REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Mohamed Boudiaf de M'sila
Faculté des Mathématiques et de l'Informatique
Département de Mathématiques

Mémoire de Master

Domaine : Mathématiques et Informatique
Filière : Mathématiques
Option : Algèbre et Mathématiques Discrète

Thème

Sur les Codes Cycliques Sur Un Corps Fini

Présenté par :
KHALFA Mebarka
SAAI Soumia

Devant le jury composé de :

MIHOUBI Douadi Prof, Université de M'sila **Président.**
HEBOUB Lakhdar M.A. A, Université de M'sila **Encadreur.**
GHADBANE Nasser M.C. A, Université de M'sila **Examinateur.**

Année universitaire 2020/2021

Remerciements

Avant tout, nous remercions Dieu, le tout puissant d'avoir, éclairé notre vie, renforcer notre courage et notre volonté pour pouvoir achever ce travail.

Nous tenons à remercier particulièrement notre directeur de recherche, monsieur ***HEBOUB Lakhdar****, pour toute l'aide qui nous a apporté, ainsi que sa patience et ses pertinents conseils en dirigeant ce travail avec beaucoup d'intérêt.*

Nous remercions également monsieur ***MIHOUBI Douadi****, d'avoir accepté de présider notre mémoire.*

Nous portons nos sincères remerciements à monsieur ***GHADBANE Nasser****, d'avoir accepté d'examiner notre mémoire.*

Nos remerciements s'adressent à tous les enseignants du département de mathématiques, sans oublier nos chers collègues et amies, tous les étudiants et étudiantes de notre promotion, ainsi tous ceux qui ont participé de près ou de loin à l'élaboration de ce mémoire.

Nous accordons tout notre respect à ceux qui nous ont soutenus, en particulier à nos chers parents, nos sœurs et nos frères.

Finalement, nous présentons nos sincères remerciements à toutes les personnes ; la famille et les amis qui ont contribué d'une manière directe ou indirecte à la réalisation de ce travail.

Notations

$|G|$: L'ordre d'un groupe fini ou le cardinal d'un ensemble fini G.

$\mathbb{N}$: L'ensemble des entiers naturels.

$\mathbb{Z}$: L'ensemble des entiers relatifs.

$\mathbb{Z}/p\mathbb{Z}$: L'ensemble des entiers modulo p.

$C(n,k)$: Code correcteur de longueur n et dimension k.

$\overline{X}$: La classe de X modulo une relation d'équivalence.

$\mathbb{k}^*$: Le groupe multiplicatif d'un corps $\mathbb{k}$ avec $\mathbb{k}^* - \{0\}$.

$\mathbb{F}_q$: Un corps fini de cardinal q.

$A[x]$: L'anneau des polynômes à une déterminée x sur un anneau.

$(f(x))$: L'idéal engendré par $f(x)$ dans $A[x]$.

$\cong$: Isomorphisme de groupe, de corps, d'espaces vectoriels.

$[x]$: La partie entière d'un réel x.

$w(x)$: Le poids de Hamming d'un mots x.

rgH: Le rang d'une matrice H.

$\ker H$: L'espace nul d'une matrice H.

$d(x,y)$: Distance de Hamming entre x et y.

$C^{\perp}$: Le code dual du code considéré.

Table des matières

Introduction

Les codes correcteurs d'erreurs sont utilisés pour corriger des erreurs quand les messages sont transmis par le biais d'un canal de communication comportant des parasites. Le transfert de l'information n'est pas parfait, c'est pourquoi il est nécessaire de détecter, et dans certains cas de pouvoir même corriger les erreurs contenues dans le message reçu, les codes cycliques, parmi les codes correcteurs, correspondent à ce besoin. Dans ce mémoire, on s'intéresse à l'étude de codes cycliques sur un corps fini, Ce travail est subdivisé en trois chapitres :

Le premier chapitre est un chapitre d'introduction où nous présentons les notions et les propriétés fondamentales nécessaires pour la réalisation de ce travail tels que : les anneaux, anneaux principaux, anneaux des polynômes, corps finis et construction d'un corps fini. Les notions citées dans ce chapitre représentent l'outil mathématique utilise pour l'étude des codes cycliques.

Le deuxième chapitre regroupe les définitions et les propriétés fondamentales des codes linéaires et des codes cycliques.

La troisième et dernière partie de cet mémoire est consacrée à l'étude de codes cycliques maximaux.

Chapitre 1

Les corps finis

Dans ce chapitre nous rappellons les définitions, et les notions de base, tels que : corps fini, anneaux, extension d'un corps fini et construction d'un corps fini.

1.1 Rappel sur les anneaux

Définition 1.1

Soit un ensemble non vide A, muni de deux lois de composition interne «+»(addition) et «$\cdot$ »(multiplication). On dit que $(A, +, \cdot)$ est un anneaux si selement si :

1. $(A, +)$ soit un groupe commutatif.
2. La loi « $\cdot$ » est associative :

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \text{ pour tout } x, y, z \in A.$$

3. La loi « $\cdot$ » est distributive par rapport à « + » :

$$x \cdot (y + z) = x \cdot y + x \cdot z \; et \; (y + z) \cdot x = y \cdot x + z \cdot x \text{ pour tout } x, y, z \in A.$$

Remarque 1.1

a) si la loi « $\cdot$ » posséde un élément neutre 1_A :

$$\forall x \in A, x \cdot 1_A = 1_A \cdot x = x$$

on dit que l' anneau est unitaire.

b) si la loi «$\cdot$» commutatif :

$$\forall x, \; y \in A, \; x \cdot y = y \cdot x$$

on dit que l' anneau est commutatif.

c) soit $x \in A$ anneau on dit que x est inversible par la loi « $\cdot$ », s'il existe $y \in A$ telles que :

$$x \cdot y = y \cdot x = 1_A.$$

Définition 1.2

Un anneau commutatif A est dit intégre s'il non nul, et si pour tous $a, b \in A$, la condition $a \cdot b = 0_A \Longrightarrow a = 0_A$ ou $b = 0_A$.

1. $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif unitaire de même $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.
2. $2\mathbb{Z} = \{2k \backslash k \in \mathbb{Z}\}$, $(2\mathbb{Z}, +, \cdot)$ anneau commutatif non unitaire.

Idéal d'un anneau

Définition 1.3

Une partie I d'un anneau commutatif A est un idéal de A si elle vérifie :

1. I est un sous-groupe de pour " $+$ ".
2. Pour tout $x \in I$ et $a \in A$, on a $ax \in I$.

Un idéal de A est dit propre s'il est différent de A (c'est- à-dire $I \neq A$).

Idéaux premiers et maximaux

Définition 1.4

Un idéal I de A est dit premier si A/I est intègre. De manière équvalente cela signifi : $A \neq I$, et la condition $a, b \in I \Longrightarrow a \in I$ ou $b \in I$.

Exemple 1.1

1. les idéaux premier de $\mathbb{Z}$ sont $\{0\}$ et les $n\mathbb{Z}$ pour n premier.

Proposition 1.1

A anneau commutatif unitaire intégre, I idéal de A.

$$I \text{ premier} \Longleftrightarrow A/I \text{ intégre.}$$

Définition 1.5

Un idéal I maximal de A un idéal différent de A qui verifie : pour tout $J \subset A$, on a $I \subset J \subset A \Longrightarrow J = I$ ou $J = A$.
Le plus grand idéal dans lequel I peut être inclus strictement est A.

1.2 Anneaux principaux

Définition 1.6

Un anneau commutatif A est dit principal s'il est intègre et si tous idéaux sont la forme $(a) = aA$ avec $a \in A$.

Définition 1.7

Un anneau intégre A est dit euclidien s'il existe une application : $\varphi : A\backslash\{0\} \rightarrow \mathbb{N}$ telle que

$\forall a \in A\backslash\{0\}, b \in A$, il existe uniqe $(q, r) \in A^2$, $b = aq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(a)$.

Exemple 1.2

L'anneau des entier $\mathbb{Z}$ est euclidien pour la valeur absolue.

Théorème 1.1

Tout anneau A euclidien est principal.

Preuve.

Soit A un anneau euclidien et I un idéal de A. Si $I \neq \{0\}$, il exist un élément non nul dans I. On choisit un élément x de I tel que $\varphi(x)$ soit minimal. Alors $I = (x)$. En effet, pour tout $y \in I$, on écrit $y = xq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(x)$. Comme $r = y - xq$, $r \in I$ et par minimalité de $\varphi(r)$, $r = 0$. Donc $y \in (x)$. ■

1.3 Anneau des polynômes

Définition 1.8

Soit A anneau commutatif, une polynôme P est de degré n à cofficients dans A est sous la forme :

$$P(x) = a_0 + a_1 x + ... + a_n x^n,\ a_i \in A,\ n \in \mathbb{N}$$

avec $a_i \in A$ pour tout $i \in \{0, 1, 2, ..., n\}$, $a_n \neq 0$.

