Solution Set #1

Quantum Error Correction
Instructor: Daniel Gottesman

Problem #1. QECC Conditions and the 9-Qubit Code

a) There are 28 possibilities for each error E_a or E_b: X, Y, or Z on each of the 9 qubits or I. However, within each set of three qubits, all three qubits are the same, and all three blocks are the same, so we only need to separate the cases where both errors are the identity, one error is the identity, both errors act on the same qubit, both errors act on different qubits in the same block of three, and both errors act on different blocks of three. Below, X_k, Y_k, and Z_k refer to X, Y, and Z acting on the kth qubit.

Case I: $E_a = E_b = I$. In this case, clearly $\langle \psi_i | \psi_i \rangle = 1$, so $C_{II} = 1$.

Case II: $E_a = I$. We consider the subcases where $E_b = X_k, Y_k, Z_k$. It does not matter which qubit E_b acts on. In all three cases, $E_b \left(|000\rangle \pm |111\rangle \right)$ is orthogonal to $|000\rangle \pm |111\rangle$, so $C_{IX_k} = C_{IY_k} = C_{IZ_k} = 0$. Similarly, $C_{X_k I} = C_{Y_k I} = C_{Z_k I} = 0$.

Case III: E_a and E_b act on the same qubit; it does not matter which one. The first subcase is when $E_a = E_b$. Then normalization implies $C_{ab} = 1$, so $C_{X_k X_k} = C_{Y_k Y_k} = C_{Z_k Z_k} = 1$. The second subcase is when they are different, in which case $E_a^\dagger E_b$ is equal to $\pm i$ times another Pauli matrix X, Y, or Z. That brings us back to the second case, so the appropriate matrix entries are all zero:

$$C_{X_k Y_k} = C_{X_k Z_k} = C_{Y_k X_k} = C_{Y_k Z_k} = C_{Z_k X_k} = C_{Z_k Y_k} = 0. \tag{1}$$

Case IV: E_a and E_b act on different qubits in the same block of three. This is the most interesting case. First let us consider $E_a = X_k$, $E_b = X_{k'}$. Then $E_a \left(|000\rangle \pm |111\rangle \right)$ is orthogonal to $E_b \left(|000\rangle \pm |111\rangle \right)$, and similarly when $E_a = X_k$, $E_b = Y_{k'}$ (or vice-versa) and when $E_a = Y_k$, $E_b = Y_{k'}$. Thus we have

$$C_{X_k X_{k'}} = C_{X_k Y_{k'}} = C_{Y_k X_{k'}} = C_{Y_k Y_{k'}} = 0 \;\; (k \text{ and } k' \text{ in same block of 3}). \tag{2}$$

When $E_a = X_k$ or Y_k and $E_b = Z_k$ (or vice-versa), we again get 0, since $E_a \left(|000\rangle \pm |111\rangle \right)$ is also orthogonal to $|000\rangle \mp |111\rangle$. Thus

$$C_{X_k Z_{k'}} = C_{Y_k Z_{k'}} = C_{Z_k X_{k'}} = C_{Z_k Y_{k'}} = 0 \;\; (k \text{ and } k' \text{ in same block of 3}). \tag{3}$$

Finally, the subcase in which $E_a = Z_k$, $E_b = Z_{k'}$. Then

$$E_a \left(|000\rangle \pm |111\rangle \right) = E_b \left(|000\rangle \pm |111\rangle \right) = |000\rangle \mp |111\rangle, \tag{4}$$

so $C_{Z_k Z_{k'}} = 1$ when k and k' are in the same block of 3.

Case V: E_a and E_b act on different blocks of three. Using the logic of case II, we find that on each block of three, we always get an orthogonal state, so

$$C_{X_k X_{k'}} = C_{X_k Y_{k'}} = C_{X_k Z_{k'}} = C_{Y_k X_{k'}} = C_{Y_k Y_{k'}} = C_{Y_k Z_{k'}} = C_{Z_k X_{k'}} = C_{Z_k Y_{k'}} = C_{Z_k Z_{k'}} = 0. \tag{5}$$

Note that the answers we get never depended on which basis states $|\psi_i\rangle$ and $|\psi_j\rangle$ we used, as should be the case for a QECC.

b) From part a, the only off-diagonal matrix elements we had were $C_{Z_k Z_{k'}} = 1$ when k and k' are in the same block of 3. Therefore, we can leave I, X_k and Y_k as basis errors, and simply replace the Z_ks in each block of three by an appropriate linear combination of Z_ks. For instance, we may choose

$$\begin{aligned}
F_1 &= (Z_1 + Z_2 + Z_3)/3 && (6)\\
F_2 &= (Z_1 - Z_2)/2 && (7)\\
F_3 &= (Z_2 - Z_3)/2 && (8)\\
F_4 &= (Z_4 + Z_5 + Z_6)/3 && (9)\\
F_5 &= (Z_4 - Z_5)/2 && (10)\\
F_6 &= (Z_5 - Z_6)/2 && (11)\\
F_7 &= (Z_7 + Z_8 + Z_9)/3 && (12)\\
F_8 &= (Z_7 - Z_8)/2 && (13)\\
F_9 &= (Z_8 - Z_9)/2. && (14)
\end{aligned}$$

Then

$$C_{F_1 F_1} = C_{F_4 F_4} = C_{F_7 F_7} = 1, \qquad (15)$$

but

$$F_2|\psi_i\rangle = F_3|\psi_i\rangle = F_5|\psi_i\rangle = F_6|\psi_i\rangle = F_8|\psi_i\rangle = F_9|\psi_i\rangle = 0, \qquad (16)$$

so any matrix element C_{ab} including one of these six Fs is zero as well. The matrix elements between I, X, or Y and F_1, F_4, and F_7 remain zero, so this change of basis diagonalizes C_{ab}, giving us 6 zero eigenvalues.

