Exercise Set 12
Quantum Computation

**Reminder and terminology.** We first recap some terminology. (You can skip this at first read, but return to it when terminology used in an exercise is not clear.) A *stabilizer code* on $n$ physical qubits is described by Pauli strings $g_1, \ldots, g_r$ that pairwise commute. These strings are called *stabilizer generators* of the code. The code space $\mathcal{C}$, i.e. the span of all encoded states, is the joint +1-eigenspace of the stabilizers:

$$\mathcal{C} = \{|\psi\rangle : g_j |\psi\rangle = |\psi\rangle \text{ for all } j\}.$$

If the generators are independent, the code is said to encode $k = n - r$ logical qubits. Measuring each generator returns a $\pm 1$ value, and the collection of all $r$ values obtained gives the *syndrome*, namely the list of signs $(s_1, \ldots, s_r) \in \{\pm 1\}^r$. An error is *detectable* when at least one syndrome sign changes from $+1$ to $-1$. An error is *correctable* when the syndrome identifies a suitable recovery operation.

A CSS code is a special kind of stabilizer code whose generators separate into purely $X$-type and purely $Z$-type checks. We only consider CSS codes in this exercise sheet. For a binary vector $h = (h_1, \ldots, h_n) \in \mathbb{F}_2^n$, write

$$X^h := \prod_{j : h_j = 1} X_j, \qquad Z^h := \prod_{j : h_j = 1} Z_j.$$

A CSS code is specified by a binary matrix $H_X$, whose rows give the $X$-type stabilizers $X^h$, and a binary matrix $H_Z$, whose rows give the $Z$-type stabilizers $Z^h$. The CSS commutation condition is

$$H_X H_Z^T = 0 \pmod 2.$$

This condition guarantees that the associated stabilizers commute. This is because $X^h$ and $Z^{h'}$ anticommute once for each qubit where both vectors have a 1, thus they commute exactly when $h \cdot h' = 0 \pmod 2$.

**Exercise 1 (Terminology through a two-qubit example)** Consider the two two-qubit stabilizer generators

$$g_X = X_1 X_2, \qquad g_Z = Z_1 Z_2.$$

This small example does not specify a proper error-correcting code, because it does not even encode a qubit; but it is useful for fixing the terminology used in the rest of the sheet.

(a) Show that $g_X$ and $g_Z$ commute. Verify that

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

is a simultaneous +1-eigenvector of both generators. Why is the common +1-eigenspace one-dimensional?

(b) Write the CSS check matrices $H_X$ and $H_Z$ for this example and check that $H_X H_Z^T = 0$ modulo 2. How many independent stabilizer generators are there? Call this number $r$. What is $k = n - r$?

(c) Complete the syndrome table. In the last column, name the generator or generators whose measurement outcome changes sign.

| error $E$ | syndrome $(g_X, g_Z)$ | flipped check(s) |
|---|---|---|
| $I$ | | |
| $X_i,\ i = 1, 2$ | | |
| $Z_i,\ i = 1, 2$ | | |
| $Y_i,\ i = 1, 2$ | | |

(d) In this example, are all single-qubit Pauli errors detected? Are the errors $X_1$ and $X_2$ distinguished by the syndrome? Explain why this stabilizer code is a detection example, not a code for protecting an unknown logical qubit.

**Exercise 2 (A small code that detects, but does not correct)** Consider the four-qubit stabilizer code $\mathcal{C}$ defined as the simultaneous +1-eigenspace of

$$g_X = X_1 X_2 X_3 X_4, \qquad g_Z = Z_1 Z_2 Z_3 Z_4.$$

(a) Show that $g_X$ and $g_Z$ commute. How many independent stabilizer generators $r$ are there, and how many logical qubits $k = n - 2$ are encoded?

(b) Before completing the table below, work out one example in detail: for a code state $|\psi\rangle \in \mathcal{C}$, show that

$$g_X X_2 |\psi\rangle = +X_2 |\psi\rangle, \qquad g_Z X_2 |\psi\rangle = -X_2 |\psi\rangle.$$

Deduce that the syndrome associated with the error $X_2$ is $(+1, -1)$. Now complete the syndrome table. The syndrome is ordered as $(g_X, g_Z)$, and $i \in \{1, 2, 3, 4\}$.

| error $E$ | syndrome $(g_X, g_Z)$ |
|---|---|
| $I$ | |
| $X_i$ | |
| $Z_i$ | |
| $Y_i$ | |

(c) Verify that the following four states form an orthonormal basis of $\mathcal{C}$:

$$|\overline{00}\rangle = \frac{|0000\rangle + |1111\rangle}{\sqrt{2}}, \quad |\overline{01}\rangle = \frac{|0011\rangle + |1100\rangle}{\sqrt{2}},$$
$$|\overline{10}\rangle = \frac{|0101\rangle + |1010\rangle}{\sqrt{2}}, \quad |\overline{11}\rangle = \frac{|0110\rangle + |1001\rangle}{\sqrt{2}}.$$

(d) Use the table to explain why $\mathcal{C}$ detects every single-qubit Pauli error. Why can it not correct arbitrary single-qubit errors?

(e) Give an example of a weight-2 Pauli error which is not detected by these two stabilizers. Is your example a product of the stabilizer generators?

**Exercise 3 (Syndrome decoding in the Steane code)** Recall the Hamming $(7,4,3)$ parity-check matrix, with rows $h_1, h_2, h_3$:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Let

$$C_1 = \{x \in \mathbb{F}_2^7 : Hx^T = 0\}, \qquad C_2 = \mathrm{row}(H) = \{uH : u \in \mathbb{F}_2^3\}.$$

The Steane code has the following stabilizers:

$$g_1 = X_4X_5X_6X_7, \quad g_2 = X_2X_3X_6X_7, \quad g_3 = X_1X_3X_5X_7,$$
$$g_4 = Z_4Z_5Z_6Z_7, \quad g_5 = Z_2Z_3Z_6Z_7, \quad g_6 = Z_1Z_3Z_5Z_7.$$

Recall that for each error $E$, the syndrome is the six-tuple $(s_1, \ldots, s_6)$, where $g_j E|\psi\rangle = s_j E|\psi\rangle$ for all code states $|\psi\rangle$.

(a) Complete the following table. In the last column, give the natural recovery operation suggested by the syndrome.

| error $E$ | syndrome $(s_1, s_2, s_3, s_4, s_5, s_6)$ | recovery |
|---|---|---|
| $X_5$ | | |
| $Z_2$ | | |
| $Y_6$ | | |
| $X_1Z_4$ | | |

(b) Suppose that a bit-flip error $X_1X_2$ occurs. Compute its syndrome. Which single-qubit $X$-error has the same syndrome?

(c) If the decoder from part (b) applies the corresponding single-qubit correction, what residual operator remains? Check that this residual operator commutes with all six stabilizer generators.

(d) Describe a one-ancilla circuit to measure $g_6 = Z_1Z_3Z_5Z_7$ without measuring the physical qubits individually. Which ancilla measurement outcome corresponds to eigenvalue $-1$?

(e) How would you modify the previous circuit to measure $g_1 = X_4X_5X_6X_7$ instead? Give either a circuit diagram or a short verbal description.