- on note $\deg(p)$ le dégré n de p et on appelle a_n le cofficient dominant de p.
- $A[x]$ est l'ensemble des polynômes à cofficients dans A.

Anneau quotient

Définition 1.9

Soit A un anneau commutatif I un idéal de A. Alors l'ensemble quotient A/I muni de l'addition $\oplus$ et la multiplication $\odot$ est un anneau.

Exemple 1.3

Soit $\Bbbk$ un corps commutatif. On disine par $A = \Bbbk[x]$ l'anneau des polynômes à cofficient dans le corps $\Bbbk$, $f(x) \in \Bbbk[x]$ de dégré n,

$I = (f(x)) = \{h(x)f(x)/h(x) \in A\}$ Impliqe $A/I = \Bbbk[x]/(f(x))$ anneau quotient.

1. $\deg(g) < n = \deg(f)$ donc $\overline{g}(x) = g(x) + I \in A/I$.
2. $\deg(g) \geq n$ Par la dévision euclidienne de g par f dans $\Bbbk[x]$, il existe $q(x)$, $r(x) \in \Bbbk[x]$ tel que : $g(x) = q(x) \cdot f(x) + r(x)$ $\deg r < \deg f = n$ dans $\Bbbk[x]/f$

$$\overline{g(x)} = \overline{q(x) \cdot f(x)} + \overline{r(x)} = \overline{0} + \overline{r(x)} = \overline{r(x)}.$$

1.4 Corps finis

Définition 1.10

Un corps est un anneau commutatif unitaire non réduit à $\{0\}$ dans tous les élément non nuls sont inversibles.

Exemples 1.4

1. $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sont des corps commutatifs.
2. $(\mathbb{Z}/p\mathbb{Z})^x = \{\overline{x} \in \mathbb{Z}/p\mathbb{Z} : (x, p) = 1\}$.
   $= \{\overline{1}, \overline{2}, \overline{3}, ..., \overline{p-1}\} = \mathbb{Z}/p\mathbb{Z} - \{0\}$.
   si p premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Définition 1.11

Le corps fini à q éléments et noté $\mathbb{F}_q$ ou $GF(q)$. C'est le corps de Galois d'order q.

Exemple 1.5

Si $p \in \mathbb{N}^*$ est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps finis à p éléments.

Définition 1.12

S étant partie non vide d'un corps $\mathbb{k}$, on appelle sous-corps de $\mathbb{k}$ engedré par S, l'intersection de tous les sous-corps de $\mathbb{k}$ contenant S ; c'est donc le plus petit sous-corps de $\mathbb{k}$ cntenant S.

Théorème 1.2 *(Théorème de Wedderburn)*

Tout corps fini est commutatif.

1.4.1 Caractéristique et cardinal

1. Caractéristique d'un corps

Définition 1.13

Soit $\mathbb{k}$ un corps commutatif. On appelle caractéristique du corps $\mathbb{k}$ le plus petit entier positif non nul vérifant :

$$n \cdot 1_k = 0_k$$

C'est l'order additif de 1 et aussi celui de tout les élément non nul de $\mathbb{k}$

Exemple 1.6

Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des caractéristique 0, si p est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ et de caractéristique p.

Théorème 1.3

La caractéristique d'un corps fini p est forcément un nombre premier.

Preuve.

Si p n'est pas premier alors il existe $i, j \in \mathbb{N}^*$ tel que $p = i \cdot j$.

Mais alors $p \cdot 1 = 0 \Longrightarrow (i \cdot 1)(j \cdot 1) = 0 \Longrightarrow$par intégruté du corps K, on a $i \cdot 1 = 0$ ou $j \cdot 1 = 0$, ce qui contredit la minimalité de p donc p est prmier. ■

Théorème 1.4

Soit $\mathbb{F}_q$ un corps fini de cadinal q. Le groupe multiplicatif $\left(\mathbb{F}_q^*, \cdot\right)$ est un groupe cyclique d'ordre $q - 1$.

2. Cardinal d'un corps finis

Théorème 1.5

Soit $\mathbb{k}$ *un corps fini de caractéristique* p*. Alors il existe* $n \in \mathbb{N}$ *telle que* $card(\mathbb{k}) = p^n$.

Preuve.

$\mathbb{k}$ est un espace vectoriel et possèd un nombre fini d'élément, il possèd une dimestion finie n. Soit $B = (e_1, e_2, ..., e_n)$ une base de $\mathbb{k}$. Tout élément de $\mathbb{k}$ peut donc s'écrire sous la forme d'une unique combinaison linéair de cette famille de vecteurs de $\mathbb{k}$.

soit $k \in \mathbb{k}$. Alors il existe $\lambda_1, \lambda_2, ..., \lambda_n \in \mathbb{F}$ telle que :

$k = \lambda_1 \cdot e_1 + \lambda_2 \cdot e_2 + ... + \lambda_n \cdot e_n$.

k est entiérement déterminé par le choix de ces n coordonnée dans B. Pour chaque λ_i, il ya p possiblités parmi les éléments de $\mathbb{F}$ ce qui nous donne au total p^n possibilités pour k. ■

Corollaire 1.1

Soit K *un corps fini de cardinal* p*. Alors* K *isomorphe à* $\mathbb{F}_p$.

Elément primitif d'un corps fini

Définition 1.14

On appelle un élément primitif de $\mathbb{F}_q$ tout générateur du groupe multiplicatif $\mathbb{F}_q^*$.

Définition 1.15

Un élément α dans un groupe fini $\mathbb{F}_q$ est appelé élément primitif (ou générateur) de $\mathbb{F}_q$ si :

$$\mathbb{F}_q = \left\{0, 1, \alpha, \alpha^2, ..., \alpha^{q-1}\right\}.$$

Proposition 1.2

Si k *est un corps fini de caractéristique* p*, alors* $(a+b)^{p^i} = a^{p^i} + b^{p^i}$ *pour tout* $a, b \in k$ *et* $i \in \mathbb{N}^*$.

Preuve.

On raisonne par récurrence sur i. Si $i = 1$, la formule du binôme de Newton s'écrit$(a+b)^p = \sum_{m=0}^{p} C_p^m a^m b^{p-m}$ et l'on vérifie que tous les coefficients C_p^m sont

divisibles par p dès que $0 < m < p$. En effet, de $p(p-1)...(p-m+1) = m!C_p^m$ on déduit que p divise $m!C_p^m$.

Comme p est premier, il est premier avec tout nombre qu'il ne divise pas, donc en particulier avec chacun des facteurs du produit $m!.p$ est donc premier avec $m!$, et comme il divise le produit $m!C_p^m$, il divisera C_p^m d'après le Théorème de Gauss. On aura donc $(a+b)^p = a^p + b^p$.

Enfin, si la propriété est vraie jusqu'au rang i.

$$(x+y)^{p^{i+1}} = (x+y)^{p^i \cdot p} = \left[(x+y)^{p^i}\right]^p = (x^{p^i}+y^{p^i})^p = (x^{p^i})^p + (y^{p^i})^p = x^{p^{i+1}} + y^{p^{i+1}}.$$

■

Proposition 1.3

Soient $m, n \in \mathbb{N}^*$, p est premier. On a

$$\mathbb{F}_{P^m} \subset \mathbb{F}_{P^n} \Longleftrightarrow m \mid n.$$

Preuve.

L'iclusion $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ entraîne

$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_{q^m}] \cdot [\mathbb{F}_{q^m} : \mathbb{F}_q]$ de sorte que m divise n.

Réciproquement , si $m \mid n$ si K désigne une clôture algébrique de $\mathbb{F}_{q^n}$, donne $\mathbb{F}_{q^s} = \left\{x \in K \ / \ x^{q^s} - x = 0\right\}$, et l'on peut écrire

$m \mid n \Longrightarrow q^m - 1 \mid q^n - 1$

$\Longrightarrow (x^{q^m-1} - 1) \mid (x^{q^n-1} - 1)$

Le polynôme $x^{q^m} - x$ divisera $x^{q^n} - x$ et l'on aura

$\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$.

Exemple 1.7

Le sous-corps de $\mathbb{F}_{2^{24}}$ sont les sous-corps $\mathbb{F}_{2^k}$ tels que $k/24$.

■

Les diviseurs de 24 sont $1, 2, 3, 4, 6, 8, 12, 24$.

Alors les sous corps de $\mathbb{F}_{2^{24}}$ sont $\mathbb{F}_2$,$\mathbb{F}_{2^2}$,$\mathbb{F}_{2^3}$,$\mathbb{F}_{2^4}$,$\mathbb{F}_{2^6}$,$\mathbb{F}_{2^{12}}$, $\mathbb{F}_{2^{24}}$.

