COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 2 **due: 12:59PM, October 14th, 2025**

Ground rules:

Please format your solutions so that each problem begins on a new page, and so that your name appears at the top of each page.

You are encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them. If you use an AI tool to partially solve a question, or improve your write-up of a solution, then you should also mention it. All questions on the homework, including requests for clarifications or typos, should be directed to the Ed forum.

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of an academic committee.

Each of the four problem set counts for 20% of the total homework grade. (Each of the two readings will count for 10% of the final homework grade.)

In this problem set we learn about various type of bipartite and tripartite correlations. The first two exercises consider forms of tripartite entanglement. The first exercise shows that tripartite entanglement can beat the classical bound in a three-player game (this is in contrast to the "2-out-of-3" CHSH game seen in exercise session). Exercise 2 explores how entanglement can be "lost" when some of the qubits, or parties, are discarded. Finally, Exercise 3 explores a generalization of quantum correlations and nevertheless respects the no-signaling condition. While these generalized correlations can be stronger and lead to higher success probabilities in some games such as the CHSH games, they also have limitations (which we will later use for cryptography).
The first two exercises are shorter. The third exercise is longer. Question 3(f) is the longest. Question 3(g) is interesting but somewhat technical and entirely optional.

Revisions since the first posting are in blue.

Problems:

1. (6 points) **A three-player game.**

   We learned about the CHSH game in class. In this problem we'll explore another nonlocal game, this time with *three players* (called Alice, Bob and Charlie).

   The referee chooses three bits (x, y, z) uniformly at random from the set

   $$\big\{(0,0,0),(0,1,1),(1,1,0),(1,0,1)\big\}\ .$$

   Alice gets x, Bob gets y, and Charlie gets z. They respond with bits $a, b, c \in \{0,1\}$, respectively, and they win if $a \oplus b \oplus c = x \vee y \vee z$.

(a) Suppose that Alice, Bob, and Charlie use a classical strategy. Compute their maximum winning probability.

(b) Suppose that Alice, Bob and Charlie share the tripartite entangled state

$$|\psi\rangle = \frac{1}{2}\Big(|000\rangle - |011\rangle - |101\rangle - |110\rangle \Big) .$$

If a player gets question 0, they measure their qubit in the standard basis (i.e., measures the Z observable) and output their answer. If they get question 1, they measure their qubit using the X observable and output their answer.[1]

Show that this strategy wins this nonlocal game with probability 1.

(c) Is $|\psi\rangle$ maximally entangled between Alice and Bob (or between any pair of players)?

2. (6 points) **Robustness of GHZ and W States.**
In this problem we explore two classes of N-qubit states that are especially useful for cryptography and communication, but behave very differently under tracing out a single qubit. Let's first define them for $N = 3$:

$$\text{GHZ state:} \quad |GHZ_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$
$$\text{W state:} \quad |W_3\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$$

Note that both states are symmetric under permutation of the three qubits, so without loss of generality we may trace out the last one, Tr_3. Also, we have analogously $|GHZ_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|W_2\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$.

In the following we consider the *overlap* between N-qubit GHZ and W states with one qubit discarded (i.e. traced out) and their $(N-1)$-qubit counterparts. The overlap of density matrices ρ and σ is defined as $\mathrm{Tr}\rho\sigma$, a measure of "closeness" that generalizes the expression $|\langle\phi|\psi\rangle|^2$ for pure states.

(a) Calculate the overlap between $|GHZ_2\rangle\langle GHZ_2|$ and $\mathrm{Tr}_3 |GHZ_3\rangle\langle GHZ_3|$.

(b) Calculate the overlap between $|W_2\rangle\langle W_2|$ and $\mathrm{Tr}_3 |W_3\rangle\langle W_3|$).

Now we generalize to the N-qubit case. As you might expect, $|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$ and $|W_N\rangle$ is an equal superposition of all N-bit strings with exactly one 1 and $N-1$ 0's.

(c) What is the overlap $\mathrm{Tr}(|GHZ_{N-1}\rangle\langle GHZ_{N-1}| \,\mathrm{Tr}_N |GHZ_N\rangle\langle GHZ_N|)$ in the limit $N \to \infty$?

[1] Recall the Pauli observables

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} .$$

(d) What is the overlap $\mathrm{Tr}(|W_{N-1}\rangle\langle W_{N-1}|\,\mathrm{Tr}_N\,|W_N\rangle\langle W_N|)$ in the limit $N \to \infty$?

The interpretation of these results is that W states are more "robust" against loss of a single qubit than GHZ states.

3. (8 points) **Nonlocal boxes.**
Given an integer n and finite sets $\mathcal{X}_1, \ldots, \mathcal{X}_n$ ("inputs") and $\mathcal{A}_1, \ldots, \mathcal{A}_n$ ("outputs"), an n-partite *non-local box* is a family of distributions $\{p(\cdot|x_1, \ldots, x_n),\, x_1, \ldots, x_n \in \mathcal{X}_1 \times \cdots \times \mathcal{X}_n\}$, each defined on $\mathcal{A}_1 \times \cdots \times \mathcal{A}_n$, i.e.

$$\sum_{a_i \in \mathcal{A}_i} p(a_1, \ldots, a_n|x_1, \ldots, x_n) = 1 \quad \forall x_i, \quad \text{and} \quad p(a_1, \ldots, a_n|x_1, \ldots, x_n) \geq 0 \quad \forall x_i, a_i.$$

Intuitively, a non-local box is called *non-signaling* if the i-th output does not provide information about the j-th input, for $i \neq j$. This is a natural condition if we think of each output, a_i, as being produced locally given the input x_i: in that case, the distribution of a_i should not depend on what the inputs x_j where at other locations $j \neq i$. More formally, it is required that for each $i \in \{1, \ldots, n\}$ and all input tuples $(x_1, \ldots, x_n)$ and $(x'_1, \ldots, x'_n)$ such that $x_i = x'_i$,

$$\forall a_i \in \mathcal{A}_i, \qquad \sum_{a_j : j \neq i} p(a_1, \ldots, a_n|x_1, \ldots, x_n) \;=\; \sum_{a_j : j \neq i} p(a_1, \ldots, a_n|x'_1, \ldots, x'_n).$$

Similarly, the condition is required when taking marginals on more than one location, e.g. the marginal on any pair (a_i, a_j) should be independent of questions x_k for $k \notin \{i, j\}$ This condition implies that the marginal distribution on any single coordinate i is a well-defined distribution which only depends on the input x_i associated with that coordinate.

