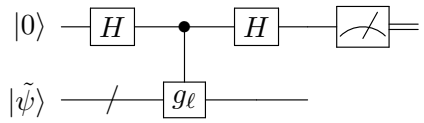
E2 210 (Jan.–Apr. 2025)

Homework Assignment 4 Solutions

1. Recall that $g_\ell E = (-1)^{s_\ell} E g_\ell$, and hence, for $|\tilde{\psi}\rangle = E\,|\psi\rangle$, with $|\psi\rangle \in \mathcal{Q}_{\mathcal{S}}$, we have

$$g_\ell\,|\tilde{\psi}\rangle = g_\ell E\,|\psi\rangle = (-1)^{s_\ell} E g_\ell\,|\psi\rangle = (-1)^{s_\ell} E\,|\psi\rangle = (-1)^{s_\ell}\,|\tilde{\psi}\rangle\,.$$

Now, let us analyze the given circuit:



After the first Hadamard and the controlled-g_ℓ operation, the joint state of all the qubits in the system is

$$\frac{1}{\sqrt{2}}\left(|0\rangle\,|\tilde{\psi}\rangle + |1\rangle\,g_\ell|\tilde{\psi}\rangle\right) \;=\; \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{s_\ell}\,|1\rangle\right)|\tilde{\psi}\rangle \;=\; \begin{cases} |+\rangle\,|\tilde{\psi}\rangle & \text{if } s_\ell = 0 \\ |-\rangle\,|\tilde{\psi}\rangle & \text{if } s_\ell = 1 \end{cases}$$

Now, applying the second Hadamard, the joint state becomes $|s_\ell\rangle\,|\tilde{\psi}\rangle$, so that measuring the first qubit in the computational basis yields s_ℓ without affecting $|\tilde{\psi}\rangle$.

2. Since $\mathcal{C}_1^\perp \subsetneq \mathcal{C}_2$, we have $n - k_1 < k_2$, so that the code $\mathcal{Q}$ has dimension $\dim(\mathcal{Q}) = 2^{k_1+k_2-n} > 1$. Therefore, the minimum distance of $\mathcal{Q}$ is equal to the least weight of an operator in $C(\mathcal{S}) \setminus \mathcal{S}$. (Both in $C(\mathcal{S})$ and in $\mathcal{S}$, we ignore the i^ℓ phase factors in front of Pauli operators of the form $X(\mathbf{a})Z(\mathbf{b})$.) Here, $\mathcal{S}$ is the stabilizer group generated by the Pauli operators represented by the check matrix

$$H = \begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix}.$$

As shown in class, the Pauli operator $X(\mathbf{a})Z(\mathbf{b})$ is in $C(\mathcal{S})$ iff $[\mathbf{b}\;\;\mathbf{a}]$ is in the nullspace of H. It is easily verified that

$$\text{nullspace}(H) \;=\; \big\{[\mathbf{c}_1\;\;\mathbf{c}_2] : \mathbf{c}_1 \in \mathcal{C}_1, \mathbf{c}_2 \in \mathcal{C}_2\big\}.$$

Therefore, the centralizer $C(\mathcal{S})$ consists of all the Pauli operators $X(\mathbf{c}_2)Z(\mathbf{c}_1)$, with $\mathbf{c}_2 \in \mathcal{C}_2$ and $\mathbf{c}_1 \in \mathcal{C}_1$.

Moreover, the stabilizers in $\mathcal{S}$ are precisely the Pauli operators represented by the binary vectors in the rowspace of H. Clearly (since the rows of H_i generate $\mathcal{C}_i^\perp$, $i = 1, 2$), we have

$$\text{rowspace}(H) \;=\; \big\{[\mathbf{b}_1\;\;\mathbf{b}_2] : \mathbf{b}_1 \in \mathcal{C}_1^\perp, \mathbf{b}_2 \in \mathcal{C}_2^\perp\big\}.$$

Therefore, the stabilizer $\mathcal{S}$ consists of all the Pauli operators $X(\mathbf{b}_1)Z(\mathbf{b}_2)$, with $\mathbf{b}_1 \in \mathcal{C}_1^\perp$ and $\mathbf{b}_2 \in \mathcal{C}_2^\perp$.