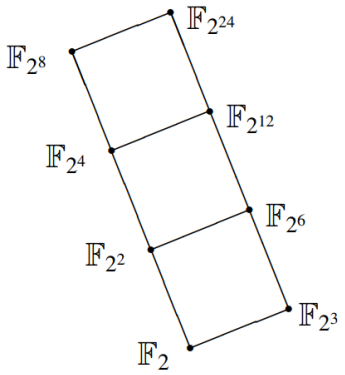

Figure 1.1

Corollaire 1.2

1. Tout extension fini d'un corps fini $\mathbb{F}_q$ est un extension simple, i.e. de la forme $\mathbb{F}_q(\alpha)$.
2. Pour tout entier $n \geq 1$ il existe au moins un Polynôme irréductible de degré n dans $\mathbb{F}_q[x]$.

1.4.2 Polynômes irréductibles sur un corps fini

Définition 1.16

Soit P un polynôme est irréductible dans $K[x]$ s'il non-contants (non inversible) et si ses selus diviseurs sont les inversibles $K[x]$ c'est -à-dire les polynômes constants non nuls et les polynômes qui lui sont associté c'est -à-dire les polynômes de la forme λP, $\lambda \in K^*$.
Auterment dit, on peut pas écrire P sous la forme d'un produit de deux polynômes Q et R de degré suprérieur ou égal à 1.

Exemple 1.8

$P(x) = x^2 + 1 = (x - i)(x + i)$ n'est pas irréductible dans $\mathbb{C}[x]$.

Proposition 1.4

Soit $p \in K[x]$ et de degré égal à 2 ou 3.
On a l'équvalonce : P irréduclible sur $K[x] \iff P$ n'a pas de racines dans K.

Corollaire 1.3

Tout extension simple algébrique dans corps K est isomorphe à un corps de la forme $K[x]/p(x)$, ou $p(x)$ est un polynôme unitaire et irréductible de $K[x]$.

Soit l'anneau $\mathbb{Z}/2\mathbb{Z}[x]$ des polynômes des cofficioents dans $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.
Pour tester l'irréductibilité des polynômes de degré 2, il suffit de chercher les éventuelles racines.
Si $P(x) = x^2 + 1 \in \mathbb{Z}/2\mathbb{Z}[x] \Longrightarrow P(1) = 1 + 1 = 0$ et $P(0) = 0 + 1 = 1 \Longrightarrow p$ admet une racine $\Longrightarrow$il n'et pas irréductible.
Si $P(x) = x^2 + x + 1 \in \mathbb{Z}/2\mathbb{Z}[x] \Longrightarrow P(1) = 1 + 1 + 1 = 1$ et $P(0) = 0 + 0 + 1 = 1 \Longrightarrow p$ sans racine $\Longrightarrow$il et irréductible.

1.5 Extension d'un corps fini

Définition 1.17

Soient L et $\Bbbk$ deux corps, on appelle L extension de $\Bbbk$ si L contient un sous-corps isomorphe à $\Bbbk$. i.e. $\Bbbk \subset L$.

Tout corps de caractéristique 0 est une extension des corps $\mathbb{Q}$. en particulier, les inclusion $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ montrent que $\mathbb{R}$ et $\mathbb{C}$ sont des extensions de $\mathbb{Q}$ et que $\mathbb{C}$ est extension de $\mathbb{R}$.
Tout corps de caractéristique $p \neq 0$ est extension du corps $\mathbb{Z}/p\mathbb{Z}$.

Définition 1.18

Tout corps $\Bbbk$ contenant le corps $\mathbb{F}$ s'appelle extension de $\mathbb{F}$. $\Bbbk$ est un espace vectoriel sur $\mathbb{F}$ et on a sa dimension $[\Bbbk : \mathbb{F}]$.

Théorème 1.6

Le sous-corps premier d'un corps quelconque est isomorphe soit à $\mathbb{Q}$, soit à un corps du type $\mathbb{Z}/p\mathbb{Z}$.

Lemme 1.1

Soit K l'extention finie de corps $\mathbb{F}$, avec $d = [K : \mathbb{F}]$. Alors $|K| = |\mathbb{F}|^d$.

Preuve.

Soit $\{\alpha_1, \alpha_2, ..., \alpha_d\}$ une base de K sur $\mathbb{F}$. Alors chaque élément de K à une représentation unique de la forme

$$a_1\alpha_1 + a_2\alpha_2 + ... + a_d\alpha_d \text{ avec } \alpha_i \in \mathbb{F}$$

■

Comme $a_i \in \mathbb{F}$, il y a $|\mathbb{F}|$ possibilités pour le coefficient de cach a_j $(j = 1, 2, ..., d)$, et puisque chaque possibilité donne lieu à un élément différent de K, on en déduit que

$$|K| = |\mathbb{F}|^d .$$

Extension algébrique

Définition 1.19

Soit L une extension du corps $\Bbbk$, et soit α un élément de L. On dit que α est algébrique sur $\Bbbk$ s'il existe un polynôme non nul $p \in K[x]$ tel que $P(\alpha) = 0$.
L'extension L de $\Bbbk$ est dit algébrique si tout élément α de L sont algébrique sur $\Bbbk$.

1. Le corps $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$.
2. Le réel$\sqrt{2}$ est algébrique sur $\mathbb{Q}$.

Extension simple

Définition 1.20

Soit E une extension du corps $\mathbb{F}$ et soit $\alpha \in E$ alors $\mathbb{F}(\alpha)$ est défini comme étant le plus petit corps contenant $\mathbb{F}$ et α. Tout corps de la forme est un extension de $\mathbb{F}$.

Extension par adjonction

Le fait qu'un corps L est extension d'un corps de K se traduit symboliquement par la formule $L : K$.

Définition 1.21

Soit $L : K$ une extension de corps. On suppose $K \subseteq L$; alors pour toute partie non vide T de L, le sous corps de L engendré par $K \cup T$ est noté $K(T)$ et appelé extension de K obtenue par l'adjonction de T à K.

Extension finie

Définition 1.22

Une extension E de $\mathbb{F}$. Le degré de l'extension E est la dimension de E en tant que $\mathbb{F}$ espace vectoriel. On le note $[E : \mathbb{F}]$, on dit que l'extension est finie si $[E : \mathbb{F}]$ est finie.

Exemple 1.9

$\mathbb{R} \subset \mathbb{C}, \mathbb{C}$ extension finie de $\mathbb{R}$, $[\mathbb{C} : \mathbb{R}] = 2$.

1.6 Corps de décomposition

Théorème 1.7

Soit $f(x)$ un polynôme non constant de $K[x]$; alors il existe une extension E de K telle que

1. $K \subseteq E$ et $f(x)$ est scindé sur E.
2. $(K \subseteq E' \subseteq E$ et est scindé sur $E') \Longrightarrow E' = E$.

Proposition 1.5

Soit E un corps de décomposition d'un polynôme $f(x)$ non constant de $K[x]$; si $n = \deg f > 0$ et $\alpha_1, ..., \alpha_n$ sont les racines distinctes ou confendus de f dans E, alors

$$\mathbb{E} = K(\alpha_1, ..., \alpha_n)$$

donc E est une extension algébrique de degré fini sur K.

1.7 Construction d'un corps fini

On va montrer que pour tout nombre premier p et m un entier strictement positive on peut construir un corps de cardinal p^m.

Soit $\mathbb{F}$ un corps alors $\mathbb{F}[x]$ est un anneau principal. C-à-d pour tout idéal I dans $\mathbb{F}_q[x]$ on a $I = (p(x))$ ou $p(x)$ est un polynôme non nul de plus petit degré dans I.

Soit $p(x) \in \mathbb{F}_q[x]$, l'idéal engendré par $p(x)$ est

$$(p(x)) = \{p(x)g(x) : g(x) \in \mathbb{F}_q[x]\}$$

et l'anneau quotient $\mathbb{F}[x]/(p(x))$ est

$$\mathbb{F}[x]/(p(x)) = \{f(x) + I : f(x) \in \mathbb{F}[x]\}$$

on note $f(x) + I$ par $\overline{f(x)}$ ainsi $\overline{p(x)} = \overline{0}$ cet anneau est muni des opération :
L'addition : $\overline{f(x)} + \overline{g(x)} = \overline{f(x) + g(x)}$.
La multiplication : $\overline{f(x) \cdot g(x)} = \overline{f(x)} \cdot \overline{g(x)}$.

Théorème 1.8

Soit $\mathbb{F}$ un corps et soit $p(x)$ un polynôme irréductible non constant dans $\mathbb{F}[x]$. Alors il existe une extension E de $\mathbb{F}$ et un élément $\alpha \in E$ tel que $p(\alpha) = 0$.

Preuve.

