Quantum Aspects of Cryptography

Assignment 2—Quantum Review (cont.)
(For lectures 1, 2 and 3)
Assigned: Thursday, Jan 23, 2024
Due (3 weeks): Thursday, Feb 13, 2025

Instructions.

1. Same as those for Assignment 1.
2. If your name is *Alice* and you're submitting answers to *Assignment 2*, use `Alice2.pdf` as your filename when submitting.
3. Please submit your assignment using this OneDrive link for Assignment 2.

Remark. Since most of you are already familiar with the basics of quantum, I borrowed these more interesting questions from an introductory course on quantum information. Understanding non-locality will be helpful for us later as well. If something is unclear, please write to me.

Bell's theorem—Nonlocality. Reminder: Consider an experiment where two distant systems A and B are measured. On system A one measurement $x \in \{1, \dots, k_A\}$ among k_A possibilities is performed, resulting in an outcome $a \in \{1, \dots, d_A\}$. Similarly, on system B one measurement $y \in \{1, \dots, k_B\}$ among k_B possibilities is performed, resulting in an outcome $b \in \{1, \dots, d_B\}$. We denote by $P(ab|xy)$, the corresponding joint probabilities.

We say that the joint probabilities $P(ab|xy)$ admit a local hidden-variable model, or simply are local, if we can write

$$P(ab|xy) = \int d\lambda \rho(\lambda) P(a|x,\lambda) P(b|y,\lambda)\,. \tag{1}$$

If the joint probabilities cannot be written as above, as e.g. witnessed by the violation of a Bell inequality, we say that they are non-local.

We say that the joint probabilities $P(ab|xy)$ admit a quantum representation, or simply are quantum, if we can write

$$P(ab|xy) = \mathrm{tr}\left[\rho_{AB} M_{a|x} \otimes M_{b|y}\right]\,. \tag{2}$$

Finally, we say that they are no-signalling if

$$\sum_a P(ab|xy) = P(b|xy) = P(b|y), \qquad \sum_b P(ab|xy) = P(a|xy) = P(a|x)\,. \tag{3}$$

Exercise 1. Necessary condition for non-locality.

a. Show that if either $k_A = 1$ or $k_B = 1$, then $P(ab|xy)$ necessarily admits a local hidden-variable description. That is, the violation of a Bell inequality necessarily requires at least two measurement choices on each side.

b. Show that if ρ_{AB} is separable, i.e., can be written as $\rho_{AB} = \sum_i p_i \sigma_i \otimes \tau_i$, then necessarily $P(ab|xy)$ is local. Thus the violation of a Bell inequality requires and witnesses the presence of entanglement.

c. Show that if all measurement operators on A (or similarly on B) commute, then $P(ab|xy)$ is local. Thus the violation of a Bell inequality requires on each side a choice between incompatible measurements.

Exercise 2. Tsirelson bound: Assume $x, y \in \{0, 1\}$ and $a, b \in \{\pm 1\}$. The CHSH expression is

$$I = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle\,, \tag{4}$$

where $\langle A_x B_y \rangle = \sum_{ab} ab P(ab|xy)$. Show that according to quantum theory $I \leq 2\sqrt{2}$. This bound is known as the Tsirelson bound.

Hint: analyze the spectrum of the operator $\hat{I}$, where $\hat{I} = A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1$, where A_x, B_y denote the observables corresponding to the measurements x and y.

Exercise 3. No-signalling bound for CHSH: If we assume only no-signalling and nothing more, what is the maximal value of the CHSH expression? Construct an explicit joint distribution $P(ab|xy)$ reaching this maximal value.

Exercise 4. No-signalling, non-locality, and randomness: In the previous exercise, you should have found that the no-signalling distribution reaching the maximal value of the CHSH expression has completely random marginals.

a. Suppose that Alice and Bob share correlations achieving the maximal value of the CHSH expression and at the same time such that the marginals of Alice are not uniformly random. Show an explicit procedure through which Alice could signal to Bob.

b. More generally, show that any correlations that are both non-local and no-signalling cannot be compatible with a and b being deterministic.

Exercise 5. Consequences of non-local "super-quantum" correlations for communication complexity: Consider the following problem of communication complexity: Alice receives a string x of n bits and Bob a string y of n bits. Bob has to evaluate a boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ that takes as input the two stings n-bit strings, x and y (a boolean function is a function that returns 1 bit, that is to say $f(x,y) = 0$ or $f(x,y) = 1$). One is interested in finding the least amount of communication that must take place between Alice and Bob which allows the evaluation of the function. For certain functions f it has been shown that if Alice and Bob share an entangled state, they can reduce the amount of communication compared to the best classical protocol. On the other hand, there exist functions f for which the communication complexity in the quantum case is the essentially the same as that in its classical counterpart. One example of such a function is the "scalar product" defined as

$$f(x,y) = \sum_i x_i y_i \tag{5}$$

where the summation is modulo 2. Even if Alice and Bob share an infinite amount of entanglement, the communication complexity is n bits (which is the maximum possible because Alice can always send her n-bit input to Bob who can then evaluate any function $f(x,y)$).

a. Show that if Alice and Bob share systems which attain the maximum violation of CHSH (which is 4 and therefore beyond the quantum limit $2/\sqrt{2}$), they can evaluate the function (5) with 1 bit of communication from Alice to Bob, regardless of the sizes of their inputs, n.

b. Generalise this result to all functions f by using the fact that all boolean functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ can be expressed as a polynomial of some variables and modulo 2 arithmetic (this follows simply from the fact that the elementary boolean operations like AND, OR, NOT can be calculated with addition and multiplication on $\{0,1\}$).

This hints at why such super-quantum systems don't exist: they would solve any distributed computing problem with a single bit of communication.