Quantum Error Correction: Solution Set #1

It for Qubit
Lecturer: Daniel Gottesman

Wed., July 20, 2016

Problem #1. The 9-Qubit Code

All parts of this problem refer to the 9-qubit code using the error correction method discussed in lecture. X_i, Y_i, or Z_i represents X, Y, or Z applied to the ith qubit.

a) Which of the following errors can be corrected by the 9-qubit code: X_1X_3, X_2X_7, X_5Z_6, Z_5Z_6, Y_2Z_8, $X_2 + X_1X_3$, $X_1 + X_2X_7$?

Solution: The nine-qubit code can correct one bit flip error in each set of three qubits, plus one phase error. Also, two phase errors in the same set of three qubits act the same on the codewords, so do nothing to the state (the product is in the stabilizer). Thus, the code can correct X_2X_7, X_5Z_6, and Z_5Z_6. X_1X_3 cannot be corrected because it involves two bit flip errors in the same set of three, and Y_2Z_8 cannot be corrected because it involves two phase flip errors on different sets of three (the bit flip part of Y_2 can be corrected, however).

In addition, a QECC can correct any superposition of errors that it can correct. Since it can correct both X_1 and X_2X_7, it also corrects $X_1 + X_2X_7$. However, if given the superposition $X_2 + X_1X_3$, it will not correct that error.

b) Suppose we perform the usual error correction procedure on the 9-qubit code after one of the errors from part a has occurred. This returns us to an encoded state, but it may not be the correct encoded state. For those errors that cannot be corrected, calculate the operation that is performed on the encoded state. That is, if we start with $\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle$, what state do we end up with?

Solution: For X_1X_3, the error correction procedure notes that qubit number 2 is the misfit, and "corrects" it by performing the bit flip operation X_2. Thus, the net effect is to flip all of the first three qubits. Thus, the encoded $|\overline{0}\rangle$ state does not change (as $|000\rangle + |111\rangle$ becomes $|111\rangle + |000\rangle$), but the encoded $|\overline{1}\rangle$ state becomes $-|\overline{1}\rangle$ (as $|000\rangle - |111\rangle$ becomes $|111\rangle - |000\rangle$). That is, $\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle$ becomes $\alpha|\overline{0}\rangle - \beta|\overline{1}\rangle$; the logical operation is an encoded Z.

For Y_2Z_8, we can write $Y_2 = iX_2Z_2$. The code can correct X_2, but the residual phase error Z_2Z_8 cannot be corrected. (The factor i is an overall phase, which has no physical significance and does not count as an error.) The correction procedure notes that the phase on the middle block of three is different, and tries to fix it with a Z_5, say, making the overall error a $Z_2Z_5Z_8$. Thus, $|000\rangle + |111\rangle$ becomes $|000\rangle - |111\rangle$ on all three blocks and vice-versa, changing $|\overline{0}\rangle$ into $|\overline{1}\rangle$. This is a logical X operation: $\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle$ becomes $\beta|\overline{0}\rangle + \alpha|\overline{1}\rangle$.

When the error $X_2 + X_1X_3$ occurs, the measurement of the error syndrome always identifies X_2 as the error, which is only partially correct. After doing the "correction" with X_2, the overall operation is now $I + X_1X_2X_3$. We have already seen that the effect of $X_1X_2X_3$ is the logical phase flip. Thus, the final state is

$$(\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle) + (\alpha|\overline{0}\rangle - \beta|\overline{1}\rangle) = |\overline{0}\rangle \qquad (1)$$

(up to normalization).

c) For the 9-qubit code, calculate the matrix C_{ab} for the QECC conditions, $\langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = C_{ab}\delta_{ij}$, where E_a and E_b run over the identity and the single-qubit Pauli matrices. (You may wish to lump together cases related by some straightforward symmetry.)

Solution: 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, $C_{X_kI} = C_{Y_kI} = C_{Z_kI} = 0$.

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 $C_{X_kX_k} = C_{Y_kY_k} = C_{Z_kZ_k} = 1$. 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:

$$C_{X_kY_k} = C_{X_kZ_k} = C_{Y_kX_k} = C_{Y_kZ_k} = C_{Z_kX_k} = C_{Z_kY_k} = 0. \tag{2}$$

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

$$C_{X_kX_{k'}} = C_{X_kY_{k'}} = C_{Y_kX_{k'}} = C_{Y_kY_{k'}} = 0 \quad (k \text{ and } k' \text{ in same block of 3}). \tag{3}$$

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

$$C_{X_kZ_{k'}} = C_{Y_kZ_{k'}} = C_{Z_kX_{k'}} = C_{Z_kY_{k'}} = 0 \quad (k \text{ and } k' \text{ in same block of 3}). \tag{4}$$

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

$$E_a\left(|000\rangle \pm |111\rangle\right) = E_b\left(|000\rangle \pm |111\rangle\right) = |000\rangle \mp |111\rangle, \tag{5}$$

so $C_{Z_kZ_{k'}} = 1$ 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

$$C_{X_kX_{k'}} = C_{X_kY_{k'}} = C_{X_kZ_{k'}} = C_{Y_kX_{k'}} = C_{Y_kY_{k'}} = C_{Y_kZ_{k'}} = C_{Z_kX_{k'}} = C_{Z_kY_{k'}} = C_{Z_kZ_{k'}} = 0. \tag{6}$$

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.

d) Diagonalize C_{ab} for the 9-qubit code, and give a basis of errors for which the matrix is diagonal.

