Remerciements

En premier lieu je remercie **ALLAH** pour m'avoir guidé et donner la force pour la finalisation de ce mémoire. Je tiens également à exprimer mes plus vifs remerciements à Monsieur **C. MIHOUBI** pour l'intéressant sujet qu'il m'a proposé. Il m'est impossible de lui exprimer toute ma gratitude en seulement quelques lignes. Je lui suis également reconnaissant pour la confiance qu'il ma accordée J'exprime ici ma profonde gratitude à Monsieur **A. AMROUNE**, Professeur à université de M'sila. Pour m'avoir fait l'honneur de présider mon jury et Monsieur **N. GHADBANE**, Maître de Assistant à université de M'sila. Je ne saurais oublier de remercier tous mes professeurs et toutes les personnes ayant contribué de près ou de loin à l'aboutissement de ce travail.

Pour finir mes derniers mots de remerciements vont tout naturellement à ma famille et mes amis.

Notations

- G : Groupe.
- A : Anneau.
- I : Idéal de A.
- K : Corps fini.
- $\mathbb{F}_q$: Un corps fini de cardinal q.
- $car(k)$: Caractéristique d'un corps fini K.
- $im\varphi$: Image de l'application φ.
- $\underset{anneau}{\preccurlyeq}$: Sous-anneau.
- $\mathbb{F}_q^*$: Un groupe d'ordre $(q-1)$.
- $[\mathbb{F} : K]$: Dimension de $\mathbb{F}$ sur K.
- $A[X]$: L'ensemble des polynômes en x sur A.
- $f^*(x)$: Polynôme réciproque de $f(x)$.
- $\mathbb{F}_q[x]$: Anneau des polynômes à coeffcients dans $\mathbb{F}_q$.
- $\mathbb{F}_q[x]/\langle p\rangle$: Anneau des classe modulo $p(x)$.
- $\mathbb{F}_q[x]/(x^n-1)$: L'anneau quotient (des classes de polynôme de degré inférieur à n).
- $\mathbb{F}_q^n$: Espace vectoriel des vecteurs de longueur n sur $\mathbb{F}_q$.
- $Irr(\alpha, K, x)$: Le polynôme minimal de α sur K.
- $C[n, k, d]$: Code de paramètres n, k, d .
- c : Mot de code C .
- $d_H(x, y)$: Distance de Hamming.

- $w_H(x)$: Pois de Hamming de x.
- d : La distance minimale.
- $C^{\perp}$: Le dual de code C.
- G : Matrice génératrice.
- H : Matrice de contrôle.
- $g(x)$: Polynôme générateur.
- $h(x)$: Polynôme de contrôle.
- k/n : Rendement ou taux d'un code $C[n, k, d]$.

Résumé

On considère les codes cycliques de rendement $\frac{1}{2}$ de paramètre $[n, n/2]$ sur le corps fini $GF(7)$, le but de ce sujet est de trouver les codes cycliques iso-duaux sur $GF(7)$ pour n inférieur ou égal à 50, où n est pair et non multiple de 7 et $n/2$ soit impair et premier.

Mots clés : Corps finis, anneaux des polynômes $A[x]$, polynômes irréductibles, polynômes réciproques, polynôme générateur, codes linéaires, codes cycliques, codes iso-duaux.

Abstract

We consider the cyclic codes to rate $\frac{1}{2}$, to parameter $[n, n/2]$ on the finite field $GF(7)$, the purpose of this is to find cyclic codes iso-duals over $GF(7)$. For n less than or equal to 50, where n is even and not a multiple of 7 and $n/2$ is odd and prime.

Key words : Finite fields, rings of polynomials $A[x]$, irreducible polynomials , reciprocals polynomials, generator polynomial, linear codes, cyclic codes, isodual codes.

Table des matières

Introduction

Les codes correcteurs d'erreurs sont présents aujourd'hui dans tous les réseaux. Voyons tout d'abord pourquoi cette nécessité de codage, en informatique et dans les télécommunications.

Le transfert d'informations prend de plus en plus d'importance dans notre société. Que ce soit pour la transmission de photographies de planètes éloignées, pour des communications entre ordinateurs ou encore pour la lecture de nos disques lasers, le besoin de communications efficaces et sans erreurs est plus important que jamais. Nous savons tous que des communications sans erreurs sont physiquement impossibles. Les codes ne sont pas là pour éliminer les erreurs mais plutôt pour les détecter et si possible les corriger. Afin d'illustrer sommairement un code, exploitons une idée intuitive qui consiste à répéter l'information un certain nombre de fois.

En mathématiques et en informatique, un code cyclique est un code correcteur linéaire. Ce type de code possède non seulement la capacité de détecter les erreurs, mais aussi de les corriger sous réserve d'altérations modérées.

Dans ce travail on s'intéresse aux codes iso-duaux $[n, n/2]$, sur le corps fini $\mathbb{F}_7$. En considérant les codes cycliques de paramètres $[n, n/2]$, pour n est pair, nous avons recherché ces codes au sens du polynôme réciproque.

Déroulement du mémoire :

Dans le premier chapitre nous présentons les notions et propriétés fondamentales nécessaires pour la réalisation de ce travail concernant : Groupe, anneau, corps fini, construction d'un corps fini.

Le deuxième chapitre regroupe les définitions et les propriétés fondamentales des polynômes sur un corps fini, division Euclidienne dans $K[x]$ et factorisation de $x^n - 1$, en polynômes irréductibles, sur un corps fini.

Enfin, dans le dernier chapitre, on présente les codes linéaires et codes cycliques, puis on va rechercher les codes cycliques iso-duaux de rendement $1/2$ sur $\mathbb{F}_7$ pour $n \leq 50$, telle que n soit pair et $\frac{n}{2}$ est premier et impair.

Chapitre 1

Corps finis

Dans ce chapitre, nous rappelons les notions de groupes, anneaux, corps finis, construction d'un corps fini et nous en donnons quelques théorèmes fondamentaux qui vont nous servir dans la suite de ce mémoire.

1.1 Groupes

Définition 1.1.1 *Un groupe est la donnée d'un ensemble non vide G et d'une loi de composition interne noté $(*)$*

$$\begin{aligned} G \times G &\longrightarrow G \\ (x, y) &\longmapsto x * y \end{aligned}$$

Vérifiant les propriétés suivantes :

(i) $\forall x, y, z \in G,\ (x * y) * z = x * (y * z)$ *(l'associativité de la loi)*

(ii) $\exists e \in G$*,tel que* $\forall x \in G,\ x * e = e * x = x$ *(l'élément neutre pour la loi)*

(iii) $\forall x \in G, \exists x^{-1} \in G$ *,tel que,* $x * x^{-1} = x^{-1} * x = e$ *(x^{-1} l'élément symétrique de x).*

- On note souvent un groupe comme un triplé $(G, *, e)$, ou plus simplement $(G, *)$ ou même G s'il n'y a pas d'ambiguïté sur l'élément neutre et l'opération binaire. Lorsque $*$ est commutative, on dit que le groupe est commutatif ou abélien.

Exemple 1.1.1 $(\mathbb{R}, +, 0)$ *et* $(\mathbb{R}\backslash\{0\}, ., 1)$ *sont des groupes.*

- Il existe aussi des groupes finis. Par exemple $\mathbb{Z}_n$ représente l'ensemble des restes par la division par n (n entier positif) de tous les entiers.

$$\mathbb{Z}_n = \{0, 1, ..., n-1\}.$$

On note respectivement $a + b$ et $a.b$ la somme et le produit usuels de a et b réduits modulo n.

Exemple 1.1.2 *La structure* $(\mathbb{Z}_4, \times, 1)$ *peut être définie par sa table de multiplication :*

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Cette structure ne forme pas un groupe car les éléments 0 *et* 2 *n'admettent pas d'inverse (il n'existe pas de*1 *sur la ligne ou la colonne correspondant à* 0 *ou* 2*).*

Le groupe additif $(\mathbb{Z}_4, +, 1)$ *peut être défini par sa table d'addition :*

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

1.2 Anneaux

Définition 1.2.1 *Un anneau* $(A, +, \times)$*est un ensemble non vide dans lequel on a défini une addition* $+$ *et une multiplication* $\times$ *telles que :*

- $(A, +)$ *est un groupe commutatif d'élément neutre* 0_A*.*
- *la multiplication est associative, distributive à gauche et à droite sur l'addition, et possède un élément neutre* 1_A*.*

Si la multiplication est commutative, on dit que A *est un anneau unitaire commutatif.*

Exemple 1.2.1 *a) L'ensemble des entiers relatifs $\mathbb{Z}$, muni de l'addition et de la multiplication usuelles, est un anneau commutatif.*

b) Pour tout entier $n > 0$, le groupe abélien $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication définie par $cl(p)cl(q) = cl(pq)$ est un anneau commutatif, dont l'unité est $cl(1)$, où $cl(x)$ désigne la classe dans $\mathbb{Z}/n\mathbb{Z}$ de l'élément x de $\mathbb{Z}$.