Consequently, we find that $C(\mathcal{S}) \setminus \mathcal{S}$ consists of all operators of the form $X(\mathbf{a})Z(\mathbf{b})$, where either $\mathbf{a} \in \mathcal{C}_2 \setminus \mathcal{C}_1^\perp$ or $\mathbf{b} \in \mathcal{C}_1 \setminus \mathcal{C}_2^\perp$ (or both). Among these, the operators of least weight must be either of the form $X(\mathbf{a})Z(\mathbf{0})$ with $\mathbf{a} \in \mathcal{C}_2 \setminus \mathcal{C}_1^\perp$, or of the form $X(\mathbf{0})Z(\mathbf{b})$ with $\mathbf{b} \in \mathcal{C}_1 \setminus \mathcal{C}_2^\perp$. We conclude that the least weight among operators in $C(\mathcal{S}) \setminus \mathcal{S}$ is the smaller of $d_{\min}(\mathcal{C}_2 \setminus \mathcal{C}_1^\perp)$ and $d_{\min}(\mathcal{C}_1 \setminus \mathcal{C}_2^\perp)$. (Here, for a set A of binary vectors, $d_{\min}(A)$ refers to the least Hamming weight among the vectors in A.)

3. (a) Since $H_1 H_1^T = 0$, any row, $\mathbf{h}$, of H_1 has to be orthogonal to itself: $\mathbf{h} \cdot \mathbf{h} = 0 \pmod 2$. Since $\mathbf{h} \cdot \mathbf{h}$ is equal to the number of 1's in $\mathbf{h}$ (i.e., the Hamming weight of $\mathbf{h}$), we see that $\mathbf{h}$ must have even Hamming weight. In particular, this means that any stabilizer generator g is either composed of an even number of X operators, or an even number of Z operators. In either case, it commutes with $X^{\otimes n}$ and $Z^{\otimes n}$. Thus, $X^{\otimes n}$ and $Z^{\otimes n}$ are both in the centralizer $C(\mathcal{S})$.

   For $X^{\otimes n}$ and $Z^{\otimes n}$ to **not** be logical identity operators, they must not be in the stabilizer $\mathcal{S}$. A necessary and sufficient condition for this is that the all-ones vector $\mathbf{1}$ must not be in the rowspace of H_1. For instance, if n is odd, then $\mathbf{1}$ cannot be in the rowspace of H_1. This is because any vector $\mathbf{h}$ in the rowspace of H_1 must be self-orthogonal for $H_1 H_1^T = 0$ to hold, and binary vectors of odd Hamming weight cannot be self-orthogonal over $\mathbb{F}_2$.

   (b) Let $\overline{E} = H^{\otimes n}$. We first show that for every stabilizer generator g, there is another stabilizer generator g' such that $g \cdot \overline{H} = \overline{H} \cdot g'$. Note that any operator of the form $X_{\mathbf{b}} = \bigotimes_i X_i^{b_i}$, where $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ is a binary vector, we have

$$X_{\mathbf{b}} \cdot \overline{H} \;=\; \bigotimes_i (X_i^{b_i} \cdot H) \;=\; \bigotimes_i (H \cdot Z_i^{b_i}) \;=\; \overline{H} \cdot Z_{\mathbf{b}},$$

   where we used the fact that $X \cdot H = H \cdot Z$. Analogously, $Z_{\mathbf{b}} \cdot \overline{H} = \overline{H} \cdot X_{\mathbf{b}}$.

   Now, since the check matrix of the CSS code is of the form

$$\begin{bmatrix} H_1 & \mathbf{0} \\ \mathbf{0} & H_1 \end{bmatrix},$$

   the stabilizer generators are of the form $X_{\mathbf{b}}$ and $Z_{\mathbf{b}}$, and moreover, $X_{\mathbf{b}}$ is a stabilizer generator iff $Z_{\mathbf{b}}$ is also a stabilizer generator. We conclude that for every stabilizer generator g, there is another stabilizer generator g' such that $g \cdot \overline{H} = \overline{H} \cdot g'$.

   Now, consider any codestate $|\psi\rangle \in \mathcal{Q}$ and let $|\varphi\rangle = \overline{H}\,|\psi\rangle$. Then, for any stabilizer generator g, we have

$$g\,|\varphi\rangle = g\overline{H}\,|\psi\rangle = \overline{H} g'\,|\psi\rangle = \overline{H}\,|\psi\rangle = |\varphi\rangle\,.$$

   Therefore, $\overline{H}\,|\psi\rangle \in \mathcal{Q}$ for any $|\psi\rangle \in \mathcal{Q}$, which proves that $\overline{H}$ is a logical operator for $\mathcal{Q}$.