Nous souhaitons trouver une extension E de $\mathbb{F}$ conteneant un élément α tel que $p(\alpha) = 0$. l'idéail $(p(x))$ engendré par $p(x)$ est un idéail maximal dans $\mathbb{F}_q[x]$, alors $\mathbb{F}[x]/(p(x))$ est un corps.
Nous prétendons que $E = \mathbb{F}[x]/(p(x))$ est le corps désiré.
Nous montrons tout d'abord que E est une extension de $\mathbb{F}$.
Nous posons définir un hommorphisme d'anneaux commutatifs par l'application

$$\Psi : \mathbb{F} \longrightarrow \mathbb{F}[x]/(p(x))$$

$$\Psi(a) = a + (p(x)) \text{ pour } a \in \mathbb{F}$$

il est facile de vérifie qu'il s'agit d'un hommorphisme d'anneaux on a :

$$\Psi(a) + \Psi(b) = (a + p(x)) + (b + p(x)) \Longrightarrow (a + b) + p(x) = \Psi(a + b)$$

et

$$\Psi(a)\Psi(b) = (a + p(x))(b + p(x)) = ab + p(x) = \Psi(ab)$$

l'appliction Ψ est injective car :

$$\Psi(a) = \Psi(b) \Longrightarrow a + (p(x)) = b + (p(x)) \Longrightarrow a - b \text{ multiple de } p(x)$$

puisque le polynôme $p(x)$ non constant, la seule possibilité $a - b = 0$ alors $a = b$.
Nous pousons identifie $\mathbb{F}$ avec le sous-corps $\{a + (p(x)) : a \in \mathbb{F}\}$ de E. E une extn-sion de $\mathbb{F}$.
Il nous reste à prouver que $p(x)$ à un zero $\alpha \in E$.
On pose $\alpha = x + (p(x))$ alors dans E.
Si $p(x) = a_0 + a_1x + ... + a_nx^n$ alors

$$\begin{aligned} p(\alpha) &= a_0 + a_1(x + p(x)) + ... + a_n(x + (p(x))^n \\ &= a_0 + a_1x + ... + a_nx^n + (p(x)) = 0 + (p(x)) \end{aligned}$$

par conséquent, nous avons trouvé un élément $\alpha \in E = \mathbb{F}[x]/(p(x))$ tel que $p(\alpha) = 0$. ■

Exemple 1.10

Construire $\mathbb{F}_9$ (corps fini à 9 éléments)

Dans $\mathbb{F}_3$, le polynôme $p(x) = x^2 + x + 2$ est irréductible sur $\mathbb{F}_3[x]$, on détermine les éléments de $\mathbb{F}_{3^2}$ en le regardat comme extension et obtenue par adjonction à $\mathbb{F}_3$ d'une racine de $p(x)$, ainsi $\mathbb{F}_{3^2} = \mathbb{F}_3[x]/(p(x))$, soit α une racine de $p(x)$, alors $\{1, \alpha\}$ est une base de $\mathbb{F}_{3^2}$.
(Représentaion polynômiale) :

Tout polynôme de corps $\mathbb{F}_3[x]/(p(x))$ peut-être modulo $p(x)$ en utilisant le fait que :

$$p(\alpha) = 0$$

Dans $\mathbb{F}_3$, c-à-d que : $\alpha^2 + \alpha + 2 = 0$ et on aura :

$$\begin{aligned} \mathbb{F}_{3^2} &= \mathbb{F}_3[x]/(p(x)) \\ &= \left\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\right\} \end{aligned}$$

	comme un polynôme	comme une puissance de α
00	0	0
10	1	1
01	α	α
12	$1 + 2\alpha$	α^2
22	$2 + 2\alpha$	α^3
20	2	α^4
02	2α	α^5
21	$2 + \alpha$	α^6
11	$1 + \alpha$	α^7

avec $\alpha^2 + \alpha + 2 = 0$ et $\alpha^8 = 1$.

Chapitre 2

Les codes linéaires et les codes cycliques

Dans ce chapitre on va présenter , queleques notions sur la théorie des codes. On donner la définition des codes (les codes linéaires et aussi les codes cycliques).

2.1 Les codes

Définition 2.1

Soit $\mathbb{F}$ (un alphabet)de cardinal fini q. Un code C de longueur n sur $\mathbb{F}$ est un sous ensemble de $\mathbb{F}^n$. On appelle mot de code tout élément du code C et on appelle taille M du code son cardinal.

1. Le code $C = \{011010, 111011, 111111, 110000, 011100\}$ est un code de longueur 6 sur l'aphabte $A = \{0, 1\}$.
2. $C = \{aabb, mmmm, accc, zzkk\}$ est un code de longueur 4 et de cardinal 4 sur l'aphabte de la language française.

Distance de Hamming

Définition 2.2

Soit $\mathbb{F}_q^n$ l'éspace vectoriel de dimension n sur $\mathbb{F}_q$ (l'ensemble des mots de longueur n sur $\mathbb{F}_q$), $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ et $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$.

La distance de Hamming entre x et y est

$$d(x,y) = |\{i : 0 \leqslant i \leqslant n-1 \ , x_i \neq y_i\}| .$$

i) Soit $A = \{0,1\}$ et $x = 01010$, $y = 01101$, $z = 11101$.
$d(x,y) = d(01010, 01101) = 3, d(y,z) = d(01101, 11101) = 1$ et $d(11101, 01010)$.

ii) Dans $\mathbb{F}_3^4$, $d(aabe, abca) = 3$.

Proposition 2.1

Soit x, y, z des mots de longueur n sur $\mathbb{F}_q^n$. On a alors :

1. $0 \leq d(y,x) \leq n$.
2. $d(x,y) = 0$ si et seulement si $x = y$.
3. $d(x,y) = d(y,x)$.
4. $d(x,y) \leq d(x,z) + d(z,y)$ (inégalité triangulaire).

Distance minimale d'un code

Définition 2.3

On appelle distance minimale d'un code C sur $\mathbb{F}_q$, l'entier

$$d = \min\{d(x,y)/x, y \in C \text{ et } x \neq y\}$$

On appelle poids minimale d'un code C, l'entier $\min\{\omega_H(x), x \in C \text{ et } x \neq 0\}$.
Par exemple
$C = \{001, 111, 101\} \subset \mathbb{F}_2^3$, $d(c) = 1$.

Le poids de Hamming

Définition 2.4

Le poids de Hamming $\omega(x)$ d'un élément $x \in \mathbb{F}_q^n$ et défini par

$$\omega(x) = |\{i \ / \ x_i \neq 0\}|$$

1. Dans $\mathbb{F}_2, n = 4, \omega(1101) = 3$ et $\omega(1100) = 2$.

2. Dans $\mathbb{F}_3, n = 6, \omega(000120) = 2$.

2.2 Codes linéaires

Définition 2.5

On appelle code linéaire de longueur n sur $\mathbb{F}_q$ tout $\mathbb{F}_q$ sous espace vectoriel de $\mathbb{F}_q^n$.

Remarque 2.1

1. Pour un code linéaire le poids minimal est égale à la distance minimale.
2. Si C est un code linéaire, il a un dimension que l'on note k. Si sa distance minimale est d on note ses paramètre $[n, k, d]$.

Matrice génératrice et matrice de parité

Soit un $[n, k]$-code sur $\mathbb{F}_q$. Comme C est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension k, on peut le représenter par une de ses $\mathbb{F}_q$-base $(c_1, ..., c_k)$.

Définition 2.6

Soit C un $[n, k]$-code sur $\mathbb{F}_q$. Soit $(c_1, ..., c_k)$ une base de C. Alors la matrice

$$G = \begin{pmatrix} c_1 \\ c_2 \\ . \\ . \\ . \\ c_k \end{pmatrix}$$

est appelée une matrice génératrice de C.

Exemple 2.1

Soit G la matrice génératrice du $[3, 2]$ code binaire C telle que :

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

Alors

$$\begin{aligned} C &= \{c_1(1,0,0) + c_2(0,1,0) / c_1, c_2 \in \mathbb{F}_2\} \\ C &= \{000, 100, 010, 110\} \end{aligned}$$

Ainsi le code C est de paramètre $[3,2,1]$ et $|C| = q^k = 2^2 = 4$, par exemple le message 11 est codé par $c = 11G = 110$.

Proposition 2.2

Soit G une matrice génératrice d'un code C. On dit qu'elle génére C, ca en effet, tout mot de code $c \in C$ est obtenu par multiplication à gauche de G par un vecteur $\mathbb{F}_q^k$.

$$\text{pour tout } c \in C, \text{ il existe } m \in \mathbb{F}_q^k \text{ tel que } mG = c$$

Du fait qu'un code est un sous-espace vectoriel, on peut effectuer n'mporte quelle opération inversible sur les linges de G, la matrice résultante sera toujours une matrice génératrice.

