Solution Set #2

Quantum Error Correction
Instructor: Daniel Gottesman

Problem #1. Distance 2 Stabilizer Codes

a) A distance 2 code should be able to detect a single X, Y, or Z error on any qubit, so we need generators that anticommute with all of these. For instance, we can use $X \otimes X \otimes X \otimes X$ and $Z \otimes Z \otimes Z \otimes Z$: The first will anticommute with Z, the second will anticommute with X, and both will anticommute with Y, allowing us to detect all three types of errors. There are two generators, so this is a $[[4, 2, 2]]$ code as desired.

We can choose logical Z operators $\overline{Z}_1 = Z \otimes Z \otimes I \otimes I$ and $\overline{Z}_2 = Z \otimes I \otimes Z \otimes I$. These both commute with the stabilizer, so are valid logical operations. Note that two other obvious choices $I \otimes I \otimes Z \otimes Z$ and $I \otimes Z \otimes I \otimes Z$ are equivalent to $\overline{Z}_1$ and $\overline{Z}_2$, respectively, by multiplication by an element of the stabilizer, while $I \otimes Z \otimes Z \otimes I = \overline{Z}_1 \overline{Z}_2$ (and $Z \otimes I \otimes I \otimes Z$ is equivalent to it).

Therefore our logical basis states should be eigenstates of the two generators of the stabilizer and of $\overline{Z}_1$ and $\overline{Z}_2$ (with eigenvalues $+1$ for the stabilizer generators and different eigenvalues, depending on the basis state, for the other two operators). Thus:

$$|\overline{00}\rangle = |0000\rangle + |1111\rangle \quad (1)$$
$$|\overline{10}\rangle = |0101\rangle + |1010\rangle \quad (2)$$
$$|\overline{01}\rangle = |0011\rangle + |1100\rangle \quad (3)$$
$$|\overline{11}\rangle = |0110\rangle + |1001\rangle \quad (4)$$

b) As in part a, we need generators that anticommute with X, Y, and Z on each qubit. For the $n = 2k$ codes, we can just take the straightforward generalization of the $[[4, 2, 2]]$ code: $X^{\otimes n}$ and $Z^{\otimes n}$. These two operators commute, so this is a valid stabilizer code, with parameters $[[2k, 2k - 2, 2]]$, as desired.

However, for $n = 2k + 1$, these operators do not commute. We can still take $X^{\otimes n}$ as one generator, allowing us to detect Y or Z on any qubit, but for our second generator we are stuck with something like $Z^{\otimes(n-1)}$, which commutes with the first generator (since $n - 1$ is even), but only detects X errors on the first $n - 1$ qubits. We need a third generator, such as $Z_{n-1}Z_n$ (Z operators acting only the last two qubits). Since there are three generators, the parameters of the code are $[[2k + 1, 2k - 2, 2]]$.

c) As in the solution to part b, the problem with a $[[3, 1, 2]]$ stabilizer code is the failure to commute of possible generators. We are only allowed to choose two generators to still have one encoded qubit, and at least one of those two generators must anticommute with X, Y, and Z on each qubit. Consider the possibilities for how the generators can act on a particular qubit:

- The two generators act as I on this qubit. Then neither anticommutes with X, Y, or Z.
- One generator acts as I, while the other acts as X. Then we can detect Y and Z on this qubit, but not X. Similarly if the second generator acts as Y or Z — there will always be one Pauli matrix which cannot be detected.
- The two generators act as the same non-trivial Pauli matrix, for instance X. In this case, both will commute with X, so we again cannot detect X.

- The two generators act as different non-trivial Pauli matrices on the qubit. In this case, we can detect all three possibilities, X, Y, and Z, on this qubit.

This tells us that each generator must act non-trivially on all three qubits, and that the two generators act differently on each qubit. But different Pauli matrices anticommute, so the overall phase produced by trying to commute one generator past the other is thus $(-1)^3 = -1$, and the generators would have to commute. We thus cannot find a stabilizer code with parameters $[[3, 1, 2]]$.

Problem #2. The 9-Qubit Code as a CSS Code

a) We can just copy the parity check matrices from the stabilizer:

$$H_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \tag{5}$$

$$H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{6}$$

The generator matrices are then the duals of these two matrices, which we can find by choosing orthogonal vectors. We know they should have three and seven rows, respectively.