Définition 1.2.2 *(**Anneau intègre**): Un anneau intègre est un anneau unitaire commutatif ne possède pas de diviseur de zéro i.e: $\forall x, y : x.y = 0 \Rightarrow x = 0$ ou $y = 0$.*

Définition 1.2.3 *(**Anneau factoriel**): Un anneau A est factoriel si A est intègre et :*

(i) $\forall x \in A, x \neq 0, x \notin U(A)$, x est le produit des éléments irréductibles de A ($x = p_1.p_2..p_i..p_k$, p_i irréductible dans A).

(ii) L'écriture précédente est unique c-à-d: $x = p_1.p_2..p_i..p_k = q_1.q_1..q_j..q_s$ avec p_i, q_j irréductible dans A, Alors $k = s$, et $\forall i, \exists! j : p_i \sim q_j$.

Exemple 1.2.2 *$\mathbb{Z}$ est factoriel.*

1.2.1 Idéal d'un anneau

Définition 1.2.4 *Une partie I de A est appelée un idéal à gauche (resp. à droite) de A si elle vérifie les conditions suivantes :*

(i) I est un sous-groupe additif de A.

(ii) Pour tout $(a, x) \in A \times I$,on $a : ax \in I$ (resp.$xa \in I$.).

Un idéal bilatère de A, ou plus simplement un idéal de A, est une partie de A qui est à la fois un idéal à gauche et un idéal à droite de A.

Exemple 1.2.3 *Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.*

Définition 1.2.5 *(**Idéal principal**) : Un idéal de I de A est principal s'il existe un élément $a \in A$ tel que: $I = \langle a \rangle$.*

Définition 1.2.6 *(**Anneau principal**) : L'anneau A (intègre, unitaire) est dit principal si tout idéal de A est principal.*

Exemple 1.2.4 *$\mathbb{Z}$ est un anneau principal car : Si I est un idéal, alors $\exists n \in \mathbb{N}$ tel que : $I = n\mathbb{Z} = \langle n \rangle$.*

Proposition 1.2.1 *Tout anneau principal est factoriel.*

Définition 1.2.7 *(**Anneau quotient**) : L'ensemble des classes résiduelles d'un anneau A modulo un idéal I frome un anneau noté A/I dont les deux opérations sont définies par :*

1) $(a + I) + (b + I) = (a + b) + I$.

2) $(a + I)(b + I) = ab + I$.

1.3 Corps finis

Définition 1.3.1 *(**Corps**) : Un anneau non nul est un corps si tous ses éléments non nuls sont inversibles.*

Théorème 1.3.1 *Soit $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

Définition 1.3.2 *(**Corps finis**) : Un corps fini qui possède un nombre fini d'éléments est appelé "corps fini".*

Remarque 1.3.1 *Un corps fini de q éléments est noté $\mathbb{F}_q$ ou $GF(q)$ [Galois Field of q éléments] .*

Définition 1.3.3 *(**Corps premiers**) : Les corps premiers sont les corps $\mathbb{Z}/p\mathbb{Z}$, notés aussi $\mathbb{F}_p$, avec p premier.*

Théorème 1.3.2 *(**Wedderburn**) : Tout corps fini est commutatif.*

Preuve. Voir [17] ■

1.3.1 Caractéristique d'un corps fini

Définition 1.3.4 *Soit K un corps fini, le plus petit entier positif n tels que :*

$$n.1_K = \underbrace{1_k + 1_k + ... + 1_k}_{n\ fois} = 0$$

est appelé caractéristique de K, $(car(K) = n, n \in \mathbb{N})$. Sinon on dit que K est la caractéristique nul.

Exemple 1.3.1 *1) $K = \mathbb{Z}/p\mathbb{Z}$, p premier, on a $p.\overline{1} = 0$, alors $car(\mathbb{Z}/p\mathbb{Z}) = p$.*

2) $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $car(K) = 0$.

Remarque 1.3.2 *Si le corps K est de caractéristique n, alors :*

$$\forall x \in K : n.x = 0\ , (n.x = (n.1).x = 0.x = 0).$$

Corollaire 1.3.1 *Si K un corps fini, alors $car(K) = p$ est premier.*

Preuve. Soit l'application :

$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & K \\ & & n & \mapsto & n.1 \end{array}$$

- $\varphi(n+m) = (n+m).1$
  $= n.1 + m.1$
  $= \varphi(n) + \varphi(m)$
- $\varphi(n.m) = nm.1 = (n.1).(m.1)$
  $= \varphi(n).\varphi(m)$
- $\varphi(1_{\mathbb{Z}}) = 1_K$

φ est un morphisme d'anneaux.

- $\ker\varphi$ ideal de $\mathbb{Z}$.
- $\mathbb{Z}/\ker\varphi \cong im\varphi$.

$\ker\varphi = \{m \in \mathbb{Z} : m.1_K = 0\} = \langle n \rangle = n\mathbb{Z}$, ($n \in \mathbb{N}$ le plus petit entier $\geqslant 0$ tq $n.1_K = 0$)

$n = car(K)$

$*$) **1^{er}cas** : $\ker\varphi = \{0\}, n = 0 = car(K)$.

$\mathbb{Z}/\ker\varphi \cong im\varphi$, $\mathbb{Z}/\{0\} \simeq \mathbb{Z} \cong im\varphi$

Donc $\mathbb{Z} \cong im\varphi \underset{anneau}{\preccurlyeq} K$

• K contient une copie de $\mathbb{Z}$ ($\mathbb{Z}$ à iso-prés)

comme $\mathbb{Q}$ est contient la copie de fractions de $\mathbb{Z}$ donc K contient

une copie de $\mathbb{Q}$ ($\mathbb{Q}$ à un iso-prés)

• Si $car(K) = 0$, alors K est infini et contient $\mathbb{Q}$ (à un iso-prés)

$*$) **$2^{ème}$cas** : $\ker\varphi \neq \{0\}$

$\ker\varphi = n\mathbb{Z}$, $n = car(K)$

$\mathbb{Z}/n\mathbb{Z} \cong im\varphi \underset{anneau}{\preccurlyeq} K$

On a K corps (intègre) $\Longrightarrow$ $im\varphi$ est intègre $\Longrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ est intègre $\Longrightarrow$ n est premier

$\mathbb{Z}/n\mathbb{Z}$ corps $\cong im\varphi$ corps $\subset K$ corps.

Donc: $Car(k) = n$ est premier et K contient le corps fini $\mathbb{Z}/n\mathbb{Z}$ (à un iso-prés). ■

1.3.2 Cardinal d'un corps fini

Théorème 1.3.3 *Soit $\mathbb{F}$ un corps fini de caractéristique p, $\mathbb{F}$ est un $\mathbb{F}_p$ espace vectoriel de dimension finie (disons n) et par conséquent, $|\mathbb{F}| = p^n$ (où $|\mathbb{F}|$ désigne le cardinal de $\mathbb{F}$).*

Preuve. $\mathbb{F}$ est un $\mathbb{F}_p$-espace vectoriel et, par hypothèse, $\mathbb{F}$ est fini. Par conséquent, la dimension de $\mathbb{F}$ en tant que $\mathbb{F}_p$-espace vectoriel est forcément finie (disons n). D'où $|\mathbb{F}| = (|\mathbb{F}_p|)^n = p^n$. Donc un corps fini a forcément p^n éléments ou p est un nombre premier. D'une manière générale, si $\mathbb{F}$ est un corps fini et que K est un sous-corps de $\mathbb{F}$, on peut toujours voir $\mathbb{F}$ comme un K-espace vectoriel (de dimension finie). ■

Théorème 1.3.4 *Soit K un corps fini à q éléments*

1) $q = p^n$, p premier , $n \geq 1$

2) $\forall x \in K$, $x^q - x = 0$.

Preuve. 1) K un corps fini, $car(K) = p$ et $\mathbb{Z}/p\mathbb{Z} \subset K$, K est un esp-vect sur $\mathbb{Z}/p\mathbb{Z}$, comme K est fini alors $[K : \mathbb{Z}/p\mathbb{Z}]$ est fini. $[K : \mathbb{Z}/p\mathbb{Z}] = n \geq 1$

$$K \cong (\mathbb{Z}/p\mathbb{Z})^n \text{ alors } |K| = |(\mathbb{Z}/p\mathbb{Z})^n|$$

Donc $q = p^n$

2) Si $x = 0$, $0^q - 0 = 0$

si $x \neq 0$ $(x \in K^* = K - \{0\})$

$K^* = U(K)$ est un groupe d'ordre $q - 1$

Rappel : Si G un groupe fini d'ordre s, alors $\forall g \in G : g^s = 1$.

Donc $\forall x \in K : x^{q-1} = 1$.

d'où : $\forall x \in K : x^q - x = 0$. ■

Proposition 1.3.1 *Soit K un corps fini à $q = p^n$ éléments alors :*

$\forall x, y \in K : (x + y)^{p^s} = x^{p^s} + y^{p^s}$, $s \in \mathbb{N}$.

Preuve. (Récurrence sur $s \geq 1$)

Pour $s = 1$ on a

$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i$.

