Assignment 5
Due date: 11:59pm, December 5, 2023

1. **Diagnosing errors in the Shor code [12 points; 4 each].**
Suppose that you are given a Shor-code encoding of a state, which is of the form

$$\alpha_0\Big(\frac{|000\rangle+|111\rangle}{\sqrt{2}}\Big)\Big(\frac{|000\rangle+|111\rangle}{\sqrt{2}}\Big)\Big(\frac{|000\rangle+|111\rangle}{\sqrt{2}}\Big)$$
$$+\,\alpha_1\Big(\frac{|000\rangle-|111\rangle}{\sqrt{2}}\Big)\Big(\frac{|000\rangle-|111\rangle}{\sqrt{2}}\Big)\Big(\frac{|000\rangle-|111\rangle}{\sqrt{2}}\Big), \tag{1}$$

and a single qubit unitary error from the set $\{X, Y, Z\}$ is applied to this state. Is it possible to deduce what the error was? Here, *deduce the error* means construct some measurement procedure that does the following. The input to the procedure is the 9-qubit state that results after the error occurred. The output is a description of what the error was (such as "X was applied to qubit 7", or "Y was applied to qubit 3").

   (a) Show that if the error is an X-error then it is possible to determine on what qubit it was applied.

   (b) Show that if the error is a Z-error then it is impossible to determine on what qubit it was applied. You can show this by exhibiting two different Z-errors that have the same effect on the encoded state.

   (c) What happens in the case of Y-errors? Either show that: if the error is a Y-error then it is possible to determine on what qubit it was applied; or show that this is impossible by exhibiting two different Y-errors that have the same effect on the encoded state.

2. **Correcting erasure errors in the Steane code [10 points].**
It is possible to deduce that the Steane code can correct two erasure errors in various ways. Here we will analyze an aspect of this in concrete terms.

We begin with some discussion to set up this question. The Steane-code encoding of a one-qubit state $\alpha_0|0\rangle+\alpha_1|1\rangle$ is

$$\alpha_0\frac{1}{\sqrt{8}}\Big(|0000000\rangle+|1010101\rangle+|0110011\rangle+|1100110\rangle$$
$$+|0001111\rangle+|1011010\rangle+|0111100\rangle+|1101001\rangle\Big)$$
$$+\,\alpha_1\frac{1}{\sqrt{8}}\Big(|1111111\rangle+|0101010\rangle+|1001100\rangle+|0011001\rangle$$
$$+|1110000\rangle+|0100101\rangle+|1000011\rangle+|0010110\rangle\Big). \tag{2}$$

CONTINUED ON NEXT PAGE

Suppose that the first two qubits of this encoding state are lost—which can be modeled as being traced out. Our goal is to recover the data from the remaining five qubits. Tracing out the first two qubits produces the same mixed state that occurs if the first two qubits are measured in the computational basis but we do not see the classical part of the outcome.

To analyze the result of such a measurement process, it helps to rewrite the above encoded state as

$$\begin{aligned}
&\frac{1}{2}|00\rangle\left(\alpha_0|0\rangle\Big(\frac{|0000\rangle+|1111\rangle}{\sqrt{2}}\Big)+\alpha_1|1\rangle\Big(\frac{|1001\rangle+|0110\rangle}{\sqrt{2}}\Big)\right)\\
&+\frac{1}{2}|01\rangle\left(\alpha_0|1\rangle\Big(\frac{|0011\rangle+|1100\rangle}{\sqrt{2}}\Big)+\alpha_1|0\rangle\Big(\frac{|1010\rangle+|0101\rangle}{\sqrt{2}}\Big)\right)\\
&+\frac{1}{2}|10\rangle\left(\alpha_0|1\rangle\Big(\frac{|0101\rangle+|1010\rangle}{\sqrt{2}}\Big)+\alpha_1|0\rangle\Big(\frac{|1100\rangle+|0011\rangle}{\sqrt{2}}\Big)\right)\\
&+\frac{1}{2}|11\rangle\left(\alpha_0|0\rangle\Big(\frac{|0110\rangle+|1001\rangle}{\sqrt{2}}\Big)+\alpha_1|1\rangle\Big(\frac{|1111\rangle+|0000\rangle}{\sqrt{2}}\Big)\right). \qquad (3)
\end{aligned}$$

(It is straightforward to see that the states (2) and (3) are identical; please take a moment to convince yourself of this.)

