Solution Set #3

CO 639: Quantum Error Correction
Instructor: Daniel Gottesman

Due Tues., Feb. 24

Problem 1. Clifford Group Manipulations

a) We wish to calculate (C-U)P(C-U†), where C-U is either the controlled-Z gate or the controlled-Y gate, and P runs over $X \otimes I$, $I \otimes X$, $Z \otimes I$, and $I \otimes Z$.

We can see that C-Z, which is a diagonal matrix, commutes with $Z \otimes I$ and $I \otimes Z$, which are also both diagonal. C-Z also acts the same way on the first or second qubit (phase of -1 iff both are 1), so we only need calculate its action on $X \otimes I$. We do so by considering the overall matrix acting on a basis state (keeping close attention to phases):

$$\begin{aligned} (\text{C-Z})(X \otimes I)(\text{C-Z})|a,b\rangle &= (-1)^{ab}(\text{C-Z})(X \otimes I)|a,b\rangle && (1)\\ &= (-1)^{ab}(\text{C-Z})|a \oplus 1, b\rangle && (2)\\ &= (-1)^{ab+(a\oplus 1)b}|a \oplus 1, b\rangle && (3)\\ &= (-1)^{b}|a \oplus 1, b\rangle. && (4) \end{aligned}$$

We can recognize this matrix action as $X \otimes Z$. Thus, under C-Z:

$$\begin{aligned} X \otimes I &\rightarrow X \otimes Z && (5)\\ Z \otimes I &\rightarrow Z \otimes I && (6)\\ I \otimes X &\rightarrow Z \otimes X && (7)\\ I \otimes Z &\rightarrow I \otimes Z. && (8) \end{aligned}$$

Thus, the C-Z gate is in the Clifford group.

We have to do a bit more work to calculate the behavior of the C-Y gate. It commutes with $Z \otimes I$, but not with $X \otimes I$:

$$\begin{aligned} (\text{C-Y})(X \otimes I)(\text{C-Y})|a,b\rangle &= i^a(-1)^{ab}(\text{C-Y})(X \otimes I)|a,b \oplus a\rangle && (9)\\ &= i^a(-1)^{ab}(\text{C-Y})|a \oplus 1, b \oplus a\rangle && (10)\\ &= i^{a+(a\oplus 1)}(-1)^{ab+(a\oplus 1)(a\oplus b)}|a \oplus 1, b \oplus 1\rangle && (11)\\ &= i(-1)^{b}|a \oplus 1, b \oplus 1\rangle. && (12) \end{aligned}$$

The last equality follows because one of a and $(a \oplus 1)$ is always 0 and the other is 1. This operation is identifiable as $X \otimes Y$. For $I \otimes X$:

$$\begin{aligned} (\text{C-Y})(I \otimes X)(\text{C-Y})|a,b\rangle &= i^a(-1)^{ab}(\text{C-Y})(I \otimes X)|a,b \oplus a\rangle && (13)\\ &= i^a(-1)^{ab}(\text{C-Y})|a, b \oplus a \oplus 1\rangle && (14)\\ &= i^{2a}(-1)^{ab+a(b\oplus a\oplus 1)}|a, b \oplus 1\rangle && (15)\\ &= (-1)^{a}|a, b \oplus 1\rangle. && (16) \end{aligned}$$

We can thus identify this operation as $Z \otimes X$. Finally, for $I \otimes Z$:

$$\begin{aligned}
(\text{C-Y})(I \otimes Z)(\text{C-Y})|a,b\rangle &= i^a(-1)^{ab}(\text{C-Y})(I \otimes Z)|a, b \oplus a\rangle && (17)\\
&= i^a(-1)^{ab+(a\oplus b)}(\text{C-Y})|a, b \oplus a\rangle && (18)\\
&= i^{2a}(-1)^{ab+(a\oplus b)+a(a\oplus b)}|a,b\rangle && (19)\\
&= (-1)^{a+b}|a,b\rangle. && (20)
\end{aligned}$$

This is $Z \otimes Z$. Thus, under C-Y:

$$\begin{aligned}
X \otimes I &\rightarrow X \otimes Y && (21)\\
Z \otimes I &\rightarrow Z \otimes I && (22)\\
I \otimes X &\rightarrow Z \otimes X && (23)\\
I \otimes Z &\rightarrow Z \otimes Z. && (24)
\end{aligned}$$

Thus, C-Y is also in the Clifford group.

b) We start with the standard values for the $\overline{X}$s and $\overline{Z}$s:

$$\begin{array}{ll}
\overline{X}_1 & X \otimes I \otimes I\\
\overline{X}_2 & I \otimes X \otimes I\\
\overline{X}_3 & I \otimes I \otimes X\\
\overline{Z}_1 & Z \otimes I \otimes I\\
\overline{Z}_2 & I \otimes Z \otimes I\\
\overline{Z}_3 & I \otimes I \otimes Z.
\end{array} \tag{25}$$

