QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F14)

Assignment 5
Due date: December 4, 2014

For any part of a question, you will receive 25% of the grade (rounded up to an integer) if you write "I DO NOT KNOW HOW TO ANSWER THIS QUESTION" instead of an answer.

1. **Correcting errors at known positions.** Here we consider error correcting codes for scenarios where, after the qubits have been transmitted, the location of the possible error is known (but not the error itself). Consider the 4-qubit quantum error correcting Code A with basis codewords

$$|c_0\rangle = \tfrac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle) \quad (1)$$
$$|c_1\rangle = \tfrac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle). \quad (2)$$

A qubit $\alpha|0\rangle + \beta|1\rangle$ is encoded as $\alpha|c_0\rangle + \beta|c_1\rangle$. This code does not protect against an arbitrary one-qubit error as the 9-qubit Shor code does. However, if, after the transmission of the codeword, we are given $k \in \{1, 2, 3, 4\}$ which is *the location* of the (potential) error but not the error itself then it is possible to correct it. For example, if $k = 3$ then we can assume that we received a state of the form $(I \otimes I \otimes U \otimes I)(\alpha|c_0\rangle + \beta|c_1\rangle)$ but we don't know what U (the error on qubit 3) is. Our goal is to recover $\alpha|c_0\rangle + \beta|c_1\rangle$ from this.

   (a) Show how Code A (described above) protects against I and X errors of known location. In other words, along with the four qubits, we are given $k \in \{1, 2, 3, 4\}$ and either I or X has been applied to the k^{th} qubit received (but we don't know which one). Show how to undo the error in this scenario. By the symmetry of $|c_0\rangle$ and $|c_1\rangle$, you may simply show how to undo the error in the case where $k = 4$; the other three cases would be very similar to explain.

   (b) Consider Code B, with basis codewords, $|c_0'\rangle = H^{\otimes 4}|c_0\rangle$ and $|c_1'\rangle = H^{\otimes 4}|c_1\rangle$, where $\alpha|0\rangle + \beta|1\rangle$ is encoded as $\alpha|c_0'\rangle + \beta|c_1'\rangle$. First, give explicit expressions for $|c_0'\rangle$ and $|c_1'\rangle$. Next, show how Code B protects against I and X errors (in the same sense that Code A does in part (a)).

   (c) Show how Code A protects against I, X, Z, and XZ errors of known location. (Hint: make use of the results established in parts (a) and (b).)

   (d) Show how Code A protects against any one-qubit unitary U error of known location. You may use the results from parts (a), (b) and (c) here.

2. **Searching when the fraction of marked items is** $1/4$ **and** $1/2$**.**

   (a) Suppose that $f : \{0,1\}^n \to \{0,1\}$ has the property that, for exactly $\frac{1}{4}2^n$ of the values of $x \in \{0,1\}^n$, $f(x) = 1$ and the goal is to find such an x. Show how to do this with a single query to f. (Hint: consider a single iteration of Grover's algorithm.)

   (b) Same question as part (a), except assume that f has the property that for exactly $\frac{1}{2}2^n$ of the values of $x \in \{0,1\}^n$, $f(x) = 1$. Can the x still be found with one query?

3. **Secret key encryption for qubits.** Recall the classical *one-time pad* encryption scheme restricted to a single bit. Alice wants to send a bit of information to Bob over a channel that is possibly being monitored by (eavesdropper) Eve. Alice and Bob share a secret key, which was set up in advance. The secret key is a randomly chosen (uniformly distributed) $k \in \{0,1\}$, which is known by Alice and Bob, but—importantly—not by Eve. If Alice wants to send a bit m to Bob then Alice computes $c = m \oplus k$ and sends c over the channel. When Bob receives c, he computes $m' = c \oplus k$. It is easy to show that $m' = m$ and Eve acquires no information about m from looking at c.

   Here, we consider a similar scenario, but where Alice wants to send a qubit $|\psi\rangle$ to Bob over a quantum channel that is possibly being monitored by Eve. How can this be accomplished so that if Eve performs a measurement on the data that goes through the channel, she cannot acquire any information about what $|\psi\rangle$ was?

   (a) If Alice and Bob share a classical secret key bit $k \in \{0,1\}$, then one approach is for Alice to send $X^k|\psi\rangle$ to Bob. This seems analogous to the classical protocol: Alice flips or doesn't flip according the key bit. Show that this is highly insecure by giving two quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$ whose encryptions Eve can perfectly distinguish.

   (b) Suppose that Alice and Bob have two (independently generated) key bits k_1, k_2, and Alice encrypts $|\psi\rangle$ as the state $Z^{k_1}X^{k_2}|\psi\rangle$. (Note that Bob can decrypt this since he has k_1 and k_2.) Show that this is perfectly secure. For the purposes of this question, you may prove this by showing that the scheme has the following property: for any two pure states $|\psi_0\rangle$ and $|\psi_1\rangle$, if Alice is encrypting either $|\psi_0\rangle$ or $|\psi_1\rangle$ and Eve can perform any measurement on the encrypted data, then Eve cannot distinguish between the two cases with probability better than $\frac{1}{2}$.

4. **Distributed testing of $|00\rangle + |11\rangle$ states.** Consider the scenario that arises in the Lo-Chau cryptosystem, where Alice and Bob share a two-qubit state and they want to test if it is $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with local measurements and classical communication.

   We consider the following procedure. They randomly select a measurement basis: with probability $\frac{1}{2}$, they both measure in the computational basis; and, with probability $\frac{1}{2}$, they both measure in the Hadamard basis. Then they perform the measurement and they accept if their outcomes are the same.

   (a) Show that the state $|\phi^+\rangle$ is always (i.e., with probability 1) accepted by this test.

   (b) Show that $|\phi^+\rangle$ is the *only* state that this test accepts with probability 1.

5. **Two noisy channels.** Consider these two noise models for a one-qubit channel. The first channel performs

$$\begin{cases} I & \text{with probability } 1-p \\ X & \text{with probability } p/3 \\ Y & \text{with probability } p/3 \\ Z & \text{with probability } p/3 \end{cases} \tag{3}$$

   and the second channel leaves its qubit intact with probability $1-q$ and replaces its qubit with one in state $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ with probability q. Show that, for all $q \in [0,1]$, there is a value of $p \in [0,1]$ for which the first channel is equivalent to the second one. Give an expression for p as a function of q.