$\binom{p}{i} = C_p^i = \frac{p!}{i!(p-i)!}$.

$(x + y)^p = x^p + y^p + \sum_{1 \leq i \leq p-1} C_p^i x^{p-i} y^i$.

$(car(K) = p$ premier alors $px = 0)$

$C_p^i = \frac{p!}{i!(p-i)!} \qquad 1 \leq i \leq p - 1$

$p! = C_p^i . i!.(p - i)!$

On a $p | C_p^i . i!.(p - i)!$

p premier, $1 \leq i \leq p - 1$ alors $p | C_p^i$. (ie:$C_p^i x^{p-i} y^i = 0$)

Donc $(x + y)^p = x^p + y^p$

$(x + y)^{p^{s+1}} = (x + y)^{p^s \cdot p} = [(x + y)^{p^s}]^p$

$= (x^{p^s} + y^{p^s})^p = (x^{p^s})^p + (y^{p^s})^p$

$= x^{p^{s+1}} + y^{p^{s+1}}$ ■

Théorème 1.3.5 *(**Groupe multiplicatif d'un corps fini**) :*

Soit K un corps fini de cardinal $q = p^n$. Le groupe multiplicatif $K^* = K\backslash\{0\}$ est un groupe cyclique d'ordre $q-1$.

Proposition 1.3.2 *Deux corps finis de même cardinal sont isomorphes.*

Preuve. voir[15]. ■

Définition 1.3.5 *(**Elément primitif**) : On appelle élément primitif de d'un corps fini $\mathbb{F}$ tout générateur du groupe multiplicatif $\mathbb{F}^*$, C à d: $\alpha^{q-1} = 1$, Avec $|\mathbb{F}| = q$ et α générateur de $\mathbb{F}^*$.*

Théorème 1.3.6 *Soit α un élément primitif d'un corps fini $\mathbb{F}$. si $|\mathbb{F}| = q$, alors :*

$\mathbb{F} = \{1, \alpha, ..., \alpha^{q-2}\}$, en plus, α^k est primitif si seulement si $p\gcd(k, q-1) = 1$.

Exemple 1.3.2 *$\mathbb{F} = \mathbb{Z}_{11}, \alpha = 2$. $\mathbb{F}^*$ s'écrit:*

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
1	2	4	8	5	10	9	7	3	6	1	2

Donc $\alpha^{10} = 1$: α est une racine dixième.

$\mathbb{F} = \{0\} \cup \{1, \alpha, ..., \alpha^{p^n-2}\}, \alpha \in \mathbb{F}$

$\mathbb{F} = \mathbb{Z}_{11} = \{0\} \cup \{1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\}$.

Définition 1.3.6 *K un corps fini à $q = p^n$ éléments l'application :*

$$\sigma : K \longrightarrow K$$

$$x \mapsto x^p$$

*est appelé **"l'automorphisme de Forbenius"***

- $\sigma(x+y) = (x+y)^p = x^p + y^p = \sigma(x) + \sigma(y)$.

  $\sigma(x.y) = (x.y)^p = x^p.y^p = \sigma(x).\sigma(y)$.

  $\sigma(1) = 1$.

  Alors σ est morphisme.

• σ est injective

$$\sigma(x) = \sigma(y) \Longleftrightarrow x^p = y^p \Longleftrightarrow x^p - y^p = 0$$
$$\Longleftrightarrow (x-y)^p = 0$$
$$\Longleftrightarrow (x-y) = 0$$
$$\Longleftrightarrow x = y$$

Et comme K est fini, alors σ est bijective.

Définition 1.3.7 *1) On dit que le corps (commutatif) E est algébriquement clos si tout polynôme non constant possède (au mois) une racine dans E*

2) $K \subset E$ extension algébrique de K si $\forall \alpha \in E, \alpha$ algébrique sur K

3) On dit que E est une clôture algébrique de K si :

i) E extension algébrique de K.

ii) E est algébriquement clos.

Théorème 1.3.7 ***(Existence et Unicité des Corps Finis)***

Soit $q = p^m$ où p désigne un nombre premier et $m \in \mathbb{N}^*$. Il existe un corps à q éléments et ce corps est unique à isomorphisme près.

Preuve. S'il existe un corps k à q éléments, alors tout $x \in k^*$ vérifie $x^{q-1} = 1$ d'après le Théorème de Lagrange appliqué au groupe multiplicatif k^* de k. Par suite $x^q = x$ pour tout $x \in k$ .Soit K une clôture algébrique de $\mathbb{F}_p$. On appelle ainsi toute extension algébrique de K qui est elle-même algébriquement close, et l'on sait qu'une telle clôture algébrique existe et est unique à isomorphisme près. L'ensemble

$$k = \{x \in K / x^q - x = 0\}$$

est un sous-corps de K. En effet 0 et 1 appartiennent à k. Si $a, b \in k$, le Lemme 1 permet d'écrire $(a-b)^q = a^q - b^q = a - b$, d'où $a - b \in k$. Pour finir $(ab^{-1})^q = ab^{-1}$ montre que $ab^{-1} \in k$ pour tous $a, b \in k^*$. Le corps k sera de cardinal q puisque les racines de $x^q - x$ sont distinctes (en effet, le polynôme dérivé -1 ne s'annule jamais sur K).

Montrons maintenant l'unicité d'un tel corps. Si k' désigne un autre corps à q éléments, il est de caractéristique p et le monomorphisme $\phi : \mathbb{F}_p \to k'$ fait apparaître k' comme une

extension de degré fini de $\mathbb{F}_p$. Une clôture algébrique de K' de k' sera aussi une clôture algébrique de $\mathbb{F}_p$, donc isomorphe à K. Si $\psi : K' \to K$ est un isomorphisme, $\psi(k')$ sera un sous-corps de K à q éléments, donc tout élément x de $\psi(k')$ vérifiera l'équation $x^q - x = 0$ d'après le théorème de Lagrange. Autrement dit $\psi(k') \subset k$, et cette dernière inclusion est en fait une égalité puisque les deux ensembles ont même cardinal. ■

1.4 Sous-corps

Lemme 1.4.1 *Etant donné un corps K et un entier $n > 1$, alors pour $s \in \mathbb{N}$,*

$$x^s - 1 | x^n - 1, \text{ dans } K[x] \iff s | n, \text{ dans } \mathbb{N}^*$$

Théorème 1.4.1 *Quels que soient le nombre premier p et l'entier $n \geq 1$, il existe une bijection entre l'ensemble des sous-corps de $\mathbb{F}_{p^n}$ et l'ensemble des diviseurs de n dans $\mathbb{N}^*$.Plus précisément*

$$\mathbb{F}_{p^s} \text{ sous -corps de } \mathbb{F}_{p^n} \iff s | n, \text{ dans } \mathbb{N}^*$$

Preuve. voir [16] ■

Exemple 1.4.1 *Les sous-corps de $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ sont de la forme $\mathbb{F}_{2^s}$ tel que :*
$s|4 \iff s \in \{1, 2, 4\}$ *donc les sous-corps sont:* $\mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^4}$.

Définition 1.4.1 *Soit $\mathbb{F}$ un corps fini et soit K un sous-corps de $\mathbb{F}$. La dimension de $\mathbb{F}$ sur K en tant qu'espace vectoriel sera appelée degré de $\mathbb{F}$ sur K et notée $[\mathbb{F} : K]$. On notera que, par exemple , $\mathbb{C}$ est une extension de degré 2 sur $\mathbb{R}$ (puisque l'on obtient $\mathbb{C}$ en ajoutant i à $\mathbb{R}$, une base de $\mathbb{C}$ sur $\mathbb{R}$ est donc $\{1, i\}$). On a alors la proposition suivante (qui pourra parfois être bien utile) :*

Proposition 1.4.1 *Soit $\mathbb{F}$ un corps fini, et soient $H \subseteq K \subseteq \mathbb{F}$ deux sous-corps de $\mathbb{F}$, on a*

$$[\mathbb{F} : H] = [\mathbb{F} : K].[K : H]$$

Preuve. voir [16] ■

1.5 Construction d'un corps fini

Définition 1.5.1 *(**Polynôme irréductible**): Un polynôme non constant $f \in \mathbb{F}[x]$ est dit irréductible sur $\mathbb{F}$ si l'égalité $f(x) = g(x).h(x) \Rightarrow g(x) \in \mathbb{F}^*$ ou $h(x) \in \mathbb{F}^*$. Sinon, le polynôme f est réductible.*

Exemple 1.5.1

$f(x) = x^2 + x + 1$ est le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$.

$g(x) = x^2 + x + 2$ est irréductible sur $\mathbb{F}_3$.

Théorème 1.5.1 *Soit p un nombre premier et $f(x)$ un polynôme irréductible de degré n dans l'anneau $\mathbb{F}_p[X]$. Alors l'anneau quotient $\mathbb{F}_p[X]/\langle f(x)\rangle$ est un corps de p^n éléments.*

$$\mathbb{F}_p[X]/\langle f(x)\rangle = \{a_0 + a_1x + ... + a_{n-1}x^{n-1} + \langle f(x)\rangle \ | a_i \in \mathbb{F}_p\}$$

si on pose $\alpha = \overline{x} = x + \langle f(x)\rangle$, alors $\mathbb{F}_p[X]/\langle f(x)\rangle = K(\alpha)$ avec $\{1, \alpha, ..., \alpha^{n-1}\}$ une base et $K(\alpha)$ est un corps, extension par adjonction d'une racine α du polynôme irréductible $f(x)$ sur $\mathbb{F}_p$.

