Chapitre 3 Codes cycliques.

3.1 Introduction

Les codes cycliques sont une classe importante et puissante de codes linéaires utilisés dans le domaine des communications numériques et de la théorie de l'information. Ils ont été largement étudiés et appliqués dans diverses technologies de communication, notamment dans les systèmes de télécommunications, les réseaux informatiques et les dispositifs de stockage de données.

Les codes cycliques sont des codes correcteurs linéaires qui se fondent sur la théorie des corps finis, et en particulier les extensions de Galois, ainsi que sur les propriétés algébriques spéciales des polynômes cycliques qui sont exploitées pour concevoir un mécanisme efficace de détection et de correction d'erreurs. La principale caractéristique des codes cycliques réside dans leur capacité à garantir la détection et la correction d'un certain nombre d'erreurs, en utilisant des techniques de codage et de décodage relativement simples.

Dans ce chapitre, nous explorerons les principaux concepts et caractéristiques des codes cycliques, y compris leurs structures, leurs représentations polynomiales, leurs polynômes générateurs, leurs matrices génératrices, leurs matrices de contrôles et leur technique de codage systématique en utilisant le syndrome polynomial.

3.2 Définition et description d'un code cyclique

3.2.1 Définition et exemples

Définition 3.1.

Un code linéaire C de longueur *n* sur un corps fini $\mathbb{K}$ est dit **code cyclique** s'il vérifie la propriété suivante:

Pour tout $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{K}^n$:

$$c = (c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow c' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$$

● c' qui n'est que la permutation circulaire des composantes de *c* est appelée **shift** de *c*. C'est à dire que $c' = (c_{n-1}, c_0, \ldots, c_{n-2})$ est le shift de $c = (c_0, c_1, \ldots, c_{n-1})$.

Exemple 3.1.

1. $\{0\}$ et $\mathbb{K}^n$ sont des codes cycliques dits triviaux.

2. Le code $C = \{000,101,011,110\}$ est un code cyclique.

3. Tout code de Hamming est un code cyclique.

4. Le code $C = \{0000,1001,0110,1111\}$ n'est pas un code cyclique, car le mot c=1001$\in C$ et son shift c'=1100$\notin C$.

3.2.2 Représentation polynomial d'un code cyclique

Tout mot $c = (c_0, c_1, \ldots, c_{n-1})$ d'un code linéaire C sur un corps fini $\mathbb{K}$ peut être identifier à un polynôme $c(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1}$ de $\mathbb{K}[X]$.

On associée au mot shift $c' = (c_{n-1}, c_0, \ldots, c_{n-2})$ du mot c , le polynôme

$c'(X) = c_{n-1} + c_0X + \ldots + c_{n-2}X^{n-1}$ de $\mathbb{K}[X]$, ce polynôme peut être obtenu en calculant le produit $Xc(X)$ et en considérant que $X^n = 1$, c'est-à-dire en calculant modulo $X^n - 1$, et précisément ce calcul se fait dans l'anneau quotient $\mathbb{K}[X]/< X^n - 1 >$.

De ce qui précède, on obtient la proposition suivante :

Proposition 3.1.

Un code linéaire $C(n, k)$ est cyclique si, et seulement si, pour tout mot c de C, le polynôme $Xc(X)$ calculé modulo $X^n - 1$, est le polynôme associée au mot $c' = (c_{n-1}, c_0, .., c_{n-2})$ de C.

Définition 3.2.

Soit $\mathbb{K}$ un corps fini et n un entier non nul.

● On appelle **représentation polynomiale de $\mathbb{K}^n$**, l'application θ définie par

$$\theta : \mathbb{K}^n \to \mathbb{K}[X]/< X^n - 1 >$$

$$c = (c_0, c_1, \ldots, c_{n-1}) \mapsto \theta(c) = c(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1}$$

Le polynôme $c(X)$ est dit **représentation polynomiale du mot** c.

● On appelle **représentation polynomiale d'un code cyclique** C de $\mathbb{K}^n$, l'ensemble des représentations polynomiales des mots du code C, c'est-à-dire :

$$\theta(C) = \{\theta(c) : c \in C\} = Im(\theta).$$

Proposition 3.2.

Soit C un code linéaire de langueur *n* sur un corps fini $\mathbb{K}$.

C est un code cyclique si, et seulement si, sa représentation polynomiale $\theta(C)$ est un idéal de l'anneau $\mathbb{K}[X]/< X^n - 1 >$.

Preuve.

Supposons que C est un code cyclique et soit $c(X) = \sum_{i=0}^{n-1} c_i X^i$, $d(X) = \sum_{i=0}^{n-1} d_i X^i$ dans $\theta(C)$, donc $c = (c_0, c_1, \ldots, c_{n-1})$ et $d = (d_0, d_1, \ldots, d_{n-1}) \in C$, et comme *C* est un sous-espace vectoriel, alors pour $\alpha, \beta \in \mathbb{K}$, le mot $m = \alpha c + \beta d \in C$, ce qui donne en représentation polynomiale : $m(X) = \alpha c(X) + \beta d(X) \in \theta(C)$, d'où $\theta(C)$ est un espace vectoriel sur $\mathbb{K}[X]$. De plus soit $p(X) = \sum_{i=0}^{n-1} a_i X^i \in \mathbb{K}[X]/< X^n - 1 >$, alors comme $c(X) \in \theta(C)$ et C cyclique alors $c(X), Xc(X), X^2c(X), \ldots, X^ic(X), \ldots \in \theta(C)$ et donc $a_0c(X) + a_1Xc(X) + a_2X^2c(X) + \ldots \in \theta(C)$, par la suite $p(X)c(X) \in \theta(C)$, d'où $\theta(C)$est un idéal de $\mathbb{K}[X]/< X^n - 1 >$.

Inversement, soit $\theta(C)$ un idéal de $\mathbb{K}[X]/< X^n - 1 >$. Alors si $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ alors $c(X) = \sum_{i=0}^{n-1} c_i X^i \in \theta(C)$ et donc $Xc(X) \in \theta(C) \Rightarrow c' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$, ce qui montre que C est un code cyclique.

