Problem 1

Assume we want to send qubits through some channel that can arbitrarily corrupt a single qubit by applying an $H$ (Hadamard) operation to that qubit. We would like to use Shor’s code to protect against this type of error. Let’s say we want to send the qubit $|–\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

A) What is the encoding of $|–\rangle$ in Shor’s code?

B) Assuming the channel introduces an $H$ error on one qubit of the coded state, describe how you can use Shor’s code to correct this error (Hint: express $H$ in terms of $X$ and $Z$).

Solution:

A) To find the encoding of $|–\rangle$, we simply write it in the computational basis and then replace $|0\rangle$ and $|1\rangle$ with their Shor code (logical) form:

$$|–\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow |–\rangle_L = \frac{1}{\sqrt{2}}(|0\rangle_L - |1\rangle_L)$$

Where:

$$|0\rangle_L = \frac{1}{2\sqrt{2}}(|00000000\rangle + |11111111\rangle)(|00000000\rangle + |11111111\rangle)(|00000000\rangle + |11111111\rangle)$$

$$|1\rangle_L = \frac{1}{2\sqrt{2}}(|00000000\rangle - |11111111\rangle)(|00000000\rangle - |11111111\rangle)(|00000000\rangle - |11111111\rangle)$$

We could expand the state further, and cancel terms (like $|00000000\rangle$), however this is not necessary, since we can work with the logical qubits.

B) We know that:

$$H = \frac{1}{\sqrt{2}}(X + Z)$$
Without loss of generality, we can assume that the $H$ error affects qubit 1. This makes our new state:

$$H_1 |\sim\rangle_L = \frac{1}{\sqrt{2}}(X_1 |\sim\rangle_L + Z_1 |\sim\rangle_L)$$

Now note that $|\sim\rangle_L$ is a state in the “no-error” subspace. The first term in the above superposition, $X_1 |\sim\rangle_L$, corresponds to a bit-flip error on the first qubit. The second term, $Z_1 |\sim\rangle_L$, corresponds to a phase error. But also note that a phase error means no bit-flip error.

We now simply run the procedure for detecting a bit flip error, followed by the procedure for detecting a phase flip error. Recall that detecting bit flip errors in Shor’s code is done by measuring the operators $Z_1Z_2, Z_2Z_3$ (these will detect an error among the first 3 qubits), $Z_3Z_4, Z_4Z_5$ (these will detect an error among the middle 3 qubits) and finally $Z_5Z_6, Z_7Z_8$ (these will detect an error among the last 3 qubits).

We first measure $Z_1Z_2$. When performing this measurement, the state will collapse to either $X_1 |\sim\rangle_L$ or to $Z_1 |\sim\rangle_L$. In the first case, the $Z_1Z_2$ measurement will return outcome $-1$ indicating that there is a bit flip among the first two qubits. If one then measures the $Z_2Z_3$ operator, it will return $+1$ indicating that there is no bit flip between qubits 2 and 3. This then implies a bit flip error on the first qubit, which we correct for. If the measurement outcome for $Z_1Z_2$ had been $+1$, the state would have collapsed to $Z_1 |\sim\rangle_L$ and the bit flip syndrome measurements would all have returned outcome $+1$, indicating no bit flips.

We now move on to phase flip errors. In this case we only measure two operators: $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$. The outcome of the first tells us whether a phase flip error occurred among the first 6 qubits, whereas the second tells us of a phase flip among the last 6 qubits. If the bit flip measurements detected a bit flip error, i.e. the state collapsed to $X_1 |\sim\rangle_L$, then the phase flip syndromes will indicate no error. We therefore need only correct for the bit flip on the first qubit, by applying $X_1$ to the state. On the other hand, if the bit flip measurements indicated no error, i.e. the state collapsed to $Z_1 |\sim\rangle_L$, then $X_1X_2X_3X_4X_5X_6$ would yield outcome $-1$ whereas $X_4X_5X_6X_7X_8X_9$ yields outcome $+1$. This tells us that there is a phase flip error among the first 3 qubits, which we can correct for by applying a $Z$ operation on any of the first 3 qubits.

The end result is that we have corrected for the Hadamard error.

**Problem 2**

**A)** Show that the three qubit bit flip code (spanned by $|000\rangle$ and $|111\rangle$) has the stabilizer generated by $Z_1Z_2$ and $Z_2Z_3$.

**B)** Now prove that indeed this code can correct flip errors on each of the three qubits by showing that every possible product of two elements from the error set $\{X_1, X_2, X_3\}$ anti-commutes with at least one of the generators, or is part of the stabilizer set.

