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
Filiére : Mathématiques
Option : Algébre et Mathématiques Discrètes

Thème

Quelques codes cycliques de longeur 2p

Présenté par :
Nor Elhouda Chenni

Devant le jury composé de :

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

Année universitaire 2021/2022

REMERCIEMENTS

Tout d’abord, Nous tenons à remercier ALLAH tout-puissant et Miséricordieux qui nous a donné la force et la patience d’accomplir ce travail. En second lieu, nous tenons à exprimer notre reconnaissance à notre encadreur Mr L.Heboub Nous le remercions de nous avoir encadrés, orientés aidés et conseillés. Tout notre respect et nos remerciements vont vers les membres du jury qui vont pleinement consacrer leur temps et leur attention afin d’évaluer notre travail qui espérons le sera à la hauteur de leur attente.

DÉDICACE

A mon père Ahmed et ma mère Amel, à qui je dois tout et qui m'ont soutenu jusqu au bout

A mon cher mari qui m'apporté tout son soutien et ses conseils .

A mes soeurs Faiza , Ikram, Israa .

A mon frère saber ayoub .

Amon frère çaid hocine .

A Ratil et mohamed et sajed .

Table des matières

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.

$\mathbb{R}$: L'ensemble des nombres rééls.

$\mathbb{Q}$: L'ensemble des nombres rationneles.

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

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

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

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

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

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

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

$C^{\perp}$: Le code dual d'un code considéré.

$d_{\min}$: La distance minimale.

$(f(x))$: Idéal engendré par $f(x)$.

$\deg(g(x))$: Le degré de polynôme g.

$\mathbb{F}_q[x]$: Anneau des polynômes à coeffcients dans $\mathbb{F}_q$.

$\mathbb{F}_q[x]/(x^n - 1)$: L'annaux quotient.

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 . Dans ce mémoire, on s'intéresse à l'étude de quelques codes cycliques de longueur $2p$ sur un corps fini $\mathbb{F}_q$.

Le premier chapitre est un chapitre d'introduction où nous présentons les propriétés fondamentales nécessaires pour la réalisation de ce travail tels que : rappel sur les anneaux, anneaux des polynômes, corps finis et construction d'un corps fini. factorisation de $x^n - 1$ sur un corps fini, Ce chapitre représentent l'outil mathématique utilise pour l'étude des codes cycliques .

Le deuxième chapitre est consacré à l'étude des codes et les codes linéaires, nous étudions les définitions et les propriétés des codes linéaires, puis on va présenter les codes cycliques et aussi nous étudions les définitions et les propiétés des codes cycliques.

Enfin dans le troisieme chapitre , on va etudier quelques codes cycliques de longueur $2p$ sur un corps fini $\mathbb{F}_q$ où p et q sont des nombres premiers impairs distincts et $p - 1$ est l'order multiplicatif de q modulo $2p$.

Chapitre 1

Les corps finis

contenu

1.1 Anneaux

1.1.1 Définition

On appelle anneau tout ensemble A muni de deux opérations binaires $+$ et $.$, l'une est une loi de groupe l'autre associative et doublement distributive par rapport à la premiére.

1.1.2 Idéal d'un anneau

Définition 1.1.1.
Un ensembte non vide I de A est dit idéal si :

1. *I est un sous groupe de $(A, +)$*
2. *$\forall a \in I, \forall b \in A, ab \in I$ et $ba \in I$.*

Exemple 1.1.1.
Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Définition 1.1.2.
L'ensemble des classes résiduèlles d'un anneu A modulo un idéal I forme un anneau noté A/I dont les deux opérations sont définies par :

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

1.1.3 Anneaux des polynômes

Définition 1.1.3.
Soit A un anneau commutatif unitaire. toute suite d'étéments de A n'ayant qu'un nombre fini de termes non nuls est dite polynôme à coefficients dans A. l'ensemble des polynômes sur A est noté $A[x]$.

Si $f = (a_0, a_1, ..., a_n, 0, 0, ...) \in A[x]$ on notera $f = (a_0, a_1, ..., a_n)$.

Si $a_n \neq 0$, on appelle n le degré de $f (n = deg f)$ si $a_n = 1$, on dit que f est unitaire.

on pose $\deg(0, 0, ...) = -\infty$, les polynômes de degré $= 0$ sont les constantes.

