CONTRÔLE CONTINU N° 1 – B

NOM Prénom : .....

Numéro d'étudiant : .....

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

Exercice 1. *Soit $\mathcal{C}$ le code de longueur 4 sur $\mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z}$ dont les mots sont de la forme $(c_1, c_2, c_1 - c_2, c_1 + c_2)$.*

a) *Écrire une matrice génératrice pour $\mathcal{C}$.*
b) *Combien y a-t-il de mots dans $\mathcal{C}$? Justifier.*
c) *Quel sont les paramètres de C ? Justifier.*
d) *Est-ce que $\mathcal{C}$ est autodual ? Justifier.*
e) *Est-ce que $\mathcal{C}$ est MDS ? Justifier.*
f) *Est-ce que $v = (1, 1, 1, 2)$ appartient à $\mathcal{C}$? Si non, le corriger (c'est-à dire, trouver le mot du code le plus proche à v).*

Solution :

a) $(c_1, c_2, c_1 - c_2, c_1 + c_2) = c_1(1, 0, 1, 1) + c_2(0, 1, 2, 1)$, et les deux vecteurs sont linéairement indépendentes, de manière qu'une matrice génératrice pour $\mathcal{C}$ est
$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{bmatrix}$$
b) Tout mot est une combinaisons linéaire des deux vecteurs d'une base avec coefficients dans $\mathbb{F}_3$. Ainsi il y a $3^2 = 9$ mots.
c) La longueur est 4 et la dimension est 2. Une matrice de parité pour $\mathcal{C}$ est (par le résultat vu en cours)
$$H = \begin{bmatrix} 1 & 2 & 2 & 0 \\ 1 & 1 & 0 & 2 \end{bmatrix},$$
qui n'a pas ni de colonnes nulles ni de colonnes qui sont l'une un multiple de l'autre. Donc, par le résultat vu en cours, la distance minimale est au moins 3. Puisque dans le code il y a de mots de poids 3 (par exemple les lignes de G), la distance minimale est 3.
d) Soient h_1 et h_2 les deux lignes de H. On a que $-h_1 - h_2$ est égale à la première ligne de G et $h_1 - h_2$ est égale à la deuxième ligne de G, de manière que le code engendré par H est $\mathcal{C}$, qui est donc autodual.
e) Oui, parce que $3 = 4 - 2 + 1$.
f) Le vecteur $v = (1, 1, 1, 2)$ n'appartient pas à $\mathcal{C}$. En effet, $v_3 = 1 \neq 0 = v_1 - v_2$. Le mot $c = (1, 1, 0, 2)$ a distance 1 de v et il est donc le plus proche (car la distance minimale est 3). Pour le trouver, on aurait pu utiliser la méthode de décodage par syndrome aussi.

Exercice 2. *Soit C un $[n, k, d]$ code avec matrice génératrice $G = [I_k|A]$, où I_k est la matrice identité de taille $k \times k$ sur $\mathbb{F}_2$. Supposons $k \geq 3$.*

a) *Montrer que $d \geq 3$ si et seulement si toute ligne de G a poids au moins 3 et toutes les lignes de A sont différentes.*

b) *Soit $A = U + I_k$, où U est la matrice de taille $k \times k$ sur $\mathbb{F}_2$ avec toute entrée égale à 1. Est-ce que le mot*

$$v = (1, \underbrace{0, \ldots, 0}_{2k-2 \text{ fois}}, 1)$$

appartient au code C ?

c) *Soit $A = U + I_k$ comme dans le point* b). *Le mot recu*

$$u = (\underbrace{0, \ldots, 0}_{k-1 \text{ fois}}, \underbrace{1, \ldots, 1}_{k+1 \text{ fois}})$$

n'appartient pas au code C. Le corriger (c'est-à dire, trouver le mot du code le plus proche à u).

Solution :

a) Puisque G est en forme systématique, $H = [A^T|I_{n-k}]$, par le cours. Par le cours, on a aussi que $d \geq 3$ si et seulement si toute colonne de H est non nulle et il n'y a pas de colonnes égales. Cette dernière condition équivaut au fait que les colonnes de A^T (qui sont les lignes de A) aient poids au moins 2 (pour être non nulles et différentes de celles de I_{n-k}) et qu'elles soient différentes, ce qui est équivalent au fait que toute ligne de G a poids au moins 3 et toutes les lignes de A sont différentes.

b) Toutes les lignes de $A = U + I_k$ sont différentes et toute ligne de G a poids $k = 1 + (k - 1)$. Donc la distance minimale de C est 3 par a). Ainsi v, qui a poids 2, n'appartient pas à C.

c) Puisque $A^T = A$, on a que $H = [A|I_k]$. Ainsi Hu^T, qui est la somme des $k + 1$ dernières colonnes de H, est égale à

$$Hu^T = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}.$$

Cela est la dernière colonne de H, c'est-à-dire le syndrome de

$$e = (0, 0, \ldots, 0, 1),$$

de manière que la correction de u est

$$c = u - e = (\underbrace{0, \ldots, 0}_{k-1 \text{ fois}}, \underbrace{1, \ldots, 1}_{k \text{ fois}}, 0)$$