Solutions: Exercise Set 11

Convention used throughout. Let g be a stabilizer generator and E a Pauli error. If $|\psi\rangle$ is a code state, then $g|\psi\rangle = |\psi\rangle$. Hence

$$gE|\psi\rangle = \begin{cases} E|\psi\rangle, & \text{if } gE = Eg, \\ -E|\psi\rangle, & \text{if } gE = -Eg. \end{cases}$$

Thus the syndrome sign for g is $+1$ exactly when E commutes with g, and it is -1 exactly when E anticommutes with g. In a CSS code this is especially simple: an X-error is detected by the Z-type checks, and a Z-error is detected by the X-type checks.

Solution 1 (Terminology through a two-qubit example) (a) The two generators are

$$g_X = X_1X_2, \qquad g_Z = Z_1Z_2.$$

They commute because the two single-qubit anticommutations cancel:

$$\begin{aligned} g_Xg_Z &= X_1X_2Z_1Z_2 = (X_1Z_1)(X_2Z_2) \\ &= (-Z_1X_1)(-Z_2X_2) = Z_1Z_2X_1X_2 = g_Zg_X. \end{aligned}$$

Equivalently, the supports of g_X and g_Z overlap on two qubits, and two is even.

Now check the proposed state

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

For g_X, we use that $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$:

$$X_1X_2|\Phi^+\rangle = \frac{|11\rangle + |00\rangle}{\sqrt{2}} = |\Phi^+\rangle.$$

For g_Z, we use that $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$:

$$Z_1Z_2|\Phi^+\rangle = \frac{|00\rangle + (-1)^2|11\rangle}{\sqrt{2}} = |\Phi^+\rangle.$$

Thus $|\Phi^+\rangle$ is a simultaneous $+1$-eigenvector.

The common $+1$-eigenspace is one-dimensional. One way to see this is the stabilizer counting rule: there are $n = 2$ physical qubits and $r = 2$ independent commuting stabilizer generators, so the dimension is $2^{n-r} = 2^0 = 1$. Concretely, the condition $Z_1Z_2 = +1$ restricts us to the even-parity subspace

$$a|00\rangle + b|11\rangle.$$

The additional condition $X_1X_2 = +1$ forces $a = b$. This leaves only the line spanned by $|\Phi^+\rangle$.

(b) The two generators are independent, so $r = 2$. Therefore

$$k = n - r = 2 - 2 = 0.$$

This code fixes a state; it does not encode any logical qubit.

(c) We use the commutation rule from the beginning of the solution sheet. The identity commutes with everything. The error X_i commutes with $g_X = X_1X_2$, but anticommutes with $g_Z = Z_1Z_2$, because there is exactly one qubit where X_i meets a Z_i. Similarly, Z_i anticommutes with g_X and commutes with g_Z. Finally, Y_i anticommutes with both X_i and Z_i, so it flips both checks. Hence, for $i = 1, 2$,

error E	syndrome (g_X, g_Z)	flipped check(s)
I	$(+1, +1)$	none
X_i	$(+1, -1)$	g_Z
Z_i	$(-1, +1)$	g_X
Y_i	$(-1, -1)$	g_X, g_Z

(d) All single-qubit Pauli errors are detected, because every non-identity single-qubit Pauli error in the table has at least one syndrome entry equal to -1. However, the syndrome does not distinguish the position of the error: X_1 and X_2 both have syndrome $(+1, -1)$, and similarly for the other Pauli types.

This example is therefore best understood as a stabilizer-state or error-detection example, not as a code protecting an unknown logical qubit. The reason is not only that some syndromes coincide; the more fundamental reason is that $k = 0$. The code space is one-dimensional, so there is no logical degree of freedom in which to store an unknown qubit state.

Solution 2 (A small code that detects, but does not correct) $g_X = X_1X_2X_3X_4$ and $g_Z = Z_1Z_2Z_3Z_4$ overlap on four qubits, and four is even, so the two Pauli strings commute.

The two stabilizer generators are independent: neither is the identity, and neither can be obtained as a product of the other. Hence $r = 2$. The number of encoded logical qubits is therefore

$$k = n - r = 4 - 2 = 2.$$

Let $|\psi\rangle \in \mathcal{C}$. By definition, $g_X |\psi\rangle = |\psi\rangle$ and $g_Z |\psi\rangle = |\psi\rangle$. The error X_2 commutes with g_X, because g_X is also made only of X's. Therefore

$$g_X X_2 |\psi\rangle = X_2 g_X |\psi\rangle = X_2 |\psi\rangle .$$

On the other hand, X_2 anticommutes with the factor Z_2 inside g_Z, and it commutes with all other factors in g_Z. Hence

$$g_Z X_2 = -X_2 g_Z,$$

and so

$$g_Z X_2 |\psi\rangle = -X_2 g_Z |\psi\rangle = -X_2 |\psi\rangle .$$

Thus the syndrome of X_2 is $(+1, -1)$.