4. (a) Let $\mathcal{C}_1$ be the $[7, 4]$ Hamming code with parity-check matrix H_1 as given. It is straightforward to check that $H_1 \cdot H_1^T \;=\; 0$, so that $\mathcal{C}_1^\perp \subseteq \mathcal{C}_1$. But we also have $\dim(\mathcal{C}_1^\perp) = n - \dim(\mathcal{C}_1) = 7 - 4 = 3 < \dim(\mathcal{C}_1)$, and so $\mathcal{C}_1^\perp \subsetneq \mathcal{C}_1$. Applying the result of Problem 2 above, we see that the minimum distance of the Steane code is equal to $d_{\min}(\mathcal{C}_1 \setminus \mathcal{C}_1^\perp)$.

   Now, $\mathcal{C}_1^\perp$ is equal to the rowspace of H_1. Running through all the vectors in rowspace(H_1), we can check that every nonzero codeword of $\mathcal{C}_1^\perp$ has Hamming weight equal to 4. Since the Hamming code $\mathcal{C}_1$ has minimum distance 3, it follows that $d_{\min}(\mathcal{C}_1 \setminus \mathcal{C}_1^\perp) = 3$.

   Thus, the minimum distance of the Steane code is 3, making it a $[[7, 1, 3]]_2$ code capable of correcting a single qubit-error.

   (b) Note that for any $|\mathbf{b}\rangle$ in the computational basis of an n-qubit Hilbert space, we have $X^{\otimes n}\,|\mathbf{b}\rangle = |\mathbf{1} \oplus \mathbf{b}\rangle$, where $\mathbf{1}$ is the all-ones binary vector of length n. Also,

$$Z^{\otimes n}\,|\mathbf{b}\rangle \;=\; (-1)^{\mathbf{1}\cdot\mathbf{b}}\,|\mathbf{b}\rangle \;=\; \begin{cases} |\mathbf{b}\rangle & \text{if } \mathbf{b} \text{ has even Hamming weight} \\ -\,|\mathbf{b}\rangle & \text{if } \mathbf{b} \text{ has odd Hamming weight.} \end{cases}$$

From these observations and the given expressions for $|\overline{0}\rangle$ and $|\overline{1}\rangle$, it is immediate that

$$\overline{X}\,|\overline{0}\rangle = |\overline{1}\rangle\,, \quad \overline{X}\,|\overline{1}\rangle = |\overline{0}\rangle\,, \quad \overline{Z}\,|\overline{0}\rangle = |\overline{0}\rangle\,, \quad \overline{Z}\,|\overline{1}\rangle = -\,|\overline{1}\rangle$$

(c) For any $|\mathbf{b}\rangle = |b_1 b_2 \ldots b_n\rangle$ in the computational basis, we have $H^{\otimes n} = \bigotimes_i |\sigma_i\rangle$, where $\sigma_i = +$ if $b_i = 0$, and $\sigma_i = -$ if $b_i = 1$. Applying this to each of the computational basis states involved in the superpositions that make up $|\overline{0}\rangle$ and $|\overline{1}\rangle$, we can indeed verify that

$$\overline{H}\,|\overline{0}\rangle = \frac{1}{\sqrt{2}}\,(|\overline{0}\rangle + |\overline{1}\rangle) \quad \text{and} \quad \overline{H}\,|\overline{1}\rangle = \frac{1}{\sqrt{2}}\,(|\overline{0}\rangle - |\overline{1}\rangle).$$

However, doing this by hand is quite tedious, which is why this should be verified by writing a small computer program.

In some sources, it is suggested that it suffices to verify that $\overline{H}\,\overline{X}\,\overline{H} = \overline{Z}$ and $\overline{H}\,\overline{Z}\,\overline{H} = \overline{X}$ (these are of course very easy to verify). But this is not strictly correct, since these identities will also be satisfied if we replace $\overline{H}$ by $-\overline{H}$, which is not exactly the same operator.

(d) For any $|\mathbf{b}\rangle$ in the computational basis, we have $S^{\otimes n}\,|\mathbf{b}\rangle = i^{w(\mathbf{b})}\mathbf{b}$ and $(S^\dagger)^{\otimes n}\,|\mathbf{b}\rangle = (-i)^{w(\mathbf{b})}\,|\mathbf{b}\rangle$, where $w(\mathbf{b})$ is the Hamming weight of the binary vector $\mathbf{b}$. Using this, it is easy to check that

$$(S^\dagger)^{\otimes 7}\,|\overline{0}\rangle = |\overline{0}\rangle \quad \text{and} \quad (S^\dagger)^{\otimes 7}\,|\overline{1}\rangle = i\,|\overline{1}\rangle\,.$$

This is because each computational basis state involved in the superposition in $|\overline{0}\rangle$ has Hamming weight 4 (and $(-i)^4 = 1$), while each computational basis state involved in the superposition in $|\overline{1}\rangle$ has Hamming weight 3 (and $(-i)^3 = i$).