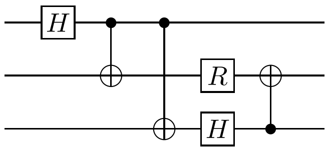
Solution Set #3

Quantum Error Correction
Instructor: Daniel Gottesman

Problem #1. A Clifford Group Circuit



a) We follow the evolution of $\overline{X}_i$ and $\overline{Z}_i$, $i = 1, \ldots, 3$:

$$\begin{array}{cccccccccc}
\overline{X}_1 \xrightarrow{H} & Z \otimes I \otimes I & \xrightarrow{CNOT} & Z \otimes I \otimes I & \xrightarrow{CNOT} & Z \otimes I \otimes I & \xrightarrow{R \otimes H} & Z \otimes I \otimes I & \xrightarrow{CNOT} & Z \otimes I \otimes I \\
\overline{X}_2 \xrightarrow{H} & I \otimes X \otimes I & \xrightarrow{CNOT} & I \otimes X \otimes I & \xrightarrow{CNOT} & I \otimes X \otimes I & \xrightarrow{R \otimes H} & I \otimes Y \otimes I & \xrightarrow{CNOT} & I \otimes Y \otimes Z \\
\overline{X}_3 \xrightarrow{H} & I \otimes I \otimes X & \xrightarrow{CNOT} & I \otimes I \otimes X & \xrightarrow{CNOT} & I \otimes I \otimes X & \xrightarrow{R \otimes H} & I \otimes I \otimes Z & \xrightarrow{CNOT} & I \otimes I \otimes Z \\
\overline{Z}_1 \xrightarrow{H} & X \otimes I \otimes I & \xrightarrow{CNOT} & X \otimes X \otimes I & \xrightarrow{CNOT} & X \otimes X \otimes X & \xrightarrow{R \otimes H} & X \otimes Y \otimes Z & \xrightarrow{CNOT} & X \otimes Y \otimes I \\
\overline{Z}_2 \xrightarrow{H} & I \otimes Z \otimes I & \xrightarrow{CNOT} & Z \otimes Z \otimes I & \xrightarrow{CNOT} & Z \otimes Z \otimes I & \xrightarrow{R \otimes H} & Z \otimes Z \otimes I & \xrightarrow{CNOT} & Z \otimes Z \otimes Z \\
\overline{Z}_3 \xrightarrow{H} & I \otimes I \otimes Z & \xrightarrow{CNOT} & I \otimes I \otimes Z & \xrightarrow{CNOT} & Z \otimes I \otimes Z & \xrightarrow{R \otimes H} & Z \otimes I \otimes X & \xrightarrow{CNOT} & Z \otimes X \otimes X
\end{array} \tag{1}$$

b) If the first and third qubits start as $|0\rangle$, we start with a stabilizer generated by $Z \otimes I \otimes I$ and $I \otimes I \otimes Z$. We then end with

$$X \otimes Y \otimes I \tag{2}$$
$$Z \otimes X \otimes X \tag{3}$$
$$\overline{X} = \overline{X}_2 = I \otimes Y \otimes Z \tag{4}$$
$$\overline{Z} = \overline{Z}_2 = Z \otimes Z \otimes Z, \tag{5}$$

with the first two lines giving the generators of the stabilizer.

Z_1 anticommutes with the first generator of the stabilizer, so the outcome if we measure it is a random bit $a = \pm 1$, and we end with

$$(-1)^a \quad Z \otimes I \otimes I \tag{6}$$
$$(-1)^a \quad I \otimes X \otimes X \tag{7}$$
$$\overline{X} = \overline{X}_2 = \quad I \otimes Y \otimes Z \tag{8}$$
$$\overline{Z} = \overline{Z}_2 = \quad (-1)^a \quad I \otimes Z \otimes Z. \tag{9}$$

The second stabilizer generator and $\overline{Z}$ have been multiplied by the first stabilizer generator in order to separate out the now measured first qubit.

If we measure Z_2, we still get a random bit b, and the state is

$$\begin{aligned}
& (-1)^b & I \otimes Z \otimes I \quad (10) \\
& (-1)^{b\oplus 1} & Y \otimes I \otimes X \quad (11) \\
\overline{X} = \overline{X}_2 = & & X \otimes I \otimes Z \quad (12) \\
\overline{Z} = \overline{Z}_2 = & (-1)^b & Z \otimes I \otimes Z. \quad (13)
\end{aligned}$$

To get this, we must multiply the original second stabilizer generator and $\overline{X}$ by the original first stabilizer generator in order to get things that commute with the measured operator. The extra factor of -1 appears in the eigenvalue of the new second generator because of the factors of i that appear when multiplying Pauli operators. (For instance, $Y = iXZ$.)

