Chapitre 2. Codes cycliques

Introduction

Les codes cycliques sont des codes correcteur linéaires, qui se fondent sur la théorie des corps finis, et en particulier les extensions de Galois ainsi que les polynômes. Ils ont été étudiés pour la première fois par Prange en 1957.

Ces codes sont en réalité les plus utilisés car ils ne nécessitent que très peu d'information pour être définis, et ils peuvent être très facilement implémentés.

Beaucoup de codes importants en pratique sont des codes cycliques : les codes de Hamming binaires, les codes BCH, les codes Reed-Solomon, ces derniers peuvent être considérés comme la sous-classe la plus importante des codes cycliques.

Mais trouver de bons codes ne suffit pas, il faut également, pouvoir trouver des méthodes de décodage efficaces. De nombreuses recherches ont porté et portent sur le décodage, elles ont permis de fournir de bons algorithmes et techniques de décodage efficaces, parmi ces méthodes on a: la méthode de Meggitt, la méthode algebrique et la méthode de décodage des codes Reed-Solomon par transformation de Fourier discrète etc.

2.1 Définition d'un code cyclique.

Définition 2.1

●Un code linéaire C de longueur n sur un corps fini $\mathbb{K}$ est dit code cyclique s'il vérifie la propriété suivante : $\forall c=(c_0,c_1,...,c_{n-1})\in C \Rightarrow c'=(c_{n-1},c_0,...,c_{n-2})\in C$. On dit dans ce cas que C est stable par décalage circulaire.

●La permutation circulaire des composantes est appelée shift. Le mot $c'=(c_{n-1},c_0,...,c_{n-2})$ est dit le shift de $c=(c_0,c_1,...,c_{n-1})$.

Exemples

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. le code $C=\{0000,1001,0110,1111\}$ n'est pas un code cyclique

2.2 Représentation polynomial d'un code cyclique.

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

On associée au mot shift $c'=(c_{n-1},c_0,...,c_{n-2})$ du mot c , le polynôme $c'(X)=c_{n-1}+c_0X+...+c_{n-2}X^{n-1}$ 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 dans l'anneau quotient $\mathbb{K}[X]/<X^n-1>$.

Proposition 2.2

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 à un mot c' de C

Définition 2.3

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

●On appelle représentation polynomiale de $\mathbb{K}^n$ l'application

$$\theta : \mathbb{K}^n \to \mathbb{K}[X]/<X^n-1>$$
$$c=(c_0,c_1,...,c_{n-1}) \mapsto \theta(c)=c(X)=c_0+c_1X+...+c_{n-1}X^{n-1}$$

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

●On appelle représentation polynomiale d'un code linéaire C de $\mathbb{K}$, l'ensemble des représentations polynomiales des mots du code C c'est-à-dire $\theta(C)=\{\theta(c)/c\in C\}$.

Proposition 2.4

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

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 $c(X)=\sum_{i=0}^{n-1}c_iX^i$, $d(X)=\sum_{i=0}^{n-1}d_iX^i$, dans $\theta(C)$ donc $c=(c_0,c_1,...,c_{n-1})$ et $d=(d_0,d_1,...,d_{n-1})\in C$ et comme C est un espace vectoriel alors pour $\alpha,\beta\in\mathbb{K}$ $m=\alpha c+\beta d\in C$ et donc $m(X)=\alpha c(X)+\beta d(X)\in\theta(C)$ d'où $\theta(C)$ est un espace vectoriel sur $\mathbb{K}[X]$, de plus soit $p(X)=\sum_{i=0}^{n-1}a_iX^i\in\mathbb{K}[X]/<X^n-1>$, alors comme $c(X)\in\theta(C)$ et C cyclique alors $c(X), Xc(X), X^2c(X),...,X^ic(X),...\in\theta(C)$ et donc

$a_0c(X)+a_1Xc(X)+a_2X^2c(X)+...\in\theta(C)$ par suit $p(X)c(X)\in\theta(C)$ d'où $\theta(\mathrm{C})$ est un idéal de $\mathbb{K}[X]/<X^n-1>$.

