CONTRÔLE CONTINU N° 1

NOM Prénom : .....

Numéro d'étudiant : .....

Barême : Ex1-10 points, Ex2-10 points.

Répondre aux questions en justifiant la réponse. La qualité de la rédaction sera prise en compte.

Exercice 1. *Soit $\mathcal{C}$ le code linéaire de longueur 5 sur $\mathbb{F}_5 \cong \mathbb{Z}/5\mathbb{Z}$ dont une matrice génératrice est*

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}.$$

a) *Donner la définition de code linéaire et des ses paramètres. Quel sont les paramètres de $\mathcal{C}$? Justifier.*
b) *Combien y a-t-il de mots dans $\mathcal{C}$? Justifier.*
c) *Donner une matrice de parité pour $\mathcal{C}$ et calculer le syndrome de*

$$v = (0, 1, 2, 3, 4).$$

Est-ce que v appartient à $\mathcal{C}$? Si non, le corriger.

Solution :

a) Un code linéaire $\mathcal{C}$ de longueur n sur un corps fini K est un sous-espace de l'espace vectoriel K^n. Ses paramètres sont sa longueur n, sa dimension k et sa distance minimale, i.e.

$$d = \mathrm{d}(\mathcal{C}) = \min_{c,c' \in \mathcal{C}, c \neq c'} d(c, c').$$

Puisque une matrice génératrice est une matrice dont les lignes forment une base de $\mathcal{C}$, on a que la longueur de $\mathcal{C}$ est 5 et sa dimension est 3. Pour calculer sa distance minimale, on calcule d'abord une matrice de parité : par un résultat du cours, on a que

$$H = \begin{bmatrix} 1 & 1 & 1 & 4 & 0 \\ 1 & 2 & 3 & 0 & 4 \end{bmatrix}$$

est une matrice de parité pour $\mathcal{C}$. Cette matrice n'a pas de colonnes nulles, ni de couples de colonnes liés, donc la distance minimale est au moins 3 par le résultat vu dans le cours. Mais toute ligne de la matrice génératrice a poids 3, de manière que la distance minimale est exactement 3.

b) Dans $\mathcal{C}$ il y a $125 = 5^3$ mots, par le résultat vu dans le cours.

c) Au point a) on a calculé une matrice de parité H. On peut donc calculer le syndrome de v avec H :

$$vH^T = (0, 4).$$

Il est diffént du vecteur nul. Donc v n'appartient pas à $\mathcal{C}$. On peut remarquer facilement qu'il est égal à la dernière colonne de H. Ainsi

$$(0, 0, 0, 0, 1)H^T = vH^T.$$

Par conséquent, le mot corrigé est

$$v - (0, 0, 0, 0, 1) = (0, 1, 2, 3, 3).$$

Exercice 2. *Soit $\mathcal{C}$ un $[n, k, d]$ code sur $\mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z}$ tel que $\mathcal{C} \subseteq \mathcal{C}^\perp$ (un tel code est dit **auto-orthogonal**).*

a) *Montrer tout mot de $\mathcal{C}$ a poids pair.*
b) *Montrer que $\mathbf{1} = (1, 1, \ldots, 1) \in \mathcal{C}^\perp$.*
c) *Montrer que $\dim \mathcal{C} \leq n/2$.*
d) *Montrer que si G est une matrice génératrice pour $\mathcal{C}$, alors GG^T est égale à la matrice nulle $k \times k$.*
e) *En sachant que tout le mot non nul d'un code simplexe $\mathcal{S}_m$ a poids 2^{m-1}, montrer que, pour $m \geq 3$, $\mathcal{S}_m \subseteq \mathcal{H}_m$ ($\mathcal{H}_m$ est un code de Hamming).*

Solution :

a) Tout mot c doit être orthogonal à soi même. Or, sur $\mathbb{F}_2$ on a $1 \cdot 1 = 1$, de manière que $\mathrm{wt}(c) \equiv \langle c, c\rangle \bmod 2$. Ainsi, forcement le poids de c est pair.
b) Pour tout mot $c \in \mathcal{C}$ on a

$$\langle c, \mathbf{1}\rangle \equiv \mathrm{wt}(c) \bmod 2$$

et donc $\langle c, \mathbf{1}\rangle = 0$ par le point a). Ainsi, par la définition du code dual, $\mathbf{1} \in \mathcal{C}^\perp$.
c) $\dim \mathcal{C} \leq \mathcal{C}^\perp = n - \dim \mathcal{C}$. Ainsi $2 \dim \mathcal{C} \leq n$.
d) Le coefficient (i, j) de GG^T est égale au produit scalaire de la i-ème ligne de G fois la j-ème ligne de G. Puisque le code est auto-orthogonal, ce produit est nul.
e) Puisque $\mathcal{H}_m$ est le dual d'un code simplexe, on doit juste montrer que $\mathcal{S}_m$ est auto-orthogonal. Pour le faire, il suffit (par définition de code dual) de montrer que si x, y sont deux mots de $\mathcal{S}_m$, alors $\langle x, y\rangle = 0$. Sur $\mathbb{F}_2$ on a que $\langle x, y\rangle \equiv \#\{i | x_i = 1 \text{ et } y_i = 1\} \bmod 2$. En plus

$$\mathrm{wt}(x + y) = \mathrm{wt}(x) + \mathrm{wt}(y) - 2\#\{i | x_i = 1 \text{ et } y_i = 1\}.$$

Puisque $\mathrm{wt}(x + y), \mathrm{wt}(x)$ et $\mathrm{wt}(y)$ sont divisibles par 4, on a que $\#\{i | x_i = 1 \text{ et } y_i = 1\}$ est pair, de manière que $\langle x, y\rangle \equiv 0 \bmod 2$.