If we measure Z_3, we get a random bit c and state

$$\begin{aligned}
& & X \otimes Y \otimes I \quad (14) \\
& (-1)^c & I \otimes I \otimes Z \quad (15) \\
\overline{X} = \overline{X}_2 = & (-1)^c & I \otimes Y \otimes I \quad (16) \\
\overline{Z} = \overline{Z}_2 = & (-1)^c & Z \otimes Z \otimes I. \quad (17)
\end{aligned}$$

If we measure Z_1 and then Z_2, we get random bits a and b, but leave the state

$$\begin{aligned}
& (-1)^a & Z \otimes I \otimes I \quad (18) \\
& (-1)^b & I \otimes Z \otimes I \quad (19) \\
\overline{X} = \overline{X}_2 = & (-1)^{a\oplus b} & I \otimes I \otimes Y \quad (20) \\
\overline{Z} = \overline{Z}_2 = & (-1)^{a\oplus b} & I \otimes I \otimes Z. \quad (21)
\end{aligned}$$

Then measuring Z_3 measures the logical state, the outcome being a measurement of the input qubit on the second wire, reversed if $a \neq b$.

Problem #2. Equivalence of Stabilizer Entangled States

a) Corrected from the original problem set, the stabilizer should be:

$$\begin{array}{ccc}
Y \otimes Y & \otimes & X \otimes X \\
Z \otimes Z & \otimes & Y \otimes Z \\
I \otimes X & \otimes & Y \otimes X \\
Z \otimes X & \otimes & I \otimes X
\end{array}$$

The stabilizer for two EPR pairs is

$$\begin{array}{ccc}
X \otimes I & \otimes & X \otimes I \\
I \otimes X & \otimes & I \otimes X \\
Z \otimes I & \otimes & Z \otimes I \\
I \otimes Z & \otimes & I \otimes Z
\end{array}$$

We must match up generators of the original stabilizer with these four generators. In doing so, we must preserve commutation on Alice's and Bob's halves separately, since we are only doing local Clifford gates. We decide to map the first generator to the first generator:

$$(Y \otimes Y) \otimes (X \otimes X) \longrightarrow (X \otimes I) \otimes (X \otimes I). \quad (22)$$

We need to choose something that locally commutes with it to map to the next generator; let us pick the fourth one from the original stabilizer:

$$(Z \otimes X) \otimes (I \otimes X) \longrightarrow (I \otimes X) \otimes (I \otimes X). \tag{23}$$

We then need something that locally anticommutes with the first generator and commutes with the second generator to be our next operator:

$$(I \otimes X) \otimes (Y \otimes X) \longrightarrow (Z \otimes I) \otimes (Z \otimes I). \tag{24}$$

Then to finish up, we need something that anticommutes with the original fourth generator and commutes with the other three. The second generator does not fit the bill, since it anticommutes with both the third and fourth original generators, but the product of the first two generators works:

$$-(X \otimes X) \otimes (Z \otimes Y) \longrightarrow (I \otimes Z) \otimes (I \otimes Z). \tag{25}$$

We then must perform the following Clifford group operation on Alice's side:

$$\begin{aligned} Y \otimes Y &\rightarrow X \otimes I &(26)\\ Z \otimes X &\rightarrow I \otimes X &(27)\\ I \otimes X &\rightarrow Z \otimes I &(28)\\ -X \otimes X &\rightarrow I \otimes Z. &(29) \end{aligned}$$

On Bob's side, we do the Clifford group gate

$$\begin{aligned} X \otimes X &\rightarrow X \otimes I &(30)\\ I \otimes X &\rightarrow I \otimes X &(31)\\ Y \otimes X &\rightarrow Z \otimes I &(32)\\ Z \otimes Y &\rightarrow I \otimes Z. &(33) \end{aligned}$$

b) The stabilizer of k EPR pairs is generated by pairs of Pauli operators which anticommute on each side. Each pair commutes locally with all the other pairs, and with the single-qubit Z generators for the $|0\rangle$ qubits. We must therefore choose a new set of generators for the original stabilizer which are divided into pairs of Pauli operators which anticommute on Alice's (and Bob's) side with each other but commute with everything else, plus some additional generators which locally commute with everything.

   We can do this by taking any element of the stabilizer M which anticommutes locally with at least one other element N, assuming one exists. We can choose the remaining generators of the stabilizer to locally commute with both of these: If we have a candidate generator P that locally anticommutes with M, then NP locally commutes, and similarly, if P locally anticommutes with N, MP locally commutes.

   Then, using local Clifford operations, we can map $M \rightarrow X_1 \otimes X_1$ and $N \rightarrow Z_1 \otimes Z_1$. This is true because $M = M_A \otimes M_B$ and $N = N_A \otimes N_B$. Since M and N commute, both pairs of factors anticommute: $\{M_A, N_A\} = \{M_B, N_B\} = 0$. They are thus both not the identity, so there is some Clifford group operation that maps $M_A \rightarrow X_1$, $N_A \rightarrow Z_1$, and similarly on Bob's side. Since the remaining generators commute with M and N, they are mapped to operators which act trivially on the first qubit on each side (since only the identity commutes with both X and Z). Therefore, we now have a tensor product of an EPR pair with a stabilizer state on $n_A - 1$ and $n_B - 1$ qubits.

