CS120, Quantum Cryptography, Fall 2016

Homework # 4 **due: 10:29AM, November 1st, 2016**

Ground rules:

Your homework should be submitted to the marked bins that will be by Annenberg 241.

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 strongly 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.

Some of the problems are inspired from problems available on EdX. You are not allowed to look up the EdX problems for hints (such as the multiple answers provided). Focus on the present pset!

Late homework will not be accepted or graded. Extensions will not be granted, except on the recommendation of a dean. We will grade as many problems as possible, but sometimes one or two problems will not be graded. Your lowest homework grade of the quarter will be dropped from your final grade.

Place all your problems in the first (top) bin in the box by Annenberg 241. Start each problem on a new page, with your name clearly marked at the top of the page.

Problems:

1. (8 points) **Robustness of GHZ and W states, part 2.**
We return to the multi-qubit GHZ and W states originally introduced in HW 2 Problem 4. As a reminder:

$$\begin{aligned}|GHZ_N\rangle &= \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}),\\ |W_N\rangle &= \frac{1}{\sqrt{N}}(|100\cdots00\rangle + |010\cdots00\rangle + \cdots + |000\cdots01\rangle).\end{aligned}$$

This week we learned to distinguish product states from (pure) entangled states by calculating the Schmidt rank of A bipartite state $|\Psi\rangle_{AB}$, i.e. the rank of the reduced state $\rho_A = \mathrm{Tr}_B\,|\Psi\rangle\langle\Psi|_{AB}$. In particular $|\Psi\rangle_{AB}$ is pure if and only if its Schmidt rank is 1. In the following, we denote by Tr_N the operation of tracing out only the last of N qubits.

(a) What are the ranks r_{GHZ} of $\mathrm{Tr}_N\,|GHZ_N\rangle\langle GHZ_N|$ and r_W of $\mathrm{Tr}_N\,|W_N\rangle\langle W_N|$? (Note that these are the Schmidt ranks of $|GHZ_N\rangle$ and $|W_N\rangle$ if we partition each of them between the first $N-1$ qubits and the last qubit.)

Let's now introduce a more discriminating (in fact, continuous) measure of the entanglement of a state $|\Psi\rangle_{AB}$: namely, the **purity** of the reduced state ρ_A, defined as $\mathrm{Tr}\,\rho_A^2$.

(b) What are the minimum and maximum values of $\mathrm{Tr}\,\rho^2$ that can be attained by an arbitrary density matrix ρ on a d-dimensional Hilbert space? For each extreme, prove that it is indeed optimal and give an example of a state ρ that achieves it.

(c) Would you expect the purity of ρ_A to increase or decrease as the full state $|\Psi\rangle_{AB}$ gets "more entangled"? Give a qualitative justification for your answer. [*NB: The reduced-state purity can in fact be proven to be an entanglement monotone, i.e. it only changes in one direction under local operations and classical communication. The proof is beyond the scope of this problem but can be found in* `https://arxiv.org/abs/quant-ph/0506181`.]

(d) What is the purity of $\mathrm{Tr}_N\,|GHZ_N\rangle\langle GHZ_N|$ in the limit $N \to \infty$?

(e) What is the purity of $\mathrm{Tr}_N\,|W_N\rangle\langle W_N|$ in the limit $N \to \infty$? Comparing with part (d), explain why we can conclude that the entanglement in the W states is more " robust" to the loss of a single qubit.

(f) Repeat the analysis of parts (d) and (e) for the general case of tracing out some constant number of qubits. That is, fix constant m and compute the limits as $N \to \infty$ of the purities of the N-qubit GHZ and W states with m qubits traced out, as functions of m.

2. (4 points) **Dimension of a purifying system.**
Consider the following protocol for preparing an arbitrary (possibly mixed) state ρ_A on a *qudit* A with dimension d, i.e. a system whose Hilbert space has basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$:

- Prepare a pure state $|\Psi\rangle_{AB}$ on A and a D-dimensional ancilla qudit B (for some integer D), satisfying $\mathrm{Tr}_B\,|\Psi\rangle\langle\Psi|_{AB} = \rho_A$.
- Discard the ancilla qudit B.

(a) What is the minimum value of the ancilla dimension D for which we can have $\rho_A = \frac{1}{2}(|0\rangle\langle 0| + |3\rangle\langle 3|)$? Argue explicitly that no smaller dimension will work.