Dans $A[x]$ on définit l'addition et la multiplication comme suit :

$$(a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$$
$$(a_0, a_1, ...)(b_0, b_1, ...) = (c_0, c_1, ...) \text{ où } c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

Notons que si A est intégre on a : $\deg fg = \deg f + \deg g$.

Muni des deux opérations $+$ et $.$, $A[x]$ est anneau commutatif avec unité $(1, 0, 0, ...)$.

$(A[x], +, .)$.) est appelé l'anneau des polynômes sur A.

dans $A[x]$, on définit : $x = (0,1,0,0,...), x^2 = (0,0,1,0,...), ...$ avec $x^0 = (1,0,0,...)$ ce qui permet d'écrire tout polynôme P de degré n comme :

$p = a_0 + a_1 x + ... + a_n x^n$

soit $f, g \in A[x]$, avec $\deg f > 0$. dit que f divise g noté $(f \mid g)$ si $g = fh$ pour $h \in A[x]$

et $\deg f < \deg g$, f est alors appelé un diviseur propre de g.

Définition 1.1.4.
L'anneau des polynômes $F_q[x]$ (ou $K[x]$ en général, K corps) est l'ensemble des polyômes $f(x)$ à coefficients dans F_q (quis satisfait les propriétés d'un anneau).

Définition 1.1.5. ***(Idéal principal)***
Soit I un idéal de $F_q[x]$. On dit que I un idéal principal s'il existe un polynôme P dans $F_q[x]$ tel que $I = (P)$.
Notons que (P), l'idéal engendré par le polynôme P, est défini par :

$$(P) = \{f \in F_q[x] | (\exists Q \in F_q[x]) f = PQ\}$$

Théorème 1.1.1.
Soit K un corps, alors l'anneau des polynômes $K[x]$ est principal.

Preuve.
On va montrer que tout idéal dans $K[x]$ est principal.
Soit I un idéal de $K[x]$. si $I = \{0\}$, alors $I = (0)$.
Supposons $I \neq \{0\}$. alors $I - \{0\} \neq \phi$. Soit G un polynôme de $I - \{0\}$ vérifiant

$$\deg(G) = min\{\deg(P) \in \mathbb{N} | P \in I - \{0\}\}.$$

Sachant que $G \in I$ équivaut à $(G) \subset I$. Soit $A \in I$, par la division Euclidienne, il existe un unique couple

de polynômes (Q, R) tel que :

$$A = GQ + R \text{ et } \deg(R) < \deg(G)$$

Comme G et A sont des éléments de I, et que I est un idéal, on a :

$$R = A - GQ \in I$$

De

$$R \in I, \deg(G) = min\{\deg(P) \in \mathbb{N} | P \in I - \{0\}\}$$

et

$$\deg(R) < \deg(G)$$

on déduit :

$$R = 0$$

D'où

$$A = GQ$$

et donc $I \subset (G)$. Comme, d'autre part, $(G) \subset I$ on obtient :

$$I = (G)$$

□

1.2 Corps finis

Un corps fini est un corps dont le cardinal est fini. les corps fini sont aussi appelés de Galois en L'honneur du mathématicien du dix-neuviéme siécle Evarist Galois qui fut l'un des premiers à les étudier.

Définition 1.2.1.
Soit p un nombre premier. On not $\mathbb{F}_p$ un corps fini à p éléments $\mathbb{Z}/p\mathbb{Z}$,

Définition 1.2.2.
un corps fini est un corps qui posséde un nombre fini d'éléments .

Exemple 1.2.1.
Pour tout entier p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps à p éléments.

1.2.1 Caractéristique et cardinal

1. Caractéristique et cardinal

Définition 1.2.3.
Soit $\mathbb{K}$ un corps commutatif, la caractéristique de $\mathbb{K}$ est :

Soit le plus petit entier $n > 0$ vérifiant $n.1_k = 0$ (s'il existe). Soit le zéro (0) dans le cas contraire avec

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

1_k élément neutre de "." dans $\mathbb{K}$. car $(k) \in \mathbb{N}$.

Théorème 1.2.1.
L'anneau $(\mathbb{Z}_p, +, .)$ est un corps si et seulement si p est un nombre premier.