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \tag{7}$$

$$G_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \tag{8}$$

Notice that the rows of H_1 are also rows of G_2 ($C_1^\perp \subseteq C_2$) and that the rows of H_2 are within the span of the rows of G_1 ($C_2^\perp \subseteq C_1$), as had to be true for a CSS code.

b) C_1 has distance $d_1 = 3$, as is clear from the generator matrix: all codewords have weight which is a multiple of 3. C_2, however, has distance $d_2 = 2$, as is also clear from the generator matrix. There are no codewords of weight only 1, but there are many of weight 2. Thus, $\min(d_1, d_2) = 2$.

However, the 9-qubit code has distance 3 because it is degenerate. The phase errors which take us from one classical codeword in C_2 to another act the same on the quantum code because their product is in the stabilizer. You can see that the weight two codewords in G_2 are all also in H_1.

Problem #3. Stabilizer Entangled States

a) Let us start with $|00\rangle + |11\rangle$. We note that both kets in the superposition have even parity, so this state is a $+1$ eigenstate of $Z \otimes Z$. It is also invariant when we flip both qubits, so is a $+1$ eigenstate of $X \otimes X$. Thus, the stabilizer is generated by $\langle Z \otimes Z,\ X \otimes X \rangle$.

For $|00\rangle - |11\rangle$, we can use the same operators, but the eigenvalue of $X \otimes X$ is -1 instead of $+1$. Thus the stabilizer is $\langle Z \otimes Z,\ -X \otimes X \rangle$.

Similarly, $|01\rangle + |10\rangle$ has eigenvalues -1 and $+1$ for these two operators, so the stabilizer is $\langle -Z \otimes Z,\ X \otimes X \rangle$. $|01\rangle - |10\rangle$ has eigenvalue -1 for both, so its stabilizer is $\langle -Z \otimes Z,\ -X \otimes X \rangle$.

The state $|010\rangle - |101\rangle$ has even parity for the first and third qubits, so is a $+1$ eigenstate of $Z \otimes I \otimes Z$. It has uniformly odd parity for the first two qubits, so is a -1 eigenstate of $Z \otimes Z \otimes I$, and is similarly a -1 eigenstate of $I \otimes Z \otimes Z$. However, this third operator is just the product of the first two, so is not independent. For the third generator of the stabilizer, we go to $X \otimes X \otimes X$, which has eigenvalue -1 for this state. Thus, the complete stabilizer is $\langle -Z \otimes Z \otimes I, Z \otimes I \otimes Z, -X \otimes X \otimes X \rangle$.

b) Clearly S_A is Abelian, since it is a subset of S, and clearly it does not contain -1, again since $S_A \subseteq S$. We need only show S_A is closed under multiplication, making it a group. But S is a group, so if $P_A \otimes I_B \in S$ and $Q_A \otimes I_B \in S$, then $P_A Q_A \otimes I_B I_B \in S$, and this product has the desired form, so $P_A Q_A \in S_A$.

c) The projector onto the code space of a stabilizer S is $\sum_{M \in S} M/2^r$, and the density matrix of a pure state is just the projector onto its one-dimensional subspace, so the density matrix of the full stabilizer state is $\rho = \sum_{M \in S} M/2^n$. Then the density matrix ρ_A of the qubits in set A is given by the partial trace over B:

$$\rho_A = \mathrm{Tr}_B \left(\frac{1}{2^n} \sum_{M \in S} M \right) = \frac{1}{2^n} \sum_{M \in S} \mathrm{Tr}_B\, M. \tag{9}$$

But $\mathrm{Tr}_B\, M = M_A (\mathrm{Tr}_B\, M_B)$, where $M = M_A \otimes M_B$, M_A acting on A, M_B acting on B. The non-trivial Pauli matrices are traceless, so $\mathrm{Tr}_B\, M = 0$ unless $M = M_A \otimes I_B$, which also means $M_A \in S_A$. Thus, the sum is just a sum over elements of S_A:

$$\rho_A = \frac{1}{2^n} \sum_{M_A \in S_A} M_A\, \mathrm{Tr}_B\, I_B = \frac{1}{2^{n_A}} \sum_{M_A \in S_A} M_A, \tag{10}$$

where n_A is the number of qubits in A. (Note that we do not have to worry about M_A appearing more than once, since $M_A \otimes I$ can itself only appear once in S.)

This density matrix ρ_A in general no longer represents a pure state, since S_A might have fewer than n_A generators. However, $\Pi_A = \sum_{M_A \in S_A} M_A/2^{r_A}$ (where r_A is the number of generators of S_A) is the projector onto the subspace $T(S_A)$, and $\rho_A = \Pi_A / 2^{n_A - r_A}$, which is the uniform mixture over states in the subspace.