(b) What is the minimum value of D for which we can have

$$\rho_A = \frac{1}{5}\big(\,|1\rangle\langle 1| + |2\rangle\langle 2| + |2\rangle\langle 3| + |3\rangle\langle 2| + |3\rangle\langle 3| + |4\rangle\langle 4| + |4\rangle\langle 5| + |5\rangle\langle 4| + |5\rangle\langle 5|\,\big)?$$

Again argue explicitly that no smaller dimension will work.

(c) For a general ρ_A, explain how to find the minimum ancilla dimension D for which there exists a pure purifying state $|\Psi\rangle_{AB}$.

(d) **Bonus question:** Suppose in part (c) that we are somehow limited to ancilla systems of some fixed dimension $m < \mathrm{rank}(\rho_A)$. In this case it may not be possible to find a pure $|\Psi\rangle_{AB}$ such that $\mathrm{Tr}_B |\Psi\rangle\langle\Psi|_{AB} = \rho_A$. Suppose then we look for a mixed state σ_{AB} such that $\mathrm{Tr}_B(\sigma_{AB}) = \rho_A$. How would you go about finding the minimum attainable rank of the joint state σ_{AB}? What about the state with the highest attainable purity $\mathrm{Tr}\,\sigma_{AB}^2$? The more thorough, generic and analytical your explanation, the better!

3. (6 points) **Secret sharing among three people.**
In the EdX materials for Week 3 you learn how to share a classical secret between two people using an entangled state. Here we will create a scheme that shares a classical secret among three people, Alice, Bob and Charlie. We encode the secret $b \in \{0, 1\}$ in a GHZ-like state of the form

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B |0\rangle_C + (-1)^b |1\rangle_A |1\rangle_B |1\rangle_C).$$

(a) Calculate the single-party reduced density matrices ρ_A, ρ_B, and ρ_C. Verify that no single one of Alice, Bob, and Charlie can recover the secret on their own.

(b) Calculate the two-party reduced densities ρ_{AB}, ρ_{BC}, and ρ_{AC}. Verify that no pair of Alice, Bob, and Charlie can recover the secret on their own.

(c) Suppose each of Alice, Bob, and Charlie is limited to the following operations:

- Local Hadamard operator on their qubit;
- Local measurement of their qubit in the computational basis $\{|0\rangle, |1\rangle\}$;
- Sending a (classical) measurement outcome to one of the other two.

Devise a scheme by which they can together recover the secret b. (Such a scheme is called an *LOCC protocol*, for "local operations and classical communication". You may wish to think if there exists a secret-sharing scheme such that even an LOCC protocol would not allow colluding parties to recover the secret...)

4. (10 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.

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

Intuitively, a non-local box is called *non-signaling* if the i-th output does not provide information about the j-th input, for $i \neq j$. More formally, it is required that for each

$i \in \{1, \dots, n\}$ and all input tuples $(x_1, \dots, x_n)$ and $(x'_1, \dots, x'_n)$ such that $x_i = x'_i$,

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

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 additional condition was missing in previous versions of the problem. It is needed for questions (e), (f) and (g) only. If you did the questions without the condition, explain your answer, and we will not take out any points.**] 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.

Let's first investigate some examples of bipartite ($n = 2$) nonlocal boxes. 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:

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

(a) Verify that each of these indeed specifies a nonlocal box, i.e. that the probabilities add up to 1 when they should.

(b) Among the four boxes, which are non-signaling?

(c) 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)?

(d) 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 $\mathrm{Tr}\left((A_x^A \otimes B_y^b)\rho_{AB}\right) = p(a, b|x, y)$ for all (a, b, x, y). If it cannot, provide an 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).

(e) Show that any non-signaling tripartite extension of the (PR) box must have a product form, i.e. $q(a,b,c|x,y,z) = p(a,b|x,y)p'(c|z)$ for some family of distributions $\{p'(\cdot|z)\}$.

(f) Show that this is not true of the (CH) box: find a non-product extension of that box which nevertheless satisfies all non-signaling conditions.

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) 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). Prove either analytically or numerically (in the latter case, include and briefly explain your code) that the optimum success probability achieved by any non-signaling tripartite box in this game is at most 3/4. Another manifestation of monogamy!