

CPSC 599.36 Topics in Quantum Computing

Assignment 4

Due date: April 15

1. **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 a $k \in \{1, 2, 3, 4\}$ such that if an error did occur then it occurred in the k^{th} qubit then it is possible to correct the error. For example, if $k = 3$ then we know that we have 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 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), or (c) here.

2. **Basics of density matrices.** Up until now, we have represented the states of qubits as vectors of the form $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. An alternative way of representing the state of a qubit is in terms of its *density matrix*. The density matrix of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is defined to be

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{pmatrix}.$$

Density matrices also exist for the *probabilistic states* that were defined in question 4 of Assignment 2 (please refer to Assignment 2 for their definition). The technical term for such a state is a *mixed state* (and any state whose density matrix is of the form $|\psi\rangle\langle\psi|$ is called a *pure state*). For the mixed (i.e. probabilistic) state corresponding to p_1, \dots, p_k and $|\psi_1\rangle, \dots, |\psi_k\rangle$, the density matrix is defined to be

$$\rho = \sum_{i=1}^k p_i |\psi_i\rangle\langle\psi_i|.$$

- (a) For each density matrix, give a corresponding quantum state (which may be a pure or mixed state):

$$\frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad \frac{1}{4} \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$$

- (b) Referring to question 4 of Assignment 2, consider the state that Alice sends Bob, the state that Carol sends Bob and the state that Ted send Bob. Give the density matrix corresponding to each of these states.
- (c) If Bob receives a mixed state whose density matrix is ρ and applies a unitary U to this state, what is the density matrix of the resulting state? Give an expression for the new density matrix in terms of ρ and U .
Also, if Bob measures a mixed state whose density matrix is ρ , what are the outcome probabilities?
- (d) Using the information above, redo question 4(d) of Assignment 2 (it should be quite simple to do this in terms of density matrices).

3. **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) $k \in \{0, 1\}$, 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 $|\psi\rangle$ as $X^{k_1}Z^{k_2}|\psi\rangle$. (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.