Théorème 3.1.

Soient $\mathbb{K}$ un corps fini et *n* un entier non nul, C un code cyclique de longueur *n* non réduit à $\{0\}$. Alors $\theta(C)$ est un idéal principal de l'anneau $\mathbb{K}[X]/< X^n - 1 >$.

Preuve

Soit $g(X)$ un polynôme non nul et unitaire dans $\theta(C)$, de degré minimum. En effectuant la division Euclidienne de $X^n - 1$ par $g(X)$ (dans $\mathbb{K}[X]$), on trouve

$X^n - 1 = g(X)q(X) + r(X)$ avec $r(X) = 0$ ou $d^\circ\big(r(X)\big) < d^\circ\big(g(X)\big)$, donc dans $\mathbb{K}[X]/< X^n - 1 >$: $g(X)q(X) = -r(X) \in \theta(C)$, avec $d^\circ\big(r(X)\big) < d^\circ\big(g(X)\big)$, ce qui contredit la définition de $g(X)$ et donc $r(X) = 0$ et $X^n - 1 = g(X)q(X)$, d'où $g(X)$ divise $X^n - 1$.

Montrons que $\theta(C) =< g(X) >$. Soit $f(X) \in \theta(C)$, en divisant $f(X)$ par $g(X)$ dans $\mathbb{K}[X]$, alors il existe $q'(X), r'(X)$ dans $\mathbb{K}[X]$: $f(X) = q'(X)g(X) + r'(X)$ avec $r'(X) = 0$ ou $d^\circ\big(r'(X)\big) < d^\circ\big(g(X)\big)$, on trouve comme précédemment $r'(X) = 0$ et donc $f(X)$ est un multiple de $g(X)$ et $\theta(C)$ est un idéal principal engendré par $g(X)$.

3.2.3 Polynôme générateur et matrice génératrice d'un code cyclique

Définition 3.3.

Le polynôme $g(X)$ dans le Théorème 3.1 engendrant $\theta(C)$ est appelé le **polynôme générateur** du code cyclique *C*. $\theta(C)$ est l'idéal constitué des multiples de $g(X)$ dans $\mathbb{K}[X]/< X^n - 1 >$.

On a : $c \in C \Leftrightarrow c(X) \in \theta(C) \Leftrightarrow \exists\, q(X) \in \mathbb{K}[X]: c(X) = q(X)g(X)$. Du Théorème 3.1, on déduit les propriétés suivantes du polynôme générateur $g(X)$.

Proposition 3.1.

1. Le polynôme $g(X)$ est de degré minimale dans $\theta(C)$.
2. Le polynôme $g(X)$ est unitaire et unique.
3. Tout mot du code cyclique est multiple du polynôme générateur.
4. $g(X)$ divise $X^n - 1$.

Exemple 3.2.

Soit $C\,(3,2)$ un code cyclique tel que $\theta(C) = \{0,1 + X, 1 + X^2, X + X^2\}$

Le polynôme $X + 1$ est le polynôme générateur du code C.

Remarque 3.1.

Pour trouver tous les codes cycliques de longueur *n* sur $\mathbb{F}_p$, il suffit de trouver tous les diviseurs du polynôme $X^n - 1$ sur $\mathbb{F}_p$. Pour cela il faut décomposer le polynôme $X^n - 1$ en produit de polynômes irréductibles sur $\mathbb{F}_p$.

Exemple 3.3.

Les codes cycliques non nuls de longueur *n=5* sur le corps $\mathbb{F}_2$:

La décomposition de $X^5 - 1$ sur $\mathbb{F}_2$ en polynômes cyclotomiques donne

$$\begin{aligned} X^5 - 1 &= \prod_{d/5} \phi_d(X) \\ &= \phi_1(X)\phi_5(X) \\ &= (X-1)(X^4 + X^3 + X^2 + X + 1) \end{aligned}$$

Soit $\mathbb{K}=\mathbb{F}_{2^r}$, le corps des racines 5$^{\text{ieme}}$ de l'unité sur $\mathbb{F}_2$, où *r* est le plus petit entier non nul tel que *n*=5 divise $2^r - 1$, alors on trouve *r=4* et donc $\mathbb{K} = \mathbb{F}_{16}$. $\phi_5(X)$ est irréductible sur $\mathbb{F}_2$ car φ(5)=*r*=4. Chaque diviseur donne un générateur d'un code cyclique de longueur $n = 5$ sur$\mathbb{F}_2$
Si on note $g_i(X)$ le générateur du code C_i on trouve :
C_0: $g_0(X) = X^5 - 1 = 0 \rightarrow C_0 = \{0\}$.

$C_1: g_1(X) = X - 1.$

$C_2: g_2(X) = X^4 + X^3 + X^2 + X + 1.$

$C_3: g_3(X) = 1 \rightarrow C_3 = \mathbb{K}^5.$

Exemple 3.4.

Les codes cycliques non nuls de longueur *n=7* sur le corps $\mathbb{F}_2$.

La décomposition de $X^7 - 1$ sur $\mathbb{F}_2$ en polynômes cyclotomiques donne :

$$\begin{aligned} X^7 - 1 &= \prod_{d/7} \phi_d(X) \\ &= \phi_1(X)\phi_7(X) \\ &= (X-1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1) \end{aligned}$$

Soit $\mathbb{K}= \mathbb{F}_{2^r}$, le corps des racines 5^{ieme} de l'unité sur $\mathbb{F}_2$, où *r* est le plus petit entier non nul tel que *n=7* divise $2^r - 1$, alors *r=3* et donc $\mathbb{K}=\mathbb{F}_8$.

Le degré de $\phi_7(X)$ est $\varphi(7) = card\{i \in \mathbb{N} \ / \ i < 7 \ et \ i \wedge 7 = 1\} = 6$ donc $\phi_7(X)$ n'est pas irreductible, mais il se décompose en produit de $\frac{\varphi(7)}{r} = 2$ polynômes irréductibles de degré *r=3* sur$\mathbb{F}_2$, donc $\phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = (X^3 + bX^2 + cX + 1)(X^3 + b'X^2 + c'X + 1)$, après identification on trouve : $b = c' = 0$ et $c = b' = 1$, donc

$\phi_7(X) = (X^3 + X^2 + X + 1)(X^3 + X^2 + X + 1)$, d'où la décomposition de $X^7 - 1$ est :

$X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$ et chaque diviseur $g_i(X)$ de $X^7 - 1$ engendre un code cyclique C_i de longueur *n=7* sur $\mathbb{F}_2$.

