6.S895, Quantum Cryptography, Spring 2024

Homework # 0 **no due date**

This is an optional set and will not be graded.

Problems:

1. **The simplest quantum communication task.** In this question we investigate the simplest of quantum communication tasks: sending a classical bit using a qubit. Let's recruit our two favorite protagonists: Alice and Bob. Alice wants to send some information to Bob. Bob only accepts messages coming through their shared quantum communication device, which can prepare, send, receive and measure qubits. Imagine Alice wants to send a very simple message, that consists of a single bit $a \in \{0, 1\}$. In order to do this she encodes her binary value by preparing a qubit in the standard basis according to the encoding scheme

$$0 \longrightarrow |0\rangle$$
$$1 \longrightarrow |1\rangle$$

Let's further suppose, for now, that Bob knows that Alice sent a qubit encoded in the standard basis. Thus upon reception of Alice's qubit, Bob measures it in the standard basis. Let $b \in \{0, 1\}$ denote Bob's outcome. Let p_0 be the probability that $b = 0$, and p_1 the probability that $b = 1$.

   (a) Compute p_0 and p_1, first in the case that Alice's bit is $a = 0$ and then in case it is $a = 1$.

Suppose now that instead of encoding her bit a in the computational basis, Alice chooses to encode it in the Hadamard basis, so

$$0 \longrightarrow |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$1 \longrightarrow |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

This means that if Alice wants to send the bit 0 she sends the state $|+\rangle$ to Bob.

   (b) Assume that Bob is unaware of Alice's change of encoding scheme, so that he still measures in the standard basis. Compute p_0 and p_1 in both cases, $a = 0$ and $a = 1$.

   (c) In both scenarios we considered Alice attempts to send a classical bit to Bob by encoding it in a quantum state. However in only one of the scenarios Bob could reliably retrieve Alice's bit from the measurement he makes. Which of the two scenarios is this?

(d) Suppose Bob knows that Alice is encoding her bit in the Hadamard basis. Describe a unitary operation U such that if Bob applies U to the qubit he receives from Alice, and then measures it in the computational basis, he always obtains the correct outocme? (i.e. the outcome 0 when Alice sends a $|+\rangle$ state, and the outcome 1 when Alice sends a $|-\rangle$ state.)

Lastly, imagine that Alice's qubit preparation machine is somewhat broken and, when she asks it to prepare her qubit in the state $|0\rangle$ it actually prepares the state

$$|\phi\rangle = \frac{\sqrt{2}}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle$$

Now imagine Bob knows this, but his machine is also faulty and he can't correct for the error. The only thing he can do is decide to measure in either the standard basis or in the Hadamard basis.

(e) Which of Bob's two possible basis choices gives him the highest probability of obtaining the outcome 0, and what is the associated probability?

2. **Copying qubits.** Consider a unitary operation U that can copy the eigenstates of the standard basis. That is, U is a 4×4 unitary matrix such that $U(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$ and $U(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle$.

(a) Does such a U exist? If so, justify; if not, prove why not.

(b) Assume such a U does exist. Can you infer what vector it sends $|-\rangle|0\rangle$ to? Give a formal statement for the version of the "no-cloning theorem" that you have just proved.

(c) Suppose that $\{|\psi_1\rangle, |\psi_2\rangle\}$ are qubit states such that $0 < |\langle\psi_1|\psi_2\rangle| < 1$. Prove that there does not exist a U that satisfies $U(|\psi_i\rangle|0\rangle) = |\psi_i\rangle|\psi_i\rangle$ for $i \in \{1, 2\}$. *[Hint: this does not use the previous questions. Think about what you know of unitary matrices]* Deduce a second formal statement for a "no-cloning theorem", that matches what you just proved.

3. **The EPR pair.** Recall the definition of the EPR pair,

$$|\text{EPR}\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\big) .$$

Prove that there do not exist two single-qubit states $|\psi\rangle$ and $|\phi\rangle$ such that $|\text{EPR}\rangle = |\psi\rangle \otimes |\phi\rangle$. *[Hint: Reason by contradiction. Expand everything in the standard basis.]*

4. **State discrimination.**

Suppose you are given two single-qubit states, $|\psi_1\rangle$ 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

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

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 (1) 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 (1) 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 (1) 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 (1), as a function of the original states $|\psi_1\rangle$ and $|\psi_2\rangle$? What is the basis which achieves the optimum?