Inversement soit θ(C) un idéal de $\mathbb{K}[X]/<X^n-1>$, alors si $c=(c_0,c_1,...,c_{n-1})\in C$ par suit $c(X)=\sum_{i=0}^{n-1}c_iX^i\in\theta(C)$, donc $Xc(X)\in\theta(\mathrm{C})\Rightarrow c'=(c_{n-1},c_0,...,c_{n-2})\in C$ donc C est cyclique.

Théorème 2.5

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

Preuve. Soit $g(X)$ un polynôme unitaire de $\theta(\mathrm{C})$ 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 $d^\circ(r(X))<d^\circ(g(X))$ donc dans $\mathbb{K}[X]/<X^n-1>$:

$g(X)q(X)=-r(X)\in\theta(C)$ 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.

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

$\theta(C)=\langle g(X)\rangle=\{q(X)g(X)/q(X)\in\mathbb{K}[X]/<X^n-1>\}$.

2.3 Polynôme générateur et matrice génératrice d'un code cyclique

Définition 2.6

Le polynôme unitaire $g(X)$ engendrant $\theta(C)$ est appelé le générateur du code cyclique C

Propriétés 2.7

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

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

Le polynôme $(1+X)$ est le polynôme générateur de C

Remarque

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

Exemple

1. 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

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

Soit $\mathbb{K}=\mathbb{F}_{2^r}$ le corps des racines 5ieme de l'unité sur $\mathbb{F}_2$ ou r est le plus petit entier non nul tel que $n=5$ divise 2^r-1 alors $r=4$ et donc $\mathbb{K}=\mathbb{F}_{16}$. donc ϕ_5 est irréductible sur $\mathbb{F}_2$.

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 :

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

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

$C_0 : g_0(X) = X^5 - 1 = 0 \rightarrow C_0 = \{0\}$

2. 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

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

Soit $\mathbb{K}=\mathbb{F}_{2^r}$ le corps des racines 5ieme de l'unité sur $\mathbb{F}_2$ ou 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 $\varphi(7) = \text{card}\{i \in \mathbb{N} / i < 7 et\ i \wedge 7 = 1\} = 6$ donc $\phi_7(X)$ se décompose en produit de $\frac{\varphi(7)}{r} = 2$ polynôme irréductibles de degré $r=3$ sur $\mathbb{F}_2$.

$\theta_7(X) = (X^3 + bX^2 + cX + 1)(X^3 + b'X^2 + c'X + 1)$ et après les calculs on trouve $b = c' = 0$ et $b' = c = 1$ donc $\theta_7(X) = (X^3 + X^2 + X + 1)(X^3 + X^2 + X + 1)$ d'où

$X^7 - 1 = (X-1)(X^3 + X + 1)(X^3 + X^2 + 1)$) et chaque diviseur de $X^7 - 1$ donne un générateur d'un code cyclique de longueur $n=7$ sur $\mathbb{F}_2$.

Si on note $g_i(X)$ le générateur du code C_i on trouve :

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

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

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

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

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

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

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

Pour tout i, la réorientation polynomiale $\theta(C)$ est formée par tous multiples, modulo $X^7 - 1$ de $g_i(X)$ c'est-à-dire de produit $a(X)g_i(X)$, et le code C_i est formée par tous les mots correspondants à ces produits.

Théorème 2.8

Soit C un code cyclique de longueur n sur un corps fini $\mathbb{K}$ de polynôme générateur $g(X) = g_0 + g_1X + g_2X^2 + ... + g_tX^t$ avec $d^\circ g(X) = t$ alors $\dim C = k = n - t$ et admet une matrice génératrice :

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

Preuve

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

$c(X)=a(X)g(X)=(a_0+a_1X+a_2X^2+\dots+a_sX^s)(g(X))=a_0g(X)+a_1Xg(X)+a_2X^2g(X)+\dots+a_sX^sg(X)$ avec $a_s\in\mathbb{K}$ et $0\le s\le n-1$, les polynômes $g(X),Xg(X),\dots,X^sg(X)$ forment donc une famille génératrice de $\theta(C)$.

