Exercise Set 13: Solution
Quantum Computation

**Exercise 1** *The Steane code*

(a) The columns of the parity check matrix of the Hamming $(7,4)$ code are given by all binary non-zero vectors with $r = 3$ components (so that $2^r - 1 = 7$):

$$H_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

The generator matrix of $C_2 = C_1^{\perp}$ is given by vectors perpendicular to $C_1$. Since a vector $c \in C_1$ satisfies $H_1 \, c^T = 0$, the rows of $H_1$ are 3 vectors $\perp$ to $C_1$. Note that $C_1$ has dimension 4, so $C_1^{\perp} = \{x \in \{0,1\}^7 \ : \ x \cdot c = 0, \ \forall c \in C_1\}$ has dimension $7 - 4 = 3$ and $G_2 = H_1$ is therefore the generator matrix of $C_2$.

Codewords of $C_2$ are given by

$$(u_1, u_2, u_3) \cdot G_2 = (u_3, u_2, u_2 \oplus u_3, u_1, u_1 \oplus u_3, u_1 \oplus u_2, u_1 \oplus u_2 \oplus u_3)$$

with $(u_1, u_2, u_3) \in \{0,1\}^3$. The list of codewords of $C_2$ is therefore

$$0000000,\ 1010101,\ 0110011,\ 0001111,\ 0111100,\ 1011010,\ 1100110,\ 1101001 \tag{1}$$

To show that $C_2 \subset C_1$, it suffices to check that

$$H_1 \cdot (uG_2)^T = 0 \quad \forall u \in \{0,1\}^3$$

which is satisfied if $H_1 \cdot G_2^T = H_1 \cdot H_1^T = 0$. This is indeed the case, as each row of $H_1$ has an even number of 1's.

Finally, $C_1$ corrects 1 error, because all pairs of columns of $H_1$ are independent and its third column is a linear combination of the first two, and therefore the minimal distance (between codewords) is $d = 3$ (and $t = 1$).

Moreover, $C_2^{\perp} = (C_1^{\perp})^{\perp} = C_1$ corrects also 1 error.

(b) The CSS$(C_2, C_1)$ code possesses parameters: $n = 7$ (length) dim$\mathcal{H} = 2^7$ ($\mathcal{H}$ sbspace of Hilbert space of the 7 qubits).

$k_1 - k_2 = \dim(C_1) - \dim(C_2) = 4 - 3 = 1$. The code CSS$(C_2, C_1)$ is a subspace of $\mathcal{H}$ of dimension $2^1 = 2$. The code corrects $t = 1$ error.

(c) **Codewords:**
The equivalence class (or coset) of $c_0 = (0,0,0,0,0,0,0) \in C_1$ is:

$$
\begin{aligned}
|0\rangle_{\text{Steane}} &= \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |y\rangle \\
&= \frac{1}{\sqrt{8}} \Big\{ |0000000\rangle + |1010101\rangle + |0110011\rangle + |0001111\rangle + \\
&\qquad + |0111100\rangle + |1011010\rangle + |1100110\rangle + |1101001\rangle \Big\}.
\end{aligned}
$$

where we used the list of 8 (classical) codewords of $C_2$ given in (1).

Besides, $c_1 = (1,1,1,1,1,1,1)$ is a codeword in $C_1$ which is not in $C_2$ (check!). Its equivalence class gives the other independent vector of Steane's code:

$$
\begin{aligned}
|1\rangle_{\text{Steane}} &= \frac{1}{\sqrt{|C_2|}} \sum_{y \in c_1 \oplus C_2} |y\rangle \\
&= \frac{1}{\sqrt{8}} \Big\{ |1111111\rangle + |0101010\rangle + |1001100\rangle + |1110000\rangle + \\
&\qquad + |100011\rangle + |0100101\rangle + |0011001\rangle + |0010110\rangle \Big\}.
\end{aligned}
$$

A general codeword is a linear combination (by the superposition principle of quantum mechanics)

$$
|\psi\rangle = \alpha\, |0\rangle_{\text{Steane}} + \beta\, |1\rangle_{\text{Steane}}
$$

with $|\alpha|^2 + |\beta|^2 = 1; \alpha, \beta \in \mathbb{C}$. This code needs 7 qubits to correct an error (bit, phase, or bit-phase flip) on $t = 1$ qubit.