COM-440, Introduction to Quantum Cryptography, Fall 2025

Homework # 1 **due: 12:59PM, October 8th, 2019**

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.

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 semester will be dropped from your final grade.

Problems:

1. **An optimal attack**
   Let
   $$N_1 = \frac{1}{\sqrt{12}} \begin{pmatrix} 3 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad N_2 = \frac{1}{\sqrt{12}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 3 \end{pmatrix} .$$

   (a) Show that (N_1, N_2) are valid Kraus operators in the definition of a quantum channel $\mathcal{N}(\rho) = N_1 \rho N_1^\dagger + N_2 \rho N_2^\dagger$ mapping one qubit to two qubits.

   (b) Show that using $\mathcal{N}$, a quantum adversary succeeds in the CLONE security game for Wiesner's quantum money scheme with probability $\frac{3}{4}$.

2. (4 points) **Superdense Coding**
   In Homework 1, you were introduced to the idea of "quantum teleportation". By sending just two bits of classical information, Alice was able to "teleport" her single-qubit quantum state to Bob, provided they shared a pair of maximally entangled qubits to begin with.
   In this problem, Alice instead wants to share two classical bits with Bob, but she only has a quantum channel at her disposal, and she is only allowed to use it once (i.e. send only one single-qubit state). Can she succeed?

   (a) The first idea she has is to encode her two classical bits into her preparation of one of four states in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and then send this qubit to Bob.

Suppose that the a priori distribution of Alice's two classical bits is uniform. What is the maximum probability with which Bob can correctly guess both of Alice's two classical bits?

(b) Suppose that Alice and Bob share a maximally entangled pair of qubits. Alice thinks that it is a good idea to start by performing one of four unitary transformations on the qubit in her possession depending on the value of the two classical bits that she wishes to communicate and send her qubit to Bob. What next? Help Alice (and Bob) devise a scheme that achieves the desired task with certainty.

(c) After all the thought that Alice and Bob put into coming up with a working scheme, they finally decide to employ it.
Unfortunately, the tireless eavesdropper Eve has heard of their new scheme, and as soon as Alice and Bob use it, she intercepts the qubit as it's sent from Alice to Bob. Can Eve recover information about the two confidential classical bits that Alice intended to share with Bob?

3. (6 points) **Secret sharing among three people.**
In class we saw how to share a classical secret between two people using an entangled state. In this problem we 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 operation 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 players.

Devise a scheme by which they can together recover the secret b.

[A scheme of the type considered in part (c) 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? Intuitively, such a scheme would have the property that the secret is hidden "deep inside the entanglement", in the sense that even if everyone decides to collaborate in cheating *but* is restricted to LOCC then they still can't recover

the secret. In such a situtation the only way to recover the secret would be to get access to the entire quantum state at once and make a general measurement on all the shares (as opposed to local measurements followed by exchange of classical information).]

4. (4 points) **A Guessing Game.**
Imagine that Alice and Eve play a guessing game where they share a two-qubit state ρ_{AE}. First, Alice produces a random bit $\theta \in \{0,1\}$, and she measures her qubit in the standard basis if $\theta = 0$ and in the Hadamard basis if $\theta = 1$. In both cases she obtains a bit $x \in \{0,1\}$ as measurement outcome. She then announces θ to Eve. Eve's goal is to guess the bit x. Imagine that $\rho_{AE} = |\text{EPR}\rangle\langle\text{EPR}|$, where as usual $|\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, so Alice and Eve share a maximally entangled pair of qubits. In this scenario we know that if Eve measures in the same basis as Alice she will get the same outcome and this thus able to guess x perfectly.

   (a) Suppose now that Alice wants to foil Eve so, before measuring, she first applies some unitary U_A to her qubit, and then measures. Of course Eve, being really smart, gets wind of this so she will know what unitary Alice has used before measuring. So they share the state

$$|\Phi_U\rangle = (U_A \otimes \mathbf{1}_E)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

   and Eve knows θ and U_A. In this scenario, what is Eve's optimal guessing probability, and what is a strategy that achieves it?

   (b) Consider now a scenario in which Alice's strategy consists in choosing one out of three possible unitaries, according to a distribution that may depend on her choice of θ. The three unitaries are the same whether $\theta = 0$ or $\theta = 1$, and Eve knows what they are as well as the distribution used by Alice, but she does not learn which unitary Alice eventually selected. Provide a set of three unitaries that makes Eve's guessing probability the lowest possible. (You do not need to prove that your strategy is optimal.)