$C_0: g_0(X) = X^7 - 1 = 0, C_0 = \{0\}$ est le code cyclique trivial.

$C_1: g_1(X) = X - 1$

$C_2: g_2(X) = X^3 + X + 1$

$C_3: g_3(X) = X^3 + X^2 + 1$

$C_4: g_4(X) = (X - 1)(X^3 + X + 1) = X^4 + X^3 + X^2 + 1$

$C_5: g_5(X) = (X - 1)(X^3 + X^2 + 1) = X^4 + X^2 + X + 1$

$C_6: g_6(X) = (X^3 + X + 1)(X^3 + X^2 + 1) = X^6 + X^5 + X^4 + X^3 + X^2 + 1$

Pour tout *i*, la représentation polynomiale $\theta(C_i)$ est formée par tous les multiples de $g_i(X)$ modulo $X^7 - 1$, c'est-à-dire par les produits $q(X)g_i(X)$, $q(X) \in \mathbb{K}[X]/< X^7 - 1 >$ et donc le code C_i est formée par tous les mots correspondants à ces produits.

Théorème 3.2.

Soit C un code cyclique de longueur n sur un corps fini $\mathbb{K}$ de polynôme générateur

$g(X) = g_0 + g_1X + g_2X^2 + \ldots + g_{t-1}X^{t-1} + X^t$ avec $d°g(X) = t$. Alors $\dim C = k = n - t$.

Et C admet la matrice suivante G comme matrice génératrice :

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \ldots & g_t & 0 & \ldots & \ldots & 0 \\ 0 & g_0 & g_1 & g_2 & \ldots & g_t & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & g_0 & g_1 & g_2 & \ldots & g_t & 0 \\ 0 & \ldots & \ldots & 0 & g_0 & g_1 & g_2 & \ldots & g_t \end{pmatrix}.$$

Preuve.

Soit C un code cyclique de longueur n sur $\mathbb{K}$ et $g(X)$ le générateur de C, tel que $d°\big(g(X)\big) = t$. Tout polynôme $c(X)$ de la représentation $\theta(C)$ est de la forme :

$c(X) = a(X)g(X) = (a_0 + a_1X + a_2X^2 + \cdots + a_sX^s)\big(g(X)\big)$

$= a_0g(X) + a_1Xg(X) + a_2X^2g(X) + \ldots + a_sX^sg(X)$, avec $a_s \in \mathbb{K}$ et $0 \leq s \leq n-1$, les polynômes $g(X), Xg(X), \ldots, X^sg(X)$ forment donc une famille génératrice de $\theta(C)$. On va extraire de cette famille génératrice une base pour $\theta(C)$.

Soit $c(X) = a(X)g(X) \in \theta(C)$ et $h(X) = X^n - 1/g(X)$ dans $\mathbb{K}[X]$. En utilisant la division Euclidienne de $a(X)$ par $h(X)$ dans $\mathbb{K}[X]$, on obtient

$a(X) = q(X)h(X) + r(X)$, avec $d°r(X) < d°h(X) = n - t$, donc $r(X)$ est de la forme:

$$r(X) = r_0 + r_1X + \ldots + r_{n-t-1}X^{n-t-1},$$

en conséquence

$$\begin{aligned} a(X)g(X) &= q(X)h(X)g(X) + r(X)g(X) \\ &= (X^n - 1)q(X) + r(X)g(X). \end{aligned}$$

En calculant dans l'anneau quotient $\mathbb{K}[X] / < X^n - 1 >$, on déduit que

$a(X)g(X) = r(X)g(X)$ $donc$ $c(X) = r_0g(X) + r_1Xg(X) + \ldots + r_{n-t-1}X^{n-t-1}g(X)$, d'où la famille des polynômes $g(X), Xg(X), \ldots, X^{n-t-1}g(X)$ est une famille génératrice de $\theta(C)$.

Montrons que cette famille est libre ? Dans $\mathbb{K}[X] / < X^n - 1 >$ considérons l'égalité:

$$\alpha_0g(X) + \alpha_1Xg(X) + \cdots + \alpha_{n-t-1}X^{n-t-1}g(x) = 0, \ldots(*)$$

avec $\alpha_i \in \mathbb{K}$ et $i \in \{0, 1, \ldots, n-t-1\}$. L'égalité (*) implique que dans $\mathbb{K}[X]$, on a:

$$(\alpha_0 + \alpha_1 X + \cdots + \alpha_{n-t-1} X^{n-t-1}) g(X) \equiv 0 (mod\ X^n - 1)$$

Posons $d(X) = (\alpha_0 + \alpha_1 X + \cdots + \alpha_{n-t-1} X^{n-t-1}) g(X)$, alors $d(X)$ est de degré au plus $n-1$ et $d(X)$ divisible par $X^n - 1$, cela conduit à $d(X) = 0$. Comme $\mathbb{K}[X]$ est intègre et $g(X)$ n'est pas nul, alors $\alpha_0 + \alpha_1 X + \alpha_{n-t-1} X^{n-t-1} = 0$, donc $\alpha_0 = \cdots = \alpha_{n-t-1} = 0$, et d'où la famille $\{g(X), Xg(X), \ldots, X^{n-t-1} g(X)\}$ est libre et donc elle forme une base de $\theta(C)$ et la dimension de C est: *k*= *n-t*. Les mots $l_0, l_1, \ldots, l_{n-t}$ correspondants respectivement au polynômes $g(X), Xg(X), \ldots, X^{n-t-1} g(X)$ forme une base du code C et donc la matrice G dont les lignes sont les mots:

$l_0 = g_0 g_1 g_2 \ldots g_t 0 \ldots 0$, $l_1 = 0 g_0 g_1 g_2 \ldots g_t 0 \ldots 0$, $\ldots$, $l_{n-t-1} = 0 \ldots 0 g_0 g_1 g_2 \ldots g_t$ est une matrice génératrice de C.