After the first CNOT gate, we have:

$$\begin{array}{ll}
\overline{X}_1 & X \otimes I \otimes I\\
\overline{X}_2 & X \otimes X \otimes I\\
\overline{X}_3 & I \otimes I \otimes X\\
\overline{Z}_1 & Z \otimes Z \otimes I\\
\overline{Z}_2 & I \otimes Z \otimes I\\
\overline{Z}_3 & I \otimes I \otimes Z.
\end{array} \tag{26}$$

After the Hadamard gate, we have:

$$\begin{array}{ll}
\overline{X}_1 & X \otimes I \otimes I\\
\overline{X}_2 & X \otimes Z \otimes I\\
\overline{X}_3 & I \otimes I \otimes X\\
\overline{Z}_1 & Z \otimes X \otimes I\\
\overline{Z}_2 & I \otimes X \otimes I\\
\overline{Z}_3 & I \otimes I \otimes Z.
\end{array} \tag{27}$$

After the first C-Z gate, we have:

$$\begin{array}{ll}
\overline{X}_1 & X \otimes I \otimes I\\
\overline{X}_2 & X \otimes Z \otimes I\\
\overline{X}_3 & I \otimes Z \otimes X\\
\overline{Z}_1 & Z \otimes X \otimes Z\\
\overline{Z}_2 & I \otimes X \otimes Z\\
\overline{Z}_3 & I \otimes I \otimes Z.
\end{array} \tag{28}$$

After the second C-Z gate, we have:

$$\begin{array}{ll}
\overline{X}_1 & X \otimes Z \otimes I\\
\overline{X}_2 & X \otimes I \otimes I\\
\overline{X}_3 & I \otimes Z \otimes X\\
\overline{Z}_1 & I \otimes X \otimes Z\\
\overline{Z}_2 & Z \otimes X \otimes Z\\
\overline{Z}_3 & I \otimes I \otimes Z.
\end{array} \tag{29}$$

And then, after the final CNOT, we have:

$$\begin{array}{ll} \overline{X}_1 & X \otimes Z \otimes X \\ \overline{X}_2 & X \otimes I \otimes X \\ \overline{X}_3 & I \otimes Z \otimes X \\ \overline{Z}_1 & Z \otimes X \otimes Z \\ \overline{Z}_2 & I \otimes X \otimes Z \\ \overline{Z}_3 & Z \otimes I \otimes Z. \end{array} \tag{30}$$

c) We notice that the initial state $|000\rangle$ maps to a +1-eigenstate of the three final $\overline{Z}$ operators, namely $(|000\rangle + |010\rangle)/\sqrt{2}$. Thus, the first column of the matrix has entries $1/\sqrt{2}$ in the 000 and 010 rows and is 0 elsewhere. Applying the $\overline{X}$ operators, we get the other columns:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}. \tag{31}$$

d) The evolution of $\overline{X}$ is the same as the $\overline{X}_1$ above, and the evolution of $\overline{Z}$ is the same as $\overline{Z}_1$ above. The stabilizer generator $I \otimes X \otimes X$ becomes $X \otimes Z \otimes I$, and the generator $I \otimes Z \otimes Z$ becomes $Z \otimes X \otimes I$. Thus, we find:

$$\overline{X} \rightarrow X \otimes Z \otimes X = I \otimes I \otimes X \tag{32}$$

$$\overline{Z} \rightarrow Z \otimes X \otimes Z = I \otimes I \otimes Z. \tag{33}$$

That is, the logical qubit ends up in the third register after this circuit.

Problem 2. Generating the Clifford Group

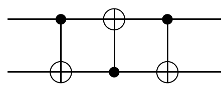
a) This follows immediately from a lemma I proved in class: If we let u_i be the $2n$-bit binary vector corresponding to $\overline{X}_i$ and v_i be the $2n$-bit binary vector corresponding to $\overline{Z}_i$, then there exists a $2n$-bit binary vector w with symplectic inner product s_i with u_i and symplectic inner product t_i with v_i. Then the Pauli operator E corresponding to w changes the phases of $\overline{X}_i \mapsto (-1)^{s_i}\overline{X}_i$ and $\overline{Z}_i \mapsto (-1)^{t_i}\overline{Z}_i$. Then if U changes $X_i \mapsto \overline{X}_i$, $Z_i \mapsto \overline{Z}_i$, then EU is the desired Clifford group operation.

b) We start with H ($X \mapsto Z$, $Y \mapsto -Y$, and $Z \mapsto X$) and P ($X \mapsto Y$, $Y \mapsto -X$, and $Z \mapsto Z$). These perform the permutations (13) and (12) on the ordered set (X, Y, Z). These two permutations generate all of S_3, so the other 4 are definitely possible. I give explicit constructions below:

- (): No change; this is the identity operation.
- (23): HPH, maps $X \mapsto X$, $Z \mapsto -Y$ (so $Y \mapsto Z$). Call this gate Q.
- (123): HP, maps $X \mapsto -Y$, $Z \mapsto X$ (so $Y \mapsto Z$). Call this gate T.
- (132): PH, maps $X \mapsto Z$, $Z \mapsto Y$ (so $Y \mapsto X$). This gate is equal to XT^2.