On va extraire de cette famille génératrice une base

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 $a(X)$ a(X) par $h(X)$ dans $\mathbb{K}$[X], on obtient

$a(X)=q(X)h(X)+r(X)$, $d^\circ(r(X))<d^\circ(h(X))=n-t$ donc

$r(X)=r_0+r_1X+\dots+r_{n-t-1}X^{n-t-1}$ en conséquence

$$c(X)=a(X)g(X)=q(X)h(X)g(X)+r(X)g(X)=(X^n-1)q(X)+r(X)g(X)$$

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

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

Montrons que cette famille est libre.

Dans $\mathbb{K}[X]/<X^n-1>$ considérons l'égalité :

$\alpha_0g(X)+\alpha_1Xg(X)+\dots+\alpha_{n-t-1}X^{n-t-1}g(x)=0$ …(*), Avec $\alpha_i\in\mathbb{K}$ et $i\in\{0,1,\dots,n-t-1\}$

L'égalité $(*)$ implique que dans $\mathbb{K}$[X] : $(\alpha_0+\alpha_1X+\dots+\alpha_{n-t-1}X^{n-t-1})g(X)\equiv 0(mod\ X^n-1)$

Posons $d(X)=(\alpha_0+\alpha_1X+\dots+\alpha_{n-t-1}X^{n-t-1})g(X)$ alors $d(X)$ est de degré au plus $n-1$ et il est divisible par X^n-1alors $d(X)=0$, Comme $\mathbb{K}$[X] est intègre et $g(X)$ n'est pas nul alors

$\alpha_0+\alpha_1X+\alpha_{n-t-1}X^{n-t-1}=0$ donc $\alpha_0=\alpha_1=\dots=\alpha_{n-t-1}=0$ et d'où la famille $\{g(X),Xg(X),\dots,X^{n-t-1}g(X)\}$ est libre donc elle forme une base de $\theta(C)$ et la dimension de C est $n-t$,et les mots $l_0,l_1,\dots,l_{n-t}$ correspond respectivement au polynômes $g(X),Xg(X),\dots,X^{n-t-1}g(X)$ forment une base du code C et la matrice G

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

dont les lignes sont les mots

$l_1 = g_0 g_1 g_2 \ldots g_t 0 \ldots 0,\ l_2 = 0 g_0 g_1 g_2 \ldots g_t 0 \ldots 0,\ \ldots,\ l_{n-t} = 0 \ldots 0 g_0 g_1 g_2 \ldots g_t$ est une matrice génératrice de C.

Exemple

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

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

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

Pour le code cyclique C_3 admet comme générateur le polynôme $g_3(X) = X^3 + X^2 + 1$ et la matrice génératrice $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

2.4 Orthogonal et matrice de contrôle d'un code cyclique

Définition 2.9

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 $h(X) = \dfrac{X^n - 1}{g(X)}$ est dit polynôme de contrôle de C.

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

Théorème 2.10

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

- L'orthogonal $C^{\perp}$ d'un code cyclique C est un code cyclique.
- Si $h(X) = h_0 + h_1 X + h_2 X^2 + \ldots + h_k X^k$ est le polynôme de contrôle du code cyclique C non trivial alors le générateur de $C^{\perp}$ est $h_1(X) = h_0^{-1} \overline{h}(X)$ où $\overline{h}(X) = X^k h(X^{-1})$ est le polynôme

réciproque de $h(X)$. La matrice H_1 suivante est une matrice de contrôle de C :