Solution: From part c, 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

$$\begin{aligned}
F_1 &= (Z_1 + Z_2 + Z_3)/3 && (7)\\
F_2 &= (Z_1 - Z_2)/2 && (8)\\
F_3 &= (Z_2 - Z_3)/2 && (9)\\
F_4 &= (Z_4 + Z_5 + Z_6)/3 && (10)\\
F_5 &= (Z_4 - Z_5)/2 && (11)\\
F_6 &= (Z_5 - Z_6)/2 && (12)\\
F_7 &= (Z_7 + Z_8 + Z_9)/3 && (13)\\
F_8 &= (Z_7 - Z_8)/2 && (14)\\
F_9 &= (Z_8 - Z_9)/2. && (15)
\end{aligned}$$

Then

$$C_{F_1 F_1} = C_{F_4 F_4} = C_{F_7 F_7} = 1, \qquad (16)$$

but

$$F_2|\psi_i\rangle = F_3|\psi_i\rangle = F_5|\psi_i\rangle = F_6|\psi_i\rangle = F_8|\psi_i\rangle = F_9|\psi_i\rangle = 0, \qquad (17)$$

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. Quantum Secret Sharing

A quantum secret sharing scheme is an encoding of a quantum state which splits it among n people such that for any set of people, either that set of people can reconstruct the encoded quantum state, or that set of people by themselves have no information about the state. (Note that this must be true for encodings of all superpositions as well as the basis states.) More concretely, imagine that we encode a state in $N \geq n$ qubits and give qubits $a_{i-1}+1, \ldots, a_i$ to person i ($i = 1, \ldots, n$, $a_0 = 0$), so person i gets $a_i - a_{i-1}$ qubits. In general, we might allow the procedure to throw away qubits, but for this problem, consider the case with $a_n = N$; we call this a *pure state encoding.*

a) Some sets A of people should be able to reconstruct the encoded state; we call these *authorized sets.* Formulate this condition precisely in terms of correcting erasure errors.

Solution: 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 $\{1, \ldots, n\} \setminus A$ of A.

b) Other sets B of people should have no information about the original encoded state; these are the *unauthorized sets.* Formulate this condition precisely in terms of the density matrix ρ_B jointly held by the people in set B.

Solution: 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) Show that for a pure state quantum secret sharing scheme, a set B is an unauthorized set iff its complement $\{1, \ldots, n\} \setminus B$ is an authorized set.

Solution: 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) In a *threshold scheme*, whether a set is authorized or unauthorized depends only on the number of people in the set: If there are $\geq k$ people in the set, it is authorized, and if there are $< k$ people, the set is unauthorized. For a pure state quantum secret sharing scheme, figure out the possible values for k and n based on part c. (It turns out that all of these values are actually achievable.)

Solution: 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.

e) Consider the following method of encoding 1 qutrit (a 3-dimensional Hilbert space) in 3 qutrits:

$$|0\rangle \mapsto |000\rangle + |111\rangle + |222\rangle \tag{18}$$

$$|1\rangle \mapsto |012\rangle + |120\rangle + |201\rangle \tag{19}$$

$$|2\rangle \mapsto |021\rangle + |210\rangle + |102\rangle. \tag{20}$$

Give one qutrit to each person. (If you prefer to formulate this in terms of qubits, imagine giving each person two qubits, with $|0\rangle \rightarrow |00\rangle$, $|1\rangle \rightarrow |01\rangle$, and $|2\rangle \rightarrow |10\rangle$.) Show that this gives a threshold quantum secret sharing scheme. What are k and n?

Solution: Clearly $n = 3$. This is a pure state scheme, so if it is a quantum secret sharing scheme, it must have $k = 2$. In order for sets of size 2 to be authorized, the density matrix of a single share must be independent of the encoded state. Indeed, this is so: For any basis state (and therefore for any superposition of basis states), for any of the three shares, the density matrix of the share is a uniform mixture of $|0\rangle$, $|1\rangle$, and $|2\rangle$, the maximally mixed state. This also shows that sets of size 1 are not authorized: a single share has no information about the encoded state so it is certainly not possible to reconstruct the input state from one share.

f) Prove that there cannot exist a threshold quantum secret sharing scheme (pure or not) with $k \leq n/2$.

Solution: Suppose there were such a quantum secret sharing scheme. Then we could take a qubit, encode it using this scheme, and separate the qubits into two sets of k shares each, possibly with some qubits left over. A set of k shares is authorized, so for each of those two sets we could reconstruct the original secret qubit without touching the other set. This would give us two copies of the input qubit, a violation of the no-cloning theorem.