Preuve.
$\Rightarrow)(\mathbb{Z}_p, +, .)$ est un corps. Si $p = ab$, avec $1 < a, b < n$, alors
$b = a^{-1}ab = a^{-1}p = 0 \mod p$, contradiction.
$\Leftarrow)p$ est un nombre premier. Tout nombre $1 \leq q \leq p - 1$ est premier avec p.

D'après le théorème de Bezout il existe des entiers u et v tels que $up + vq = 1$ d'où en passant à $\mathbb{Z}_p, \overline{vq} \equiv \overline{1}$ et $\overline{q}$ est inversible, donc $(\mathbb{Z}_p, +, .)$ est un corps. □

Exemple 1.2.2.

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

2. $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}, p.\overline{1} = \overline{0}.\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}$

Proposition 1.2.1.
Soit $\mathbb{K}$ *un corps fini de caractéristique* p *premier.* $\mathbb{K}$ *a nécessairement* $q = p^n$ *éléments, pour* $n \geq 1$. $\mathbb{K}$ *contient* $\mathbb{Z}/p\mathbb{Z}$ *appelé le sous-corps premier de* $\mathbb{K}$. *le corps* $\mathbb{K}$ *est un espace vectoriel de dimension* n *sur* $\mathbb{Z}/p\mathbb{Z}$.
Il existe donc une base de n *éléments de* $\mathbb{K}$ $(e_1, ..., e_n)$ *telle que pour tout* x *dans* $\mathbb{K}$ *il existe un unique* $(\alpha_1, ..., \alpha_n)$ *dans* $\mathbb{Z}/p\mathbb{Z}$ *tel que*

$$x = \sum_{i=1}^{n} \alpha_i e_i$$

Réciproquement, pour tout nombre premier p *et tout* $n \geq 1, q = p^n$, *il existe un corps fini et un seul (à isomorphisme près) à* q *éléments. On le note* $\mathbb{F}_q$, *ou* $GF(q)$.

Proposition 1.2.2.
Soit $\mathbb{F}_q$ *un corps fini avec* $q = p^n$, *alors on a* $(x+y)^p = x^p + y^p$ *pour tout* $x, y \in \mathbb{F}_q$.

L'application $f : x \longmapsto x^p$ *est un automorphisme dit de Frobenius :*

$f(x+y) = f(x) + f(y), f(xy) = f(x)f(y)$ *et* f *est une bijection. Les éléments tels que* $f(x) = x$ *sont exactement les éléments de* $\mathbb{F}_p \subset \mathbb{F}_q$

Théorème 1.2.2.
Soit $\mathbb{K}$ *un corps fini de cardinal* q.
Le groupe multiplicatif $(\mathbb{K}^*, .)$ *est cyclique d'ordre* $q - 1$.

Preuve.
Le groupe $(\mathbb{K}^*, .)$ est commutatif (car tout corps fini est commutatif, c'est le théorème de WEDDERBURN) et fini . D'après le théorème précédent, ils existent des groupes cycliques $H_1, ..., H_r$ tel que :

$$\mathbb{K}^* \cong H_1 \times H_2 \times ... \times H_r$$

et pour tout $i = 1, 2, ..., r-1, |H_i|$ divise $|H_{i+1}|$

L'entier $s = H_r$ est donc un exposant de chaque élément de $\mathbb{K}^*$, donc pour tout $x \in \mathbb{K}^*, x^s = 1$, en d'autre terme tout les élément de $\mathbb{K}^*$ sont racine du polynôme $x^s - 1 \in k[x]$ or ce polynôme admet au plus s racines donc

$$|\mathbb{K}^*| \leq s$$

Mais $|H_r| = s$ divise $|\mathbb{K}^*|$, d'ou $|H_r| = |\mathbb{K}^*|$, et comme $\mathbb{K}^*$ est fini cela entraîne que $\mathbb{K}^* = H_r$ □

2. Cardinal d'un corps fini

Définition 1.2.4.
Soit $\mathbb{F}$ *un corps fini de caractéristique* p. *Le nombre des élément de* $\mathbb{F}$ *est de la forme*

$$|\mathbb{F}| = p^n$$

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 forcement finie. D'ou $|\mathbb{F}_p|= |\mathbb{F}|^n= p^n$.

Donc, un corps fini a forcement p^n éléments ou p est un nombre premier.

□

Remarque 1.2.1.