Proposition 2.3

Soit G une matrice génératrice de C. Soit $S \in M_{k,n-k}(\mathbb{F}_q)$ une matrice inversible. Alors $G' = SG$ est toujours une matrice génératrice de C.

Code dual

La contrainte de la linéarité sur le code donne naturellement naissance à la notion de code dual d'un code linéaire. Puisque C est un espace vectoriel, on peut considérer l'ensemble des formes qui s'annulent sur C. Cet ensemble est un espace vectoriel que l'on appelle code dual de C.

Définition 2.7

soient $c = (c_1, ..., c_n)$ et $d = (d_1, ..., d_n)$ des vecteur de $\mathbb{F}_q^n$. On appelle le produit scalaire entre c et d la quantité

$$\langle c, d \rangle = \sum_{i=0}^{n} c_i d_i$$

Remarquons que le terme de produit sclaire est en fait un abus de langage (cette application bilinéaire n'est pas définie positive).

Définition 2.8

Soit C un $[n,k]$-code sur $\mathbb{F}_q$. On définit son code dual noté $C^\perp$par

$$C^\perp = \left\{ d \in \mathbb{F}_q^n \text{ pour tout } c \in C,\ \langle c, d\rangle = 0 \right\}$$

Exemple 2.2

Le code dual du code $C = \{0000, 1111\}$ est :

$C^\perp = \{0000, 1100, 1001, 0110, 0101, 0011, 1111\}$.

Matrice de parité

Définition 2.9

Soit C un $[n,k]$-code sur $\mathbb{F}_q$. On appelle matrice de parité de C toute matrice génératrice H de son code dual $C^\perp$. On a donc

$$\text{pour tout } c \in C, \quad H^t \cdot c = 0$$

Ainsi, si G est une matrice génératrice de C, on a

$$G^t \cdot H = 0$$

Exemple 2.3

Sopposon $q = 2$, $n = 5$, $k = 2$ donc $M = 2^2 = 4$, soit C le code de paramétres $[5, 2]$ donné par la de contrôle

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

$$\begin{aligned} c &= (c_1, c_2, c_3, c_4, c_5) \in C \Leftrightarrow H^t c = 0 \\ &\Leftrightarrow \begin{cases} c_1 + c_2 = 0 \\ c_1 + c_3 + c_4 = 0 \\ c_1 + c_3 c_1 + c_3 c_5 = 0 \end{cases} \Leftrightarrow \begin{cases} c_2 = -c_1 \\ c_4 = -c_3 - c_1 = c_1 + c_3 \\ c_5 = -c_3 - c_1 = c_4 \end{cases} \end{aligned}$$

$$\begin{aligned} c &\in C \Leftrightarrow c = (c_1, c_1, c_3, c_1 + c_3, c_1 + c_3) \\ &\Leftrightarrow c = c_1(1,1,0,1,1) + c_3(0,0,1,1,1) \end{aligned}$$

Le code C contient 2^2 mots de code :
$\{00000, 11011, 00111, 11100\}$.

2.3 Codes cycliques

Définition 2.10

Un code linéaire C de longueur n sur un corps fini $\mathbb{F}_q$ est cyclique si pour tout mot de code $c = (c_0, c_1,..., c_{n-2}, c_{n-1})$ de C, $(c_{n-1}, c_0, c_1,..., c_{n-2})$ appartient aussi à C.
L'espace $\mathbb{F}_q^n$ peut être identifie à l'algèbre quotient de polynômes $R_n = \mathbb{F}[x]/(x^n-1)$ comme suit : à chaque vecteur $c = (c_0, c_1,..., c_{n-1})$ de $\mathbb{F}_q^n$ corespond $c(x) = \sum_{i=0}^{n-1} c_i x^i$.

1. Le code linéaire
$$C = \{000, 001, 100, 010\}$$
est un code cyclique car $100 \in C \Rightarrow 010 \in C$, $010 \in C \Rightarrow 001 \in C$ et $001 \in C \Rightarrow 100 \in C$. La représentation polynomiale de 100 est x.
2. Le code linéaire $C = \{10010, 11001, 11101, 00000\}$ n'est pas code cyclique car $10010 \in C$ mais $01001 \notin C$.

Théorème 2.1

Le code linéaire C est cyclique si et seulement si C est un idéal de $R_n = \mathbb{F}[x]/(x^n - 1)$.

Théorème 2.2

SoitC_1 et C_2 des codes cycliques avec des polynômes générateurs $g_1(x)$ et $g_2(x)$. Alors $C_1 \subseteq C_2$ si et selement si $g_2(x)$ divise $g_1(x)$.

Preuve.

Cela suit depuis $C_1 \subseteq C_2$ si et selement si $\langle g_1(x)\rangle \subseteq \langle g_2(x)\rangle$ si et selement si $g_2(x)$ divise $g_1(x)$. ■

Théorème 2.3

Soit $g(x) = g_0 + g_1x + g_2x^2 + \ldots + g_{n-k}x^{n-k}$ le polynôme générateur d'un code cyclique C dans $\mathbb{F}_q^n$ avec $\deg g(x) = n - k$. Puis la matrice

Théorème 2.4

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} = \begin{pmatrix} g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & \ldots & 0 \\ 0 & g_0 & \ldots & \ldots & g_{n-k} & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & & g_0 & g_1 & \ldots & g_{n-k} & 0 \\ 0 & \ldots & 0 & & g_0 & g_1 & \ldots & g_{n-k} \end{pmatrix}$$

Est une matrice génératrice de C (notez que nous identifions un vecteur avec un polynôme).

Preuve.

Il suffit de montrer que $g(x), xg(x), ..., x^{k-1}g(x)$ forment une base de C . Il est clair qu'ils sont linéairement indépendants sur $\mathbb{F}_q$, nous savons que $\dim(C) = k$. ■

Exemple 2.4

Considérons le code binaire$[7, 4]$-cyclique avec le polynôme générateur $g(x) = 1 + x^2 + x^3$. Alors ce code a une matrice génératrice

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Code engendré par le polynôme de contrôle

Définition 2.11

Soit C un code cyclique de polynôme générateur $g(x)$. Le polynôme de contrôle de C, est définie par $h(x) = \frac{x^n-1}{g(x)}$.

Proposition 2.4

Soit C un code cyclique dans R_n

1. Le polynôme générateur unique .
2. Tout mot d'un code cyclique est un multiple du polynôme générateur. On a $C = \langle g \rangle$.
3. Le polynôme générateur divise $x^n - 1$.

Preuve.

1. supposons que g_1 et g_2 deux polynômes générateur. Alors $g_1 - g_2$ est un polynôme générateur de degré strictement inférieur au degré de g_i .
2. Soit $c(x) \in C$ on effectue la division euclidienne de c par $g : c = ag + r$ avec $\deg(r) < \deg(g)$. Or, le rest r qui est la différence de deux mots du code appartient au code.Si $r \neq 0$, on contredit l'hypothese sur le degré minimum de g.
3. On a $x^n-1 = ag+r$ avec $\deg(r) < \deg(g)$ et on conclut comme précédemment qui r doit être nul.

■

Théorème 2.5

Soit $h(x)$ le polynôme de contrôle d'un code cyclique C dans R_n.

a) *Le code C peut être d'ecrire par :*

$$C = \{p(x) \in R_n \ / \ p(x)h(x) = 0\}$$

b) *Si $h(x) = h_0 + h_1x + \ldots + h_{n-r}x^{n-r}$, alors la matrice de contrôle de parité de code C est donnée par*

$$H = \begin{bmatrix} h_{n-r} & \ldots & & \ldots & h_0 & 0 & \ldots & \ldots & 0 \\ 0 & h_{n-r} & \ldots & \ldots & \ldots & h_0 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & h_{n-r} & \ldots & & \ldots & h_0 & 0 \\ 0 & \ldots & \ldots & 0 & h_{n-r} & \ldots & & \ldots & h_0 \end{bmatrix}$$

Exemple 2.5

Considérons le code binaire $C(7,4)$ généré par $g(x) = 1 + x + x^3$ sa matrice génératrice est composée à partir du polynôme générateur

$$g(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_r x^r$$

est

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & g_3 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & g_3 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 \end{pmatrix}$$

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

Calculer la matrice de contrôle à partir de la matrice génératrice n'est pas en généralaisé, par contre, on peut facilement trouver le polynôme de contrôle $h(x)$ qui est telque :

$$h(x)g(x) = 0$$

et donc

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

et la matrice de contrôle correspondant est

$$\begin{aligned} H &= \begin{pmatrix} h_4 & h_3 & h_2 & h_1 & h_0 & 0 & 0 \\ 0 & h_4 & h_3 & h_2 & h_1 & h_0 & 0 \\ 0 & 0 & h_4 & h_3 & h_2 & h_1 & h_0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \end{aligned}$$

Pour encoder 0111 en utilisant le produit polynomial, on doit multiplier le polynôme $m(x) = x^3 + x^2 + x$ correspondant par $g(x) = 1 + x + x^3$.