Problem #2. Correcting Small Shifts

a) There are two ways to approach this problem using the techniques we have developed so far. One is to apply the quantum error correction conditions, and the other is to give an explicit syndrome measurement and decoding procedure. It is probably easier in this case to apply the QECC conditions (which in any case will point us towards a decoding procedure), so let us do that:

First, note that any state of the form $X^a Z^b|\overline{\psi_i}\rangle$ is a superposition (with whatever phase) of kets which are equal to a mod 3, and that furthermore, $X^a Z^b|\overline{0}\rangle$ are a mod 6 while $X^a Z^b|\overline{1}\rangle$ are $(a+3)$ mod 6. Thus, we find

$$\langle\overline{\psi_i}|Z^{-b}X^{-a}X^{a'}Z^{b'}|\overline{\psi_j}\rangle = M_{ibb'}\delta_{aa'}\delta_{ij} \qquad (17)$$

(using the fact that $X^\dagger = X^{-1}$ and $Z^\dagger = Z^{-1}$), so we need only verify that

$$\langle\overline{0}|Z^{b'-b}|\overline{0}\rangle = \langle\overline{1}|Z^{b'-b}|\overline{1}\rangle. \qquad (18)$$

This is easily done:

$$\begin{aligned}
\langle\overline{0}|Z^{b'-b}|\overline{0}\rangle &= \frac{1}{3}\left(\langle 0| + \langle 6| + \langle 12|\right)\left(|0\rangle + \omega^{6(b'-b)}|6\rangle + \omega^{12(b'-b)}|12\rangle\right) && (19)\\
&= \frac{1}{3}(1 + \omega^{6(b'-b)} + \omega^{12(b'-b)}) && (20)\\
&= \delta_{bb'} && (21)\\
\langle\overline{1}|Z^{b'-b}|\overline{1}\rangle &= \frac{1}{3}\left(\langle 3| + \langle 9| + \langle 15|\right)\left(\omega^{3(b'-b)}|3\rangle + \omega^{9(b'-b)}|9\rangle + \omega^{15(b'-b)}|15\rangle\right) && (22)\\
&= \frac{1}{3}(\omega^{3(b'-b)} + \omega^{9(b'-b)} + \omega^{15(b'-b)}) && (23)\\
&= \delta_{bb'}. && (24)
\end{aligned}$$

Both equations use the fact that $\omega^6 = \exp(2\pi i/3)$, so $1 + \omega^6 + \omega^{12} = 0$, and require that $|b' - b| \leq 2$, which follows from $b, b' \in \{-1, 0, +1\}$.

The original version of this problem asked if the code was degenerate or non-degenerate, but the question was removed since we hadn't yet had a chance to discuss the terms in class. However, we can see that since the errors all give orthogonal states, this is a non-degenerate code for these errors.

b) If the state experiences an error X^2, we will get a superposition of kets which are 2 mod 3. We will mistake these as having been generated by X^{-1}, which also gives 2 mod 3 kets, so we will correct by multiplying by an additional factor of X. This gives the overall error X^3, which takes $|\bar{0}\rangle$ to $|\bar{1}\rangle$ and $|\bar{1}\rangle$ to $|\bar{0}\rangle$. That is, the encoded qubit has experienced a bit flip error.

c) There are a number of possibilities, which can be generated by products of the operators X^6 and Z^6. We can directly check both of these operators leave the codewords unchanged, as do such combinations as $X^6 Z^6$ or X^{12}.

Problem #3. Quantum Secret Sharing

a) In order for a set A of people to be able to reconstruct the state, the overall encoding must have the property that it can correct for the erasure of the qubits held by people not in A. That is, A is an authorized set if the encoding corrects erasure errors for the qubits held by the complement $\{1, \dots, n\} \setminus A$ of A.

b) The set B of people has no information if the density matrix ρ_B held by the people in B is independent of the encoded state $|\psi\rangle$. If this is not true, then people in B can always gain some information about $|\psi\rangle$ by making an appropriate measurement that would partially distinguish $\rho_B(|\psi\rangle)$ from $\rho_B(|\phi\rangle)$ for some pair of states $|\psi\rangle$ and $|\phi\rangle$ with different density matrices ρ_B.

c) Let A and B be complementary sets. A is an authorized set iff the encoding corrects erasure errors on B, which by the quantum error correction conditions, is equivalent to saying $\mathrm{Tr}(\rho E)$ is independent of encoded state $|\psi\rangle$ for all operators E acting on B. (ρ is the global density matrix.). Since E acts only on B, $\mathrm{Tr}(\rho E) = \mathrm{Tr}_B(\rho_B E)$, and by choosing a basis of Es (e.g., $E = |i\rangle\langle j|$), we find that $\mathrm{Tr}_B(\rho_B E)$ is independent of $|\psi\rangle$ for all E iff ρ_B is independent of $|\psi\rangle$ for all E, which is the definition from part b of an unauthorized set. Thus A is authorized iff B is unauthorized.

d) If A is a set containing r people, the complement B has $n - r$ people. Since A is authorized iff B is unauthorized, we need that $r \geq k$ iff $n - r \leq k - 1$. Plugging in $r = k$, we find $n - k \leq k - 1$, so $n \leq 2k - 1$. Plugging in $r = k - 1$, we also get $n - k + 1 > k - 1$, or $n > 2k - 2$. Thus $n = 2k - 1$. These are the only allowed values for a pure state threshold quantum secret sharing scheme. Note that n must be odd.

In fact, quantum secret sharing schemes do exist for these parameters, and the construction uses quantum error-correcting codes, but we will not encounter the appropriate codes until later in the course.