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

Preuve

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

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

si $h(X) = \sum_{j=0}^{n-1} h_j X^j$ 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 calculé modulo n) on déduit que $\forall i \in \{0,...,n-1\} : \sum_{j=0}^{i} a_j h_{i-j} = 0$ pour $\forall i \in \{k,...,n-1\}$ on trouve les relations suivantes :

Si (i=k) alors $a_0 h_k + a_1 h_{k-1} + a_2 h_{k-2} + \dots + a_k h_0 + a_{k+1} 0 + \dots + a_{n-1} 0 = 0$ 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) alors $a_0 0 + a_1 h_k + a_2 h_{k-1} + \dots + a_k h_1 + a_{k+1} h_0 + \dots + a_{n-1} 0 = 0$ 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) alors $a_0 0 + a_1 0 + a_2 h_k + \dots + a_k h_2 + a_{k+1} h_1 + \dots + a_{n-1} 0 = 0$ 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 $a_0 0 + a_1 0 + a_2 0 + \dots + a_{n-k-2} 0 + a_{n-k-1} h_k + \dots + a_{n-1} h_0 = 0$ donc

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

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 :

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

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

La matrice constitué des $t = n - k$ premières colonnes extraite du tableau ci-dessus est triangulaire inversible car $h_k \neq 0$. la matrice H_1 formée par ces mots est de rang t et ses lignes forment une base à $C^{\perp}$. Donc H_1 est une matrice de contrôle du code C .

$h(0) = h_0 \neq 0$ car $h(X)$ divise $X^n - 1$ alors la matrice $H = h_0^{-1} H_1$ est aussi une matrice de contrôle de C, de plus le polynôme associé à la première ligne de H

$h_1(X) = h_0^{-1}h_k + h_0^{-1}h_{k-1}X + \ldots + X^k = h_0^{-1}\overline{h}(X)$ (où $\overline{h}(X)$ est le polynôme réciproque de $h(X)$) est un polynôme unitaire divisant $X^n - 1$ donc $h_1(X)$ est **le générateur** du code $C^{\perp}$.

$C^{\perp}$ est cyclique car si $c \in C^{\perp}$ donc $c(X) \in \theta(C^{\perp}) = < h_1(X) >$, alors $c(X) = h_1(X)q(X)$ et $Xc(X) = h_1(X)Xq(X) = h_1(X)q'(X)$ ce qui montre que le shift de c(X) est dans $\theta(C^{\perp})$ alors $C^{\perp}$ est cyclique.

Par ailleurs on constat que la matrice H est une matrice génératrice du code cyclique $C^{\perp}$ engendré par le polynôme $h_1(X)$.

Exemple .1

Soit C un code cyclique sur $\mathbb{F}_2$ de longueur 7 et de polynôme générateur $g(X) = X^3 + X^2 + 1$, alors le polynôme de contrôle de C est :

$$h(X) = X^7 - 1/(X^3 + X^2) = X^4 + X^3 + X^2 + 1$$

L'orthogonal de C est engendré par le polynôme $h_1(X) = X^4 h(X^{-1}) = X^4 + X^2 + X + 1$ et sa matrice génératrice $H_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$.

2.5 Codes cycliques systématiques

Définition 2.11

Un code cyclique $C(n,k)$ sur un corps fini $\mathbb{K}$ est dit systématique (ou normalisé) 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 $M \in M_{k,n-k}(\ )$.

Exemple

Le code cyclique C de longueur n=7 et de générateur $g(X) = X^4 + X + 1$ sur $\mathbb{F}_2$, admet comme matrice génératrice normalisée

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

Donc c'est un code cyclique systématique.

Codage systématique par un code cyclique

Soit C un code cyclique de longueur n sur un corps fini $\mathbb{K}$ de générateur $g(X) = g_0 + g_1X + g_2X^2 + \ldots + g_tX^t$ tel que $d^\circ(g(X)) = t$.

