Practice problem set 7

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

Problem 1: Corrupted measurement devices (Example 7.2.1)

Consider the purified version of the BB'84 protocol, i.e., where Alice and Bob both measure halves of EPR pairs. Suppose that Eve prepares the state ρ_{ABE} to be the following:

$$\rho_{ABE} = \frac{1}{4} \sum_{x,z \in \{0,1\}} |xz\rangle\langle xz|_A \otimes |xz\rangle\langle xz|_B \otimes |xz\rangle\langle xz|_E.$$

Last week, we saw that if Alice and Bob follow the purified protocol perfectly, then they still have a good probability of detecting an eavesdropping Eve. This time, we will consider what happens when Eve also supplies the measurement devices. The devices are the same for Alice and Bob. Eve programs them to do the following:

- On the instruction "Computational-basis measurement": measure the first qubit in the system in the computational basis.
- On the instruction "Hadamard-basis measurement": measure the second qubit in the system in the computational basis.

(a) What is the probability that Alice and Bob get the same measurement outcome if they choose the same basis? What is the probability that they get a different outcome if they choose different bases?

(b) How much information can Eve learn about the exchanged key?

Problem 2: Commuting observables

In this exercise, you will compute a special case of the following fact: if A, B are commuting observables (i.e., $AB = BA$), then the product of the results of measuring A and then B is the same as the result of measuring AB.

Consider $X \otimes X$ and $Z \otimes Z$. Since they commute, they have a simultaneous eigenbasis. It consists of the Bell states $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$.

(a) Suppose we measure a two-qubit state $|\varphi\rangle$ using the observable $X \otimes X$ and receive the outcome -1. Give a 2-dimensional eigenspace of $X \otimes X$ to which the post-measurement state belongs.

(b) Next, we measure the observable $Z \otimes Z$ on the resulting state, and receive outcome 1. What is the post-measurement state $|\varphi'\rangle$?

(c) Suppose that instead, we performed the measurement $-Y \otimes Y = (X \otimes X)(Z \otimes Z)$ directly, and the post-measurement state had nonzero overlap with $|\varphi'\rangle$. What measurement outcome would we have received? Compare your answer to the product of the answers of the previous subexercises.

Problem 3: Another pseudo-telepathy game

Alice and Bob tell their friend Eve that they have a magic 3×3 square of numbers with the following property: every entry is either 1 or -1, the product of each column is 1, and the product of each row is -1. Eve is not convinced by Alice and Bob's claim (why?). She asks them to play the following game. Alice and Bob receive random inputs $i, j \in \{0, 1, 2\}$ respectively. They each produce a triple of ± 1 numbers $\vec{a} = (a_0, a_1, a_2)$ and $\vec{b} = (b_0, b_1, b_2)$. They win if $\vec{a}$ is a valid column of the magic square, and $\vec{b}$ a valid row.

(a) What is the highest possible success probability Alice and Bob can achieve with a deterministic classical strategy?

(b) Can they do better if they start the game with shared randomness?

(c) Consider the following 3×3 square of observables:

$$\begin{pmatrix} -I \otimes Z & X \otimes I & X \otimes Z \\ -Z \otimes I & I \otimes X & Z \otimes X \\ Z \otimes Z & X \otimes X & Y \otimes Y \end{pmatrix}.$$

Which of these observables commute? Can you find a pattern?

(d) The product of the first row of the magic square is $(-I\otimes Z)(X\otimes I)(X\otimes Z)$. What are the eigenvalues of this operator? What about the other rows? And the columns?

(e) Suppose Alice and Bob are allowed to share two EPR pairs for the magic square game. Use the 3×3 square of observables, plus result from the previous exercise, to find an optimal strategy for Alice and Bob.

Problem 4: A coherent attack on a non-local game

Consider the following cooperative game G. Alice receives an input bit s, and Bob an input bit t. They are promised that $(s,t) \in_R \{(0,0),(0,1),(1,0)\}$. They generate output bits $a, b \in \{0,1\}$ respectively, and win if $a \vee s \neq b \vee t$.

(a) Analyze the winning probability for the trivial strategy $a = s$ and $b = t$.

(b) In the two-parallel version $G^{(2)}$ of this game, Alice and Bob receive *two* pairs (s_0,t_0) and (s_1,t_1), selected independently and uniformly at random from $\{(0,0),(0,1),(1,0)\}$. (Alice gets (s_0,s_1), Bob gets (t_0,t_1).) They win if their responses (a_0,a_1) and (b_0,b_1) are such that $a_i \vee s_i \neq b_i \vee t_i$ for all $i \in \{0,1\}$.
Describe a classical strategy for $G^{(2)}$ with a winning probability of $\frac{2}{3}$.

(c) Suppose Alice and Bob have a valid classical strategy for $G^{(2)}$ which wins with probability ω_c. Describe a classical strategy for G guaranteeing the same winning probability ω_c. (Recall that Alice and Bob may have shared randomness, but they may not communicate.)