Also note that $P^2 = Z$, $HP^2H = X$, and $HP^2HP^2 = -iY$.

c) The SWAP gate is constructed via the following circuit:



We follow the evolution of $\overline{X}_i$ and $\overline{Z}_i$ as follows:

$$\begin{array}{cc} \overline{X}_1 & X \otimes I \\ \overline{X}_2 & I \otimes X \\ \overline{Z}_1 & Z \otimes I \\ \overline{Z}_2 & I \otimes Z \end{array} \rightarrow \begin{array}{c} X \otimes X \\ I \otimes X \\ Z \otimes I \\ Z \otimes Z \end{array} \rightarrow \begin{array}{c} I \otimes X \\ X \otimes X \\ Z \otimes Z \\ Z \otimes I \end{array} \rightarrow \begin{array}{c} I \otimes X \\ X \otimes I \\ I \otimes Z \\ Z \otimes I \end{array} \tag{34}$$

The overall operation can thus be seen to be the SWAP gate.

The C-Z gate can be written as just $(I \otimes H)\mathrm{CNOT}(I \otimes H)$. The C-Y gate can be written as $(I \otimes P)\mathrm{CNOT}(I \otimes P^3)$ (with $P^3 = P^\dagger$). Alternatively, we could expand C-Y $= P$(C-Z)CNOT, and then expand C-Z as above. (We have a P in this expansion because $Y = iXZ$, not XZ.)

d) I picked redundant notation for this problem; let us use R_0 and R_1 instead of the Pauli operations P and Q. (They still get mapped to $X \otimes P'$ and $Z \otimes Q'$.)

First, note that since $\{R_0, R_1\} = 0$, there exists at least one qubit on which R_0 and R_1 differ, and on which neither is the identity. Then by performing a series of SWAPs, we can make this register the first qubit. Suppose R_0 on this register is A and R_1 on this register is B. Then by performing a one-qubit Clifford operation, as per part b, we know that we can map $A \mapsto X$ and $B \mapsto Z$, as $A \neq B$ and we can perform all possible permutations of X, Y, and Z. The net effect is to map $R_0 \mapsto X \otimes P'$ (for some Pauli P') and $R_1 \mapsto Z \otimes Q'$ (for some Pauli Q').

e) We wish to map $X_1 \mapsto X \otimes P'$ and $Z_1 \mapsto Z \otimes Q'$ for the specific P' and Q' we are given. Now, one feature CNOT, C-Y, and C-Z all have in common is that they leave $Z \otimes I$ invariant. Thus, if we perform CNOT from qubit 1 to qubit i ($i > 1$) whenever the ith qubit of $X \otimes P'$ is X, perform C-Y whenever the ith qubit of $X \otimes P'$ is Y, and perform C-Z whenever the ith qubit of $X \otimes P'$ is Z, then we map $X_1 \mapsto X \otimes P'$ and $Z_1 \mapsto Z \otimes I$. Then let us perform H on the first qubit so that $X_1 \mapsto Z \otimes P'$ and $Z_1 \mapsto X \otimes I$, and do the same procedure for Q'.

This maps $Z_1 \mapsto X \otimes Q'$, but what happens to the image of X_1? All of these gates leave $Z \otimes I$ alone, but many of them act on the second qubit. However, we note the following fact: CNOT, C-Y, and C-Z leave $I \otimes X$, $I \otimes Y$, and $I \otimes Z$ alone. That is, the controlled-E operation leaves $I \otimes E$ invariant when E is a Pauli matrix. Furthermore, the controlled-E operation maps $I \otimes F$ to $Z \otimes F$ whenever E and F are distinct nonidentity Pauli operators. Finally, X_1 and Z_1 anticommute, but so do X and Z, so P' and Q' anticommute. Therefore P' and Q' contain different nonidentity Pauli matrices on an even number of places, so the controlled gates for Q' produce an even number of Zs in the first qubit of the image of X_1. They therefore cancel out, and $X_1 \mapsto Z \otimes P'$.