Exemple 1.5.2 *Construction du corps $\mathbb{F}_8 = \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/\langle f(x)\rangle$,tel que $f(x) = x^3 + x + 1$ est irréductible sur $\mathbb{F}_2$, On a alors :*

$$\mathbb{F}_2[x]/\langle x^3 + x + 1\rangle = \{a + bx + cx^2 + \langle f(x)\rangle,\ a, b, c \in \mathbb{F}_2\}$$

Explicitons les éléments de $\mathbb{F}_8 = \mathbb{F}_{2^3}$. Chaque classe est représentée par un unique polynôme a coefficient dans $\mathbb{F}_2$ et degré < 3

On pose $\alpha = \overline{x}$, Donc :

$$\mathbb{F}_2[x]/\langle f(x)\rangle = \{a + b\alpha + c\alpha^2,\ a, b, c \in \mathbb{F}_2\}$$

Alors $\mathbb{F}_8 = \mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$. *On a la table suivante :*

	comme un polynôme	*comme puissance de* α
000	0	0
100	1	1
010	α	α
001	α^2	α^2
110	$\alpha+1$	α^3
011	$\alpha^2+\alpha$	α^4
111	$\alpha^2+\alpha+1$	α^5
101	α^2+1	α^6

Chapitre 2

Polynômes sur un corps fini

Dans ce chapitre, aprés quelques définitions et concepts de base sur les corps finis, nous allons étudier les polynômes à coefficients dans un corps, généralement on va étudier anneau des polynômes $A[x]$, polynômes irréductibles, polynômes réciproques et factorisation de $x^n - 1$, en polynômes irréductibles sur un corps fini.

2.1 Anneau des polynômes $A[x]$

Définition 2.1.1 *Soit A un anneau commutatif. Un polynôme d'indéterminée x et de coefficients dans A est une somme formelle*

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_ix^i + ..$$

tels que les a_i sont des éléments de A qui sont nuls pour i assez grand, On désigne par $A[x]$ l'ensemble des polynômes en x sur A.

2.1.1 L'addition et multiplication dans $A[x]$

$$\text{Soient} \begin{cases} f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n + .. \\ \text{et} \\ g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m + .. \end{cases} \text{deux polynômes appartiennent } A[x].$$

Alors

$$\begin{aligned} f(x)+g(x) &= (a_0+b_0)+(a_1+b_1)x+..... \\ &= c_0+c_1x+...+c_nx^n+... \quad , c_n=a_n+b_n \quad n\geq 0 \\ f(x)g(x) &= (a_0+a_1x+a_2x^2+....+a_ix^i+...)(b_0+b_1x+b_2x^2+....+b_jx^j+..) \\ &= (a_0b_0)+(a_1b_0+a_0b_1)x+(a_0b_2+a_1b_1+a_2b_0)x^2+.... \\ &= d_0+d_1x+.....+d_nx^n+... \end{aligned}$$

tel que $d_n=\sum_{k=0}^{n} a_kb_{n-k}$, $n\geq 0$.

Proposition 2.1.1 *$(A[x],+,.)$ est un anneau pour l'addition et multiplication des polynômes de $A[x]$.*

Remarque 2.1.1 *1) A commutatif $\Leftrightarrow$ $A[x]$ commutatif.*

2) A intègre $\Leftrightarrow$ $A[x]$ intègre.

Exemple 2.1.1 *$\mathbb{R}[x]$, $\mathbb{Z}[x]$ des anneaux des polynômes.*

Définition 2.1.2 ***(Degré d'un polynôme)**: Soit A un anneau commutatif.*

Et soit $f(x)=a_0+a_1x+a_2x^2+....\in A[x]$, on peut écrire $f(x)$ sous la forme

$$f(x)=a_0+a_1x+a_2x^2+....+a_nx^n$$

Si $a_n\neq 0$, on dit que f est de degré n et on note $\deg(f)=d^0=n$.

Convention : Si $f=0$ $(\forall i: a_i=0)$ on pose $\deg(f)=-\infty$.

Exemple 2.1.2 *Dans $\mathbb{R}[x]$*

- *x^5+3x^2+6 est un polynôme de degré 5.*
- *7 est un polynôme constant de degré 0.*

Proposition 2.1.2 *Soient A un anneau commutatif unitaire. f et $g\in A[x]-\{0\}$*

$*\ \deg(f+g)\leq Max(\deg(f),\deg(g))$ *avec egalité ssi* $\deg(f)\neq\deg(g)$.

$*$ *Si A est intègre, alors* $\deg(fg)=\deg(f)+\deg(g)$.

2.2 Division Euclidienne dans $K[x]$

Théorème 2.2.1 *Soient $A(x)$ et $B(x)$ des polynômes à coefficients dans $K[x]$, On suppose B non nul. Alors, il existe un unique couple (Q, R) d'éléments de $K[x]$ tels que*

$$A = BQ + R \text{ et } \deg(R) < \deg(B)$$

Définition 2.2.1 *(**Quotient, reste**): Le polynôme Q est le quotient de la division euclidienne de A par B, le polynôme R est le reste de la division. On note que le reste peut être nul. Dans ce cas,* $\deg(R) = -\infty$.

Preuve. voir [17]. ■

Exemple 2.2.1 *Soient $A(x) = x^4 - 3x^3 + x + 1$ et $B(x) = x^2 + 2$, deux polynômes sur $\mathbb{R}[x]$, et par division euclidienne,*

On trouve $Q(x) = x^2 - 3x - 2$ et $R(x) = 7x + 5$.

Théorème 2.2.2 *Soit $f(x) \in K[x]$ et $\alpha \in K$ un scalaire. Alors*

$$f(\alpha) = 0 \Longleftrightarrow (x - \alpha) \text{ divise } f$$

Preuve. ($\Leftarrow$) On pose $x = \alpha$, donc $f(\alpha) = (\alpha - \alpha)q(\alpha) = 0$.
($\Rightarrow$) On utilisant la division euclidienne de f par $(x - \alpha)$,
donc $f(x) = (x - \alpha)q(x) + r(x)$ avec $\deg(r(x)) < \deg(x - \alpha) = 1$.
Alors $\deg(r(x)) = cte = c$.
$0 = f(\alpha) = r(\alpha) \Rightarrow r(\alpha) = c = 0$. ■

Théorème 2.2.3 *(**Bézout**): Soient $f, g \in K[x]$ et d le p*gcd *de f et g . Alors il existe deux polynômes $u(x)$ et $v(x)$ tels que :*

$$u(x)f(x) + v(x)g(x) = d(x)$$

2.3 Polynômes irréductibles

Définition 2.3.1 *un polynôme non constant $f \in \mathbb{F}[x]$ est dit irréductible sur $\mathbb{F}$ si l'égalité $f(x) = g(x).h(x) \Rightarrow g(x) \in \mathbb{F}^*$ ou $h(x) \in \mathbb{F}^*$. Sinon, le polynôme f est réductible.*

Proposition 2.3.1 *Pour tout nombre premier p et tout entier $n \geq 1$, il existe des polynômes irréductibles de degré n dans $\mathbb{F}_p[x]$.*

2.3.1 Critères d'irréductibilité des polynômes

Proposition 2.3.2 *Un polynôme P de $K[x]$ de degré 2 ou 3 est irréductible si et seulement si il n'admet pas de racines dans K.*

Preuve. Si P a une racine $\alpha \in K$, la division euclidienne de $P(x)$ par $x - \alpha$ donne un polynôme $Q \in K[x]$ tel que

$$P(x) = (x - \alpha)Q(x) + P(\alpha) = (x - \alpha)Q(x).$$

donc P est réductible dans $K[x]$.

Réciproquement.si P est réductible, il exist Q et R dans $K[x]$ tels que $P(x) = Q(x).R(x)$.ou $deg(Q) \geq 1$. Mais nous supposons ici que $deg(P) = deg(Q)+deg(R) = 2$ ou 3, si $deg(P) = 2$, on a donc $deg(Q) = 1$ et $deg(R) = 1$;si $deg(P) = 3$. on a quitte à échanger Q et R. $deg(Q) = 1$ et $deg(R) = 2$. Par suite. Q admet une racine $\alpha \in K$ et on a $P(\alpha) = 0$ ■

Exemple 2.3.1 *Soit $f(x) = 6x^2 + x + 1 \in \mathbb{F}_7[x]$*

f est irréductible sur $\mathbb{F}_7$, Car: $f(0) = 1$, $f(1) = 1$, $f(2) = 6$, $f(3) = 2$, $f(4) = 3$, $f(5) = 2$, $f(6) = 6$.