On obtient

$$\begin{aligned} c(x) &= m(x)g(x) = \left(x^3 + x^2 + x\right)\left(1 + x + x^3\right) \\ &= x^6 + x^5 + x \\ &= c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0 \end{aligned}$$

Qui correspondant au mot code $c_0c_1c_2c_3c_4c_5c_6 = 0100011$.

2.4 Construction d'un code cyclique

Pour construire un code cyclique de longueur n, il est utile de connaître la décomposition de $x^n - 1$ en polynômes irréductibles sur le corps de base $\mathbb{F}$:

$$x^n - 1 = \prod_i f_i(x).$$

En l'absence d'un logiciel (maple, magma,...), on peut déterminer les classes cyclotomiques modulo n. Le nombre de classes donne le nombre de facteurs irréductibles. La donnée d'un polynôme irréductible diviseur de $x^n - 1$ permet alors de connaître tous les autres facteurs. Le polynôme générateur du code est un produit d'un certain nombre de facteurs trouvés.

Exemple 2.6

Considérons les codes binaires de longueur 7 sur $\mathbb{F}_2$. Nous avons alors la factorisatin en facteurs irréductibles suivante :

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(\ x^3 + x^2 + 1)$$

Comme il y a 3 facteurs irréductibles, il y a $2^3 = 8$ codes cycliques.
Ainis les 8 polynômes générateur sont :

(1) $1 = 1$

(2) $x + 1 = x + 1$

(3) $x^3 + x + 1 = x^3 + x + 1$

(4) $x^3 + x^2 + 1 = x^3 + x^2 + 1$

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

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

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

(8)$(x+1)(x^3+x+1)(x^3+x^2+1) = x^7+1$.

Chapitre 3

Les codes cycliques maximaux

3.1 Décomposition de $x^n - 1$ sur un corps fini $\mathbb{F}_q$

Polynôme minimal

Dans toute cette section q sera une puissance d'un nombre premier p, m et n seront deux entiers positifs non nuls, n sera premier avec q.

Définition 3.1

Soit $\alpha \in \mathbb{F}_{q^m}$, Le polynôme minimal de α sur $\mathbb{F}_q$ est le polynôme unitaire de plus bas degré $f(x) \in \mathbb{F}_q[x]$ vérifiant $f(\alpha) = 0$. Nous le notons $M_\alpha(x)$.

Proposition 3.1

Soit $\alpha \in \mathbb{F}_{q^m}$ Soit d un entier positif non nul. Le degré $M_\alpha(x)$ du polynôme minimal $M_\alpha(x)$ sur $\mathbb{F}_q$ est égal à d si et seulement si d est le plus petit entier positif non nul tel que $\alpha^{q^d} = \alpha$.

Rappelons que l'ordre de α (dans le groupe multiplicatif $\mathbb{F}_{q^m}^*$) est le plus petit entier positif non nul l tel que $\alpha^l = 1$.

Lemme 3.1

Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α. Soit d un entier positif non nul. Alors d est le plus petit entier positif non nul tel que $\alpha^{q^d} = \alpha$ si et seulement si $d = ord_l(q)$.

Preuve.

Notons $r = ord_l(q)$. D'aprés la définition de l'ordre de q modulo l, nous avons $l \mid q^r - 1$. Mais $\alpha^l = 1$, donc $\alpha^{q^r - 1} = 1$ et $\alpha^{q^d} = \alpha$. Et r est le plus petit entier positif non nul avec cette propriété, compte tenu de la même définition. Donc r est

égal à d si et seulement si d est le plus petit entier positif non nul tel que $\alpha^{q^d} = \alpha$.

■

Corollaire 3.1

Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α Alors

$$\deg M_\alpha(x) = ord_l(q).$$

Preuve.

C'est une conséquence directe de la proposition et du lemme précédent. ■

Proposition 3.2

Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α alors

$$M_\alpha(x) = \prod_{i=0}^{ord_l(q)-1} \left(x - \alpha^{q^i}\right)$$

c'est-à-dire $\left\{\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots, \alpha^{q^{ord_l(q)-1}}\right\}$ est l'ensemble des racines de $M_\alpha(x)$.

Remarque 3.1

La proposition et la corollaire précédent nous montrent que

$$\alpha^{q^{ord_l(q)}} = \alpha.$$

Proposition 3.3

Soit $\alpha \in \mathbb{F}_{q^m}$. Toutes les racines de $M_\alpha(x)$ sont de même ordre.

Conjugaison

Définition 3.2

La conjugaison dans $\mathbb{F}_{q^m}$ est la relation R définie par

$$\alpha R \beta \text{ si } M_\alpha(x) = M_\beta(x).$$

Proposition 3.4

La conjugaison dans $\mathbb{F}_{q^m}$ est une relation d'equivalence.

Définition 3.3

Les conjugués d'un élément α de $\mathbb{F}_{q^m}$ sont les éléments de la classe d'equivalence de α pour la conjugaison dans $\mathbb{F}_{q^m}$.

Proposition 3.5

Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α. Les conjugués de α sont

$$\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots, \alpha^{q^{ord_l(q)-1}}.$$

Ils sont distincts deux à deux.

Preuve.

C'est une conséquence directe de la définition précédent et de la proposition dans polynôme minimal. ■

Remarque 3.2

En résumé, tous les éléments de $\mathbb{F}_{q^m}$ sont divisés en classes d'équivalence pour la conjugaison. Une classe déquivalence est composée de toutes les racines d'un polynôme minimal sur $\mathbb{F}_q$ Donc :

- il y a autant des classes d'équivalence que de polynômes minimaux différents des éléments de $\mathbb{F}_{q^m}$.
- le cardinal de toute classe est égal au degré du polynôme minimal correspondant.

Racines de l'unité

Rappelons que $(n, q) = 1$. Soit m un entier positif non nul tel que $n \mid q^m - 1$.

Définition 3.4

On appelle racine n-ièmes de l'unité sur $\mathbb{F}_q$, un élément de $\mathbb{F}_{q^m}$ dont l'ordre divise n, on appelle racine n-ièmes primitive de l'unité sur $\mathbb{F}_q$, un élément de $\mathbb{F}_{q^m}$ d'ordre n.

En particulier si $n = q^m - 1$, une racine primitive n-ièmes de l'unité sur $\mathbb{F}_q$ est un élément primitif de $\mathbb{F}_{q^m}$.

Les racines n-ièmes de l'unité sur $\mathbb{F}_q$ forment un sous groupe du groupe multiplicatif $\mathbb{F}_{q^m}^*$. En effet, si β et γ sont deux racines n-ièmes de l'unité sur $\mathbb{F}_q$, $(\beta\gamma)^n = \beta^n\gamma^n = 1$ et donc $\beta\gamma$ est aussi une racine n-ièmes de l'unité sur $\mathbb{F}_q$. D'ailleurs, $\left(\beta^{-1}\right)^n = (\beta^n)^{-1} = 1$. Donc les racines n-ièmes de l'unité sur $\mathbb{F}_q$ forment un sous groupe de $\mathbb{F}_{q^m}^*$. Comme $\mathbb{F}_{q^m}^*$ est cyclique, ce sous groupe est aussi cyclique.

Soit u l'entier tel que $n = q^m - 1$. Soit α un élément primitif de $\mathbb{F}_{q^m}$. Alors β est une racine n-ièmes primitive de l'unité sur $\mathbb{F}_q$, car l'ordre de α^u est égal à $\frac{q^m-1}{(q^m-1,u)} = \frac{q^m-1}{u} = n$. Donc β est un générateur de ce sous-groupe qui est dordre n.

Ce sous-groupe est composé de toutes les racines de X^n-1, i.e. la décomposition de $X^n - 1$ sur $\mathbb{F}_{q^m}$ est

$$X^n - 1 = \prod_{i=0}^{n-1} \left(X - \beta^i\right).$$

Soit γ une racine n-ièmes de l'unité sur $\mathbb{F}_q$. Ses conjugués dans $\mathbb{F}_{q^m}$ sont les puissances de γ, donc ils sont aussi des racines n-ièmes de l'unité sur $\mathbb{F}_q$. La conjugaison dans $\mathbb{F}_{q^m}$ définit donc une relation d'équivalence dans l'ensemble des racines n-ièmes de l'unité sur $\mathbb{F}_q$. On peut alors dire les mêmes choses comme dans la remarque précédent chaque classe d'équivalence est composée de toutes les racines d'un polynôme minimal, et

- il y a autant des classes d'équivalence que de polynômes minimaux différents des racines n-ièmes de l'unité sur $\mathbb{F}_q$.
- le cardinal de toute classe est égal au degré du polynôme minimal correspondant.