Then we again perform H on the first qubit, and we have the desired transformation. Since C-Y and C-Z are both products of H, P, and CNOT by part c, we have the desired decomposition.

f) $\overline{X}_i$ commutes with both $\overline{X}_1$ and $\overline{Z}_1$, so $U_1^\dagger(\overline{X}_i)$ commutes with both $U_1^\dagger(\overline{X}_1) = X_1$ and $U_1^\dagger(\overline{Z}_1) = Z_1$. Any operator that commutes with both X_1 and Z_1 must be of the form $I \otimes R_i$. Similarly, $\overline{Z}_i$ commutes with both $\overline{X}_1$ and $\overline{Z}_1$, so $U_1^\dagger(\overline{Z}_i)$ must be of the form $I \otimes S_i$.

g) When $i \neq j$, $[\overline{X}_i, \overline{X}_j] = 0$, so the images under $U_1^\dagger$ also commute, meaning $[R_i, R_j] = 0$. Similarly, $[\overline{Z}_i, \overline{Z}_j] = 0$, so $[S_i, S_j] = 0$, and $[\overline{X}_i, \overline{Z}_j] = 0$, so $[R_i, S_j] = 0$. In addition, $\{\overline{X}_i, \overline{Z}_i\} = 0$, so the images under $U_1^\dagger$ must anticommute, meaning $\{R_i, S_i\} = 0$.

Suppose then that V_2 acts on $n-1$ qubits maps $X_i \mapsto R_{i+1}$ and $Z_i \mapsto S_{i+1}$. (So $I \otimes V_2$ maps $X_i \mapsto I \otimes R_i$ and $Z_i \mapsto I \otimes S_i$.) Then $U_1(I \otimes V_2)$ performs the transformation

$$\begin{aligned} X_1 \rightarrow & \quad X_1 & \rightarrow X \otimes P' = \overline{X}_1 & \quad (35)\\ Z_1 \rightarrow & \quad Z_1 & \rightarrow Z \otimes Q' = \overline{Z}_1 & \quad (36)\\ X_i \rightarrow & \quad I \otimes R_i & \rightarrow \overline{X}_i \quad (i > 1) & \quad (37)\\ Z_i \rightarrow & \quad I \otimes S_i & \rightarrow \overline{Z}_i \quad (i > 1), & \quad (38) \end{aligned}$$

as desired.

h) Suppose we are given an arbitrary transformation $X_i \mapsto \overline{X}_i$ and $Z_i \mapsto \overline{Z}_i$ on n qubits, and suppose we already know how to break down any $(n-1)$-qubit Clifford group operation into H, P, and CNOT. Then by part d, there exists some series W_1 of H, P, and CNOT that maps $\overline{X}_1 \mapsto X \otimes P'$ and $\overline{Z}_1 \mapsto Z \otimes Q'$. Suppose W_1 maps $\overline{X}_i \mapsto \overline{X}_i'$ and $\overline{Z}_i \mapsto \overline{Z}_i'$. We know by part g that there exists a Clifford group operation $U_1(I \otimes V_2)$ which maps $X_i \mapsto \overline{X}_i'$ and $Z_i \mapsto \overline{Z}_i'$. Thus, $W_1^\dagger U_1(I \otimes V_2)$ maps $X_i \mapsto \overline{X}_i$ and $Z_i \mapsto \overline{Z}_i$. We know how to write U_1 and $W_1^\dagger$ as products of H, P, and CNOT, and by induction, V_2, which acts on $n-1$ qubits, is a Clifford group operation and can be written as a produt of H, P, and CNOT also. Since we proved the base case of $n = 1$ in part b, this completes the induction.

Counting gates, we find that W_1 involves only a constant number of gates, and U_1 involves $O(n)$ gates. Since we need n recursion steps (getting $U_2, U_3, \ldots, U_n$), we have a total of $O(n^2)$ gates.

i) We wish to find a Clifford group operation mapping

$$\begin{aligned} Z_1 &\rightarrow X \otimes Z \otimes Z \otimes X \otimes I & (39)\\ X_1 &\rightarrow Z \otimes I \otimes Z \otimes I \otimes I & (40)\\ Z_2 &\rightarrow I \otimes X \otimes Z \otimes Z \otimes X & (41)\\ X_2 &\rightarrow X \otimes Z \otimes X \otimes Y \otimes X & (42)\\ Z_3 &\rightarrow X \otimes I \otimes X \otimes Z \otimes Z & (43)\\ X_3 &\rightarrow Z \otimes Y \otimes Z \otimes I \otimes Y & (44)\\ Z_4 &\rightarrow Z \otimes X \otimes I \otimes X \otimes Z & (45)\\ X_4 &\rightarrow Z \otimes Z \otimes Z \otimes Y \otimes X & (46)\\ Z_5 &\rightarrow Z \otimes Z \otimes Z \otimes Z \otimes Z & (47)\\ X_5 &\rightarrow X \otimes X \otimes X \otimes X \otimes X. & (48) \end{aligned}$$

We don't particularly care what happens to X_1, X_2, X_3, or X_4, but we had to choose something, and they must have the right commutation relationships with the other operators. I chose values which disagreed with the corresponding Z_is on the ith position to minimize the number of SWAPs necessary in the circuit.