Remarque 2.3.1 *La proposition ne peut pas s'étendre aux degrés plus grands. En effet, le polynôme $(x^2 + 1)^2 \in \mathbb{R}[X]$ est réductible dans $\mathbb{R}[x]$ et de degré 4. mais il n'a pas de racine dans $\mathbb{R}$*

Théorème 2.3.1 *(**Crétère d'Eisenstein**): Soit A un anneau factoriel et soit K son corps de fractions.*

$$f(x) = a_0 + a_1x + ... + a_nx^n \in A[x]$$

Supposon qu'il existe un élément irréductible β de A tel que :

1) β ne divise pas a_n et β^2 ne divise pas a_0

2) Pour tout i, $0 \leq i \leq n-1, p$ divise a_i

Alors $f(x)$ est irréductible dans $A[x]$.

Définition 2.3.2 ***(Polynôme minimal)**: Le polynome $P(x) \in K[x]$, irréductible, normalisé et $P(\alpha) = 0$ est appelé le polynôme minimal de α sur K et secrit : $Irr(\alpha, K, x) = Irr_K(\alpha, x)$.*

Lemme 2.3.1 *Soit $n \geq 1$ un entier. Le polynôme $x^{p^n} - x \in \mathbb{F}_p[x]$ est exactement le produit de tous les polynômes irréductibles unitaires de $\mathbb{F}_p[x]$ de degré divisant n.*

Exemple 2.3.2 *Le polynôme $x^8 - x \in \mathbb{F}_2[x]$:*

$(x^8 - x) = (x^{2^3} - x) = x(x+1)(x^3 + x^2 + 1)(x^3 + x + 1)$.

2.4 Polynômes réciproques

Définition 2.4.1 *Soit $n \in \mathbb{N}^*$ et $f(x)$ un Polynôme de degré n sur $\mathbb{F}_p$. le Polynôme réciproque de $f(x)$ est defini par :*

$$f^*(x) = x^n f(\frac{1}{x}).$$

Exemple 2.4.1 *Soit $f(x) = x^3 + x^2 + 1$ sur $\mathbb{F}_2$.*

$$\begin{aligned} f^*(x) &= x^3(\frac{1}{x^3} + \frac{1}{x^2} + 1) \\ &= x^3 + x + 1. \end{aligned}$$

Remarque 2.4.1 *Si $f(0) \neq 0$ alors $f(x)$ et $f^*(x)$ sont de même degré.*

- Si $f^*(x) = f(x)$, on dit que $f(x)$ est auto-réciproque.

2.5 Factorisation de $x^n - 1$, en polynômes irréductibles sur un corps fini

La factorisation du polynôme $x^n - 1$ joue un rôle important dans la recherche de tous les codes cycliques de longueur n sur $\mathbb{F}_q$. Soient $\mathbb{F}_q$ un corps fini de caractéristique p et K une extension algébriquement close de $\mathbb{F}_q$. L'ensemble Γ_n des racines du polynôme $x^n - 1$ (appartenant à $\mathbb{F}_q[x]$) est appelé ensemble des racines n-ièmes de l'unité dans K, et forme un sous-groupe fini du groupe multiplicatif $(K^*, \times)$. C'est donc un groupe cyclique (Théorème 1.3.5). Si n et q ne sont pas premiers entre eux, on peut écrire $n = p^s n'$ où $pgcd(n', q) = 1$, et l'on obtient

$$x^n - 1 = x^{p^s n'} - 1 = (x^{n'} - 1)^{p^s}$$

de sorte que :

a) $\Gamma_n = \Gamma_{n'}$,

b) la factorisation de $x^n - 1$ en produit de facteurs irréductibles se déduit de celle du polynôme $x^{n'} - 1$.

Ces résultats montrent que l'on peut se borner à étudier le cas où $pgcd(n, q) = 1$.

Supposons donc que $pgcd(n, q) = 1$. Dans ce cas toutes les racines de $x^n - 1$ dans K sont simples (car le polynôme dérivé $(x^n - 1)' = nx^{n-1}$ ne s'annule jamais en une racine n-ième de l'unité) et Γ_n est un sous-groupe cyclique d'ordre n de K. Notons $m = \omega_n(q)$ l'ordre multiplicatif de q modulo n. Soit α un générateur Γ_n. On dit que α est une racine primitive n-ièmes de l'unité. Comme α est d'ordre n,

$$\alpha \in F_{q^t} \Leftrightarrow \alpha^{q^t} = \alpha \Leftrightarrow \alpha^{q^t - 1} = 1 \Leftrightarrow n|(q^t - 1) \Leftrightarrow m|t \quad (*)$$

et $\mathbb{F}_{q^m}$ apparaît comme le plus petit sous-corps de K contenant toutes les racine primitive n-ièmes de l'unité, ou, ce qui revient au même puisque $\Gamma_n = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$, le plus petit sous-corps de K contenant toutes les racines n-ièmes de l'unité. Pour le vérifier, il faut montrer que $\mathbb{F}_{q^m} = \cap k_0$ où l'intersection est prise sur tous les sous-corps k_0 de K contenant Γ_n. L'inclusion $\mathbb{F}_{q^m} \supset k_0$ est triviale puisque $\mathbb{F}_{q^m}$ est l'un des k_0 (voir les équivalences $(*)$). Réciproquement, si l'on avait $\mathbb{F}_{q^m} \subset k_0$ pour l'un des corps k_0, l'intersection $k_0 \cap \mathbb{F}_{q^m}$ serait un corps fini strictement inclus dans $\mathbb{F}_{q^m}$ et contenant Γ_n, ce qui contredit les équivalences

$(*)$. En conclusion le corps des racines $\sum_n$de $x^n - 1$ sur $\mathbb{F}_q$est $\sum_n = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, et l'on a la décomposition

$$x^n - 1 = \prod_{i=0}^{n-1}(x - \alpha^i)$$

dans $\mathbb{F}_{q^m}[x]$.

Exemple 2.5.1

-Dans $\mathbb{F}_2$ *on a* $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$

-Dans $\mathbb{F}_3$ *on a* $x^5 - 1 = (2 + x)(1 + x + x^2 + x^3 + x^4)$

-Dans $\mathbb{F}_5$ *on a* $x^4 - 1 = (1 + x)(2 + x)(3 + x)(4 + x)$

-Dans $\mathbb{F}_7$ *on a* $x^{15} - 1 = (3 + x)(5 + x)(6 + x)(1 + x + x^2 + x^3 + x^4)$
$(2 + x + 4x^2 + 2x^3 + x^4)(4 + x + 2x^2 + 4x^3 + x^4)$

-Dans $\mathbb{F}_5$ *on a* $x^{36} - 1 = (1 + x)(2 + x)(3 + x)(4 + x)(1 + x + x^2)(4 + 2x + x^2)$
$(4 + 3x + x^2)(1 + 4x + x^2)(1 + x^3 + x^6)(4 + 2x^3 + x^6)$
$(4 + 3x^3 + x^6)(1 + 4x^3 + x^6)$

Chapitre 3

Codes cycliques isoduaux de rendement $\frac{1}{2}$ sur $GF(7)$

Dans ce dernier chapitre on va étudier les codes linéaires, codes cycliques et son constructions et Codes cycliques iso-duaux de rendement $\frac{1}{2}$ sur $GF(7)$ pour $n \leq 50$, avec n est pair et $\frac{n}{2}$ premier et impair.

3.1 Codage algébrique

Définition 3.1.1 *Un alphabet est un ensemble fini non vide A*

.Un élément $a \in A$ est appelé lettre

$$A^n = \underbrace{A \times A \times .... \times A}_{n\ fois}, n \geq 1$$

.Un élément $x = (x_1, x_2, .., x_n) \in A^n$ est un mot de longueur n.

On pose $x = (x_1, x_2, .., x_n) = x_1x_2..x_n$

A^n = l'ensemble des mots de longueur n sur l'alphabet A.

A est supposé un corps fini $A = \mathbb{F}_q$, $\mathbb{F}_q^n = \{x_1x_2..x_n : x_i \in \mathbb{F}_q\}$.

Définition 3.1.2 *Un code de longueur n sur $\mathbb{F}_q$ est un sous ensemble C non vide de $\mathbb{F}_q^n$, $(\emptyset \neq C \subset \mathbb{F}_q^n)$.*

La distance de Hamming et poids de Hamming

Définition 3.1.3

- *Soit $\mathbb{F}$ un ensemble fini non vide et n entier strictement positif. L'application*

$$\begin{aligned} d_H \ : \ \mathbb{F}^n \times \mathbb{F}^n &\longrightarrow \mathbb{N} \\ (a,b) &\mapsto Card\{i \in \{1,...,n\} | a_i \neq b_i\} \end{aligned}$$

Avec $a = (a_1, ..., a_n)$ et $b = (b_1, ..., b_n)$ est la distance de Hamming sur $\mathbb{F}^n$.

- *Soit $\mathbb{F}$ un corps fini, l'application w_H définie par :*

$$w_H : \mathbb{F}^n \to \mathbb{N}$$

$$a \mapsto d_H(a, 0) = Card\{i \in \{1, ..., n\} | a_i \neq 0\}$$

est le poids de Hamming.