   (c) Suppose we restrict Alice's set of possible unitaries to contain only two. Can she still make Eve's guessing probability as low as in part (b)?

5. (6 points) **Robustness of GHZ and W States, Part II.**
We return to the multi-qubit GHZ and W states introduced in the previous exercise. In class we learned to distinguish product states from (pure) entangled states by calculating the Schmidt rank of $|\Psi\rangle_{AB}$, i.e. the rank of the reduced state $\rho_A = \text{Tr}_B |\Psi\rangle\langle\Psi|$. In particular ρ is pure if and only if $|\Psi\rangle$ has Schmidt rank 1. In the following, we denote by Tr_N the operation of tracing out only the last one out of N qubits.

   (a) What are the ranks r_{GHZ} of $\text{Tr}_N |GHZ_N\rangle\langle GHZ_N|$ and r_W of $\text{Tr}_N |W_N\rangle\langle W_N|$, respectively? (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 us 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 given by $\mathrm{Tr}\rho_A^2$. First let's see how this works in practice with the extreme cases in d dimensions:

(b) What are the purities $\mathrm{Tr}\,(\rho^2)$ for $\rho = |0\rangle\langle 0|$ and the "maximally mixed" state $\rho = \frac{1}{d} id_d$, respectively?

(c) Is the purity of ρ_A higher or lower for more entangled states $|\Psi\rangle_{AB}$? Can you explain this in terms of the definition $\mathrm{Tr}\,(\rho_A^2)$?

Now consider again the behavior of the N-qubit GHZ and W states with one qubit discarded (i.e. traced out):

(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 $N \to \infty$?

Discuss the implications for the "robustness" of multipartite entanglement under loss of one qubit in GHZ versus W states. What can we say about losses of more than one qubit?

6. **Using the Pretty-Good-Measurement**
Alice sends Bob one of the three states

$$\rho_0 = |0\rangle\langle 0|\,,\ \rho_1 = \frac{1}{2}\mathbb{I},\ \rho_2 = |1\rangle\langle 1|$$

with equal probability. Bob wants to determine which state Alice sent him. In this problem we work out the success probability of different possible strategies for Bob. A strategy is a POVM $\{B_0, B_1, B_2\}$ and its success probability is

$$p_{succ}(B) \ = \ \frac{1}{3}\mathrm{Tr}(B_0\rho_0) + \frac{1}{3}\mathrm{Tr}(B_1\rho_1) + \frac{1}{3}\mathrm{Tr}(B_2\rho_2)$$

i.e. it is the probability that Bob correctly guesses the state sent by Alice, assuming that Alice sends him each of the three states with equal probability $\frac{1}{3}$.

The first strategy that we consider consists in Bob measuring in the Hadamard basis.

(a) Bob sets $B_0 = |+\rangle\langle +|$, $B_1 = 0$ and $B_2 = |-\rangle\langle -|$. That is, if he measures $|+\rangle$, then he guesses that the state sent was $\rho_0 = |0\rangle\langle 0|$ and if he measures $|-\rangle$ he guesses that the state sent was $\rho_2 = |1\rangle\langle 1|$. What is Bob's success probability?

After trying that procedure, Bob decides to switch to measuring ρ in the standard basis.

(b) Bob sets $B_0 = |0\rangle\langle 0|$, $B_1 = 0$ and $B_2 = |1\rangle\langle 1|$. What is his new success probability?

Bob decides that he's done with ad-hoc approaches and wants to use a measurement that will be somewhat reliable.

(c) What is Bob's success probability if he uses the pretty-good measurement?

Bob wants to know whether he's found the optimal measurement. To help find this out, he will apply the following fact. Suppose that σ is a positive semidefinite matrix (not necessarily of trace 1) such that $p_i\rho_i \leq \sigma$ for each i. Then the optimal success probability of a distinguishing measurement on the ensemble $\rho = \sum_i p_i\rho_i$ is at most $\mathrm{Tr}\sigma$. (Recall that $A \leq B$ means that $B - A$ is positive semidefinite.)

(d) What is the best upper bound Bob can derive from this fact?

(e) Can you prove the above-claimed fact?