We can choose $W_1 = H_1$, so that $\overline{X}_1 \mapsto X \otimes I \otimes Z \otimes I \otimes I$ and $\overline{Z}_1 \mapsto Z \otimes Z \otimes Z \otimes X \otimes I$. Then we should choose $U_1 = H_1$ C-Z$(1,2)$ C-Z$(1,3)$ CNOT$(1,4)$ H_1 C-Z$(1,3)$. We are left to perform $I \otimes V_2$ which maps

$$\begin{aligned} Z_2 &\rightarrow I \otimes X \otimes Z \otimes Z \otimes X & (49)\\ X_2 &\rightarrow -I \otimes I \otimes Y \otimes Z \otimes X & (50)\\ Z_3 &\rightarrow I \otimes Z \otimes Y \otimes Y \otimes Z & (51)\\ X_3 &\rightarrow I \otimes Y \otimes Z \otimes I \otimes Y & (52)\\ Z_4 &\rightarrow I \otimes X \otimes I \otimes X \otimes Z & (53)\\ X_4 &\rightarrow I \otimes Z \otimes Z \otimes Y \otimes X & (54)\\ Z_5 &\rightarrow I \otimes Z \otimes Z \otimes Z \otimes Z & (55)\\ X_5 &\rightarrow -I \otimes Y \otimes Y \otimes I \otimes X. & (56) \end{aligned}$$

Now, despite our efforts in choosing the $\overline{X}_i$s, we still have to perform a SWAP operation to get $\overline{X}_2$ and $\overline{Z}_2$ to disagree on the second position: We must choose $W_2 = P_2$ SWAP$(2,3)$. Then $\overline{X}_2 \mapsto X \otimes I \otimes Z \otimes X$ and $\overline{Z}_2 \mapsto Z \otimes X \otimes Z \otimes X$ (omitting the first qubit). We should therefore choose $U_2 = H_2$ CNOT$(2,3)$ C-Z$(2,4)$ CNOT$(2,5)$ H_2 C-Z$(2,4)$ CNOT$(2,5)$. Then, to find $I \otimes I \otimes V_3$, we act on the images of V_2 by $U_2^\dagger W_2$ to get

$$\begin{aligned}
Z_3 &\rightarrow -I \otimes I \otimes Z \otimes Y \otimes Z && (57)\\
X_3 &\rightarrow -I \otimes I \otimes Z \otimes Z \otimes Z && (58)\\
Z_4 &\rightarrow I \otimes I \otimes X \otimes X \otimes Z && (59)\\
X_4 &\rightarrow -I \otimes I \otimes Y \otimes X \otimes I && (60)\\
Z_5 &\rightarrow -I \otimes I \otimes Y \otimes I \otimes Y && (61)\\
X_5 &\rightarrow I \otimes I \otimes Y \otimes I \otimes X. && (62)
\end{aligned}$$

For W_3, we should choose $W_3 = T_3\ X_3$ SWAP$(3,4)$. (The X makes the signs positive for $\overline{X}_3$ and $\overline{Z}_3$.) Then $\overline{X}_3 \mapsto I \otimes I \otimes X \otimes Z \otimes Z$ and $\overline{Z}_3 \mapsto I \otimes I \otimes Z \otimes Z \otimes Z$. We then choose $U_3 = H_3$ C-Z$(3,4)$ C-Z$(3,5)$ H_3 C-Z$(3,4)$ C-Z$(3,5)$. We act by $U_3^\dagger W_3$ to find for the action of $I \otimes I \otimes I \otimes V_4$:

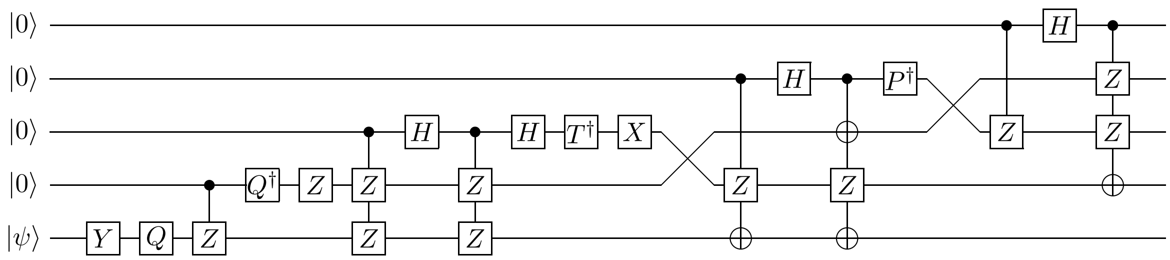
$$\begin{aligned}
Z_4 &\rightarrow -I \otimes I \otimes I \otimes Y \otimes I && (63)\\
X_4 &\rightarrow -I \otimes I \otimes I \otimes X \otimes Z && (64)\\
Z_5 &\rightarrow -I \otimes I \otimes I \otimes Y \otimes Y && (65)\\
X_5 &\rightarrow I \otimes I \otimes I \otimes Y \otimes X. && (66)
\end{aligned}$$

