CONTRÔLE CONTINU N° 2

Exercice 1. *Soit $\mathcal{C}$ le code linéaire sur $\mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z}$ dont une matrice génératrice est*

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

a) *Quel sont les paramètres de $\mathcal{C}$? Justifier.*
b) *Combien y a-t-il de mots dans $\mathcal{C}$? Justifier.*
c) *Trouver le polynôme (énumérateur) des poids $w_{\mathcal{C}}(x, y)$ de $\mathcal{C}$. Justifier.*
d) *En sachant que le coefficient de x^4y^2 dans $w_{\mathcal{C}}(x, y)$ est 4, trouver les mots de poids minimal (non nuls) de $\mathcal{C}$. Justifier.*

Solution :

a) La longueur de $\mathcal{C}$ est 6 (nombre de colonnes) et sa dimension est 4 (nombre de lignes). La matrice de parité de $\mathcal{C}$ est, par un résultat du cours,

$$H = \begin{bmatrix} 1 & 1 & 2 & 2 & 2 & 0 \\ 1 & 2 & 2 & 1 & 0 & 2 \end{bmatrix}.$$

Il n'y a pas de colonnes nulles, donc la distance minimale est au moins 2. On remarque que la troisième colonne est 2 fois la première (et la quatrième colonne est 2 fois la deuxième). Donc il y a (au moins) deux colonnes liées, de manière que la distance minimale est 2.

b) Dans $\mathcal{C}$ il y a $3^4 = 81$ mots, car 4 est la dimension de l'espace vectoriel et 3 la cardinalité du corps.

c) Puisque $\#\mathcal{C} = 81$ est trop grande, nous pouvons plus facilement déterminer le polynôme des poids de $\mathcal{C}^\perp$ et après utiliser le Théorème de MacWilliams. Puisque H (déterminée dans le point a)) est la matrice génératrice de $\mathcal{C}^\perp$, on a que les mots de $\mathcal{C}^\perp$ sont

$$\begin{aligned} c_1 &= (0,0)G = (0,0,0,0,0,0) \\ c_2 &= (0,1)G = (1,2,2,1,0,2) \\ c_3 &= (0,2)G = (2,1,1,2,0,1) \\ c_4 &= (1,0)G = (1,1,2,2,2,0) \\ c_5 &= (1,1)G = (2,0,1,0,2,2) \\ c_6 &= (1,2)G = (0,2,0,1,2,1) \\ c_7 &= (2,0)G = (2,2,1,1,1,0) \\ c_8 &= (2,1)G = (0,1,0,2,1,2) \\ c_9 &= (2,2)G = (1,0,2,0,1,1) \end{aligned}$$

On a $\mathrm{wt}(c_1) = 0$, $\mathrm{wt}(c_5) = \mathrm{wt}(c_6) = \mathrm{wt}(c_8) = \mathrm{wt}(c_9) = 4$ et $\mathrm{wt}(c_2) = \mathrm{wt}(c_3) = \mathrm{wt}(c_4) = \mathrm{wt}(c_7) = 5$, de manière que

$$w_{\mathcal{C}^\perp}(x, y) = x^6 + 4x^2y^4 + 4xy^5.$$

Ainsi, par le Théorème de MacWilliams (on utilise le fait que $(\mathcal{C}^\perp)^\perp = \mathcal{C}$), on a que

$$w_{\mathcal{C}}(x, y) = \frac{1}{\#\mathcal{C}^\perp} w_{\mathcal{C}^\perp}(x + 2y, x - y) =$$

$$= \frac{1}{9}((x + 2y)^6 + 4(x + 2y)^2(x - y)^4 + 4(x + 2y)(x - y)^5).$$

d) Le coefficient de x^4y^2 dans $w_{\mathcal{C}}(x, y)$ est 4, de manière qu'il y a 4 mots de poids 2, qui est le poids minimal pour le point a). Déjà dans le point a) on a observé deux couples de colonnes liées, ce qui nous donne les 4 mots de poids minimal :

$$(1, 0, 1, 0, 0, 0), (2, 0, 2, 0, 0, 0)$$
$$(0, 1, 0, 1, 0, 0), (0, 2, 0, 2, 0, 0).$$

