4 Codes cycliques

Exercice 4.1 Soit C le code linéaire sur $\mathbb{F}_5$ de matrice génératrice $G = \begin{pmatrix} 3 & 0 \\ 4 & 3 \\ 1 & 4 \\ 0 & 1 \end{pmatrix}$.

1. Donner la longueur n, la dimension k et le nombre de mots de C.
2. Est-ce que C est un code cyclique ? Si oui, en donner le polynôme générateur g et le polynôme de contrôle h.
3. Montrer que $H = \begin{pmatrix} 1 & 1 & 3 & 0 \\ 0 & 1 & 1 & 3 \end{pmatrix}$ est une matrice de contrôle de C.
4. Calculer la distance minimum d et la capacité de correction t de C.
5. Les mots $\gamma_1 = (1101)$, $\gamma_2 = (1111)$ et $\gamma_3 = (2311)$ sont reçus. Pour chacun d'eux, répondre aux questions suivantes.
   (a) Calculer le syndrome de γ_i.
   (b) Si cela est possible déterminer le mot de code c_i émis, et retrouver le message m_i envoyé sachant qu'il a été encodé par la matrice G.
   (c) Sinon que cela signifie-t-il ?

Exercice 4.2

1. Montrer que dans $\mathbb{F}_5[X]$, le polynôme $g = (X^2 - 1)^2$ divise le polynôme $X^{10} - 1$.

Soit C le code cyclique de longueur 10 sur $\mathbb{F}_5$, engendré par le polynôme g.

2. Quelle est la dimension k de C ? Quel est le nombre de mots de C ?
3. Donner une matrice génératrice de C.
4. Déterminer le polynôme de contrôle de C et donner une matrice de contrôle de C.
5. Montrer que la distance minimum d de C est égale à 3. Quelle est la capacité de correction t de C ?
6. Le mot $\gamma = (1111311111)$ est reçu.
   (a) Quel est le mot de code c émis ?
   (b) Quel est le message m envoyé, sachant qu'il a été encodé par le polynôme g ?

Exercice 4.3 Soit C le code linéaire sur $\mathbb{F}_7$ de matrice génératrice $G = \begin{pmatrix} 1 & 0 \\ 5 & 1 \\ 5 & 5 \\ 2 & 5 \\ 1 & 2 \\ 0 & 1 \end{pmatrix}$.

1. Quelle est la longueur n de C ? Quelle est la dimension k de C ? Quel est le nombre de mots de C ?
2. Est-ce que C est un code cyclique ? Si oui, en donner le polynôme générateur g et le polynôme de contrôle h.
3. Donner une matrice de contrôle de C.
4. Déterminer les générateurs de $(\mathbb{F}_7)^*$ puis montrer que C est un code de Reed-Solomon. En déduire la distance minimum d et la capacité de correction t de C.
5. Le mot $\gamma = (204512)$ est reçu.
   (a) Quel est le mot de code c émis ?
   (b) Quel est le message m envoyé, sachant qu'il est encodé par la matrice G ?

Exercice 4.4 On considère le corps à 8 éléments $\mathbb{K} = \mathbb{F}_2[Y]/(Y^3+Y+1)\mathbb{F}_2[Y] = \mathbb{F}_2[y]$ où y désigne la classe de Y dans $\mathbb{K}$. La table de multiplication de $\mathbb{K}^*$ est donnée ci-dessous.

$\times$	y	$1+y$	y^2	$1+y^2$	$y+y^2$	$1+y+y^2$
y	y^2	$y+y^2$	$1+y$	1	$1+y+y^2$	$1+y^2$
$1+y$	$y+y^2$	$1+y^2$	$1+y+y^2$	y^2	1	y
y^2	$1+y$	$1+y+y^2$	$y+y^2$	y	$1+y^2$	1
$1+y^2$	1	y^2	y	$1+y+y^2$	$1+y$	$y+y^2$
$y+y^2$	$1+y+y^2$	1	$1+y^2$	$1+y$	y	y^2
$1+y+y^2$	$1+y^2$	y	1	$y+y^2$	y^2	$1+y$

Les puissances successives de y sont :

i	0	1	2	3	4	5	6	7
y^i	1	y	y^2	$1+y$	$y+y^2$	$1+y+y^2$	$1+y^2$	1

On note $\mathbb{K}[x] = \mathbb{K}[X]/(X^7+1)\mathbb{K}[X]$.

1. Développer les polynômes $g = (X+1)(X+y)$ et $h = (X+y^2)(X+y^3)(X+y^4)(X+y^5)(X+y^6)$. (On peut aussi obtenir h comme quotient de X^7+1 par g.)
2. Soit $C \subset \mathbb{K}[x]$ le code de Reed-Solomon engendré par g. Quelle est la longueur n de C ? Sa dimension k ? Sa distance minimale d ? Sa capacité de correction t ? Donner une matrice génératrice G et une matrice de contrôle H de C.

On identifie $\mathbb{F}_2^3$ à $\mathbb{K}$ par l'application φ, définie par :

$$\varphi(m_0m_1m_2) = m_0 + m_1y + m_2y^2.$$

On identifie $\mathbb{F}_2^{21}$ à $\mathbb{K}[x]$ par l'application F, définie pour $m = m_0m_1m_2\ m_3m_4m_5\ \ldots\ m_{18}m_{19}m_{20}$ par :

$$F(m) = \varphi(m_0m_1m_2) + \varphi(m_3m_4m_5)x + \cdots + \varphi(m_{18}m_{19}m_{20})x^6$$

On identifie $\mathbb{F}_2^{15}$ à C par l'application E, définie pour $m = m_0m_1m_2\ m_3m_4m_5\ \ldots\ m_{12}m_{13}m_{14}$ par :

$$E(m) = \big(\varphi(m_0m_1m_2) + \varphi(m_3m_4m_5)x + \cdots + \varphi(m_{12}m_{13}m_{14})x^4\big) \times g(x).$$

3. Encoder le message $m = 100\ 001\ 010\ 111\ 100$ en un élément c de $\mathbb{F}_2^{21}$, c'est à dire : calculer $c = F^{-1}\big(E(m)\big)$.
4. Le message $\gamma = 011\ 010\ 111\ 111\ 111\ 100\ 100$ est reçu.
   (a) Quel est le mot de code c émis ? Combien de bits ont été corrigés ?
   (b) Quel est le message m envoyé, sachant que $c = F^{-1}\big(E(m)\big)$?
5. On considère C comme un code binaire de longueur 21 et de dimension 15.
   (a) Donner la matrice génératrice G' de C correspondant à l'encodage $F^{-1} \circ E$.
   (b) Donner la matrice de contrôle H' de C correspondant au polynôme de contrôle h.
   (c) Quelle est la distance minimum et la capacité de correction de C dans ce cadre ? Commenter ce résultat.