We now pick $W_4 = Q_4\ Z_4$, meaning $\overline{X}_4 \mapsto I \otimes I \otimes I \otimes X \otimes Z$ and $\overline{Z} \mapsto I \otimes I \otimes I \otimes Z \otimes I$. Then $U_4 =$ C-Z$(4,5)$, and the action of $I \otimes I \otimes I \otimes I \otimes V_5$ is:

$$\begin{aligned}
Z_5 &\rightarrow I \otimes I \otimes I \otimes I \otimes Y && (67)\\
X_5 &\rightarrow -I \otimes I \otimes I \otimes I \otimes X. && (68)
\end{aligned}$$

We then recognize V_5 as $Q_5\ Y_5 = H_5\ P_5\ H_5\ Y_5$.

Now we can put everything together: The overall encoding operation will be $W_1^\dagger U_1 W_2^\dagger U_2 W_3^\dagger U_3 W_4^\dagger U_4 V_5$, which has the following circuit:



We could, of course, replace C-Z, Q, and T in this circuit with their constructions from H, P, and CNOT to get a circuit involving only those gates.

Problem 3. Using the Quantum MacWilliams Identity

a) When the QECC has a basis $|\bar{i}\rangle$ of encoded states, we can write

$$A_d = \frac{1}{2^{2k}} \sum_{E_d} \left| \sum_i \langle \bar{i}|E_d|\bar{i}\rangle \right|^2, \qquad (69)$$

$$B_d = \frac{1}{2^k} \sum_{E_d} \sum_{i,j} \left|\langle \bar{i}|E_d|\bar{j}\rangle\right|^2. \qquad (70)$$

Clearly both of these are nonnegative numbers. When $d = 0$, the only term in the sum is $E_d = I$, and $\langle \bar{i}|E_d|\bar{j}\rangle = \delta_{ij}$. Thus, $A_0 = B_0 = 1$.

The Cauchy-Schwarz inequality says that

$$|\vec{x} \cdot \vec{y}|^2 \leq |\vec{x}|^2 |\vec{y}|^2. \qquad (71)$$

Let $\alpha_{ij} = \langle \bar{i}|E_c|\bar{j}\rangle$. Let $\vec{x}$ be a 2^{2k}-dimensional complex vector with entries α_{ij}, and let $\vec{y}$ be a 2^{2k}-dimensional vector with entries equal to $(1/2^k)\delta_{ij}$ (that is, 0 when $i \neq j$ and $1/2^k$ otherwise). Then we have

$$\left| \sum_{ii} \alpha_{ii}/2^k \right|^2 \leq \sum_{ij} |\alpha_{ij}|^2/2^k, \qquad (72)$$

which implies that $A_d \leq B_d$.

b) If the code has distance d, then the QECC conditions say that for $\mathrm{wt}(E) < d$,

$$\langle \bar{i}|E|\bar{j}\rangle = C(E)\delta_{ij}. \qquad (73)$$

Thus, for $c < d$,

$$A_c = \frac{1}{2^{2k}} \sum_{E_c} 2^{2k} |C(E_c)|^2, \qquad (74)$$

$$B_c = \frac{1}{2^k} \sum_{E_c} 2^k |C(E_c)|^2, \qquad (75)$$

and $A_c = B_c$.

c) The quantum MacWilliams identity tells us

$$\begin{aligned} B(z) &= B_0 + B_1 z + B_2 z^2 + B_3 z^3 && (76)\\ &= \frac{1}{4}(1+3z)^3 A\left(\frac{1-z}{1+3z}\right) && (77)\\ &= \frac{1}{4}\left[A_0(1+3z)^3 + A_1(1-z)(1+3z)^2 + A_2(1-z)^2(1+3z) + A_3(1-z)^3\right]. && (78) \end{aligned}$$

We calculate the coefficients of powers of z and compare, getting the following constraints:

$$\begin{aligned} 4B_0 &= A_0 + A_1 + A_2 + A_3 && (79)\\ 4B_1 &= 9A_0 + 5A_1 + A_2 - 3A_3 && (80)\\ 4B_2 &= 27A_0 + 3A_1 - 5A_2 + 3A_3 && (81)\\ 4B_3 &= 27A_0 - 9A_1 + 3A_2 - A_3. && (82) \end{aligned}$$