Remarque 3.1.1 *$(\mathbb{F}_q^n, d_H)$ est appelle l'espace de Hamming.*

On remarque que la distance de Hamming sur $\mathbb{F}_q^n$ vérifié bien les propriétés usuelle d'une distance. Rappelons brièvement les propriétés :

1- $d(x, y) = d(y, x) \geq 0$.

2-$d(x, y) = 0$ si et seulement si $x = y$.

3-$d(x, y) \leq d(x, z) + d(z, y)$.

Distance minimale d'un code

Définition 3.1.4 *C un code de longueur n sur $\mathbb{F}_q$. La distance minimale du code C est l'entier $d(C)$ défini par :*

$$d(C) = \min\{d_H(x, y) : x \neq y, x, y \in C\}$$

Exemple 3.1.1 *1) $\mathbb{F}_q = \mathbb{F}_2$, $n = 4$*

$$C = \{0100, 1000, 1100, 0000\}$$

C est un code de longueur 4 sur $\mathbb{F}_2$, $d(C) = 1$.

2) Dans $\mathbb{F}_3^4$ on a : $d(1201, 2200, 1111) = 2$, $d(2011, 1012, 2010) = 1$.

Paramètres d'un code

Définition 3.1.5 *C est un (n, M, d) code sur $\mathbb{F}_q$ tel que:*

n = la longueur.

$M = |C| = \#C$ = le cardinal de C .

$d(C) = d$ la distance minimale de C.

3.2 Codes linéaires

Définition 3.2.1 *Soit K un corps fini et soit $n > 0$. Le K-espace vectoriel K^n est muni de la métrique de Hamming.* ***Un code linéaire*** *est un K-sous-espace de K^n. Ses paramètres sont : sa* ***longueur*** *n, sa* ***dimension****, sa* ***distance minimale****. Ces deux derniers paramètres sont notés généralement k et d. On dit que le code C est un code $[n, k, d]$.*

Proposition 3.2.1 *La distance minimale d'un code linéaire est égale au plus petit poids non nul de ce code.*

$$\begin{aligned} d &= \min\{w_H(x) : x \in C, x \neq 0\} \\ d_H(x, y) &= |\{i : x_i \neq y_i\}| \\ &= |\{i : x_i - y_i \neq 0\}| \\ &= w_H(x_i - y_i). \end{aligned}$$

Matrice génératrice d'un code linéaire

Définition 3.2.2 *Une matrice génératrice d'un code linéaire de longueur n et de dimension k est une matrice de type $k \times n$ dont lignes forment une base de C*

$*$ *Si* $B = \{\underbrace{(g_{11}, .., g_{1n})}_{g_1}, \underbrace{(g_{21}, .., g_{2n})}_{g_2}, ..., \underbrace{(g_{k1}, .., g_{kn})}_{gk}\}$ *une base de C, Alors*

$$G = \begin{pmatrix} g_{11}....g_{1n} \\ g_{21}....g_{2n} \\ ..... \\ ..... \\ g_{k1}....g_{kn} \end{pmatrix} = \begin{pmatrix} g_1 \\ g_2 \\ ..... \\ ..... \\ g_k \end{pmatrix} \textit{ est une matrice génératrice de } C.$$

Exemple 3.2.1 *Soit* $\mathbb{F}_2^3 = \{000, 001, 010, 100, 011, 110, 101, 111\}$ *est un espace de Hamming.* $C = \{000, 010, 001, 011\}$ *est un* $[3, 2, 1]$ *code linéaire sur* $\mathbb{F}_2$ *et* $B = \{010, 001\}$ *est un base de* C*, alors* $G = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ *est un matrice génératrice de* C*. Alors le code* C *est donné par :*

$$\begin{aligned} C &= \{c_1(0,0,1) + c_2(0,1,1) : c_1, c_2 \in \mathbb{F}_2\} \\ &= \{000, 010, 001, 011\} \end{aligned}$$

Ainsi le code C *est de paramètres* $[3, 2, 1]$ *et* $|C| = q^k = 2^2 = 4$.

Produit scalaire sur $\mathbb{F}_q^n$:

Soient $x = x_1.x_2...x_n$ et $y = y_1.y_2...y_n \in \mathbb{F}_q^n$. On note le produit scalaire de x et y est $\langle x.y \rangle$ et défini par :

$$\langle x.y \rangle = x_1y_1 + x_2y_2 + .. + x_ny_n.$$

Code dual d'un code linéaire:

Définition 3.2.3 *Soit* C *un* $[n, k]$*code linéaire sur* $\mathbb{F}_q$*, le code dual est :*

$$\begin{aligned} C^\perp &= \{y \in \mathbb{F}_q^n : \langle x.y \rangle = 0 \ \textit{ pour tout } x \in C\} \\ y &\in C^\perp \iff \forall x \in C : \langle x.y \rangle = 0. \end{aligned}$$

Théorème 3.2.1 *Si* C *est un code linéaire de longueur* n *et de dimension* k*, alors* $C^\perp$ *est un code linéaire de longueur* n *et de dimension* $n - k$.

Preuve. voir[8]. ■

Exemple 3.2.2 *Soit* $\mathbb{F}_2^3 = \{000, 001, 010, 100, 011, 110, 101, 111\}$ *est un espace de Hamming alors:*

- $C = \{000, 001, 010, 011\}$ *est un* $[3, 2, 1]$ *code linéaire sur* $\mathbb{F}_2$.

- $C^{\perp} = \{000, 100\}$ *est un* $[3, 1, 1]$ *code linéaire sur* $\mathbb{F}_2$.

Définition 3.2.4 ***(Matrice de contrôle)*** *: Une matrice de contrôle ou parité de* C *est une matrice génératrice du code dual* $C^{\perp}$ *notée* H*. Revenons à exemple précedent,*

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

3.3 Code cyclique

Définition 3.3.1 *Un code linéaire* $C \subset \mathbb{F}_q^n$ *est dit cyclique si*

$$(a_0, .., a_{n-1}) \in C \Longleftrightarrow (a_{n-1}, a_0, .., a_{n-2}) \in C$$

Pour la suite, nous supposons que $pgcd(n, q) = 1$ et on notera $\langle x^n - 1\rangle$ l'idéal de $\mathbb{F}_q[x]$ engendré par $x^n - 1$. Alors, tout élément de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ peut être représenté par des polynômes de degré inférieur à n (ou le polynôme nul), et cet anneau est ainsi isomorphe à $\mathbb{F}_q^n$ comme $\mathbb{F}_q$-espace vectoriel.

Un isomorphisme est donné par

$$(a_0, .., a_{n-1}) \longleftrightarrow a_0 + a_1x + a_2x^2 + .. + a_{n-1}x^{n-1}$$

Cet isomorphisme permet de considérer les éléments de $\mathbb{F}_q[x]/\langle x^n-1\rangle$ comme des vecteurs de $\mathbb{F}_q^n$ ou comme des polynômes de *degré* $< n$ modulo $x^n - 1$.

La multiplication des polynômes modulo $x^n - 1$ est introduite de manière usuelle, c'est à dire, que si $g_1, g_2 \in \mathbb{F}_q[x]$ alors

$(g_1 \ mod \ (x^n - 1))(g_2 \ mod \ (x^n - 1)) = (g_1g_2) \ mod \ (x^n - 1)$,

$(g_1 \ mod \ (x^n - 1)) + (g_2 \ mod \ (x^n - 1)) = (g_1 + g_2) \ mod \ (x^n - 1)$.

Exemple 3.3.1

i) Le code binaire $C = \{000, 101, 011, 110\}$ *est cyclique.*

ii) Le code binaire $C = \{0000, 1001, 0110, 1111\}$ *n'est pas cyclique.*

3.3.1 Polynôme générateur d'un code cyclique

Définition 3.3.2 *Le polynôme générateur $g(x)$ du code cyclique C est le polynôme normalisé de plus bas degré contenu dans C.*

Proposition 3.3.1 *Le polynôme générateur est unique.*

Preuve. Supposons que g_1 et g_2 soient deux polynôme générateurs. Alors $g_1 - g_2$ est un polynôme générateur (le code est linéaire) de degré strictement inférieur au degré des g_i. Contradiction. ■

Proposition 3.3.2 *Tout mot d'un code cyclique est un multiple du polynôme générateur. On note $C = \langle g \rangle$.*

Preuve. Soit $c(x) \in C$ on effectue la division euclidienne de c par g : $c = ag + r$ avec $deg(r) < deg(g)$. Or, le reste r qui est la différence de deux mots du code appartient au code. Si $r \neq 0$, on contredit l'hypothèse sur le degré minimum de g. ■

Proposition 3.3.3 *Le polynôme générateur divise $x^n - 1$.*

Preuve. On a $x^n - 1 = ag + r$ avec $deg(r) < deg(g)$ et on conclut comme précédemment que r doit être nul (après réduction modulo $x^n - 1$). ■

Théorème 3.3.1 *Soit C un code cyclique de $\mathbb{F}_q^n$, de polynôme générateur*

$$g(x) = g_0 + g_1 x + ... + g_{n-k} x^{n-k}$$

Alors une matrice génératrice de C est la matrice $k \times n$ donnée par:

$$G = \begin{pmatrix} g_0 & g_1 & ... & g_{n-k} & 0 & 0 & ... & & 0 \\ 0 & g_0 & g_1 & ... & g_{n-k} & 0 & ... & & 0 \\ 0 & 0 & g_0 & g_1 & ... & g_{n-k} & 0 & ... & 0 \\ & ... & & & ... & & & ... & \\ 0 & 0 & ... & & & g_0 & g_1 & ... & g_{n-k} \end{pmatrix}.$$

Définition 3.3.3 *(**polynôme de contrôle**) : Soit C un $[n, k, d]$ un code cyclique de polynôme générateur $g(x)$.Le polynôme $h(x)$ vérifiant :*

$$h(x) = \frac{(x^n - 1)}{g(x)}$$

est dit polynôme de contrôle.