Exemple 3.5.

1. Le code de Hamming de paramètre $C(7, 4, 3)$ et de polynôme générateur : $g(X) = 1 + X + X^3$, admet comme matrice génératrice la matrice :

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

2. Pour les codes cycliques de longueur $n = 7$, on a le tableau suivant

Le code cyclique	Le générateur	La dimension
c_0	0	0
c_1	$X - 1$	6
c_2	$X^3 + X + 1$	4
c_3	$X^3 + X^2 + 1$	4
c_4	$X^4 + X^3 + X^2 + 1$	3
c_5	$X^4 + X^2 + X + 1$	3
c_6	$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$	1

Tableau 3.1 Table Codes cycliques de longueur *n*=7 et leurs dimensions.

1- Le code cyclique $C_4(7, 3, 3)$ admet comme générateur le polynôme $g_4(X) = X^4 + X^2 + X + 1$ et comme matrice génératrice la matrice :

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

3.3 Polynôme et matrice de contrôle d'un code cyclique

3.3.1 Polynôme d'un code cyclique

Définition 3.4.

Soit C un code cyclique de longueur n sur un corps fini $\mathbb{K}$ et de polynôme générateur $g(X)$.

Le polynôme $h(X) \in \mathbb{K}[X]$ tel que $h(X) = \frac{X^n-1}{g(X)}$ est dit **polynôme de contrôle** du code C.

- Le degré de $h(X)$ est donc $k = n - d°g(X) = n - t$.
- c est un mot de C si, et seulement si, $c(X)h(X) = 0$ dans $\mathbb{K}[X]/< X^n - 1 >$.

3.3.2 Matrice de contrôle d'un code cyclique

Théorème 3.3.

Soit C un code cyclique de longueur n sur un corps $\mathbb{K}$:

1. L'orthogonal $C^\perp$ d'un code cyclique C est un code cyclique.

2. Si $h(X) = h_0 + h_1X + h_2X^2 + \ldots + h_kX^k$ est le polynôme de contrôle du code cyclique C alors le générateur de $C^\perp$ est $h_1(X) = h_0^{-1}\bar{h}(X)$ où $\bar{h}(X) = X^k h(X^{-1})$ est le polynôme réciproque de $h(X)$.

3. La matrice H_1 suivante est une matrice de contrôle de C :

$$H_1 = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \ldots & h_0 & 0 & \ldots & \ldots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \ldots & h_0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & h_k & h_{k-1} & h_{k-2} & \ldots & h_0 & 0 \\ 0 & \ldots & \ldots & 0 & h_k & h_{k-1} & h_{k-2} & \ldots & h_0 \end{pmatrix}$$

Preuve.

On a $X^n - 1 = h(X)g(X)$ alors $h(X)g(X) = 0$ dans $\mathbb{K}[X] /< X^n - 1 >$. Soit

$a(X) = \sum_{i=0}^{n-1} a_iX^i \in \theta(C)$, donc $a(X)$ est un multiple de $g(X)$ dans $\mathbb{K}[X] /< X^n - 1 >$.

Si $h(X) = \sum_{i=0}^{n-1} h_i X^i$, alors $h(X)a(X) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_j h_{i-j} X^i = 0$ (où les différences

i-j sont calculées modulo *n*), on déduit que pour tout $i \in \{0, \dots, n-1\}$: $\sum_{j=0}^{i} a_j h_{i-j} = 0$.

En particulier, pour tout $i \in \{k, \dots, n-1\}$ on trouve les relations suivantes :

- Si *i=k*: $a_0 h_k + a_1 h_{k-1} + a_2 h_{k-2} + \cdots + a_k h_0 + a_{k+1} 0 + \cdots + a_{n-1} 0 = 0$ donc

$$(h_k, h_{k-1}, h_{k-2}, \dots, h_0, 0, \dots, 0) \perp (a_0, a_1, \dots, a_{n-1}).$$

- Si *i=k+1*: $a_0 0 + a_1 h_k + a_2 h_{k-1} + \cdots + a_k h_1 + a_{k+1} h_0 + \cdots + a_{n-1} 0 = 0$ donc

$$(0, h_k, h_{k-1}, h_{k-2}, \dots, h_0, 0, \dots, 0) \perp (a_0, a_1, \dots, a_{n-1}).$$

- Si *i=k+2*: $a_0 0 + a_1 0 + a_2 h_k + \cdots + a_k h_2 + a_{k+1} h_1 + \cdots + a_{n-1} 0 = 0$ donc

$$(0,0, h_k, h_{k-1}, \dots, h_0, 0, \dots, 0) \perp (a_0, a_1, \dots, a_{n-1}).$$

$$\vdots$$

- Si *i=n-1*: alors $a_0 . 0 + a_1 . 0 + a_2 . 0 + \cdots + a_{n-k-2} . 0 + a_{n-k-1} h_k + \cdots + a_{n-1} h_0 = 0$ donc

$$(0,0,0, \dots 0, h_k, h_{k-1}, \dots, h_1, h_0) \perp (a_0, a_1, \dots, a_{n-1}).$$

Les relations précédentes montrent que les shifts du mot $(h_k, h_{k-1}, h_{k-2}, \dots, h_0, 0, \dots, 0)$ sont orthogonaux au mot $a = (a_0, a_1, \dots, a_{n-1}) \in C$. .En d'autres termes ,les mots suivants :

$$(h_k, h_{k-1}, h_{k-2}, \dots, h_0, 0, \dots, 0)$$

$$(0, h_k, h_{k-1}, h_{k-2}, \dots, h_0, 0, \dots, 0)$$

$$\vdots$$

$$(0,0,0, \dots, h_k, h_{k-1}, \dots, h_1, h_0)$$

Sont orthogonaux au code C donc ils appartient à $C^{\perp}$.