**Solution:**

**A)** We know from the lectures that the stabilizer for the three qubit code is $S = \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$. To show that $g_1 = Z_1Z_2$ and $g_2 = Z_2Z_3$ are generators, we need only show that any element of $S$ can be written as a product of $g_1$’s and $g_2$’s. These two are already part of $S$, so let’s write the remaining elements...
as products of the generators. First we notice that:

\[ I = g_1 g_1 = g_2 g_2 \]

And additionally, we have:

\[ g_1 g_2 = (Z_1 Z_2)(Z_2 Z_3) = Z_1 Z_3 \]

So, we are done.

\[ B) \] If we take the product of an error set element with itself, we obtain identity, which is part of \( S \). Therefore, we must focus on products of distinct elements. These are: \( X_1 X_2, X_1 X_3, X_2 X_3 \). But notice that \( X_1 X_2 \) anti-commutes with \( Z_2 Z_3 \), \( X_1 X_3 \) anti-commutes with \( Z_1 Z_2 \) and \( Z_2 Z_3 \) and \( X_2 X_3 \) anti-commutes with \( Z_1 Z_2 \). The reason is that operators that act on different systems commute whereas those that act on the same system will anti-commute. As an example:

\[ \{X_1 X_3, Z_1 Z_2\} = (X_1 Z_1)Z_2 X_3 + (Z_1 X_1)Z_2 X_3 \]

But since \( XZ = -ZX \) (and in particular \( X_1 Z_1 = -Z_1 X_1 \)) we have:

\[ \{X_1 X_3, Z_1 Z_2\} = (X_1 Z_1)Z_2 X_3 - (X_1 Z_1)Z_2 X_3 = 0 \]

Thus the anti-commutator is 0. The same reasoning applies for the other cases as well.

**Problem 3**

Consider the following stabilizer generators:

<table>
<thead>
<tr>
<th>Generator</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IXZXX</td>
<td>( g_1 )</td>
</tr>
<tr>
<td>XIIXZ</td>
<td>( g_2 )</td>
</tr>
<tr>
<td>ZXIXZ</td>
<td>( g_3 )</td>
</tr>
<tr>
<td>ZZIXX</td>
<td>( g_4 )</td>
</tr>
</tbody>
</table>

These are the generators for the so-called 5-qubit code, which is capable of detecting and correcting any error on a single qubit. Since we know that any error can be expressed as \( E = aI + bX + cZ + dXZ \), it is sufficient to show that the code is able to detect and correct any \( X, Z \) or \( XZ \) error on each individual qubit. Prove this, by showing that every possible product of two elements from the set \( \{X_i, Z_i, (XZ)_i \mid i \in \{1, 2, 3, 4, 5\}\} \) anti-commutes with at least one of the generators, or is part of the stabilizer set.

**Solution:** Firstly, the product of any element from the set with itself results in identity which is contained in the stabilizer set. Now, consider the operator \( P_i Q_j \), where \( P, Q \in \{X, Z, XZ\} \) and \( i, j \in \{1, 2, 3, 4, 5\} \). Notice that for any choice of \( P \) and \( Q \), there will always exist a pair of indices \( i \) and \( j \) such that \( i < j \) and \( P_i Q_j \) anti-commutes with the first generator. This can be shown by simply running through the possibilities:

- \( P = X, Q = X \), take \( i = 1, j = 3 \).
• $P = X, Q = Z$, take $i = 1, j = 2$.
• $P = Z, Q = X$, take $i = 1, j = 3$.
• $P = Z, Q = Z$, take $i = 1, j = 2$.
• $P = X, Q = (XZ)$, take $i = 1, j = 2$.
• $P = (XZ), Q = X$, take $i = 1, j = 3$.
• $P = (XZ), Q = (XZ)$, take $i = 1, j = 3$.
• $P = (XZ), Q = Z$, take $i = 1, j = 2$.
• $P = Z, Q = (XZ)$, take $i = 1, j = 2$.

Now, we would like to show that for any $i, j, P$ and $Q$ there always exists a generator that anti-commutes with $P_i Q_j$. But notice that the other generators are cyclic shifts of the first generator. This means that for whatever $P_i Q_j$ we are considering, we can simply shift the first generator so that the corresponding operators acting on qubits $i$ and $j$ will anti-commute with $P_i Q_j$. The above result guarantees that such a shift is always possible. This implies that there always exists a generator which anti-commutes with $P_i Q_j$ and we are done.