Théorème 3.3.2 *Soit C un $[n, k, d]$ un code cyclique de polynôme de contrôle $h(x) = h_0 + h_1x + ... + h_kx^k$. La matrice H suivante est une matrice de test de C :*

$$H = \begin{pmatrix} h_k & h_{k-1} & ... & h_0 & 0 & ... & 0 \\ 0 & h_k & h_{k-1} & ... & h_0 & ... & 0 \\ & ... & & & ... & & \\ 0 & ... & 0 & h_k & h_{k-1} & ... & h_0 \end{pmatrix}.$$

3.3.2 Construction d'un code cyclique

Pour obtenir un code cyclique de dimension k et de longueur n, on peut coder les messages à transmettre (identifiés à des polynômes de *degré* $\leq k-1$) en les multipliant par un polynôme g donné de degré $n - k$ diviseur de $x^n - 1$. La correspondance

$$(a_0, .., a_{n-1}) \longleftrightarrow f(x) = a_{n-1}x^{n-1} + ... + a_1x + a_0$$

entre les vecteurs et les polynômes permet d'interpréter C comme le sous-espace suivant :

$$C = \{1.g(x), x.g(x), x^2.g(x), ..., x^{k-1}.g(x)\} \subset F_q[x]/\langle x^n - 1\rangle$$

de l'anneau quotient

$$F_q[x]/\langle x^n - 1\rangle.$$

Théorème 3.3.3 *Le code linéaire C est cyclique si et seulement si C est un idéal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.*

Preuve. Si C est un idéal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, et $(a_0, .., a_{n-1}) \in C$, alors

$$x.(a_0, .., a_{n-1}) = (a_{n-1}, a_0, .., a_{n-2}) \in C$$

Inversement, si C est cyclique, pour tout $a(x) \in C$, $xa(x) \in C$, $x^2a(x) \in C$, Et ainsi de suite, donc $b(x)a(x) \in C$ et C est un idéal.

L'anneau $\mathbb{F}_q[x]$ est principal, donc tous les idéaux de l'anneau $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ sont principaux. En particulier, tout idéal non nul est engendré par un polynôme $g(x)$ de plus bas degré qu'il contient, et $g(x)$ divise $x^n - 1$:

$$C = \{1.g(x), x.g(x), x^2.g(x), ..., x^{k-1}.g(x)\}.$$

■

Dual d'un code cyclique

Théorème 3.3.4 *Soit $C[n, k]$ un code cyclique. Alors son code dual $C^\perp$ est cyclique et il est généré par le polynôme*

$$g^\perp(x) = x^k h(x^{-1})$$

où $h(x)$, de degré k, est le polynôme de parité du code C.

Preuve. [4]. ■

3.4 Codes cycliques iso-duaux de rendement $1/2$ sur $GF(7)$ pour $n \leq 50$

Dans ce travail, nous considérons des codes cycliques au-dessus de $\mathbb{F}_7$ de rendement $1/2$. Une sous-classe importante de ces derniers est des codes iso-dual, c'est-à-dire. Code l'équivalent au leur conjugue. Nous proposons, dans le cas $n = 2m$ avec m premier et impair. La caractérisation du polynôme se produisant d'un code cyclique iso-dual est laissée comme problème non résolu provocant.

3.4.1 Codes cycliques iso-duaux sur $GF(7)$

Soit le corps fini de Galois à sept élément $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, un code $C[n, k]$ linéaire est un sous-espace vectoriel de dimension k sur $\mathbb{F}_7^n$. Les éléments de C sont appelés mots de code. Le taux d'un code $C[n, k]$ linéaire est défini par k/n. Deux codes C et C' sont équivalents si l'un est obtenu à partir de l'autre par permutation des coordonnées. A code linéaire C est dit **iso-dual** si C et $C^{\perp}$ sont équivalents.

Soit $g(x)$ le polynôme générateur du code cyclique C, alors son dual $C^{\perp}$ admet pour polynôme générateur le polynôme réciproque de:

$$h(x) = \frac{x^n - 1}{g(x)}$$

Une généralisation pour les codes cycliques $C[n, \frac{n}{2}]$ sur le corps fini $\mathbb{F}_7$, dans le cas où n est pair non multiple de 7 (le cardinal du corps), sur le fait que ces derniers sont iso-duaux.

L'utilisation de la notion de polynôme réciproque nous a permis de trouve une propriété concernant l'iso-dualité de ces codes cycliques pour $n \leq 50$. Cette iso-dualité est réalisée par le fait que le polynôme réciproque du complément du générateur $g(x)$ d'un tel code cyclique vérifie la propriété suivante :

Sachant que pour $n = 2m$, on a :

$$x^n - 1 = (x^m - 1)(x^m + 1)$$

On pose

$$(x^m - 1) = (x - 1)u(x)v(x) \quad \text{et} \quad (x^m + 1) = (x + 1)u(-x)v(-x)$$

Avec la condition que les polynômes u et v soient auto-réciproques c'est-à-dire :

$$u^* = u \quad \text{et} \quad v^* = v$$

Soit $g(x) = (x - 1)u(x)v(-x)$, alors

$$h(x) = \frac{x^n - 1}{g(x)} = (x + 1)u(-x)v(x)$$

D'où

$$\begin{aligned} h^*(x) &= \left[\frac{x^n - 1}{g(x)}\right]^* = (x + 1)u(-x)v(x) \\ &= -(-x - 1)u(-x)v(x) \\ &= -g(-x) \end{aligned}$$

Ainsi le code cyclique de générateur le polynôme $g(x)$ est iso-dual en longueur $2m$. Nous résumons ce résultat par :

Proposition 3.4.1 *Soit $(x^m - 1) = (x - 1)u(x)v(x)$ avec m impair et $u^* = u$ et $v^* = v$. Alors le code cyclique généré par le polynôme $g(x) = (x-1)u(x)v(-x)$ est isodual en longueur $2m$.*

Remarque 3.4.1 *Tous les polynômes générateurs et la correspondance ont produit des codes qui sont isodual sont enregistrés dans les tables suivantes :*

Codes cycliques $\mathbf{C[6,3]_7}$

La factorisation de polynôme $x^6 - 1$ par **Mathematica 9** donné 6 polynômes irréductibles de degré 1 :

$$(x^6 - 1) = (1 + x)(2 + x)(3 + x)(4 + x)(5 + x)(6 + x)$$

Il faut choisir 3 polynômes parmi 6, donc $\binom{6}{3} = 20$ choix pour le polynôme générateur $g(x)$.

Table 1

n°	$g(x)$	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$\left[\frac{x^6-1}{g(x)}\right]^* =$
1	6461	$\begin{bmatrix} u^*(x)=2v(x) \\ v^*(x)=4u(x) \end{bmatrix}$	$[-g(-x)]^*$
2	1001	$\begin{bmatrix} u^*(x)=-v^*(4x) \\ v^*(x)=-u^*(2x) \end{bmatrix}$	$g(-x)$
3	3311	/	non iso-dual
4	5621	/	non iso-dual
5	5511	/	non iso-dual
6	1221	$\begin{bmatrix} u^*(x)=v^*(2x) \\ v^*(x)=u^*(4x) \end{bmatrix}$	$g(-x)$
7	4631	/	non iso-dual
8	6131	$\begin{bmatrix} u^*(x)=4v(x) \\ v^*(x)=2u(x) \end{bmatrix}$	$[-g(-x)]^*$
9	3641	/	non iso-dual
10	2651	/	non iso-dual
11	3521	/	non iso-dual
12	2331	/	non iso-dual
13	1141	$\begin{bmatrix} u(x)=5v(x) \\ v^*(x)=3u(x) \end{bmatrix}$	$[-g(-x)]^*$
14	5341	/	non iso-dual
15	6251	$\begin{bmatrix} u^*(x)=2v(x) \\ v^*(x)=4u(x) \end{bmatrix}$	$-g(-x)$
16	4361	/	non iso-dual
17	4551	/	non iso-dual
18	2561	/	non iso-dual
19	6001	$\begin{bmatrix} u^*(x)=v^*(2x) \\ v^*(x)=u^*(4x) \end{bmatrix}$	$-g(-x)$
20	1411	$\begin{bmatrix} u^*(x)=4v(x) \\ v^*(x)=2v(x) \end{bmatrix}$	$[-g(-x)]^*$

