1. Suppose you have a function \( f : \{0,1\}^n \to \{0,1\}^n \), where \( f(x) = f(y) \) if and only if \( x = y \oplus s \) for some \( s \in \{0,1\}^n \). (Here \( \oplus \) means addition mod 2 for each bit of the string.) Otherwise, there is no structure in terms of which input gets assigned to which output. Recall for standard basis states: 
\[
H^{\otimes n}|x\rangle = \sum_{y=0}^{2^n-1}(-1)^{x \cdot y}|y\rangle,
\]
where \( x \cdot y = \sum_{j=1}^n x_j y_j \) where \( x_j \) is the \( j \)th bit of \( x \) and \( y_j \) is the \( j \)th bit of \( y \).

(a) What is the classical query complexity of determining \( s \)?

(b) Suppose you have a unitary that acts as 
\[
U_f|0\rangle|0\rangle = |x\rangle|f(x)\rangle.
\]
(For this algorithm, it doesn’t matter how \( U_f \) acts on other standard basis states.) If we run the following algorithm:

\[
\text{(1)}
\]
What are the states at each point?

(c) If you can find \( O(n) \) (randomly chosen) \( z \) such that \( z \cdot s = 0 \), then can figure out \( s \). Use this fact to determine the quantum query complexity of learning \( s \).

2. I said that there is a similar code to the 3-qubit bit-flip code we looked at in class that corrects \( Z \) errors. The idea is to convert from the \( |0\rangle/|1\rangle \) view to a \( |+\rangle/|−\rangle \) view, since \( |+\rangle/|−\rangle \) are sensitive to \( Z \) errors, but the approach otherwise should be similar to the 3-qubit bit-flip code.

(a) Draw a circuit that encodes a qubit \( a|0\rangle + b|1\rangle \) into a 3-qubit state that corrects against \( Z \) errors. (Your circuit should use standard gates like \( H \), \( CNOT \), etc.)

(b) Show how to detect \( Z \) errors using two ancillary qubits, control operations, and a measurement of the ancillary qubits.

(c) What is the projective measurement that your circuit in part (b) accomplishes?
Hints on 1:

- $(a \oplus b) \cdot c \equiv a \cdot c + b \cdot c \mod 2$.
- There should be two standard basis states in superposition after the measurement of the second register.

Hints on 2:

- Convert the initial state to $|+\rangle/|\!\!-\rangle$ basis. Then think about how you can convert the $|+\rangle$ into $|++\rangle$ and the $|\!\!-\rangle$ into $|--\rangle$ similarly to what we do in the bit-flip case.