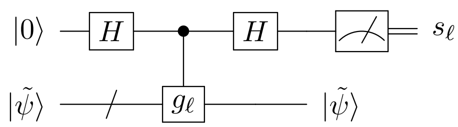
E2 210 (Jan.–Apr. 2025)

Homework Assignment 4

Submission deadline: Monday, March 31, 11:59pm

This assignment consists of two pages.

1. Let $\mathcal{S} = \langle g_1, g_2, \ldots, g_{n-k} \rangle$ be a stabilizer group in $\mathcal{P}_n$, with $\mathcal{Q}_{\mathcal{S}}$ the corresponding stabilizer code. Let $\mathbf{s} = [s_1, s_2, \ldots, s_{n-k}] \in \{0,1\}^{n-k}$ be the syndrome associated with a Pauli error E. For a codestate $|\psi\rangle \in \mathcal{Q}_{\mathcal{S}}$, let $|\tilde{\psi}\rangle = E\,|\psi\rangle$. Verify that the circuit below determines the syndrome bit s_ℓ without modifying the input state $|\tilde{\psi}\rangle$.



(The $-\!\!/\!\!-$ in the circuit denotes a wire carrying n qubits.)

2. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be, respectively, binary linear codes such that $\mathcal{C}_1^\perp \subsetneq \mathcal{C}_2$. Show that the minimum distance of the quantum code $\mathcal{Q}$ obtained via the CSS construction is $\min\{d_{\min}(\mathcal{C}_1 \setminus \mathcal{C}_2^\perp), d_{\min}(\mathcal{C}_2 \setminus \mathcal{C}_1^\perp)\}$. (Here, for a set A of binary vectors, $d_{\min}(A)$ refers to the least Hamming weight among the vectors in A.)

A *logical operator* for an n-qubit quantum code $\mathcal{Q}$ is any unitary operator U acting on n qubits such that $U(\mathcal{Q}) = \mathcal{Q}$. In other words, for any $|\psi\rangle \in \mathcal{Q}$, we have $U\,|\psi\rangle \in \mathcal{Q}$. If U acts as the identity operator on $\mathcal{Q}$, i.e., $U\,|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in \mathcal{Q}$, then we say that the operator is a *logical identity* for $\mathcal{Q}$. In the following problems, we identify some logical operators of CSS codes obtained from dual-containing binary linear codes.

3. Let $\mathcal{C}_1$ be an $[n, k_1]$ binary linear code that contains its own dual, i.e., $\mathcal{C}_1^\perp \subseteq \mathcal{C}_1$, and let H_1 be an $(n - k_1) \times n$ parity-check matrix of $\mathcal{C}_1$, so that $H_1 H_1^T = 0 \pmod 2$. Let $\mathcal{Q}$ be the $[[n, 2k_1 - n]]_2$ quantum stabilizer code obtained via the CSS construction, i.e., it is the stabilizer code associated with the check matrix

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

   (a) Show that $X^{\otimes n}$ and $Z^{\otimes n}$ are always logical operators for $\mathcal{Q}$. What property of the matrix H_1 ensures that these are <u>not</u> logical identities for $\mathcal{Q}$?
   [*Hint*: Since $H_1 H_1^T = 0 \pmod 2$, every row of H_1 must have even Hamming weight (why?). Use this to argue that $X^{\otimes n}$ and $Z^{\otimes n}$ commute with all the stabilizer generators, and hence, are in the centralizer $C(\mathcal{S})$.]

   (b) Show that $\overline{H} := H^{\otimes n}$ is also always a logical operator for $\mathcal{Q}$. (Here, H denotes the single-qubit Hadamard gate.)
   [*Hint*: First, show that every stabilizer generator g, there is another stabilizer generator g' such that $g \cdot \overline{H} = \overline{H} \cdot g'$. This follows easily from the special structure of the stabilizer generators.]

4. Let $\mathcal{C}_1$ be the $[7,4]$ Hamming code, which contains its own dual. The Steane code is the $[[7,1]]_2$ quantum stabilizer code obtained by applying the CSS construction to $\mathcal{C}_1^{\perp} \subset \mathcal{C}_1$. Thus, the check matrix of the Steane code is $\begin{bmatrix} H_1 & \mathbf{0} \\ \mathbf{0} & H_1 \end{bmatrix}$, where H_1 is a 3×7 parity-check matrix for $\mathcal{C}_1$. For concreteness, take

$$H_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Now, $\mathcal{C}_1^{\perp}$ and $\mathcal{C}_1 \backslash \mathcal{C}_1^{\perp}$ are the two cosets of $\mathcal{C}_1^{\perp}$ within $\mathcal{C}_1$. As we saw in Problem 3 of Homework Assignment #3,

$$|\overline{0}\rangle := \frac{1}{\sqrt{2^3}} \sum_{\mathbf{x} \in \mathcal{C}_1^{\perp}} |\mathbf{x}\rangle \quad \text{and} \quad |\overline{1}\rangle := \frac{1}{\sqrt{2^3}} \sum_{\mathbf{x} \in \mathcal{C}_1 \backslash \mathcal{C}_1^{\perp}} |\mathbf{x}\rangle$$

form an orthonormal basis of $\mathcal{Q}$. Explicitly,

$$|\overline{0}\rangle := \frac{1}{\sqrt{8}}(|0000000\rangle + |1101100\rangle + |1011010\rangle + |0111001\rangle + |0110110\rangle + |1100011\rangle + |1010101\rangle + |0001111\rangle)$$
$$|\overline{1}\rangle := \frac{1}{\sqrt{8}}(|1111111\rangle + |0010011\rangle + |0100101\rangle + |1000110\rangle + |1001001\rangle + |0011100\rangle + |0101010\rangle + |1110000\rangle)$$

(a) Determine the minimum distance of the Steane code.

(b) From Problem 3(a), we know that $\overline{X} := X^{\otimes 7}$ and $\overline{Z} := Z^{\otimes 7}$ are logical operators for the Steane code. Verify that these are indeed the logical-X and logical-Z operators, in the sense 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) From Problem 3(b), we know that $\overline{H} := H^{\otimes 7}$ is also a logical operator. Show that this is indeed the logical-Hadamard operator, i.e.,

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

(You may need to write a small program to verify this.)

(d) Recall that the S-gate maps $|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $i\,|1\rangle$. Verify that $\overline{S} := (S^{\dagger})^{\otimes 7}$ acts as a logical-S gate for the Steane code, i.e.,

$$\overline{S}\,|\overline{0}\rangle = |\overline{0}\rangle \quad \text{and} \quad \overline{S}\,|\overline{1}\rangle = i\,|\overline{1}\rangle$$