With the additional constraints $B_0 = A_0 = 1$, $B_1 = A_1$, $B_2 \geq A_2$, and $B_3 \geq A_3$, we are reduced to two linear equalities and two linear inequalities for three variables:

$$\begin{aligned} A_1 + \ A_2 + \ A_3 &= 3 & (83)\\ A_1 + \ A_2 - 3A_3 &= -9 & (84)\\ 3A_1 - 9A_2 + 3A_3 &\geq -27 & (85)\\ -9A_1 + 3A_2 - 5A_3 &\geq -27. & (86) \end{aligned}$$

The first two equations tell us that $A_3 = 3$ and $A_2 = -A_1$. The only possible solution with both A_1 and A_2 nonnegative is therefore $(A_0, A_1, A_2, A_3) = (1, 0, 0, 3)$. Indeed, this solution satisfies the two inequalities.

Problem 4. The Quantum Shadow Enumerator

a) The definition of Sh_d is

$$Sh_d = \frac{1}{2^k} \sum_{E_d} \mathrm{Tr}(E_d \Pi E_d^\dagger Y^{\otimes n} \Pi^* Y^{\otimes n}). \tag{87}$$

For a general QECC,

$$\begin{aligned} Sh_d &= \frac{1}{2^k} \sum_{E_d} \sum_{i,j} \langle \bar{i} | E_d^\dagger Y^{\otimes n} | \bar{j}^* \rangle \langle \bar{j}^* | Y^{\otimes n} E_d | \bar{i} \rangle & (88)\\ &= \frac{1}{2^k} \sum_{E_d} \sum_{i,j} | \langle \bar{j}^* | Y^{\otimes n} E_d | \bar{i} \rangle |^2, & (89) \end{aligned}$$

where $|\bar{j}^*\rangle$ is the state vector of $|\bar{j}\rangle$ with the coefficients in the standard basis complex-conjugated. This is still a perfectly valid state vector, so the absolute value squared of $\langle \bar{j}^* | Y^{\otimes n} E_d | \bar{i} \rangle$ remains a nonnegative number, and $Sh_d \geq 0$.

For a stabilizer code, we write $\Pi = \sum_{M \in S} M / 2^{n-k}$, so $\Pi^* = \sum_{M \in S} (-1)^{y_M} M / 2^{n-k}$, where y_M is the number of Y operators in the tensor product description of M. Then

$$Y^{\otimes n} \Pi^* Y^{\otimes n} = \frac{1}{2^{n-k}} \sum_{M \in S} (-1)^{x_M + y_M + z_M} M = \frac{1}{2^{n-k}} \sum_{M \in S} (-1)^{\mathrm{wt}(M)} M, \tag{90}$$

where x_M is the number of Xs in M and z_M is the number of Zs in M. Also,

$$E_d \Pi E_d^\dagger = \frac{1}{2^{n-k}} \sum_{M \in S} (-1)^{c(M, E_d)} M, \tag{91}$$

where $c(M, E_d)$ is the symplectic inner product between M and E_d — that is, 0 when they commute and 1 when they anticommute. Therefore,

$$\mathrm{Tr}(E_d \Pi E_d^\dagger Y^{\otimes n} \Pi^* Y^{\otimes n}) = \frac{2^n}{2^{2n-2k}} \sum_{M \in S} (-1)^{c(M, E_d) + \mathrm{wt}(M)}. \tag{92}$$

Suppose $E_d \in Sh(S)$. Then $c(M, E_d) + \mathrm{wt}(M) = 0 \bmod 2$ for all $M \in S$, and the trace gives 2^k.

Suppose on the other hand, $E_d \notin Sh(S)$. Then $\exists M \in S$ with $c(M, E_d) + \mathrm{wt}(M) = 1 \bmod 2$. Let N be another element of S. We know M and N commute. Let us suppose M and N both act nontrivially on some set of l qubits, and that $\mathrm{wt}(M) = m + l$, $\mathrm{wt}(N) = n + l$. Then $\mathrm{wt}(MN) = m + n + l'$, where l' is the number of qubits on which M and N act nontrivially but differently (e.g., M is X and N is Z). However, we know that l' must be even, since M and N commute, so

$$\mathrm{wt}(MN) \bmod 2 = m + n = \mathrm{wt}(M) + \mathrm{wt}(N) - 2l = \mathrm{wt}(M) + \mathrm{wt}(N) \bmod 2. \tag{93}$$

Also, $c(MN, E_d) = c(M, E_d) + c(N, E_d)$, so the value of $c(MN, E_d) + \mathrm{wt}(MN)$ is opposite the value of $c(N, E_d) + \mathrm{wt}(N)$. Therefore, in this case, exactly half of the elements of S satisfy $c(M, E_d) + \mathrm{wt}(M) = 1 \bmod 2$ and half satisfy $c(M, E_d) + \mathrm{wt}(M) = 0 \bmod 2$, so $\mathrm{Tr}(E_d \Pi E_d^\dagger Y^{\otimes n} \Pi^* Y^{\otimes n}) = 0$.