Exercice 2. *Soit $\mathcal{C}$ un $[n, k, d]_q$ code sur un corps fini $\mathbb{F}_q$ de cardinalité q et soit*

$$\widehat{\mathcal{C}} := \{(c_1, \ldots, c_{n+1}) \in \mathbb{F}_q^{n+1} \mid (c_1, \ldots, c_n) \in \mathcal{C} \text{ et } c_1 + \ldots + c_{n+1} = 0\}.$$

a) *Montrer $\widehat{\mathcal{C}}$ est un code linéaire.*
b) *Quels sont les paramètres de $\widehat{\mathcal{C}}$? Justifier.*
c) *Soit H une matrice de parité pour $\mathcal{C}$. Donner une matrice de parité pour $\widehat{\mathcal{C}}$ (justifier la réponse).*
d) *En déduire que $\widehat{\mathcal{H}_3} = \mathcal{RM}(1, 3)$, où $\mathcal{H}_3$ est un code de Hamming avec $m = 3$ et $\mathcal{RM}(1, 3)$ est un code de Reed-Muller d'ordre 1 et degrée m.*

Solution :

a) Il faut montrer que $\widehat{\mathcal{C}}$ est stable par combinaison linéaire. Soient

$$c = (c_1, \ldots, c_{n+1}) \quad \text{et} \quad d = (d_1, \ldots, d_{n+1})$$

deux mots dans $\widehat{\mathcal{C}}$. Alors

$$\lambda c + \mu d = (\lambda c_1 + \mu d_1, \ldots, \lambda c_{n+1} + \mu d_{n+1})$$

appartient à $\widehat{\mathcal{C}}$. En effet

$$(\lambda c_1 + \mu d_1, \ldots, \lambda c_n + \mu d_n) \in \mathcal{C},$$

car $\mathcal{C}$ est un code linéaire, et

$$\lambda c_1 + \mu d_1 + \ldots + \lambda c_{n+1} + \mu d_{n+1} = \lambda(c_1 + \ldots + c_{n+1}) + \mu(d_1 + \ldots + d_{n+1}) = 0$$

b) La longueur de $\widehat{\mathcal{C}}$ est $n+1$ par définition. À tout mot de $\mathcal{C}$ correspond un et un seul mot de $\widehat{\mathcal{C}}$, de manière que $\#\widehat{\mathcal{C}} = \#\mathcal{C}$. Donc $\dim \widehat{\mathcal{C}} = k$. Finalement, la distance minimale est d, s'il existe un mot c dans $\mathcal{C}$ de poids d tel que $c_1 + \ldots + c_n = 0$, et $d + 1$ autrement.

c) Par définition de $\widehat{\mathcal{C}}$, on a que une matrice de parité par $\widehat{\mathcal{C}}$ est

$$\left(\begin{array}{ccc|c} & \mathbf{H} & & 0 \\ & & & \vdots \\ & & & 0 \\ \hline 1 & \dots & 1 & 1 \end{array}\right)$$

car aux équations de contrôle de $\mathcal{C}$ on ajoute juste $c_1 + \ldots + c_{n+1} = 0$, qui nous donne la dernière ligne.

d) Par le point c) de par définition de code de Hamming on a que la matrice de parité de $\widehat{\mathcal{H}_3}$ est

$$\left(\begin{array}{ccc|c} & \mathbf{H}_3 & & 0 \\ & & & \vdots \\ & & & 0 \\ \hline 1 & \dots & 1 & 1 \end{array}\right)$$

qui est la matrice génératrice de $\mathcal{RM}(1,3)$, par le cours. Donc $\widehat{\mathcal{H}_3} = \mathcal{RM}(1,3)^{\perp}$. Mais, toujours par le cours, $\mathcal{RM}(1,3)^{\perp} = \mathcal{RM}(3-1-1,3) = \mathcal{RM}(1,3)$.