Nous obtenons aussi que

$$X^n - 1 = \prod_{\gamma} M_\gamma(X)$$

où γ parcourt un ensemble de représentants des classes d'équivalence, et compte tenu de la proposition dans la partie polynôme minimal, que le polynôme minimal de $\gamma = \beta^j$, $j \in \mathbb{Z}_n$, est égal à

$$M_\gamma(X) = \prod_{i=0}^{ord_l(q)-1} \left(X - \gamma^{q^i}\right) = \prod_{i=0}^{ord_l(q)-1} \left(X - \beta^{jq^i}\right)$$

où l est l'ordre de γ, $l = \frac{n}{(n,j)}$.

Cas général Prenons maintenant le cas général ou n et q ne sont pas forcément premiers entre eux. Soit $n = rp^s$, ou r est premier avec p et $s \geq 0$ (p^s est la plus grande puissance de p qui divise n). Alors

$$X^n - 1 = X^{rp^s} - 1 = (X^r - 1)^{p^s},$$

car nous travaillons sur le corps $\mathbb{F}_q$ de caractéristique p.

Puisque r est premier avec p, nous pouvons décomposer $x^r - 1$ comme ci-dessus, et en déduire la décomposition de $x^n - 1$. Plus précisément, si β est une racine r-ième primitive de l'unité sur $\mathbb{F}_q$, alors

$$X^r - 1 = \prod_{i=0}^{r-1} \left(X - \beta^i\right)$$

et donc

$$X^n - 1 = (X^r - 1)^{p^s} = \left(\prod_{i=0}^{r-1} \left(X - \beta^i\right)\right)^{p^s} = \prod_{i=0}^{r-1} \left(X - \beta^i\right)^{p^s}$$

De même,

$$x^n - 1 = (x^r - 1)^{p^s} = \left(\prod_{\gamma} M_\gamma(x)\right)^{p^s} = \prod_{\gamma} M_\gamma(x)^{p^s}.$$

où γ parcourt un ensemble de représentants des classes d'équivalence par conjugaison des racines r-ièmes de l'unité sur $\mathbb{F}_q$.

Classes cyclotomiques

Définition 3.5

Pour tout entier j, $j \in \mathbb{Z}n$, nous définissons la classe cyclotomique de j modulo n sur $\mathbb{F}_q$ comme l'ensemble

$$Cl(j) = \left\{j, qj, q^2 j, \ldots, q^{r-1} j\right\} mod\ n,$$

où r est le plus petit entier positif non nul tel que $jq^r \equiv j\ mod\ n$.

Nous pouvons donc réécrire les résultats. Nous avons que

$$r = \deg M_{\beta^j}(X) \equiv ord_l(q),$$

où l est l'ordre de β^j, nous obtenons que le polynôme minimal de $\gamma = \beta^j$, $j \in \mathbb{Z}_n$, est

$$M_\gamma(X) = \prod_{i \in Cl(j)} \left(X - \beta^i\right).$$

Le nombre de classes cyclotomiques modulo n sur $\mathbb{F}_q$ est égal au nombre de

polynômes minimaux différents des racines n-ièmes de l'unité sur $\mathbb{F}_q$. La formule nous donne

$$X^n - 1 = \prod_j M_{\beta^j}(X),$$

où j parcourt un ensemble de représentants des classes cyclotomiques modulo n sur $\mathbb{F}_q$. Donc le nombre de classes cyclotomiques modulo n sur $\mathbb{F}_q$ est égal au nombre de diviseurs irréductibles de $X^n - 1$ sur $\mathbb{F}_q$.

Exemple 3.1

Considérons le polynôme $x^7 - 1$ sur $\mathbb{F}_2$. On a $n = 7$, $q = 2$, $m = 3$ car $7 = 2^3 - 1$. Pour les classes cyclotomiques modulo 7 on a :

$$\begin{aligned} C_0 &= \{0\} = \left\{0, 2^j\right\} \\ C_1 &= \{1, 2, 4\} = \left\{1, 2^j\right\} = C_2 \\ C_3 &= \{3, 5, 6\} = \left\{3, 2^j\right\} \end{aligned}$$

Les trois polynôme minimaux sont :

$$\begin{aligned} M^{(0)}(x) &= (x-1) \\ M^{(1)}(x) &= \prod_{j \in C_1} (x - \alpha^j) = (x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right) \\ M^{(3)}(x) &= \prod_{j \in C_3} (x - \alpha^j) = \left(x-\alpha^3\right)\left(x-\alpha^6\right)\left(x-\alpha^5\right) \end{aligned}$$

(α une racine 7-ième primitive de l'unité sur $\mathbb{F}_2$).

Pour déterminierles cofficients binaire de $M^{(1)}(x)$ et $M^{(3)}(x)$, il faut faire des calculs dans $\mathbb{F}_8$, puis que $8 = 2^3$, nous considéronsun polynôme binaire de degré 3 irréductible sur $\mathbb{F}_2$, par exemple $f(x) = x^3 + x + 1$ si α racine primitive de $f(x)$, alors $f(\alpha) = 0$.

On a donc

$$\alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1, \alpha^7 = 1$$

Alors

$$\begin{aligned} M^{(1)}(x) &= (x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right) = x^3 + \left(\alpha+\alpha^2+\alpha^4\right)x^2 + \left(\alpha^3+\alpha^5+\alpha^6\right)x + \alpha^7 \\ &= x^3 + x + 1 \end{aligned}$$

Et on trouve de maniére analogue que

$$M^{(3)}(x) = x^3 + x^2 + 1$$

Et la factorisation de $x^7 - 1$ sur $\mathbb{F}_2$

$$x^7 - 1 = (x+1)\left(x^3+x^2+1\right)\left(x^3+x+1\right)$$

3.2 Éléments maximaux d'une famille

Définition 3.6

Dans cette partie, nous donnons des résultats applicables à un cas très général. En effet, nous considérons un corps fini $\mathbb{F}$ (pas nécéssairemment $\mathbb{F}_2$ ou une extension) et un entier naturel n. Soit ξ une famille de sous ensembles de $\mathbb{F}^n$. Ici, nous n'imposons pas que les éléments sont des codes (des sous espace vectoriels). Par contre, nous imposons que $C \in \xi$.

Nous munissons cette famille de la relation d'ordre la plus naturelle, l'inclusion $\subset$. Nous obtenons ainsi une famille partiellement ordonnée $(\xi, \subset)$.

Définition 3.7

Soit C un élément de $\xi \setminus \{\mathbb{F}^n\}$. C est appelé un élément maximal de ξ si :

$$(D \subset C \text{ et } D \in \xi) \Longrightarrow (D = C \text{ ou } D = \{\mathbb{F}^n\}).$$

En d'autres mots, C est un élément maximal de ξ s'il n'existe pas de code entre C et $\{\mathbb{F}^n\}$ dans $(\xi, \subset)$.

Remarque 3.3

Notons que, puisque ξ est une famille finie, le nombre d'éléments maximaux de ξ est fini.

Définition 3.8

On note $\xi_{\max} = \{C_1, ..., C_r\}$ l'ensemble des éléments maximaux de $(\xi, \subset)$.

Remarque 3.4

Si ξ n'est pas réduit à $\{0\}$, ξ possède au moins un élément maximal.

Proposition 3.6

Soit C un élément de ξ ($C \neq \{\mathbb{F}^n\}$). Alors, il existe $i \in \{1, ..., r\}$ tel que :

$$C \subset C_i.$$

Ce résultat découle de la définition d'élément maximal.

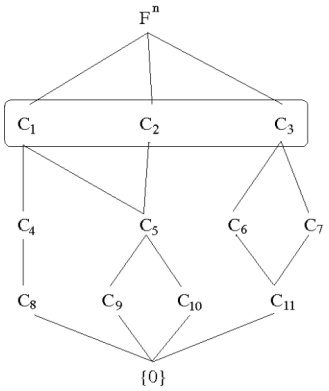

Figure 3.1

Exemple 3.2

Ce schéma se lit de la maniére suivante : un élément C est relié à un élément D placé plus haut si et seulement si $C \subset D$.

Dans cet exemple, $\{0\} \subset C_8 \subset C_4 \subset C_1 \subset \mathbb{F}^n$.

3.3 Codes maximaux

Définition 3.9

Si α est un racine n-ièmes primitive dans extension de $\mathbb{F}_q$, alors le polynôme $m_s(x) = \prod_{j \in C_s} (x - \alpha^j)$ est le polynôme minimal de α^s sur $\mathbb{F}_q$ (c_s la classe cyclotomique).

Le polynôme $x^n - 1 = \prod_s m_s(x)$ donc la factorisation de $x^n - 1$ en facteurs irréductible sur $\mathbb{F}_q$.