   We repeatedly apply the above procedure until we cannot find any two elements of the remaining stabilizer that anticommute locally, and have only m_A and m_B qubits left. We will map the remaining generators to operators of the form either $Z \otimes I$ or $I \otimes Z$. However, we need more information than simply local commutation rules to know that we can do this, since local Clifford group operators cannot map a non-trivial Pauli operator to the identity, regardless of commutation.

We note, however, that with m_A qubits held by Alice, there can be at most m_A independent commuting Pauli operators on Alice's side. We choose as many such independent generators $\tilde{m}_A$ as possible; the remaining generators are dependent on Alice's side, and thus, by suitable multiplications, can then be chosen to act as I on Alice's side. We have a total of $m_A + m_B$ qubits and thus have $m_A + m_B$ generators, which means we have $m_B + (m_A - \tilde{m}_A)$ generators left which act only on Bob's side. But since they commute and are independent, there can be at most m_B of them, so $m_A = \tilde{m}_A$.

There are then also m_B commuting independent generators which act only on Bob's side, which we might as well map, via Clifford group gates, to the Z_is on Bob's side. The generators which act on Alice's side commute with them, so all must act as a tensor product of Is and Zs on Bob's side, and by suitable multiplications, we can eliminate all Zs. Thus we are left with m_A commuting, independent operators acting only on Alice's side, and a local Clifford group operation will map them to the Z_is on Alice's side.

Problem #3. Number of Stabilizer Codes

a) We know from the linear algebra lemma that there are $2n-r$ independent Pauli operators that commute with all r generators of S. Ignoring phases, this comes to 2^{2n-r} total such Pauli operators. Since 2^r of these are already in S, there are $2^{2n-r} - 2^r$ elements in $N(S) \setminus S$.

If we pick a series $M_1, \dots, M_r$ of generators, each generator M_{i+1} must be in $N(S_i) \setminus S_i$ for the stabilizer S_i generated by $M_1, \dots M_i$. (S_0 being $\{I\}$.) There are thus a total of

$$A_{n,r} = \prod_{i=0}^{r-1} \left(2^{2n-i} - 2^i\right) = (2^{2n} - 1)(2^{2n-1} - 2) \cdots (2^{2n-r+1} - 2^{r-1}) \tag{34}$$

such sequences.

b) The first generator M_1 may be any non-identity element of S; there are $2^r - 1$ possible choices. Further generators M_{j+1} may be any element of S which is not already in S_j, the stabilizer generated by $M_1, \dots M_j$. There are $2^r - 2^j$ such operators. Thus, the total number of ways to pick an ordered set of generators is

$$B_{n,r} = \prod_{j=0}^{r-1} \left(2^r - 2^j\right) = (2^r - 1)(2^r - 2) \cdots (2^r - 2^{r-1}). \tag{35}$$

c) Without phases, we have $A_{n,r}$ ways ($r = n - k$) to pick an ordered set of generators for S from the whole Pauli group, but for every S, there are $B_{n,r}$ different ways of choosing generators that give S. Thus, the total number of stabilizers without phases is $A_{n,r}/B_{n,r}$. There are r generators, each of which can have phase ± 1. ($\pm i$ is impossible, or $-I$ would be in S, and all non-generating elements of the stabilizer have their phases determined by the phases of the generators.) Thus, the total number of stabilizer codes is

$$\begin{aligned} N_{n,k} &= 2^r \frac{A_{n,r}}{B_{n,r}} && (36) \\ &= 2^r \frac{2^{2n} - 1}{2^r - 1} \cdot \frac{2^{2n-1} - 2}{2^r - 2} \cdots \frac{2^{2n-r+1} - 2^{r-1}}{2^r - 2^{r-1}} && (37) \\ &= 2^r \prod_{i=0}^{r-1} \frac{4^{n-i} - 1}{2^{r-i} - 1}, && (38) \end{aligned}$$

with $r = n - k$.

We then take the base 2 logarithm to find

$$\log N_{n,k} = r + \sum_{i=0}^{r-1} \left[\log(4^{n-i} - 1) - \log(2^{r-i} - 1)\right] . \tag{39}$$

Let us let n be large. Then, when $i \ll r$, we have

$$\log(4^{n-i} - 1) - \log(2^{r-i} - 1) \approx 2(n - i) - (r - i) = 2n - r - i. \tag{40}$$

If r is much smaller than n, i never gets close to n, and the sum is roughly $2nr$. If, on the other hand, r is large, the terms in the sum with $r - i$ small are few and we can replace them by the $i \ll r$ approximation without much changing the sum. In that case, we have

$$\log N_{n,k} \approx r + \sum_{i=0}^{r-1}(2n - r - i) = r + (4n - 3r + 1)r/2 \approx 2nr - 3r^2/2 = n^2/2 + nk - 3k^2/2. \tag{41}$$