Soit $H_1 = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & \dots & \dots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 \\ 0 & \dots & \dots & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 \end{pmatrix}$

la matrice dont les lignes sont ces mots ci-dessus. La matrice constitué des $t=n-k$ premières colonnes de la matrice H_1 est une matrice triangulaire inversible car $h_k \neq 0$, ce qui prouve que la matrice H_1 est de rang t, donc ses lignes forment une base à $C^{\perp}$. Ce qui montre que H_1 est une matrice de contrôle du code C. Comme $h(X)$ divise $X^n - 1$, alors $h(0) = h_0 \neq 0$, et donc la matrice $H = h_0^{-1} H_1$ est aussi une autre matrice de contrôle de C, de plus le polynôme associé à la première ligne de H est le polynôme

$$h_1(X) = h_0^{-1}(h_k + h_{k-1}X + \cdots + X^k) = h_0^{-1}\bar{h}(X)$$

(où $\bar{h}(X)$ est le polynôme réciproque de $h(X)$) qui est un polynôme unitaire divisant $X^n - 1$, c'est donc « le » générateur du code cyclique $C^{\perp}$. Par ailleurs on constate que la matrice H est une matrice génératrice du code cyclique engendré par le polynôme $h_1(X)$.

Exemple 3.6.

Soit C un code cyclique sur $\mathbb{F}_2$ de longueur $n=7$ et de polynôme générateur

$$g(X) = X^3 + X^2 + 1,$$

alors le polynôme de contrôle de C est :

$$\begin{aligned} h(X) &= X^7 - 1/(X^3 + X^2 + 1) \\ &= X^4 + X^3 + X^2 + 1 \end{aligned}$$

L'orthogonal de C est engendré par le polynôme : $h_1(X) = X^4 h(X^{-1}) = X^4 + X^2 + X + 1$

et donc C admet comme matrice contrôle la matrice

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

3.4 Codes et codage cycliques systématiques

3.4.1 Codes cycliques systématiques

Définition 3.5.

Un code cyclique $C(n,k)$ sur un corps fini $\mathbb{K}$ est dit **code cyclique systématique**, s'il admet une matrice génératrice G dite **normalisée** dont les *k* dernières colonnes forment la matrice identité I_k et non pas les *k* premières colonnes dans le cas des codes linéaires. c-à-d $G = (M, I_k)$ où $M \in M_{k,n-k}(\mathbb{K})$.

Exemple 3.7.

Le code cyclique C de longueur *n*=7 et de générateur $g(X) = X^3 + X + 1$ sur $\mathbb{F}_2$, admet comme matrice génératrice la matrice suivante G :

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Qu'on peut mettre sous la forme normalisée

$$G_N = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Donc C est un code cyclique systématique.

3.4.2 Algorithme de codage systématique d'un code cyclique

Soit C un code cyclique de longueur *n* sur un corps fini $\mathbb{K}$ de générateur le polynôme

$$g(X) = g_0 + g_1X + g_2X^2 + \ldots + g_tX^t, \text{ tel que } d°(g(X)) = t.$$

Le code C admet une matrice génératrice (pas nécessairement normalisée) G de la forme

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \ldots & g_t & 0 & \ldots & \ldots & 0 \\ 0 & g_0 & g_1 & g_2 & \ldots & g_t & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & g_0 & g_1 & g_2 & \ldots & g_t & 0 \\ 0 & \ldots & \ldots & 0 & g_0 & g_1 & g_2 & \ldots & g_t \end{pmatrix}$$

$G = (M, T)$ où $M \in M_{k,n-k}(\mathbb{K})$ et T est constitué des *k*=*n*-*t* dernières colonnes de G. De plus T est triangulaire inversible car $g_t = 1 \neq 0$.

La matrice génératrice normalisée de C est la matrice $G_N = T^{-1}G = (N, I_k)$, tel que

$N = T^{-1}M$. La matrice G_N est utilisée pour le codage systématique comme suit :

Soient le mot $(a_0, a_1, \ldots, a_{k-1}) \in \mathbb{K}^k$, le mot codé *c* est le produit du mot *a* par la matrice *G*, donc $c = a.G = (aN, a) = [(a_0, a_1, \ldots, a_{k-1})N, a_0, a_1, \ldots, a_{k-1}]$. En posant

$(a_0, a_1, \ldots, a_{k-1})N = (b_0, b_1, \ldots, b_{n-k-1})$, alors en langage polynomial on obtient :

$$c(X) = b_0 + b_1X + \ldots + b_{n-k-1}X^{n-k-1} + a_0X^{n-k} + a_1X^{n-k+1} + \ldots + a_{k-1}X^{n-1}.$$

D'où $c(X) = b(X) + X^{n-k}a(X)$ où $b(X) = b_0 + b_1X + \ldots + b_{n-k-1}X^{n-k-1}$ qu'il faut déterminer. Comme $c(X) \in \theta(C)$, alors $\exists u(X) \in \mathbb{K}[X]$ tel que $c(X) = u(X)g(X)$ et donc

$X^{n-k}a(X) = u(X)g(X) + (-b(X))$ avec $d°(-b(X)) < d°(g(X))$, cela veut dire que $(-b(X))$ n'est que $r(X)$ le reste de la division Euclidienne de $X^{n-k}a(X)$ par $g(X)$ et donc $b(X) = -r(X)$.

Conséquence 3.1.

Le codage systématique d'un mot $(a_0, a_1, \ldots, a_{k-1}) \in \mathbb{K}^k$ se fait en représentation polynomiale par $a(X) \to c(X) = -r(X) + X^t a(X)$ où $r(X)$ est le reste de la division Euclidienne de $X^t a(X)$ par $g(X)$ tel que $t = d°(g(X))$.

Exemple 3.8.

On considère le code cyclique $C(7,4)$sur $\mathbb{F}_2$, de générateur $g(X) = X^3 + X^2 + 1$ et de matrice génératrice

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (M, T), \text{ où } M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

La matrice normalisé de C est la matrice $G_N = (T^{-1}M, I_4)$ où

$$T^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \text{ et } T^{-1}M = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \text{ donc } G_N = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Le codage systématique d'un mot $a(X)$ se fait comme suit :

$a(X) \to c(X) = r(X) + X^3 a(X)$ où $r(X)$ est le reste de la division Euclidienne de $X^3 a(X)$ par $g(X)$.