Le code C admet une matrice génératrice (pas nécessairement normalisée) G_1 de la forme

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

$G_1 = (M, T)$ où $M \in M_{k,n-k}(\ )$ et T est constitué des k=n-t dernières colonnes de G_1. De plus T est inversible car $g_t \neq 0$.

On considère la matrice $G = T^{-1}G_1 = (N, I_k)$ tel que $N = T^{-1}M$ donc G est une matrice génératrice normalisée de C qu'on utilise pour le codage comme suit :

Soit le mot $a = (a_0, a_1, a_2, ..., a_{k-1}) \in \mathbb{K}^k$ le mot codé c est le produit de a par la matrice G

$c = a.G = (aN, a) = [(a_0, a_1, ..., a_{k-1})N, a_0, a_1, ..., a_{k-1}]$ et en posant

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

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

D'où $c(X) = b(X) + X^{n-k}a(X)$ où $b(X) = b_0 + b_1X + ... + b_{n-k-1}X^{n-k-1}$ qu'il faut déterminer.

Comme $c(X) \in \theta(C)$ alors $\exists u(X) \in K[X]$ 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 $g(X)$.

Conséquence 2.12

Le codage systématique d'un mot $a = (a_0, a_1, a_2, ..., a_{k-1}) \in \mathbb{K}^k$ 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

On considère le code cyclique $C_3(7,4)$ sur $\mathbb{F}_2$, de générateur $g(X) = X^3 + X^2 + 1$, de matrice génératrice

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (M, T) \text{ où } M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

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

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

Le codage se fait comme suit : $a(X) \to c(X) = X^3 a(X) + r(X)$ 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, tel que $r(X)$ est le reste de la division Euclidienne de X^6 par $g(X)$. On trouve que, $r(X) = X^2 + X$. Donc $c(X) = X^6 + X^2 + X$. $a = (0,0,0,1) \to c = (0,1,1,0,0,0,1)$.

2.6 Codes B.C.H et 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 .

2.6.1 Codes B.C.H

Les codes B.C.H sont des codes particuliers qui permettent de prévoir la distance minimale 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.

Propostion 2.13 Soit 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 de racines α_i / $i \in \{1,\ldots,t\}$.

$$c = (c_0, c_1, c_2, ..., c_{n-1}) \in C \Leftrightarrow c(X) = q(X)g(X) \Leftrightarrow c(\alpha_i) = 0, \forall i \in \{1,...,t\} \Leftrightarrow cH^t = 0$$

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

Théoreme 2.14

Soit C un code cyclique C(n,k,d) sur le corps $\mathbb{K} = \mathbb{F}_{p^r}$ des racines nièmes de l'unité de générateur g(X) de degré t, $\delta \geq 2$ et $b \geq 1$ deux entiers et β une racine nieme primitive de l'unité. Si g(X) admet β^b, β^{b+1}, …, $\beta^{b+\delta-2}$ comme racines de puissances successives, alors $d \geq \delta$.

Définition 2.15

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

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 $n = p^r - 1$, r étant un entier positif on parle de code B.C.H primitif.

La matrice de contrôle d'un code BCH est définie comme suit:

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

- **<u>Construction d'un code B.C.H.</u>**

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

1. Construire le corps $\mathbb{K} = \mathbb{F}_{p^r}$ 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 du générateur $g(X)$: $\beta^b, \beta^{b+1}, ..., \beta^{b+\delta-2}$.
4. Construire $g(X) = PPCM\left(M_{\beta^b}, M_{\beta^{b+1}}, ..., M_{\beta^{b+\delta-2}}\right)$.