Définition 3.10

Le code cyclique M_s dans $R_n = \mathbb{F}_q[x]/(x^n - 1)$, engendré par $m_s(x)$, le code cyclique maximal de longeur sur $\mathbb{F}_q$.

3.3.1 Application

Soient n un entier naturel impair et $\mathbb{F}$ un corps fini de caractéristique 2. On considère

ζ la famille des codes cycliques de longueur n sur $\mathbb{F}$.

Rappelons que chaque code cyclique est généré par un facteur unitaire de $X^n - 1$. Nous avons donc la correspondance suivante :

$$\begin{array}{rcl} \Phi & : & \{\text{facteurs de } X^n - 1\} \to \zeta \\ g(X) & \to & \langle g(X) \rangle \end{array}$$

De plus, les codes cycliques maximaux de longueur n sont exactement les facteurs irréductibles de $X^n - 1$ dans $\mathbb{F}[X]$. Si on note $g_1(X), ..., g_r(X)$ les facteurs irréductibles de $X^n - 1$, alors les codes cycliques maximaux de longueur n sont exactement les $\langle g_i(X) \rangle$, $i = 1, ..., r$.

Exemple 3.3

Prenons $n = 7$ et $\mathbb{F} = \mathbb{F}_2$. $X^7 - 1$ se factorise de la façon suivante :

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

les trois facteurs étant irréductibles. Ainsi, les codes cycliques maximaux de longueur 7 sont exactement $\langle g_1(X) \rangle$, $\langle g_2(X) \rangle$ et $\langle g_3(X) \rangle$ avec

$g_1(X) = X + 1$.

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

et $g_3(X) = X^3 + X + 1$.

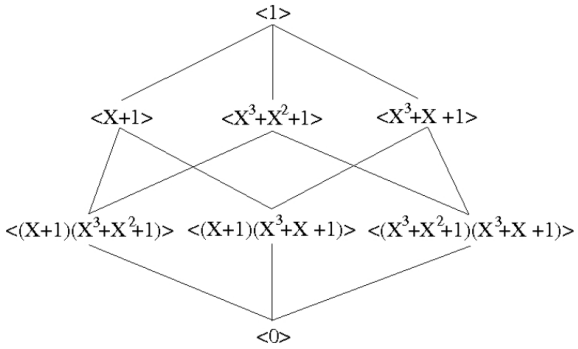

Figure 3.1 _ Structure de la famille des codes cycliques de longueur 7 sur $\mathbb{F}_2$.

Exemple 3.4

Considérons le polynôme $x^{21}-1$ sur $\mathbb{F}_2$. On a $n=21$, $q=2$. Pour les classes cyclotomiques modulo 21 on a :

$$\begin{aligned} C_0 &= \{0\} = \left\{0, 2^j\right\} \\ C_3 &= \{3, 6, 12, 24, 48, 33\} \\ C_9 &= \{9, 18, 36\} \\ C_{15} &= \{15, 30, 60, 57, 51, 39\} \\ C_{21} &= \{21, 42\} \\ C_{27} &= \{27, 54, 45\} \end{aligned}$$

Les polynômes minimaux sont :

$M_0(x) = 1 + x$,

$M_3(x) = 1 + x + x^2 + x^4 + x^6$,

$M_9(x) = 1 + x^2 + x^3$,

$M_{15}(x) = 1 + x^2 + x^4 + x^5 + x^6$,

$M_{21}(x) = 1 + x + x^2$,

$M_{27}(x) = 1 + x + x^3$.

Les codes cycliques maximaux de longueur 21 sont exactement

$\langle M_0(x)\rangle$, $\langle M_3(x)\rangle$, $\langle M_9(x)\rangle$, $\langle M_{15}(x)\rangle$, $\langle M_{21}(x)\rangle$, $\langle M_{27}(x)\rangle$.

Code	$\langle M_0(x)\rangle$	$\langle M_3(x)\rangle$	$\langle M_9(x)\rangle$	$\langle M_{15}(x)\rangle$	$\langle M_{21}(x)\rangle$	$\langle M_{27}(x)\rangle$
polynôme générateur	$M_0(x)$	$M_3(x)$	$M_9(x)$	$M_{15}(x)$	$M_{21}(x)$	$M_{27}(x)$
pramèters de code	$[21, 20]$	$[21, 15]$	$[21, 18]$	$[21, 15]$	$[21, 19]$	$[21, 18]$

conclusion

Dans ce travail on a fait une étude sur les codes cycliques sur un corps fini.

Nous avons présenté les définitions et quelques propriétés sur les corps finis.

Ensuite nous avons fait une étude sur les codes

Finalement nous donnons des exemples illustratifs

Bibliographie

[1] **A.A.Pantchichkine,** *Magistère de mathématiques (L'ENS de Lyon), 2005, Mathématiques des codes correcteurs d'erreurs.*

[2] **A.A.Pantchichkine,** *Master-1 de mathématiques (MAlg 1),2004-2005.*

[3] **A.Kraus,** Cours cryptographie, Université Pierre et Marie Curie, MM029-2009-2010.

[4] **A.Bonnecaze,** Introduction à l'algèbre pour les Codes Cycliques, Marseille Université, 2006-2007**.**

[5] **B.Martin,** Codage, cryptologie et applications, presses polytechniques et universitaires romaindes 2004.

[6] **C.Bachoc**, Cours des codes(Uecode,signal) Université Bordeaux, master CSI2-2004-2005.

[7] **C.Chabot,** Reconnaissance de codes, structure des codes quasi-cycliques, Mémoire présenté pour l'obtention du diplôme de doctorat de l'université de LIMOGES,2009.

[8] **C.Mihoubi**, *Classification des codes linéaires tertiaires optimaux [n,n/2]*, Mémoire présenté pour l'obtention du diplôme de doctorat en sciences Université de el hadj lakhdar-batena, 2012.

[9] **D.Harari,** *Anneaux et* polynômes, Agrégation, Orsay, 2016-2017.

[10] **D.J.Mercier,** Corps finis, IUFM de Guadeloupe,Morne Ferret, BP399, Pointe-à-Pitre cedex 97159, dany-jack.mercier.2003

[11] **J. Calais**, Extensions de corps Théorie de Galois , Ellipses, 2006.

[12] **L.Heboub**, *Etude de techniques de décodage des codes linéaires*, Mémoire présenté pour l'obtention du diplôme de magistèr Université de m'sila, 2009.

[13] **N.Mosquès,** Constructions de corps finis, Gymnase Auguste piccard loïc Devanthéry, 2019.

[14] **O.Debarre,** *Algèbre 2,* École Normal Supérieur, 2012-2013.

[15] **O.Moussai,** *Codes cyclique optimaux de rendement 1/2 sur F_2, Mémoire de master, Université de M*$^{\text{ed}}$ B*oudiaf m'sil, 2012-2013.*

[16] **O.Yemen,** Application des codes cycliques tordus, Université Nice Sophia Antipolis, français, 2013.

[17] **S.Damma et A.Lia**, Sur les décodage d'un c*ode cyclique, Mémoire de master, Université de M*$^{\text{ed}}$ B*oudiaf m'sil, 2018-2019.*

[18] **S.Gintaras**, *Calcul du groupe d'automorphismes des codes. Détermination de l'équivalence des codes, Université de limoges, 1999.*

[19] **S.L.Chaopingxing,** Coding Theory, A First Course, Cambridge University Press 2004.

[20] **S.Roman**. Coding and information theory, springer verlag, New York-Berlin-Heidelberg, 1992.

[21] **V.Pless**,Introduction to the Theory of Error-Correcting Codes, Wiley-Intersci. Ser. Discrete Math. Optim. (1998).

[22] **W.C Huffman et V.Pless**, Fundamentals of Error-Correcting Codes, Combridge University Press (2003).

خلاصة

يندرج هذا العمل في إطار نظرية الشفرات المصححة للأخطاء أكثر دقة دراسة الشفرات الدورية على حقل منتهي. في البداية نقدم المفاهيم الأساسية لنظرية الشفرات المصححة للأخطاء ثم نتطرق إلى الشفرات الأعظمية.

الكلمات المفتاحية: الحقول المنتهية، الشفرات الدورية.

Résumé

Ce travail s'inscrit dans le cadre de la théorie des codes correcteurs d’erreurs plus précisément l’étude de codes cycliques sur un corps fini.

Tout d'abord nous présentons les concepts fondamentaux de la théorie des codes correcteurs d'erreurs ensuite nous abordons les codes cycliques maximaux.

Mots clés: Corps finis, codes cycliques.

Abstract

This work is included in the frame of theory of error correcting codes, more precisely the study of cyclic codes over a finite field.

First we present the fundamental concepts of the theory of error correcting codes then we approach the maximal cyclic codes.

Key words: Finite fields, cyclic codes.