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. **Classical one time pad**
   We meet up with our favourite protagonists, Alice and Bob. As you know by now, Alice and Bob often encounter an adversary named Eve who is intent on listening in on their conversations. In order to protect themselves Alice and Bob have, during the the last quantum cryptography conference, exchanged a large amount of classical key which they can use to encrypt messages. Alice knows that a safe way to encrypt is to use a classical one time pad, but she feels like this uses a large amount of key. She comes up with the following encoding scheme which she claims is also secure but uses less key. Alice's scheme goes as follows. For i ranging from 1 to n, the total number of bits in her message, Alice does the following:

   - Alice flips a coin.
   - If the result is tails she uses a shared key bit to encode the i-th message bit, via addition modulo 2 as in the one-time pad.
   - If the result is heads, she uses a fresh random bit r, generated on the fly, to encode the i-th message bit again via addition modulo 2.

   Alice claims that this procedure uses less key, but is this really true?

   (a) How many bits of key will Alice use on average for an n-bit message?

   (b) This gain in key length probably comes at a price. Which of the following statements about the protocol is true?

i. The protocol is secure and correct (Bob can decode the message but Eve can not)

ii. The protocol is not secure but correct (Bob and Eve can decode the message)

iii. The protocol is secure but not correct (Neither Bob nor Eve can decode the message)

iv. The protocol is not secure and not correct (Eve can decode the message but Bob can not)

2. **Density matrices**

Suppose that Alice and Bob share a device which they can use to send qubits to each other. In this exercise we investigate what happens when the device sends states that are noisy.

Let us imagine that Alice wants to send the state $|0\rangle$ to Bob. However, 50% of the time the quantum device outputs the state $|1\rangle$ instead.

(a) Give an expression for ρ, the density matrix describing the state that Bob receives.

(b) Imagine that Bob receives two identical, independent copies of this density matrix. He chooses to measure one of them in the standard basis and the other in the Hadamard basis. What are the distributions of the outcomes $0, 1, +, -$?

(c) Now suppose that the machine on Alice's side is not noisy but simply wrong and consistently prepares qubits in the state $|+\rangle$. If Bob again has two states and measures one of them in the standard basis and one of them in the Hadamard basis what is the distribution of outcomes?

3. **Classical-quantum states**

Consider again Alice's faulty qubit transmission device. Imagine that, as in the previous exercise, when asked to produce a $|0\rangle$ state the device returns either $|0\rangle$ or $|+\rangle$ with 50% probability. But now suppose further that the device also returns a classical flag that indicates which state was produced, 0 for $|0\rangle$ and 1 for $|+\rangle$. The joint state of the flag and the qubit produced can be described by the classical-quantum state

$$\rho_{XA} = \frac{1}{2} |0\rangle\langle 0|_X \otimes |0\rangle\langle 0|_A + |1\rangle\langle 1|_X \otimes |+\rangle\langle +|_A \ , \tag{1}$$

where X is used to designate the flag bit, and A the qubit. Now imagine Alice generates a state using her machine and sends it to Bob, while keeping the classical flag to herself. From the point of view of Bob, this situation is exactly analogous to the one described in the previous exercise. In particular, Bob receives a qubit that is in the mixed state

$$\rho_B = \frac{1}{2} |0\rangle\langle 0| + \frac{1}{2} |+\rangle\langle +| \tag{2}$$

Now Bob can choose to either measure in the standard basis or in the Hadamard basis.

(a) Which one of Bob's possible measurement settings, computational or Hadamard, will give him the highest probability of getting outcome 0 (+ in the Hadamard basis)?

Now imagine that Alice also sends the flag X to Bob. Thus Bob receives two qubits in the joint state ρ_{XA}.

2. Which of the following strategies allows Bob to recover Alice's intended qubit, $|0\rangle$, with certainty?
   i. If the flag value is 0 Bob measures in the standard basis, and in the Hadamard basis otherwise.
   ii. If the flag value is 0 Bob measures in the Hadamard basis, and in the standard basis otherwise.
   iii. The flag value does not affect Bob's chances of getting the right result (outcome 0 in the standard basis, outcome + in the Hadamard basis)

4. **Quantum one-time pad**

In the chapter we saw that two classical bits of key are needed to encrypt one qubit: one for choosing whether to apply a Z, and another for choosing whether to apply an X. This was necessary because the X operation has no effect on the $|+\rangle$ state and the Z operation has no effect on the $|0\rangle$ state. Now, Alice has come up with a clever idea for a protocol that uses only one bit of key per qubit. Instead of an X or a Z operation she will apply a Hadamard H, which is the unitary transformation such that $H|0\rangle = |+\rangle$ and $H|+\rangle = |0\rangle$. This allows her to avoid the problem of leaving either standard basis states or Hadamard basis states unchanged by the encryption, while only using one bit of key (for deciding wether or not to apply H) per qubit. Before Alice rushes to publish her discovery it might be worthwhile to check if her scheme is truly secure.

(a) Specify a decryption operation such that Alice's scheme is a correct encryption scheme.

(b) Is Alice's scheme secure?

5. **State discrimination.**

Suppose you are given two distinct states of a single qubit, $|\psi_1\rangle$ and $|\psi_2\rangle$.

