## CONTRÔLE CONTINU N° 2 – A

**Exercice 1.** *Soit $\mathcal{C}$ le code sur $\mathbb{F}_7 \cong \mathbb{Z}/7\mathbb{Z}$ dont une matrice génératrice est*

$$G := \begin{bmatrix} 1 & 0 & 0 & 0 & 6 & 2 \\ 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 2 & 5 \\ 0 & 0 & 0 & 1 & 5 & 6 \end{bmatrix}.$$

a) *Quelle est la longueur de $\mathcal{C}$ ? Et sa dimension ? Combien y a-t-il de mots dans $\mathcal{C}$ ? Justifier les réponses.*
b) *Montrer que la distance minimale de $\mathcal{C}$ est égale à 3.*
c) *Montrer que la distance minimale de $\mathcal{C}^\perp$ est égale à 5.*
d) *Est-ce que $v = (0, 6, 1, 0, 0, 4)$ appartient à $\mathcal{C}$ ? Si non, le corriger (c'est-à dire, trouver le mot du code le plus proche à $v$).*

**Solution :**

a) La longueur de $\mathcal{C}$ est 6, qui est le nombre de colonnes de $G$, sa dimension est 4, qui est le nombre de lignes de $G$. Dans $\mathcal{C}$ il y a $7^4 = 2401$ mots, car la dimension est 4 et le corps est $\mathbb{F}_7$.
b) Une matrice de parité pour $\mathcal{C}$ est (par un résultat du cours)

$$H := \begin{bmatrix} 6 & 2 & 2 & 5 & 6 & 0 \\ 2 & 2 & 5 & 6 & 0 & 6 \end{bmatrix}.$$

On remarque qu'il n'y a pas de colonnes nulles, donc la distance minimale est au moins 2. On doit montrer qu'il n'existe pas deux colonnes linéairement dépendantes. Appellons $h_1, \dots, h_6$ les colonnes de $H$. Clairement les couples $h_i, h_6$, pour $i \in \{1, \dots, 5\}$, et $h_i, h_5$, pour $i \in \{1, \dots, 4\}$, sont linéairement indépendantes. Les couples $h_i, h_2$, pour $i \in \{1, 3, 4\}$ le sont aussi, car tout multiple de $h_2$ a les coefficients idéntiques. Finalement, on vérifie que le déterminant de $[h_1, h_3]$, $[h_1, h_4$ et $[h_3, h_4]$ est différent de 0 dans $\mathbb{F}_7$. Donc la distance minimale est au moins 3. On cherche un mot de poids 3. N'importe quelle ligne de $G$ (par exemple) a poids 3, donc la distance minimale est 3.
c) Puisque $3 = 6 - 4 + 1$, le code $\mathcal{C}$ est MDS. Par un résultat du cours, $\mathcal{C}^\perp$ l'est aussi. Donc sa distance minimale est égale à $6 - 2 + 1 = 5$.
d) Le syndome de $v$ est $s = Hv^T = (0, 6)^T \neq (0, 0)^T$, donc $v$ n'appartient pas à $\mathcal{C}$. On remarque que $s$ est la dernière colonne de $H$, de manière que $s = H(0, 0, 0, 0, 0, 1)^T$. Ainsi, le mot du code le plus proche à $v$ est $(0, 6, 1, 0, 0, 3) = (0, 6, 1, 0, 0, 4) - (0, 0, 0, 0, 0, 1)$.

**Exercice 2.** *Soit $\mathcal{C}$ un code linéaire sur $\mathbb{F}_2$ dont le polynôme énumerateur des poids est*

$$w_{\mathcal{C}}(x,y) = x^8 + 14x^4y^4 + y^8.$$

a) *Combien y a-t-il de mots dans $\mathcal{C}$ ? Justifier.*
b) *Quel sont les paramètres de C ? Justifier.*
c) *Trouver une matrice génératrice pour $\mathcal{C}$ (justifier). En déduire que $\mathcal{C}$ est forcement équivalent à $\mathcal{RM}(1,3)$.*
d) *Trouver le polynôme énumerateur des poids de $\mathcal{C}^\perp$. Quelle est la distance minimale de $\mathcal{C}^\perp$ ?*
e) *Est-ce que $v = (1,1,1,0,1,1,1,1)$ appartient à $\mathcal{C}$ ? Si non, le corriger (c'est-à dire, trouver le mot du code le plus proche à $v$).*

**Solution :**

a) Le nombre de mots dans $\mathcal{C}$ est la somme des coefficients de $w_{\mathcal{C}}(x,y)$, par définition de polynôme énumerateur de poids. Donc $\mathcal{C}$ a 16 mots.
b) Par le cours (et la définition de $w_{\mathcal{C}}(x,y)$), la longueur de $\mathcal{C}$ est le degré de $w_{\mathcal{C}}(x,y)$, i.e. 8. Soit $k$ la dimension de $\mathcal{C}$. On sait, par le cours, que $2^k = 16$, de manière que $k = 4$. Finalement, on a que $A_1(\mathcal{C}) = A_2(\mathcal{C}) = A_3(\mathcal{C}) = 0$ et $A_4(\mathcal{C}) = 14 \neq 0$, de manière que la distance minimale de $\mathcal{C}$ est 4. Donc $\mathcal{C}$ est un $[8,4,4]$ code.
c) Soient $c_1, c_2 \in \mathcal{C}$ de poids 4, $c_1 \neq c_2$. Le poids de $c_1 + c_2$ est forcement 4 ou 8. Dans le premier cas,

$$\#(\mathrm{supp}(c_1) \cap \mathrm{supp}(c_2)) = 2 \tag{1}$$

où $\mathrm{supp}(c) = \{i \mid c_i \neq 0\}$. Dans le deuxième cas, $c_1 + c_2 = u = (1,\ldots,1)$, qui est le seul mot de poids 8 (dans ce cas, $c_1, c_2, u$ sont linéairement dépendantes). Sans perte de généralité, on cherche une matrice génératrice du code dont la dernière ligne est $u$. Donc les autres lignes ont poids 4 et elles doient satisfaire (1). Ainsi, à près d'équivalence, on a

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

On peut observer qu'une telle matrice est de la forme

$$\begin{bmatrix} H_3 & \underline{0}^T \\ \underline{1} & 1 \end{bmatrix}.$$

qui est une matrice génératrice d'un code $\mathcal{RM}(1,3)$.
d) On sait par le cours que $\mathcal{RM}(1,3)$ est autodual. Ainsi $w_{\mathcal{C}^\perp}(x,y) = w_{\mathcal{C}}(x,y)$ et la distance minimale de $\mathcal{C}^\perp$ est 4.
e) Le mot $v$ a poids 7, donc il n'appartient pas à $\mathcal{C}$. La distance entre $v$ et $u$ (défini ci-dessus) est 1, donc $u$ est le mot du code le plus proche à $v$, car la distance minimale est 4.