{0,1\}} P(a, b|x, \tilde{y}),$$

$$\forall a, y, x, \tilde{x} \in \{0,1\} : \sum_{a \in \{0,1\}} P(a, b|x, y) = \sum_{a \in \{0,1\}} P(a, b|\tilde{x}, y),$$

where $P(a, b|x, y)$ is the probability that the box, given input bits x, y will produce output bits a, b. Does the box violate the non-signaling constraints?

(d) Now imagine we get an upgraded version of the same box. This box takes a bit string x of n bits as input on Alice's side and a single bit y on Bob's side. It outputs a string r to Alice such that $P(r_i = 0) = P(r_i = 1) = \frac{1}{2}$ for all $1 \leq i \leq n$ and outputs the string b such that $b_i = r_i + x_i \cdot y \mod 2$ for all $1 \leq i \leq n$. You can think of this as the 'string' version of the PR box.

Alice and Bob would like to use this box, and classical communication from Alice to Bob, to design another protocol for some form 1-2 oblivious transfer of strings. That is, Alice has two strings s_0, s_1 and Bob has a bit b and at the end of the protocol we would like Bob to hold the string s_b while having no knowledge of the other string. Alice inputs a random string x into the box and receives r which she uses to one-time-pad encode her first message $e_0 := s_0 \oplus r$. The other message is encoded as $e_1 := s_1 \oplus x \oplus r$. Both e_0 and e_1 are sent to Bob. Explain how Bob can recover e_y after inputting his choice bit y into the upgraded box.

Is this really 1-2 oblivious transfer? **Hint:** can we build bit commitment out of this form of 1-2 oblivious transfer? Why, or why not?