Codes cycliques $\mathbf{C[10,5]_7}$

Dans ce cas on a 4 choix pour $g(x)$ et la factorisation de polynôme x^6-1 en facteurs irréductibles par **Mathematica 9** donne :

$$(x^{10}-1) = (1+x)(6+x)(1+x+x^2+x^3+x^4)(1+6x+x^2+6x^3+x^4)$$

Table 2

n°	$g(x)$	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$\left[\frac{x^{10}-1}{g(x)}\right]^* =$
1	122221	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
2	600001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$
3	100001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
4	625251	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$

Codes cycliques $\mathbf{C[22, 11]_7}$

La factorisation de polynôme $x^{22}-1$ en facteurs irréductibles donne :

$$\begin{aligned}(x^{22}-1) &= (1+x)(6+x)(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}) \\ &\quad (1+6x+x^2+6x^3+x^4+6x^5+x^6+6x^7+x^8+6x^9+x^{10})\end{aligned}$$

Il y a deux polynômes de degré 1 et deux polynômes de degré 10, il faut choisir un polynôme de degré 1 et un polynôme de degré 10, c-à-d $\binom{2}{1} \times \binom{2}{1} = 4$ choix pour $g(x)$.

Table 3

n°	$g(x)$	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$\left[\frac{x^{22}-1}{g(x)}\right]^* =$
1	122222222221	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
2	600000000001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$
3	100000000001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
4	625252525251	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$

Codes cycliques $\mathbf{C[26, 13]_7}$

Pour les codes cycliques $C[26, 13]_7$, la factorisation de $x^{26}-1$ nous donne 4 choix possibles pour le polynôme générateur de degré 13.

$$\begin{aligned}(x^{26}-1) &= (1+x)(6+x)(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}) \\ &\quad (1+6x+x^2+6x^3+x^4+6x^5+x^6+6x^7+x^8+6x^9+x^{10}+6x^{11}+x^{12})\end{aligned}$$

Table 5

n°	$g(x)$	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$\left[\frac{x^{26}-1}{g(x)}\right]^* =$
1	12222222222221	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
2	60000000000001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$
3	10000000000001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
4	62525252525251	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$

Codes cycliques $\mathbf{C[34, 17]_7}$

De même ici on a 4 choix pour le polynôme générateur du code $[34, 17]_7$:

$$\begin{aligned}(x^{34}-1) &= (1+x)(6+x)(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10} \\ &\quad +x^{11}+x^{12}+x^{13}+x^{14}+x^{15}+x^{16})(1+6x+x^2+6x^3+x^4+6x^5 \\ &\quad +x^6+6x^7+x^8+6x^9+x^{10}+6x^{11}+x^{12}+6x^{13}+x^{14}+6x^{15}+x^{16})\end{aligned}$$

Table 5

n°	$g(x)$	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$\left[\frac{x^{34}-1}{g(x)}\right]^* =$
1	122222222222222221	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
2	600000000000000001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$
3	100000000000000001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
4	625252525252525251	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$

Codes cycliques $\mathbf{C[38, 19]_7}$

La factorisation de polynôme $x^{38}-1$ par **Mathematica 9** donné deux polynômes de degré 1 et 12 polynômes de degré 3 :

$$\begin{aligned}(x^{38}-1) &= (1+x)(6+x)(1+2x+x^3)(6+2x+x^3)(1+3x+x^2+x^3)(1+2x^2+x^3) \\ &\quad (1+x+3x^2+x^3)(6+3x+3x^2+x^3)(1+4x+3x^2+x^3)(6+x+4x^2+x^3) \\ &\quad (1+3x+4x^2+x^3)(6+4x+4x^2+x^3)(6+5x^2+x^3)(6+3x+6x^2+x^3)\end{aligned}$$

Il faut choisir 6 polynômes parmi 12 et un polynôme de degré 1, c-à-d $\binom{12}{6} \times \binom{2}{1} = 1848$ choix pour $g(x)$.

Codes cycliques $\mathbf{C[46, 23]_7}$

De même ici on a 4 choix pour le polynôme générateur du code $[46, 23]_7$:

$$\begin{aligned}(x^{46}-1) &= (1+x)(6+x)(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9\\ &\quad +x^{10}+x^{11}+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}+x^{18}+x^{19}\\ &\quad +x^{20}+x^{21}+x^{22})(1+6x+x^2+6x^3+x^4+6x^5+x^6+6x^7\\ &\quad +x^8+6x^9+x^{10}+6x^{11}+x^{12}+6x^{13}+x^{14}+6x^{15}+x^{16}\\ &\quad +6x^{17}+x^{18}+6x^{19}+x^{20}+6x^{21}+x^{22})\end{aligned}$$

Table 6

n°	$g(x)$	$\begin{bmatrix} u^*(x)= \\ v^*(x)= \end{bmatrix}$	$\left[\frac{x^{46}-1}{g(x)}\right]^* =$
1	122222222222222222221	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
2	600000000000000000000001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$
3	100000000000000000000001	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$g(-x)$
4	625252525252525252525251	$\begin{bmatrix} u^*(x)=u(x) \\ v^*(x)=v(x) \end{bmatrix}$	$-g(-x)$

Conclusion

Le travail de ce mémoire entre, en général, dans le cadre de la recherche des codes linéaires iso-duaux sur un corps fini $\mathbb{F}_q$, en particulier nous avons étudié les codes cycliques iso-duaux de rendement $1/2$ sur $\mathbb{F}_7$. Dans ce contexte nous avons recherché les codes cycliques iso-duaux de paramètres $[n, n/2]$ sur le corps fini $\mathbb{F}_7$, telle que n soit pair et $n/2$ premier et impair jusqu'à la longueur ≤ 50.

Bibliographie

[1] **A.A. Pantchichkine**. Mathématiques des codes correcteurs d'erreurs,Master-2 de mathématiques (M2P), "Cryptologie, Sécurité et Codage d'Information", 2004/2005, Module 506a.

[2] **A. Bonnecaze**. Introduction à l'algèbre pour les codes cycliques, 2006 -2007.

[3] **Alexandra Bruasse**-Bac ESIL. Corps finis, Année 2003-2004.

[4] **Cherif Mihoubi**. Classification des codes linéaires tertiaires optimaux [n,n/2]. Thèse présenté pour l'obtention du diplôme de Doctorat, Université Hadj Lakhdar Batna, 2012.

[5] **Cherif Mihoubi**. Isodual cyclic codes over GF(5). Into. J. Open problems compt. Math. Vol. 4, No.4, December 2011 ISSN 1998-6262, Copyright © ICSRS Publication, 2011 www.i-csrs.org.

[6] **Cherif Mihoubi**. Corps finis et polynômes, Cours 1^{er} Master, Université de M'sila 2014/2015.

[7] **Cherif Mihoubi. Patrick Solé.** Optimal and isodual ternary cyclic codes of rate 1/2.Received : 12 January 2012 / Revised: 9 May 2012 / Accepted: 4 July 2012 / Published online: 26 July 2012 © The Author(s) 2012. This article is published with open access at SpringerLink.com.

[8] **Christine Bachoc**. Codes et Cryptologie, Université Bordeaux 1, Licence de Sciences, Technologies, Santé, Mentions Mathématiques et Informatique, M1MI2016 Codes et Cryptologie.

[9] **Claude Carlet**. Cours de Codes Correcteurs d'erreurs (et fonctions booléennes), D.E.A de mathématiques et d'informatique de Bamako, Année 2007.

[10] **Daniel Guin et Thomas Hausberger**. Algèbre Tome 1, EDP sciences,17, avenue du Hoggar, Parc d'activités de Courtabœf, BP 112, 91944 Les Ulis Cedex A, France.

[11] **Daniel Guin**. Algébre Tome 2, EDP sciences,17, avenue du Hoggar, Parc d'activités de Courtabœf, BP 112, 91944 Les Ulis Cedex A, France.

[12] **Dany-Jack Mercier**. Corps finis, IUFM de Guadeloupe, Morne Ferret, BP399, Pointe-à-Pitre cedex 97159, dany-jack.mercier@univ-ag.fr, 11 avril 2003.

[13] **Eric Wegrzynowski**. Corps finis, Licence et Master mention informatique, USTL, 06 mars 2008.

[14] **Guy Auliac**. Mathématiques, Dunod, Paris, 2005.

[15] **Jean-Guillaume Dumas. Jean-Louis Roch. Eric Tannier. Sébastien Varrette**. Théorie des codes, Dunod, Paris, 2007.

[16] **Josette Calais**. Extensions de corps (Théorie de Galois), niveau M1-M2, Ellipses Edition Marketing S A, 2006, 32, rue Bargue 75740 Paris cedex 15.

[17] **Julien Roques**. Mathématique L3 Algèbre, Pearson Education, Publié par Pearson Education France, 47 bis, rue des Vinaigriers, 75010 Paris, 2009.