1. *Le cardinal d'un corps fini est une puissance d'un nombre premier.*
2. *Si $\mathbb{F}_q$ est un corps fini alors $\mathbb{F}_q - \{0\} = \mathbb{F}^*{}_q$*

Corollaire 1.2.1.
Tout corps $\mathbb{F}$ d'ordre premier p est isomorphe à $\mathbb{Z}_p$.

Elément primitif d'un corps fini

Définition 1.2.5.
Soit $\mathbb{F}_q$ le corps fini à q éléments, un générateur du groupe multiplicatif $\mathbb{F}^*{}_q$ est appelé un élément primitif du corps fini $\mathbb{F}_q$.
Soit α un élément primitif d'un corps fini $\mathbb{F}_q$ alors :

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

Avec $\alpha^{q-1} = 1$ de plus α^k est primitif si et seulement si k et $q-1$ sont premiers entre eux.

Proposition 1.2.3.
Soit $\mathbb{F}_q$ un corps fini à $q = p^n$ élément, p premier et $n \geq 1$ si $a, b \in \mathbb{F}_q$, alors :

$$(a+b)^{p^i} = a^{p^i} + b^{p^i}, \forall i \in \mathbb{N}.....(*)$$

Preuve.
On démontre par récurrence sur i : pour $i = 0$ c'est clair

$$(a+b)^{p^0} = a^{p^0} + b^{p^0} .$$
$$(a+b)^1 = a^1 + b^1 .(p^0 = 1)$$

supposonsque $(*)$ est vraie pour i

$$(a+b)^{p^{i+1}} = [(a+b)^{p^i}]^p = (a^{p^i} + b^{p^i})^p = (a^{p^i})^p + (b^{p^i})^p = a^{p^{i+1}} + b^{p^{i+1}}.$$

□

Proposition 1.2.4.
Soient $m, n \in N^*$, p est premier, on a :

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \Longleftrightarrow m \backslash n .$$

Preuve.
$\Longrightarrow$)$Ona : \mathbb{F}_q \subset \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$
$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_{q^m}].[\mathbb{F}_{q^m} : \mathbb{F}_q]$
$n = [\mathbb{F}_{q^n} : \mathbb{F}_{q^m}].m$
$\Longrightarrow m \backslash n$
$\Longleftarrow$)$m \backslash n \Longrightarrow q^m - 1 \backslash q^n - 1$
$\Longrightarrow x^{q^m-1} - 1 \Longrightarrow x^{q^n-1} - 1$
$\Longrightarrow x^{q^m} - x \backslash x^{q^n} - x$
donc $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$.

□

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

Polynôme minimal

Définition 1.2.6.
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 1.2.5.
Soit $\alpha \in \mathbb{F}_{q^m}$, soit d un entier positif non nul. Le degré 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 1.2.1.
Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de $\alpha, i.e\alpha^l = 1$. 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 $l|q^r - 1$. Mais $\alpha^l = 1$, $\alpha^{q^{r-1}} = 1$ 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 1.2.2.
Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α Alors :

$$degM_\alpha(x) = ord_l(q)$$

tel que $l \in \{1, 2, ..., q^m - 1\}$

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

□

Proposition 1.2.6.
Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α Alors

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

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

Remarque 1.2.2.
La proposition et le corollaire précédent nous montrent que

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

Conjugaison

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 1.2.7.
La conjugaison dans $\mathbb{F}_{q^m}$ *est une relation d'equivalence.*

Définition 1.2.7.
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 1.2.8.
Soit $\alpha \in \mathbb{F}_{q^m}$. *Soit* l *l'ordre de* α. *Les conjugués de* α *sont*

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

Ils sont distincts deux à deux.

Preuve.
C'est une conséquence directe de la définition précédente et de la proposition dans polynôme minimal. □

Remarque 1.2.3.
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 :*

1. *il y a autant des classes d'équivalence que des polynômes minimaux différents des éléments de il y a autant des classes de* $\mathbb{F}_{q^m}$.
2. *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 $n|q^m - 1$

Définition 1.2.8.
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* $\mathbb{F}_{q^m}$.