Si on prend $a(X) = X^3$, alors si $r(X)$ est le reste de la division Euclidienne de $X^3 a(X) = X^6$ par $g(X)$. En utilisant un registre à décalage circulaire, on trouve que, $r(X) = X^3+X$. Donc $c(X) = X^6 + X^2 + X$. En fin le codage du mot $a = 0001$ est le mot code $c = 0110001$.

3.5 Codes B.C.H et codes de Reed-Solomon

On présente dans cette partie, quelques codes cycliques particuliers utilisés en pratique tel que les codes B.C.H et les codes de Reed-Solomon.

3.5.1 Codes B.C.H

Les codes B.C.H sont des codes cycliques particuliers qui permettent de prévoit la distance minimale (et donc la capacité de correction) avant la construction de ces codes.

Pour obtenir un code qui corrige au moins e erreur on peut choisir un code B.C.H de distance construire égale à $2e$+1 ou à $2e$+2. Il est plus économique de choisir un code B.C.H de distance construire égale à $2e$ + 1, on obtient ainsi un polynôme générateur de degré plus petit et une dimension et un nombre de mots plus grand. On choisit donc dans la suite des codes B.C.H de distance construite $2e$ +1.

Un peu d'historique :

1959 : Découverte de ces codes par Hocquenghem

1960 : Découverte par Bose et Ray-Chaudhuri. Peterson prouve leur nature cyclique.

Peterson trouve un premier algorithme de décodage qui sera par la suite revu et généralisé par d'autres mathématiciens.

1981 : Gorenstein et Zierler généralisent ces codes aux alphabets à p^n (p premier) symboles.

Proposition 3.4.

Soient C un code cyclique de longueur n sur le corps $\mathbb{K} = \mathbb{F}_{p^r}$ des racines nièmes de l'unité, de générateur $g(X)$ de degré t et de racines α_i / $i \in \{1,\ldots,t\}$.

Alors la matrice $H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-2} & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-2} & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_t & \alpha_t^2 & \cdots & \alpha_t^{n-2} & \alpha_t^{n-1} \end{pmatrix}$ est une matrice de contrôle de C.

Preuve.

En effet on a : $c=c_0c_0 \ldots\ldots c_{n-1} \in C \Leftrightarrow c(x)=c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \theta(C)$

$\Leftrightarrow \exists\, q(x) \in \mathbb{K}[X] : c(x)= q(x)g(x) \Rightarrow$ pour tout $i \in \{1,\ldots, t\} : c(\alpha_i)= q(\alpha_i)\, g(\alpha_i)=0.$

Ce qui donne :

$$c_0 + c_1\alpha_1 x + \cdots + c_{n-1}\alpha_1^{n-1}=0 \ldots (1)$$
$$c_0 + c_1\alpha_2 x + \cdots + c_{n-1}\alpha_2^{n-1}=0 \ldots (2)$$
$$\vdots$$
$$c_0 + c_1\alpha_t x + \cdots + c_{n-1}\alpha_t^{n-1}=0 \ldots (t)$$

L'écriture matricielle de ce système de t équations donne : $c.H^t = 0$ où H est la matrice

$$H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-2} & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-2} & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_t & \alpha_t^2 & \cdots & \alpha_t^{n-2} & \alpha_t^{n-1} \end{pmatrix}$$

qui est une matrice de contrôle du code C.

Théorème 3.4.

Soit β une racine $nièmes$ primitive de l'unité sur le corps $\mathbb{F}_q$. Soient $C(n, k, d)$ un code cyclique de longueur n et g(x) son polynôme générateur. Si pour un certain entier $b \geq 0$ et un certain entier $\delta \geq 2$, nous avons : $g(\beta^b)=g(\beta^{b+1})= \cdots =g(\beta^{b+\delta-2})=0$, alors $d \geq \delta$, et δ est dite distance construite du code C.

Preuve.

Si $c=c_0c_0 \ldots\ldots c_{n-1} \in C$ un mot code alors $c(x)=c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \theta(C)$

On a: $g(\beta^b)=g(\beta^{b+1})=\ldots =g(\beta^{b+\delta-2})=0$, alors d'après la proposition précédente

la matrice suivante:

$$H = \begin{pmatrix} 1 & \beta^b & \beta^{2b} & \ldots & \beta^{(n-2)b} & \beta^{(n-1)b} \\ 1 & \beta^{b+1} & \beta^{2(b+1)} & \ldots & \beta^{(n-2)(b+1)} & \beta^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{b+\delta-2} & \beta^{2(b+\delta-2)} & \ldots & \beta^{(n-2)(b+\delta-2)} & \beta^{(n-1)(b+\delta-2)} \end{pmatrix}$$

est une matrice de contrôle du code C. Nous allons montrer que chaque $\delta - 1$ colonnes de H, sont linéairement indépendants sur $\mathbb{F}_q$. On va montrer que chaque matrice carrée

$$B_w = \begin{pmatrix} \beta^{j_1 b} & \beta^{j_2 b} & \cdots & \beta^{j_w b} \\ \beta^{j_1 (b+1)} & \beta^{j_2 (b+1)} & \cdots & \beta^{j_w (b+1)} \\ \vdots & \vdots & & \vdots \\ \beta^{j_1 (b+w-1)} & \beta^{j_2 (b+w-1)} & \cdots & \beta^{j_w (b+w-1)} \end{pmatrix}$$

d'ordre $w \leq \delta - 1$, extraite de H est de déterminant non nul. En effet on a :

$$det(\mathrm{B}_w) = \beta^{(j_1 + \cdots + j_w) b} det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta^{j_1} & \beta^{j_2} & \cdots & \beta^{j_w} \\ \vdots & \vdots & & \vdots \\ \beta^{j_1 (w-1)} & \beta^{j_2 (w-1)} & \cdots & \beta^{j_w (w-1)} \end{pmatrix}.$$

$$= \beta^{(j_1 + \cdots + j_w) b} \prod_{1 \leq i \leq k \leq w} (\beta^{j_i} - \beta^{j_k}) \neq 0,$$

car pour tout $i, k \in \{1, 2, \ldots, w\}$: $\beta^{j_i} \neq \beta^{j_k}$. Ainsi le résultat suit.