The same reasoning gives the following table, valid for each $i \in \{1, 2, 3, 4\}$:

error E	syndrome (g_X, g_Z)
I	$(+1, +1)$
X_i	$(+1, -1)$
Z_i	$(-1, +1)$
Y_i	$(-1, -1)$

Again, X_i is detected by the Z-check, Z_i is detected by the X-check, and Y_i is detected by both.

(b) We verify first that the four proposed states lie in the code space. The operator $g_Z = Z_1 Z_2 Z_3 Z_4$ acts on a computational basis state $|x_1 x_2 x_3 x_4\rangle$ by the sign

$$(-1)^{x_1+x_2+x_3+x_4} = (-1)^{\mathrm{wt}(x)}.$$

All computational basis states appearing in the four proposed code states have even Hamming weight, so each term has g_Z-eigenvalue $+1$.

The operator $g_X = X_1 X_2 X_3 X_4$ flips all four bits. For example,

$$g_X |0011\rangle = |1100\rangle, \qquad g_X |1100\rangle = |0011\rangle.$$

Thus a plus superposition of a bit string and its bitwise complement is fixed by g_X. The same argument applies to all four states:

$$|0000\rangle \leftrightarrow |1111\rangle, \quad |0011\rangle \leftrightarrow |1100\rangle,$$
$$|0101\rangle \leftrightarrow |1010\rangle, \quad |0110\rangle \leftrightarrow |1001\rangle.$$

Therefore all four proposed states are simultaneous $+1$-eigenvectors of g_X and g_Z.

They are orthonormal because each state is normalized and the four pairs of computational basis vectors are disjoint. For instance, no computational basis vector appearing in $|\overline{00}\rangle$ appears in $|\overline{01}\rangle$, $|\overline{10}\rangle$, or $|\overline{11}\rangle$. Since the code has dimension

$$2^{n-r} = 2^{4-2} = 4,$$

these four orthonormal code states form a basis of $\mathcal{C}$.

(c) The table shows that every non-identity single-qubit Pauli error has a nontrivial syndrome. Therefore every single-qubit Pauli error is detected: after such an error, at least one stabilizer measurement returns -1.

However, the code cannot correct arbitrary single-qubit errors. The reason is that the syndrome does not identify the location of the error. For example,

$$X_1, \ X_2, \ X_3, \ X_4$$

all have the same syndrome $(+1, -1)$. Suppose a decoder chooses to correct the syndrome $(+1, -1)$ by applying X_1. If the actual error was X_2, the combined effect of error followed by correction is

$$X_1 X_2.$$

This operator commutes with both stabilizer generators, so it is not detected by the stabilizer measurements.

(d) A simple example is

$$E = X_1 X_2.$$

It commutes with $g_X = X_1 X_2 X_3 X_4$, since all factors are of X-type. It also commutes with $g_Z = Z_1 Z_2 Z_3 Z_4$, because there are two places where an X meets a Z, namely qubits 1 and 2. Two anticommutations give the overall sign $(-1)^2 = +1$. Thus $X_1 X_2$ has trivial syndrome $(+1, +1)$, so it is not detected.

It is not a product of the stabilizer generators. The stabilizer group generated by g_X and g_Z is

$$\{I,\ g_X,\ g_Z,\ g_X g_Z\},$$

up to irrelevant global phases. The three non-identity stabilizers have weight 4, whereas $X_1 X_2$ has weight 2.

Solution 3 (Syndrome decoding in the Steane code) It is helpful to keep track of the columns of the Hamming parity-check matrix:

qubit j	1	2	3	4	5	6	7
$H_{\cdot j}$	0	0	0	1	1	1	1
	0	1	1	0	0	1	1
	1	0	1	0	1	0	1

The first three stabilizer generators are X-type and the last three are Z-type. Therefore:

- a Z_j error flips the signs of the X-type checks according to column j of H, and it commutes with all Z-type checks;
- an X_j error flips the signs of the Z-type checks according to column j of H, and it commutes with all X-type checks;
- a Y_j error behaves like both an X_j and a Z_j error for syndrome purposes.

Here a column entry 0 gives syndrome sign $+1$, and a column entry 1 gives syndrome sign -1.

(a) We compute each row of the table using the column rule above.

For X_5, only the Z-type checks can flip. Column 5 of H is $(1, 0, 1)^T$. Hence the last three syndrome signs are $(-1, +1, -1)$, while the first three are $+1$.

For Z_2, only the X-type checks can flip. Column 2 is $(0, 1, 0)^T$. Hence the first three syndrome signs are $(+1, -1, +1)$, while the last three are $+1$.

For Y_6, both the X- and Z-type parts contribute. Column 6 is $(1, 1, 0)^T$, so both halves of the syndrome are $(-1, -1, +1)$.