Using the encoded state in form (3), it's easy to see that measuring the first two qubits results in one of these four states:

$$|\psi_{00}\rangle=\alpha_0|0\rangle\Big(\frac{|0000\rangle+|1111\rangle}{\sqrt{2}}\Big)+\alpha_1|1\rangle\Big(\frac{|1001\rangle+|0110\rangle}{\sqrt{2}}\Big) \qquad (4)$$

$$|\psi_{01}\rangle=\alpha_0|1\rangle\Big(\frac{|0011\rangle+|1100\rangle}{\sqrt{2}}\Big)+\alpha_1|0\rangle\Big(\frac{|1010\rangle+|0101\rangle}{\sqrt{2}}\Big) \qquad (5)$$

$$|\psi_{10}\rangle=\alpha_0|1\rangle\Big(\frac{|0101\rangle+|1010\rangle}{\sqrt{2}}\Big)+\alpha_1|0\rangle\Big(\frac{|1100\rangle+|0011\rangle}{\sqrt{2}}\Big) \qquad (6)$$

$$|\psi_{11}\rangle=\alpha_0|0\rangle\Big(\frac{|0110\rangle+|1001\rangle}{\sqrt{2}}\Big)+\alpha_1|1\rangle\Big(\frac{|1111\rangle+|0000\rangle}{\sqrt{2}}\Big). \qquad (7)$$

Now we can state the decoding problem that you are asked to solve:

Suppose that $|\alpha_0|^2+|\alpha_1|^2=1$, and you receive five qubits that are in one of the four states $|\psi_{00}\rangle$, $|\psi_{01}\rangle$, $|\psi_{10}\rangle$, $|\psi_{11}\rangle$. You have no information about what α_0 and α_1 are and no information about which of the four states you have received. Your goal is to construct the state $\alpha_0|0\rangle+\alpha_1|1\rangle$ from the five qubits that you receive. Explain how to do this with a quantum circuit that takes five qubits as input and produces an output state where the first qubit is in state $\alpha_0|0\rangle+\alpha_1|1\rangle$. Your circuit should use no ancilla qubits.

CONTINUED ON NEXT PAGE

3. **A key result that's used in the construction of CSS codes [9 points].**
Let $\mathcal{C}$ be any linear subspace of $\{0,1\}^m$ of dimension n (as a vector space over $\mathbb{Z}_2$). Define the *dual* of $\mathcal{C}$ as $\mathcal{C}^\perp = \{x \in \{0,1\}^m : \text{such that } x \cdot y = 0 \text{ for all } y \in \mathcal{C}\}$, where $x \cdot y = x_1 y_1 + \cdots + x_m y_m \bmod 2$. It is straightforward to prove that the dimension of $\mathcal{C}^\perp$ is $m - n$, and we can assume this here.

Prove that $H^{\otimes m}\Big(\frac{1}{\sqrt{2^n}} \sum_{x \in \mathcal{C}} |x\rangle\Big) = \frac{1}{\sqrt{2^{m-n}}} \sum_{y \in \mathcal{C}^\perp} |y\rangle$.

Hint: This can be calculated directly by expanding the definition of $H^{\otimes m}$. If you are stuck then an alternative approach is to use the fact that there exists an $n \times m$ generator matrix G for $\mathcal{C}$ such that $\mathcal{C} = \{zG : z \in \{0,1\}^n\}$.

4. **Searching when the fraction of marked items is $\frac{1}{4}$ [9 points].**
Let $n \geq 2$ and 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 your goal be to find such an $x \in \{0,1\}^n$ such $f(x) = 1$. You are given a black-box for computing f and no other other information about f (except that the fraction of 1s is $\frac{1}{4}$).

Note that there's a simple classical algorithm that finds such an x with high probability with few queries (because a random query succeeds with probability 1/4). What if we want to solve this problem *exactly* (i.e., with error probability 0)?

   (a) [3 points] Show that, for any classical algorithm, the number of f-queries required to solve this problem exactly is exponential in n.

   (b) [6] Show that there is a quantum algorithm that makes one single f-query and is guaranteed to find an $x \in \{0,1\}^n$ such $f(x) = 1$. (Hint: consider Grover's algorithm.)

5. **Distinguishing between $\frac{1}{4}$ and $\frac{3}{4}$ fraction of satisfying assignments [10 points].**
Suppose that $f : \{0,1\}^n \to \{0,1\}$ has the property that the number of $x \in \{0,1\}^n$ for which $f(x) = 1$ is either $\frac{1}{4}2^n$ or $\frac{3}{4}2^n$ and your goal is to determine which case it is.

You are given a black-box for computing f and no other other information about f (except you know that the fraction of 1s is either $\frac{1}{4}$ or $\frac{3}{4}$). Give a quantum algorithm that solves this problem *exactly* (i.e., with error probability 0) with *two* queries to f.

6. **GHZ game with different initial state [10 points; 5 each].**
Recall the GHZ game (section 8.2 of the lecture notes on *Quantum information theory* and video lecture 20). In that game, three physically separated players, Alice, Bob, and Carol, receive inputs bits r, s, t (respectively) such that $r \oplus s \oplus t = 0$. From this—and without communicating—they must produce output bits a, b, c (respectively) such that $a \oplus b \oplus c = r \vee s \vee t$. We saw that this was possible if they possess qubits whose joint state is of the form $\frac{1}{2}|000\rangle - \frac{1}{2}|011\rangle - \frac{1}{2}|101\rangle - \frac{1}{2}|110\rangle$.

   (a) What if the joint state is changed to $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$? Either show how they can succeed at the GHZ game using this state, or explain why they cannot.

   (b) What if the joint state is changed to $\frac{1}{2}|000\rangle - \frac{1}{2}|100\rangle - \frac{1}{2}|001\rangle + \frac{1}{2}|101\rangle$? Either show how they can succeed at the GHZ game using this state, or explain why they cannot.