Définition 3.6.

Un **code B.C.H** de longueur n et de distance construite δ, est un code cyclique de longueur n, construit sur le corps $\mathbb{F}_{2^r}$ corps des racines nièmes de l'unité sur $\mathbb{F}_2$, où r est l'ordre multiplicatif de 2 modulo n, dont le polynôme générateur est le produit (sans répétition de facteur) des polynômes minimaux de β^b, β^{b+1}, …, $\beta^{b+\delta-2}$ où $\beta \in \mathbb{F}_{2^r}$ est une racine nième primitive de l'unité, b un entier strictement positif.

Il existe deux cas importants:

Si b=1, le code B.C.H est appelé **code B.C.H** au **sens strict**.

Si la longueur du code $n = 2^r - 1$, r étant un entier positif, on parle de **code B.C.H primitif**.

3.5.2 Construction d'un code B.C.H

La réalisation d'un code B.C.H ayant une capacité de correction e, peut se faire de la manière suivante :

1. Construire le corps $\mathbb{K}=\mathbb{F}_{2^r}$ des racines nièmes de l'unité.

2. Déterminer à l'aide d'un polynôme primitif M_α les éléments de $\mathbb{K}$.

3. Choisir $(\delta - 1 = 2e)$ racines de puissances successives β^b, β^{b+1}, …, $\beta^{b+\delta-2}$ du générateur $g(X)$.

4. Construire $g(X)$ le *PPCM* des polynômes minimaux des racines β^b, β^{b+1}, …, $\beta^{b+\delta-2}$, $c.\grave{a}.d.\, g(X) = PPCM\left(M_{\beta^b}, M_{\beta^{b+1}}, \ldots, M_{\beta^{b+\delta-2}}\right)$.

Exemples 3.9.

Nous voulons construire un code B.C.H au sens strict de longueur égale à n=5 et de distance construite égale à δ =3 sur $\mathbb{F}_2$. Remarquons que nous sommes en présence d'un code B.C.H qui n'est pas primitif. Calculons en premier lieu les classes cyclotomiques de 2 modulo 5. Nous obtenons : C_0= {0} ,C_1= {1,2,3,4}. Donc X^5-1=(X-1)(X-β)(X-β^2)(X-β^3)(X-β^4).

Notre choix de $\delta = 3$, nous permet de prendre comme générateur le polynôme:

$$g(X)=(X-\beta)(X-\beta^2)(X-\beta^3)(X-\beta^4),$$

où β est une racine $5^{\text{ième}}$ primitive de l'unité. Comme le plus petit entier r satisfaisant $5/2^r$-1 est r=4. On en déduit que $\beta \in \mathbb{F}_{16}$. De plus comme $s = \frac{2^r-1}{5}$=3, on en déduit que l'on peut prendre $\beta = \alpha^3$ où α est un élément primitif de $\mathbb{F}_{16}$ .On obtient alors :

$$g(X)=(X-\alpha^3)(X-\alpha^6)(X-\alpha^9)(X-\alpha^{12}),$$

en utilisant la construction de $\mathbb{F}_{2^4}$, ou encore $g(X)=\frac{X^5-1}{X-1}$, nous aurons :

$$g(X)=1+X+X^2+X^3+X^4.$$

Il est intéressant de remarquer que nous avons $\delta = 2e + 1 = 3$, comme $w[g(X)]$=5, on en déduit que la distance d=5.

Exemple 3.10.

Pour construire un code cyclique de longueur n=7, de capacité e=1, on choisit un code BCH binaire, de polynôme générateur $g(X)$ qui admet deux racines de puissances successives. On prend par exemple, $g(X) = X^3 + X + 1$, qui admet α, α^2 et α^4, comme racines dans le corps des racines 7^{emes} de l'unité $\mathbb{K}=\mathbb{F}_{2^3}=\mathbb{F}_8$, dont deux entre eux α, α^2 sont de puissances successives. Donc le code C admet comme matrice de contrôle la matrice suivante :

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} \end{pmatrix}.$$

Exemple 3.11.

Nous chercherons à construire un code de longueur n =15 et qui peut corriger jusqu'à e=2 erreurs c.à.d. avec une distance au moins égale à $\delta = 2e + 1$ =5. Pour cela, on choisit un code BCH dont le générateur admet au moins 4 racines successive. On commence par factoriser le polynôme X^{15}-1.

En utilisant les polynômes cyclotomiques, on obtient la décomposition du polynôme X^{15}-1 en produit de polynômes irréductibles sur $\mathbb{F}_2$ comme suit :

$$X^{15}\text{-}1=(X-1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1).$$

Polynômes	Racines
$X-1$	1
X^2+X+1	α^5, α^{10}
$X^4+\mathrm{X}+1$	$\alpha, \alpha^2, \alpha^4, \alpha^8$
X^4+X^3+1	$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$
$X^4+X^3+X^2+X+1$	$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$

Table Facteurs irréductible de $X^{15}-1$ et leurs racines.

En combinant ces polynômes, on obtient des codes de distance et de dimension différentes.

Pour notre cas on prend $g(X) = (X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1)$ qui admet $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}$ comme racines et parmi eux ils existent 4 racines $(\alpha, \alpha^2, \alpha^3, \alpha^4)$ de puissances successives, donc on peut prendre la distance d au moins égale à 5.

3.5.3 Codes Reed-Solomon

Les codes de Reed-Solomon forment un sous-ensemble de l'ensemble des codes cycliques. En fait, il s'agit de la sous-classe la plus importante des codes BCH. Ce sont de plus des codes M.D.S donc optimaux où ils nécessitent le minimum de redondance pour une capacité de correction fixée.

L'article sur les codes de Reed-Solomon a été soumis par Irving Reed et Gustave Solomon au Journal of the Society for Industrial and Applied Mathematics, le 21 janvier 1959 et a été publié en juin 1960 sous le titre « Polynomial Codes over Certain Finite Fields ».