That is, the trace is 0 when $E_d \notin Sh(S)$ and it is 2^k when $E_d \in Sh(S)$. Thus, Sh_d is equal to the number of elements of $Sh(S)$ of weight d.

b) Suppose S is real, so all operators in S contain an even number of Ys. Then elements of S_{even} contain an even combined number of Xs and Zs, and elements of S_{odd} contain an odd combined number of Xs and Zs. But $Y^{\otimes n}$ will commute with an operator M iff the combined number of Xs and Zs is even. Therefore, $Y^{\otimes n}$ commutes with all elements of S_{even} and anticommutes with all elements of S_{odd}, meaning $Y^{\otimes n} \in Sh(S)$.

Now suppose $Y^{\otimes n} \in Sh(S)$. This means that elements of S_{even} contain an even combined number of Xs and Zs, and elements of S_{odd} contain an odd combined number of Xs and Zs. But that means that elements of both S_{even} and S_{odd} contain an even number of Ys, so the code is real.

c) Using the hint,

$$Sh_n = \lim_{z\to\infty} Sh(z)/z^n = \frac{3^n}{2^{n-k}} A(1/3). \tag{94}$$

But $A(1/3) = \sum_d A_d (1/3)^d$, and $A_0 = 1$, $A_d \geq 0$, so $A(1/3) > 0$. Therefore, $Sh_n > 0$. By part a, we know that for a stabilizer code, Sh_n is an integer, and is equal to the number of elements of weight n in $Sh(S)$, so in particular, $Sh(S)$ contains at least one element of maximum weight.

d) The main observation is that when U is a single-qubit operation, then for all $M \in \mathcal{P}$, $U(M)$ has the same weight as M. Thus, $U(S_{\mathrm{even}}) = [U(S)]_{\mathrm{even}}$ and $U(S_{\mathrm{odd}}) = [U(S)]_{\mathrm{odd}}$. Then $Sh(U(S))$ contains those Fs that commute with elements of $U(S_{\mathrm{even}})$ and anticommute with elements of $U(S_{\mathrm{odd}})$. But if $F = U(E)$, then this is equivalent to saying that E commutes with elements of S_{even} and anticommutes with elements of S_{odd}. That is, $F \in Sh(U(S))$ iff $F = U(E)$, with $E \in Sh(S)$. Therefore, $Sh(U(S)) = U(Sh(S))$.

If U is a CNOT or other multiple-qubit operation, it can change the weight of operators, and therefore the relation need not hold. So, for instance, the $[[2,0]]$ stabilizer code with generators $Z \otimes I$ and $I \otimes Z$ has shadow $\{X \otimes X, Y \otimes Y, X \otimes Y, Y \otimes X\}$. After a CNOT, we have the same stabilizer, but applying the CNOT to the old shadow gives us $\{X \otimes I, -X \otimes Z, Y \otimes X, X \otimes Y\}$, and the first two elements are not in the shadow any more.

By part c, $Sh(S)$ always contains at least one element E of weight n. Via some tensor product U of one-qubit Clifford group operations we can transform E into $Y^{\otimes n}$ (cf. problem 2b). Thus, $U(Sh(S)) = Sh(U(S))$ contains $Y^{\otimes n}$. By part b, this implies that $U(S)$ is a real code; this shows that S is equivalent to a real code. (Recall that equivalent codes are related by permutations of the qubits, which we do not use here, and single-qubit unitary operations.)

e) We find

$$\begin{aligned} Sh(z) &= Sh_0 + Sh_1 z + Sh_2 z^2 + Sh_3 z^3 && (95)\\ &= \frac{1}{4}\left[A_0(1+3z)^3 + A_1(z-1)(1+3z)^2 + A_2(z-1)^2(1+3z) + A_3(z-1)^3\right]. && (96)\end{aligned}$$

As before, we match the coefficients of powers of z to get

$$\begin{aligned} 4Sh_0 &= A_0 - A_1 + A_2 - A_3 && (97)\\ 4Sh_1 &= 9A_0 - 5A_1 + A_2 + 3A_3 && (98)\\ 4Sh_2 &= 27A_0 - 3A_1 - 5A_2 - 3A_3 && (99)\\ 4Sh_3 &= 27A_0 + 9A_1 + 3A_2 + A_3. && (100)\end{aligned}$$

Recalling that the only solution from 3c was $(A_0, A_1, A_2, A_3) = (1, 0, 0, 3)$, we see that the shadow enumerators would give us $(Sh_0, Sh_1, Sh_2, Sh_3) = (-2, 18, 18, 30)/4$, but since $Sh_0 < 0$, they do not satisfy the appropriate constraints, and therefore no $[[3, 1, 2]]$ QECC can exist.