For $X_1 Z_4$, treat the two factors separately and multiply the syndrome signs componentwise. The factor Z_4 flips the X-type checks according to column 4, namely $(1, 0, 0)^T$. The factor X_1 flips the Z-type checks according to column 1, namely $(0, 0, 1)^T$.

Thus

error E	syndrome $(s_1, s_2, s_3, s_4, s_5, s_6)$	recovery
X_5	$(+1, +1, +1, -1, +1, -1)$	X_5
Z_2	$(+1, -1, +1, +1, +1, +1)$	Z_2
Y_6	$(-1, -1, +1, -1, -1, +1)$	Y_6
X_1Z_4	$(-1, +1, +1, +1, +1, -1)$	X_1Z_4

For the last line, the usual single-qubit-error guarantee does not apply, because X_1Z_4 has weight 2. Nevertheless, the CSS syndrome separates the bit-flip part from the phase-flip part in this particular case: the last three checks identify the X_1 component, and the first three checks identify the Z_4 component.

(b) The error X_1X_2 only affects the Z-type checks g_4, g_5, g_6. The relevant binary syndrome is the mod-2 sum of columns 1 and 2 of H:

$$H_{\cdot 1} + H_{\cdot 2} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \pmod 2.$$

This is column 3 of H. Therefore

$$\mathrm{syn}(X_1X_2) = (+1, +1, +1, +1, -1, -1).$$

This is the same syndrome as the single-qubit error X_3.

(c) If the decoder from part (b) assumes that the error was X_3, it applies the correction X_3. The actual error was X_1X_2, so the residual operator is

$$X_3X_1X_2 = X_1X_2X_3,$$

where the order does not matter because these are all X-operators on different qubits.

This residual operator commutes with all three X-type stabilizers automatically, since it is also purely X-type. We only need to check commutation with the three Z-type stabilizers:

stabilizer	support of the stabilizer	overlap with $\{1, 2, 3\}$
$g_4 = Z_4Z_5Z_6Z_7$	$\{4, 5, 6, 7\}$	0
$g_5 = Z_2Z_3Z_6Z_7$	$\{2, 3, 6, 7\}$	2
$g_6 = Z_1Z_3Z_5Z_7$	$\{1, 3, 5, 7\}$	2

All overlaps are even. Hence all anticommutation signs cancel, and $X_1X_2X_3$ commutes with g_4, g_5, g_6 as well.

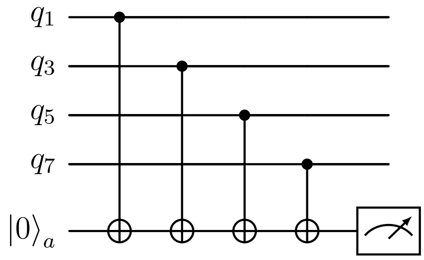
This is a useful lesson: the residual error has trivial syndrome, but it is not necessarily harmless. In fact, $X_1X_2X_3$ is not one of the X-type stabilizers of the Steane code. It is an undetected logical operator. This is exactly what can happen when two physical errors are decoded as one physical error in a distance-three code.

(d) To measure

$$g_6 = Z_1Z_3Z_5Z_7,$$

prepare one ancilla qubit in $|0\rangle$. Then apply CNOT gates from data qubits $1, 3, 5, 7$ to the ancilla, using the data qubits as controls and the ancilla as target. Finally, measure the ancilla in the computational basis.

In circuit form, omitting the data qubits that are not involved:



The ancilla records the parity $x_1 + x_3 + x_5 + x_7 \pmod 2$ when the data are in a computational-basis state $|x\rangle$. The eigenvalue of $Z_1Z_3Z_5Z_7$ is

$$(-1)^{x_1+x_3+x_5+x_7}.$$

Therefore measuring the ancilla as 0 corresponds to eigenvalue $+1$, and measuring it as 1 corresponds to eigenvalue -1.

(e) To measure

$$g_1 = X_4X_5X_6X_7,$$

we can use the same idea in the X-basis. Prepare the ancilla in

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Apply controlled-$X_4X_5X_6X_7$, with the ancilla as control. In practice this means applying four CNOT gates, all with the ancilla as control and with data qubits $4, 5, 6, 7$ as targets. Then measure the ancilla in the X-basis, i.e. distinguish $|+\rangle$ from $|-\rangle$.

Why this works: if the data state $|\psi\rangle$ is an eigenvector of g_1 with eigenvalue $\lambda \in \{+1, -1\}$, then after the controlled operation the joint state is

$$\frac{|0\rangle|\psi\rangle + |1\rangle g_1 |\psi\rangle}{\sqrt{2}} = \frac{|0\rangle + \lambda|1\rangle}{\sqrt{2}} |\psi\rangle.$$

Thus the ancilla is $|+\rangle$ when $\lambda = +1$, and $|-\rangle$ when $\lambda = -1$. Equivalently, one may Hadamard the relevant data qubits, measure the corresponding Z-type parity, and Hadamard them back.