Exemple .1

Pour construire un code de longeur 7 de capacité e=1, on choisit un code BCH binaire de polynôme générateur g(x) qui admet 2 racines sucsessives par exemple $g(X) = X^3+X+1$ qui admet comme racines dans le corps des racines 7eme de l'unité $\mathbb{K} = \mathbb{F}_{2^3} = \mathbb{F}_8$, les racines α, α^2 et α^4 donc deux entre eux sont successives(α, α^2) et admet comme matrice de contrôle la matrice

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

Exemple Nous chercherons à construire un code de longueur $n=15$. Pour cela, on factorise $X^{15}-1$

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

Dans $\mathbb{F}_2$, on a les racines suivantes :

Polynôme	Racines
$X+1$	1
X^2+X+1	β , β^2
X^4+X+1	β , β^2, β^4, β^8
X^4+X^3+1	β , β^2, β^4, β^8
$X^4+X^3+X^2+X+1$	β , β^3, β^6, β^9, β^{12}

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

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

$$=X^8+X^7+X^6+X^4+1.$$

Si β est une racine de X^4+X+1 .

admet donc les racines $\beta, \beta^2, \beta^3, \beta^4, \beta^6, \beta^8, \beta^9, \beta^{12}$ et on a donc :

$$g(\beta)=g(\beta^2)=g(\beta^3)=g(\beta^4)=0.$$

On a donc construit un code de dimension $k=n-deg(g)=15-8=7$ et de distance minimum au moins égale à $d=5$.

2.6.2 Codes Reed-Solomon

Les codes Reed-Solomon sont un sous-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 ».

Le code Reed-Solomon est le plus utilisés en pratique, il est utilisés dans la sauvegarde des données, par exemple pour les CD, DVD, dans la communication mobile, les réseaux sans fils (wireless…), les communications satellitaires, les codes à barres bidimensionnels, la télévision et radio numériques ainsi que les modems ADSL.

Définition 2.16

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

Tous les éléments non nuls de $\mathbb{F}_{2^r}$ sont racines de $X^{2^r-1}-1$. En conséquence, la décomposition sur $\mathbb{F}_{2^r}$ de $X^{2^r-1}-1$ est : $X^{2^r-1}-1=\prod_{u\in\mathbb{F}_{2^r}-\{0\}}(X-u)$

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

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

Le générateur d'un code de Reed-Solomon est donc de la forme :

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

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

Proposition 2.17

Le code Reed-Solomon a pour paramètres :

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

Exemple 1.

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

Construisons un code R-S qui corrige $e=1$ erreur, donc $t=\delta-1=2e=2$ et $k=5$.

On prend $g(X)=(X-\alpha)(X-\alpha^2)$

On a $M_\alpha(X)=X^3+X+1$ donc $\alpha^3=\alpha+1$.

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

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 2. Soit $\mathbb{K}=\mathbb{F}_8=\{0,\alpha^i/0\le i\le 6\}$ et C(7,4) un code cyclique sur $\mathbb{F}_2$.

Le polynôme générateur du code de RS qui admet 3 racines successives $\{\alpha,\alpha^2,\alpha^3\}$ est :

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

$=X^3+\alpha^4X^2+\alpha^3X+\alpha^3X^2+\alpha^6+\alpha^7X=X^3+(\alpha^4+\alpha^3)X^2+(\alpha^3+\alpha^7)X+\alpha^6$

$=X^3+\alpha^6X^2+\alpha X+\alpha^6$.

Une de ses matrices génératrice est $G=\begin{pmatrix}\alpha^6\ \alpha\ \alpha^6\ 1\ 0\ 0\ 0\\ 0\ \alpha^6\ \alpha\ \alpha^6\ 1\ 0\ 0\\ 0\ 0\ \alpha^6\ \alpha\ \alpha^6\ 1\ 0\\ 0\ 0\ 0\ \alpha^6\ \alpha\ \alpha^6\ 1\end{pmatrix}$.

Exemple 3. Le code utilisé par la NASA pour la sonde spatiale Mariner en 1973, est un code RS sur le corps $K=F_{256}$, de longeur n=255 de générateur $g(X)=\prod_{i=112}^{i=143}(X-\alpha^i)$ (t=d°(g(X)=32), de dimension k=n-t=223 et de distance d=t+1=33 (la capacité e=[d-1 /2]=16.