Exercice 1

(a) La matrice de parité du code de Hamming (7, 4) est donnée par tous vecteurs non nuls à \( r \) composantes pour \( 2^r - 1 = 7 \), c.à.d. \( r = 3 \) :

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

La matrice génératrice de \( C_2 = C_1^\perp \) est donnée par des vecteurs perpendiculaires à \( C_1 \). Comme un vecteur de \( C_1 \) satisfait \( H_1 \vec{x} = \vec{0} \), les lignes de \( H \) sont 3 vecteurs \( \perp \) à \( C_1 \). Notons que \( C_1 \) est de dimension 4, donc \( C_1^\perp \) est de dimension \( 7 - 4 = 3 \). Donc il suffit de prendre les 3 lignes de \( H \) comme matrice génératrice de \( C_1^\perp \) :

\[
G_2 = H_1^T = \begin{bmatrix}
0 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 0 \\
1 & 1 & 1
\end{bmatrix}.
\]

Les mots de code de \( C_2 \) sont donnés par

\[
\begin{bmatrix}
0 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 0 \\
1 & 1 & 1
\end{bmatrix} \begin{bmatrix}
\vec{u}_1 \\
\vec{u}_2 \\
\vec{u}_3
\end{bmatrix} = \begin{bmatrix}
\vec{u}_1 \\
\vec{u}_2 + \vec{u}_3 \\
\vec{u}_1 + \vec{u}_3 \\
\vec{u}_1 + \vec{u}_2 \\
\vec{u}_1 + \vec{u}_2 + \vec{u}_3
\end{bmatrix}
\]

avec \( (\vec{u}_1, \vec{u}_2, \vec{u}_3) \in \{0,1\}^3 \). Pour montrer que \( C_2 \subset C_1 \), il suffit de montrer que (vérifiez !)

\[
\begin{bmatrix}
0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 1
\end{bmatrix} \begin{bmatrix}
\vec{u}_3 \\
\vec{u}_2 \\
\vec{u}_1 \\
\vec{u}_2 + \vec{u}_3 \\
\vec{u}_1 + \vec{u}_3 \\
\vec{u}_1 + \vec{u}_2 \\
\vec{u}_1 + \vec{u}_2 + \vec{u}_3
\end{bmatrix} = \begin{bmatrix}
0 \\
0
\end{bmatrix}
\]
(où on prend les sommes mod 2 comme d’habitude).
Finalement $C_1$ corrige 1 erreur, car toutes paires de colonnes de $H_1$ sont indépendantes et la 4ème est combinaison linéaire des deux premières et donc $d = 3$ (et $t = 1$).
De plus, $C_2^\perp = (C_1^\perp)^\perp = C_1$ et corrige aussi 1 erreur.

(b) Le code CSS$(C_2, C_1)$ possède les paramètres : $n = 7$ (longueur), $\dim H = 2^7$.
$K_1 - K_2 = \dim C_1 - \dim C_2 = 4 - 3 = 1$. Le code est un sous-espace vectoriel de $H$ de dimension $2^1 = 2$. Le code corrige $t = 1$ erreur.

(c) **Mots de code :**
La classe d’équivalence de $\underline{x} = (0, 0, 0, 0, 0, 0) \in C_1$ est :

$$|0\rangle_{\text{Steane}} = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |y\rangle$$

$$= \frac{1}{\sqrt{8}} \left\{ |0000000\rangle + |1001101\rangle + |0101011\rangle + |0110110\rangle + |0111100\rangle + |1011010\rangle + |1100110\rangle + |1110001\rangle \right\},$$

où on a utilisé la liste des 8 mots de code de $C_2$ donnée par eq. 1.
Avec $\underline{x} = (1, 1, 1, 1, 1, 1) \in C_1$ (vérifiez) on a un mot de $C_1$ qui n’est pas dans $C_2$. Sa classe d’équivalence donne l’autre vecteur indépendant du code de Steane :

$$|1\rangle_{\text{Steane}} = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |y + \underline{x}\rangle$$

$$= \frac{1}{\sqrt{8}} \left\{ |1111111\rangle + |0110010\rangle + |1010100\rangle + |1101000\rangle + |1000111\rangle + |0100101\rangle + |0011001\rangle + |0001110\rangle \right\}.$$

Un mot de code général est (sous-espace vectoriel de dim 2)

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

avec $|\alpha|^2 + |\beta|^2 = 1; \alpha, \beta \in \mathbb{C}$. Ce code utilise 7 qubits pour corriger $t = 1$ erreur sur un qubit.