CS120, Quantum Cryptography, Fall 2016

Homework # 1 **due: 10:29AM, October 11th, 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.

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. (6 points) **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 a basis $\{|b_1\rangle, |b_2\rangle\}$ of $\mathbb{C}^2$ such that the expression

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

   is maximized.

   (b) 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 $\{|b_1'\rangle, |b_2'\rangle\}$.

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

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

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.)

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

(e) 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?

2. (8 points) **Improving Wiesner's quantum money.**

Consider the following six single-qubit states:

$$\left\{ |\psi_1\rangle = |0\rangle, |\psi_2\rangle = |1\rangle, |\psi_3\rangle = |+\rangle, |\psi_4\rangle = |-\rangle, |\psi_5\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}}, |\psi_6\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}} \right\}.$$

Suppose we create a money scheme in which each bit of a bill's serial number is encoded into one of these six states, chosen uniformly at random (so with probability 1/6 each) by the bank.

(a) Consider the attack on this scheme which attempts to copy the bill in the standard basis, using the unitary $U : |0\rangle|0\rangle \mapsto |0\rangle|0\rangle$, $U : |1\rangle|0\rangle \mapsto |1\rangle|1\rangle$. What is its success probability? Recall that the success probability is defined as

$$\sum_{k=1}^{6} \frac{1}{6} \left| \big(\langle\psi_k| \otimes \langle\psi_k| \big)\, U \big(|\psi_k\rangle \otimes |0\rangle \big) \right|^2.$$

What if we choose U to copy in the Hadamard basis instead?

(a) Can you improve on the attack described in the previous question? Give any attack that does better. [Bonus points: describe an attack with success probability 2/3.]

(b) Find a quantum money scheme which uses only four possible single-qubit states but is better than Wiesner's scheme (i.e. the scheme which uses the four states $\{|\psi_1\rangle = |0\rangle, |\psi_2\rangle = |1\rangle, |\psi_3\rangle = |+\rangle, |\psi_4\rangle = |-\rangle\}$), in the sense that the optimal attack has success probability $< 3/4$. (You do not need to prove completely formally that your scheme is better than Wiesner's, but describe the four states you would use, and argue why you think it would be better than Wiesner's.) *[Hint: Think about the Bloch sphere — use all the available space!]*

3. (10 points) **Quantum teleportation**

In class we saw that the no-cloning theorem forbids us from copying arbitrary quantum states, i.e. implementing a unitary U that takes $|\psi\rangle|0\rangle \to |\psi\rangle|\psi\rangle$ for any state $|\psi\rangle$.

(a) In general show that if there exists a unitary U taking $|\Psi\rangle \to |\Phi\rangle$, there must exist another unitary V independent of $|\Psi\rangle$ and $|\Phi\rangle$ that takes $|\Phi\rangle \to |\Psi\rangle$. In other words, no information is lost when applying a unitary to a quantum state.

(b) Suppose Alice holds a qubit in the state $|\psi\rangle = a|0\rangle + b|1\rangle$ and wants Bob to have that state as well. Why doesn't the following work? Alice measures her qubit in some basis of her choice, then prepares another qubit in the state she obtains and sends that to Bob. (Please answer without making explicit use of the no-cloning theorem.)

We now introduce a scheme by which Alice can prepare $|\psi\rangle$ on Bob's side without sending him her qubit—in fact, without sending any quantum information at all!—provided they share a Bell state. To be precise, the initial setup is as follows: Alice holds $|\psi\rangle_S$, and Alice and Bob each have a qubit of

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\big(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\big),$$

so that the joint state of all three qubits is

$$|\Psi\rangle_{SAB} = |\psi\rangle_S \otimes |\phi^+\rangle_{AB} = \big(a|0\rangle_S + b|1\rangle_S\big) \otimes \frac{1}{\sqrt{2}}\big(|00\rangle_{AB} + |11\rangle_{AB}\big). \tag{2}$$

(c) As with a single qubit, any state of a two-qubit system can be written in terms of an orthonormal basis, and also measured in such a basis. One example is the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Find a state $|\psi^-\rangle$ that, together with the following three states,

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}), \quad |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} - |11\rangle_{AB})$$
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB}),$$

$|\psi^-\rangle$ forms an orthonormal basis of the two-qubit space $\mathbb{C}^4$. This basis is called the *Bell basis*.

(d) Rewrite the joint state (2) as a linear combination of the form $\sum_{i=1}^4 |\alpha_i\rangle_{SA}|\beta_i\rangle_B$, where $|\alpha\rangle$ ranges over the four possible Bell states on Alice's two qubits S and A, and $|\beta\rangle$ is a single-qubit state on Bob's qubit.

(e) Suppose Alice measures her two qubits SA in the Bell basis and sends the result to Bob. Show that for each of the four possible outcomes, Bob can use this (classical!) information to determine a unitary, independent of $|\psi\rangle_S$, on his qubit that will map it, in all cases, to the original state $|\psi\rangle_B$ that Alice had.