(a) Show that if a non-local box p is quantum, i.e. there is an n-partite quantum state $\rho_{A_1 \cdots A_n}$ and POVM $\{A_x^{(i),a}\}_a$, for $i = 1, \ldots, n$, such that

$$\mathrm{Tr}\big((A_{x_1}^{(1),a_1} \otimes \cdots \otimes A_{x_n}^{(n),a_n})\rho_{A_1 \cdots A_n}\big) = p(a_1, \ldots, a_n|x_1, \ldots, x_n)$$

for all $(a_1, \ldots, a_n, x_1, \ldots, x_n)$, then the non-local box is non-signaling.

However, not all non-local box that is non-signaling needs to be quantum. Let's first see some examples of nonlocal boxes for the bipartite ($n = 2$) case. Here are four of them. In each case $\mathcal{X}_i = \mathcal{A}_i = \{0, 1\}$, and any un-specified probability is set to 0 by default:

$$
\begin{array}{lll}
\text{(U)} & p(a,b|x,y) = 1/4 & \forall (x,y,a,b). \\
\text{(PR)} & p(0,0|x,y) = p(1,1)|x,y) = 1/2 & \text{if } (x,y) \neq (1,1), \\
 & p(1,0|x,y) = p(0,1)|x,y) = 1/2 & \text{if } (x,y) = (1,1). \\
\text{(CH)} & p(0,0|x,y) = p(1,1)|x,y) = \frac{1}{2}\cos^2 \pi/8 & \text{and} \\
 & p(1,0|x,y) = p(0,1)|x,y) = \frac{1}{2}\sin^2 \pi/8 & \text{if } (x,y) \neq (1,1), \\
 & p(0,0|x,y) = p(1,1)|x,y) = \frac{1}{2}\sin^2 \pi/8 & \text{and} \\
 & p(1,0|x,y) = p(0,1)|x,y) = \frac{1}{2}\cos^2 \pi/8 & \text{if } (x,y) = (1,1). \\
\text{(SIG)} & p(y,x|x,y) = 1 & \forall (x,y).
\end{array}
$$

(b) Verify that each of these indeed specifies a nonlocal box, i.e. that the probabilities add up to 1 when they should. (You do not need to show your calculations—but make sure you do it to understand the definition of each of the boxes.)

(c) Among the four boxes, which are non-signaling? (You do not need to show your calculations.)

(d) For each of the boxes, evaluate its success probability in the CHSH game. That is, assuming Alice and Bob are able to generate answers distributed according to $p(a,b|x,y)$ whenever their respective inputs are x and y, what is the probability that they produce valid answers in the game (when the questions are chosen uniformly at random, as usual)? (You do not need to show your calculations.)

(e) For each of the four boxes, state which can be implemented using quantum mechanics. If it can, provide a strategy: a bipartite state ρ_{AB} and POVM $\{A_x^a\}_a$ and $\{B_y^b\}_b$, for all x and y, such that $\mathrm{Tr}\big((A_x^A \otimes B_y^b)\rho_{AB}\big) = p(a,b|x,y)$ for all (a,b,x,y). If it cannot, provide a short argument justifying your answer.

Now let's look into some tripartite ($n = 3$) nonlocal boxes. We say that a tripartite box $\{q(\cdot,\cdot,\cdot|x,y,z)\}$ is an *extension* of a bipartite box $\{p(\cdot,\cdot|x,y)\}$ if the marginals satisfy $\sum_c q(a,b,c|x,y,z) = p(a,b|x,y)$, for all (a,b,x,y).

(f) Show that any non-signaling tripartite extension of the (PR) box must have a product form, i.e. $q(a,b,c|x,y,z) = q(a,b|x,y)p'(c|z)$ for some family of distributions $\{p'(\cdot|z)\}$ (note that the marginal $q(a,b|x,y)$ is well-defined by the no-signaling condition). *[Hint: define $\{p'(\cdot|z)\}$ in some way, and then use the non-signaling conditions to show $q(a,b,c|x,y,z) = q(a,b|x,y)p'(c|z)$ for all a,b,c and x,y,z. Using the definition of (PR), many of these probabilities will equal 0.]*

Part (e) has a very important consequence for cryptography: it means that certain types of bipartite correlations imply *perfect privacy*: *any* extension of the distribution which takes into account a third system must be *completely uncorrelated* from the first two (as long as it respects the basic non-signaling conditions). This phenomenon is often referred to as a *monogamy* property of the bipartite (PR) box. While this is not true of the (CH) box, the latter still provides some limited amount of secrecy, which will be key to its use in quantum key distribution, a topic we will soon explore in class.

(g) *(Bonus 3pts)* Consider a three-player variant of the CHSH game in which each of the three possible pairs of players is chosen uniformly at random by the referee to execute the CHSH game (with the third player being ignored; see the notes on EdX for a complete description). Determine, either analytically or numerically, the optimum success probability achieved by any non-signaling tripartite box in this game. Another manifestation of monogamy! (If you used numerics, include your code.)