(a) Argue that if there is a φ such that $|\psi_2\rangle = e^{i\varphi}|\psi_1\rangle$ then no measurement will distinguish between the two states: for any choice of a basis, the probabilities of obtaining either outcome will be the same when performing the measurement on $|\psi_1\rangle$ or on $|\psi_2\rangle$.

Assuming $|\psi_1\rangle$ and $|\psi_2\rangle$ can be distinguished, we are interested in finding the optimal measurement to tell them apart. Here we need to make precise our notion of "optimal".

We would like to find an orthonormal basis $\{|b_1\rangle, |b_2\rangle\}$ of $\mathbb{C}^2$ such that the expression

$$\frac{1}{2}\mathbf{Pr}\left(\text{``}b_1\text{''}|\ |\psi_1\rangle\right) + \frac{1}{2}\mathbf{Pr}\left(\text{``}b_2\text{''}|\ |\psi_2\rangle\right) = \frac{1}{2}\left|\langle b_1|\psi_1\rangle\right|^2 + \frac{1}{2}\left|\langle b_2|\psi_2\rangle\right|^2 \tag{3}$$

is maximized. (The factors $\frac{1}{2}$ are there to represent the assumption that our "prior probability" about which state is given is uniform.)

(b) Solve the question in the following two cases: first, $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = -|0\rangle$; second, $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = -|1\rangle$. In both cases, find a basis $\{|b_1\rangle, |b_2\rangle\}$ that maximizes (3) and give the resulting value. (You do not need to justify your answer.)

(c) We now turn to the general case. Show that for the purposes of this problem we can assume without loss of generality that $|\psi_1'\rangle = |0\rangle$ and $|\psi_2'\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, for some $\theta \in [0, \pi)$. That is, given any $|\psi_1\rangle, |\psi_2\rangle$, determine an angle θ such that, given a basis $\{|b_1'\rangle, |b_2'\rangle\}$ which maximizes (3) for the pair $(|\psi_1'\rangle, |\psi_2'\rangle)$, lets you recover a basis $\{|b_1\rangle, |b_2\rangle\}$ which achieves the same value in (3) when $(|\psi_1\rangle, |\psi_2\rangle)$ is being measured. Say explicitly how to determine θ from $(|\psi_1\rangle, |\psi_2\rangle)$ and how to recover $\{|b_1\rangle, |b_2\rangle\}$ from $\{|b_1'\rangle, |b_2'\rangle\}$.

(d) Show that the optimal basis $\{|b_1'\rangle, |b_2'\rangle\}$ will always be of the form

$$|b_1'\rangle = \cos\varphi|0\rangle + \sin\varphi|1\rangle\ , \qquad |b_2'\rangle = \sin\varphi|0\rangle - \cos\varphi|1\rangle\ ,$$

for some angle $\varphi \in [0, 2\pi)$. (The reason this may not be immediate is that in general the coefficients of $|b_1'\rangle$ and $|b_2'\rangle$ in the standard basis may involve complex numbers.)

(e) Determine the optimal φ as a function of θ.

(f) Conclude: what is the maximum value of (3), as a function of the original states $|\psi_1\rangle$ and $|\psi_2\rangle$? What is the basis which achieves the optimum?

6. **Unambiguous quantum state discrimination**

In this problem we will explore a practical advantage to performing a general POVM rather than a projective measurement. Consider the following scenario: Bob sends Alice a qubit prepared in one of the two non-orthogonal states $|0\rangle$ and $|+\rangle$, each with probability $\frac{1}{2}$. Alice wants to determine which state Bob has prepared. To this end she performs a measurement on Bob's qubit whose measurement outcome identifies it as either $|0\rangle$ or $|1\rangle$. Alice's goal is to minimize the probability of mis-identifying $|0\rangle$ as $|+\rangle$, or vice versa. Let us first restrict her to projective measurements.

(a) Suppose that Alice measures in the basis $\{\ |\ 0\rangle,\ |\ 1\rangle\ \}$. She identifies the state as $|0\rangle$ if she gets the outcome $|0\rangle$ and as $|+\rangle$ if she gets the outcome $|1\rangle$. What are p, her probability of incorrectly identifying $|0\rangle$, and q, her probability of incorrectly identifying $|+\rangle$?

(b) Suppose instead Alice measures in the basis $\{\ |+\rangle,\ |-\rangle\ \}$. She identifies the state as $|+\rangle$ if she gets the outcome $|+\rangle$ and as $|0\rangle$ if she gets the outcome $|-\rangle$. What are p, her probability of incorrectly identifying $|0\rangle$, and q, her probability of incorrectly identifying $|+\rangle$?

One can show (you may try!) that Alice cannot do better than the above with any projective measurement. That is, no projective measurement gives her a smaller average probability of mis-identification $(p+q)/2$. Now suppose that we allow Alice to perform a general measurement. In particular consider the following POVM with three elements:

$$\begin{aligned} E_1 &= \frac{\sqrt{2}}{1+\sqrt{2}}\,|1\rangle\langle 1|\,1 \\ E_2 &= \frac{\sqrt{2}}{1+\sqrt{2}}\,\frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} \\ E_3 &= id - E_1 - E_2 \end{aligned}$$

(a) Alice identifies the state as $|+\rangle$ if she gets outcome 1, as $|0\rangle$ if she gets outcome 2, and makes no identification if she gets outcome 3. What are her probabilities and of mis-identifying $|0\rangle$ and $|+\rangle$ as the other, respectively?