Les code de Reed-Solomon sont les plus utilisés en pratique, ils sont utilisés dans la sauvegarde des données, par exemple pour les CD, DVD, dans la communication mobile, les réseaux sans fils (wireles), les communications satellitaires, les codes à barres bidimensionnels, la télévision et radio numériques ainsi que les modems ADSL.

Définition 3.7.

Soit $r \geq 2$ .Un **code de Reed-Solomon** de longueur $n = 2^r - 1$ est un code B.C.H primitif sur le corps de Galois $\mathbb{K} = \mathbb{F}_{2^r}$.

Remarque 3.2.

Tous les éléments non nuls du corps $\mathbb{K} = \mathbb{F}_{2^r}$ sont racines du polynôme $X^{2^r-1} - 1$. En conséquence, la décomposition sur $\mathbb{F}_{2^r}$ de $X^{2^r-1} - 1$ est la suivante:

$$X^{2^r-1} - 1 = \prod_{u \in \mathbb{F}_{2^r} - \{0\}} (X - u).$$

Si α est une racine primitive du corps $\mathbb{F}_{2^r}$, on obtient :

$$X^{2^r-1} - 1 = (X-1)(X-\alpha)\dots\left(X-\alpha^i\right)\dots\left(X-\alpha^{2^r-2}\right).$$

Le générateur de degré *t* d'un code de Reed-Solomon est donc de la forme :

$$g(X) = \left(X-\alpha^i\right)\left(X-\alpha^{i+1}\right)\dots\left(X-\alpha^{i+t-1}\right).$$

Qui admet *t* racines de puissances successives α^i, α^{i+1}, …, α^{i+t-1}.

Pour un tel générateur, le code correspondant a pour dimension $k = 2^r - 1 - t$, de distance construite $\delta = t + 1$.

Proposition 3.5.

Le code Reed-Solomon a pour paramètres :

- Longueur : $n = 2^r - 1$.
- Dimension : $k = 2^r - 1 - t$.
- Poids minimum : $d = t + 1 = n - k + 1$.

Preuve.

La longueur *n* et le dimension *k* viennent de la définition du code R-S. Pour la distance, on a d'une part d'après le borne de singleton $d \leq n\text{-}k+1=t+1$, et d'autre part d'après le théorème de la distance construite $d \geq \delta=t+1$ et donc $d=t+1$.

Exemple 3.12.

Soit $\mathbb{K} = \mathbb{F}_8$, la longueur de code R-S sur $\mathbb{K}$ est $n = 2^3 - 1 = 7$.

Construisons un code R-S qui corrige $e = 1$ erreur. Donc le générateur $g(X)$ est de degré $t = \delta - 1 = 2e = 2$, la distance $d=3$ et la dimension du code est $k = n - t = 5$. On peut prendre un code R-S au sens strict donc : $g(X) = (X - \alpha)(X - \alpha^2)$. Le polynôme primitif est le polynôme suivant : $M_\alpha(X) = X^3 + X + 1$, donc on aura : $\alpha^3 = \alpha + 1$, par la suite

$$g(X) = X^2 + (\alpha + \alpha^2)X + \alpha^3 = X^2 + \alpha^4 X + \alpha^3.$$

Le code *C* admet comme matrice génératrice la matrice G :

$$G = \begin{pmatrix} \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha^3 & \alpha^4 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^3 & \alpha^4 & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha^3 & \alpha^4 & 1 \end{pmatrix}.$$

Exemple 3.13.

Soit *C* le code R-S au sens strict de longueur $n=7$ et corrigeant $e=2$ erreurs sur le corps de Galois $\mathbb{F}_8 = \{0, \alpha^i / 0 \leq i \leq 6\}$ et donc de polynôme générateur admet $\delta - 1$=t=4 racines successives $\alpha, \alpha^2, \alpha^3, \alpha^4$ est donné par :

$$g(X)=(X - \alpha)(X - \alpha^2)(X - \alpha^3)(X - \alpha^4).$$

Le développement de g(*X*) donne :

$$g(X)=X^4 + (\alpha^4 + \alpha^3 + \alpha^2 + a)X^3 + (\alpha^6 + \alpha^4 + \alpha^3 + 1)X^2 + (\alpha^6 + \alpha^2 + \alpha + 1)X + \alpha^3$$

En utilisant la construction du corps $\mathbb{F}_8$ on trouve :

$$g(X)=X^4+\alpha^3 X^3+X^2+\alpha X+\alpha^3.$$

Une des matrices génératrices du code *C* est donc la suivante :

$$G=\begin{pmatrix} \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 & 0 \\ 1 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 \\ 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 \end{pmatrix}.$$

Exemple 3.14.

Codes R-S pour la sonde spatiale Mariner 10.

Le 3 novembre 1973, la sonde spatiale Mariner 10 est lancée avec succès, elle avait pour mission le survol de la planète Vénus et de la planète Mercure.

Types de capteurs utilisés : deux caméras moyen angle avec enregistreur numérique, radiomètre infrarouge, plasma solaire, particules chargées, champs magnétiques, spectromètre à ultraviolets, occultation radio et mécanique céleste.

Après le survol de Vénus, la sonde se dirige vers Mercure. Elle réussit à réaliser 3 passages, accumulant de nombreuses photos d'une qualité sans précédent, et permettant de comprendre certains mystères de Mercure. Mariner 10 devient ainsi la première sonde à observer Mercure.

Le code utilisé par la NASA pour la sonde spatiale Mariner 10 est un code Reed-Solomon dont les parametres sont les suivants :

Le corps $\mathbb{K}=\mathbb{F}_{2^8}=\mathbb{F}_{256}$,

La longueur $n=2^8-1=255$,

Le générateur $g(X)=\prod_{112\leq i\leq 143}(X-\alpha^i)$, avec t = d°($g(X)$) = 32,

La dimension $k=n-t=223$,

La distance $d=t+1=33$,

La capacité de correction $e=\left[\frac{t}{2}\right]=16$.

La sonde spatiale Mariner 10