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 $\gamma_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$, $\gamma_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ et $\gamma_3 = \begin{pmatrix} 2 \\ 3 \\ 1 \\ 1 \end{pmatrix}$ 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 $\gamma = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 3 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ 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 $\gamma = \begin{pmatrix} 2 \\ 0 \\ 4 \\ 5 \\ 1 \\ 2 \end{pmatrix}$ 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

L'élément y de $\mathbb{K}$ en est donc un élément primitif.

Il est assez lourd d'effectuer des calculs sur des polynômes à coefficients dans $\mathbb{K}$. Nous introduisons donc les notations suivantes des éléments de $\mathbb{K}$:

notation polynomiale		notation binaire		notation octale
0	$\longleftrightarrow$	000	$\longleftrightarrow$	0
1	$\longleftrightarrow$	001	$\longleftrightarrow$	1
y	$\longleftrightarrow$	010	$\longleftrightarrow$	2
$y + 1$	$\longleftrightarrow$	011	$\longleftrightarrow$	3
y^2	$\longleftrightarrow$	100	$\longleftrightarrow$	4
$y^2 + 1$	$\longleftrightarrow$	101	$\longleftrightarrow$	5
$y^2 + y$	$\longleftrightarrow$	110	$\longleftrightarrow$	6
$y^2 + y + 1$	$\longleftrightarrow$	111	$\longleftrightarrow$	7

Les tables d'addition et de multiplication de $\mathbb{K}$ en notation octale sont données ci-dessous. Il convient de s'y reporter pour tous les calculs. L'élément neutre pour l'addition est 0 et l'élément neutre pour la multiplication est 1, mais ATTENTION : pour les éléments de 2 à 7, ces opérations ne correspondent pas aux opérations « standards ».

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

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

1. Quelles sont les racines du polynôme $X^7 + 1$ dans $\mathbb{K}$?
2. Développer les polynômes $g = (X + 1)(X + 2)$ et $h = (X + 3)(X + 4)(X + 5)(X + 6)(X + 7)$ de $\mathbb{K}[X]$ (notation octale). (On peut aussi obtenir h comme quotient de $X^7 + 1$ par g .)
3. 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 (en notation octale).

4. Encoder le message $m = \begin{pmatrix} 4 \\ 1 \\ 2 \\ 7 \\ 4 \end{pmatrix} \in \mathbb{K}^5$ (notation octale) en un élément $c \in \mathbb{K}^7$.

5. Le message $\gamma = \begin{pmatrix} 3 \\ 2 \\ 7 \\ 7 \\ 7 \\ 4 \\ 4 \end{pmatrix} \in \mathbb{K}^7$ (notation octale) est reçu.

- (a) Quel est le mot de code c émis ? En notation binaire, combien de bits ont été corrigés ?
- (b) Quel est le message m envoyé (sachant que $c = G \times m$) ?
6. On considère C comme un code binaire de longueur 21 et de dimension 15.
 - (a) Donner la matrice génératrice G' de C en notation binaire.
 - (b) Donner la matrice de contrôle H' de C en notation binaire.
 - (c) Quelle est la distance minimum et la capacité de correction de C dans ce cadre ? Commenter ce résultat.