QIC710/CS667/CO681/PH767/AM871 Introduction to Quantum Information Processing (F11)

Assignment 5
This can be submitted up until December 22

1. **Amplitude amplification.** Consider a generalization of the search problem where, we are given a black box computing $f : \{0,1\}^n \to \{0,1\}$, and the goal is to find $x_0 \in \{0,1\}^n$ such that $f(x_0) = 1$ (for simplicity, throughout this question, we assume this x_0 is unique). Suppose that we are given another black box computing an n-qubit "guessing" unitary operation W that helps guess a satisfying assignment to f in the following sense. The property of W is formally that $\langle x_0|W|0^n\rangle = \sqrt{p}$, for some number $p \in [0,1]$. This means that applying W to state $|0^n\rangle$ and then measuring in the computational basis results in x_0 with probability p. We could build a search algorithm based on this W that operates as follows: repeatedly use W to guess a value of x and for each guess make a query to f to determine if $f(x) = 1$. On average, the number of queries to f until x_0 is found is $1/p$ times. This search algorithm is more efficient than Grover's in cases were we happen to have a W with $p \gg \frac{1}{2^n}$.

   (a) Show that the n-qubit Hadamard transform is always a guessing unitary with parameter $p = 1/2^n$.

   (b) Show that $-WU_0W^\dagger U_f$ applies a rotation by angle $2\sin^{-1}(\sqrt{p})$ in the two dimensional space spanned by $|x_0\rangle$ and $W|0^n\rangle$. Here, as in Grover's algorithm, U_f is the unitary that maps $|x\rangle$ to $(-1)^{f(x)}|x\rangle$, and U_0 is the unitary that maps $|x\rangle$ to
   $$\begin{cases} -|x\rangle & \text{if } x = 0^n \\ \ \ |x\rangle & \text{if } x \neq 0^n. \end{cases} \tag{1}$$
   (Hint: use the property of two reflections being a rotation.)

   (c) Deduce from part (b) that x_0 can be found with constant probability using only $O(\sqrt{1/p})$ queries to U_f, W, and $W^\dagger$.

2. **Two noisy channels.** Consider these two noise models for a one-qubit channel. The first channel performs
   $$\begin{cases} I & \text{with probability } 1-p \\ X & \text{with probability } p/3 \\ Y & \text{with probability } p/3 \\ Z & \text{with probability } p/3 \end{cases} \tag{2}$$
   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.

3. **Correcting errors at known positions.** Here we consider error correcting codes in 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, which uses basis codewords $|c_0\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ and $|c_1\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)$. A qubit $\alpha|0\rangle + \beta|1\rangle$ is encoded as $\alpha|c_0\rangle + \beta|c_1\rangle$. It is easy to construct a quantum circuit that performs this encoding, but we are more interested in the error-correcting capabilities of this code. 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, whose basis codewords are $|c_0'\rangle = H^{\otimes 4}|c_0\rangle$ and $|c_1'\rangle = H^{\otimes 4}|c_1\rangle$. A qubit $\alpha|0\rangle + \beta|1\rangle$ is encoded as $\alpha|c_0'\rangle + \beta|c_1'\rangle$.

      i. Give explicit expressions for $|c_0'\rangle$ and $|c_1'\rangle$.

      ii. 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.

4. **Secret key encryption.** Recall the classical one-time pad encryption scheme restricted to a single bit. The scenario is that Alice wants to send a bit of information to Bob over a channel that is possibly being monitored by Eve (an eavesdropper). We assume that Alice and Bob share a secret key, which was set up in advance. The secret key is a randomly chosen (uniformly distributed) $k \in \{0, 1\}^n$, 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. We now 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 operations (including measurements) 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 would be for Alice to send $X^k|\psi\rangle$ to Bob. This seems analogous to the classical protocol: Alice either flips or doesn't flip the (qu)bit according to a random 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 between.

(b) Suppose that Alice and Bob have two (independently generated) key bits k_1, k_2, and Alice encrypts $|\psi\rangle$ $Z^{k_1}X^{k_2}|\psi\rangle$. (Note that Bob can decrypt this since he has k_1 and k_2.) Show that this is perfectly secure in the sense that, for any two quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$, Eve cannot distinguish *at all* between their encryptions.

5. **A nonlocal game.** Consider the following game where Alice and Bob are physically separated and their goal is to produce outputs that satisfy the winning conditions specified below. Alice and Bob receive $s, t \in \{0, 1, 2\}$ as input (s to Alice and t to Bob), at which point they are forbidden from communicating with each other (so Alice has no idea what t is and Bob has no idea what s is). They each output a bit, a for Alice and b for Bob. The winning conditions are:

- $a = b$ in the cases where $s = t$.
- $a \neq b$ in the cases where $s \neq t$.

(a) Show that any classical strategy (one that uses no quantum information anywhere) of Alie and Bob that always succeeds in the $s = t$ cases can succeed with probability at most $2/3$ in the $s \neq t$ cases.

(b) Give a quantum strategy (that is, one where Alice and Bob can create an entangled state before the game starts and then base their outcomes on their measurements of their parts of this state) that always succeeds in the $s = t$ cases and succeeds with probability $3/4$ in the $s \neq t$ cases. (Hint: try the entangled state $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$ and have Alice and Bob perform rotations depending on s and t respectively.)