Proposition 1.2.9.
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, $(\beta^{-1})^n = (\beta^n)^{-1} = 1$. 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 μ l'entier tel que $\mu.n = q^m - 1$. Soit α un élément primitif de $\mathbb{F}_{q^m}$. Alors $\beta = \alpha^u$ 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

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

Soit 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

1. *Il y a autant des classes d'équivalence que de polynômes minimaux différents des racines n-ièmes de l'unité sur $\mathbb{F}_q$.*
2. *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 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

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

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

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

$$x^r - 1 = \prod_{i=0}^{r-1}(x - \beta^i)$$

et donc

$$x^n - 1 = (x^r - 1)^{p^s} = \Big(\prod_{i=0}^{r-1}(x - \beta^i)\Big)^{p^s} = \prod_{i=0}^{r-1}(x - \beta^i)^{p^s}$$

De même,

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

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

Classes cyclotomiques

Soit $(n, q) = 1$.

Soit une racine n-ièmes primitive de l'unité sur $\mathbb{F}_q$. La relation d'équivalence sur les racines n-ièmes de l'unité sur $\mathbb{F}_q$, induit une relation d'équivalence dans l'ensemble $\mathbb{Z}_n$ comme suit : $i, j \in \mathbb{Z}_n$ sont dans la même classe d'équivalence si et seulement si β^i et β^j sont dans la même classe. À la classe de $\gamma = \beta^j, i.e.$ la classe $\{\gamma, \gamma^q, \gamma^{q^2}, \gamma^{q^3}, ..., \gamma^{r-1}\} = \{\beta, \beta^{jq}, \beta^{jq^2}, \beta^{jq^3}, ..., \beta^{jq^{r-1}}\}$, correspond la classe des exposants $\{j, qj, q^2j, ..., q^{r-1}j\} \mod n$, où r est le nombre de conjugués distincts de β^j. Nous savons que r est le plus petit entier positif non nul tel que $(\beta^j)^{q^r} = \beta^j$, autrement dit, tel que $jq^r \equiv j \mod n$.

Définition 1.2.9.
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

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

où r est le plus petit entier positif non nul tel que $jq^r \equiv \mod n$, Nous pouvons donc récrire les résultats. Nous avons que

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

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

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

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 nsur $\mathbb{F}_q$. est égal au nombre de diviseurs irréductibles de $x^n - 1$ sur $\mathbb{F}_q$.

1.2.3 Construction d'un corps fini

Pour déterminer les éléments d'un corps fini $\mathbb{F}_q$ on peut suivre une des méthodes suivantes :

1. Soit en utilisant l'anneau quotient $\mathbb{F}_q[x]/\big(f(x)\big)$ où $f(x)$ est un polynôme irréductible sur $\mathbb{F}_q$.
2. Soit en utilisant le fait que $\mathbb{F}_q^*$ est un groupe cyclique où chaque élément est une puissance d'un élément générateur α appartient à $\mathbb{F}_q^*$.

Théorème 1.2.3.
Soit $\mathbb{F}_q$ un corps et $f(x) \in \mathbb{F}_q[x]$, alors $\mathbb{F}_q[x]/\big(f(x)\big)$, est un corps si et seulement si $f(x)$ est irréductible sur $\mathbb{F}_q[x]$.
La preuve de ce théorème montre non seulement que $\mathbb{F}_q[x]/\big(f(x)\big)$ est un corps, mais nous donne aussi la facon d'obtenir ses éléments.

Preuve.
On note par I l'idéal principal $\big(f(x)\big)$, supposons que $f(x)$ est irréductible sur $\mathbb{F}_q, c.a.d$ $f(x) = a(x)b(x)$ tel que $a(x), b(x)$, ont des degrés inférieur au degré de $f(x)$. On montre dans ce cas que $\mathbb{F}_q[x]/\big(f(x)\big)$ n'est pas un corps Le degré de tout polynôme non nul de I doit être supérieur où égal au degré de $f(x)$, donc $a(x) \notin I, b(x) \notin I$, par conséquent $I + a(x), I + b(x)$ sont des élément non nul de $\mathbb{F}_q[x]/I$. Mais on a :

$$(I + a(x))(I + b(x)) = I + f(x) = I$$

ce qui montre que $\mathbb{F}_q[x]/I$ ne peut être un corps donc $f(x)$ doit être irréductible sur $\mathbb{F}_q$ Inversement, supposons que maintenant que $f(x)$ est irréductible sur $\mathbb{F}_q$.
$\mathbb{F}_q[x]/I$ est un anneau commutatif d'élément unité $I + e$ (ou e est l'unité de $\mathbb{F}_q$), il sur t donc de démontre que tout élément non nul de $\mathbb{F}_q[x]/I$ admet un inverse dans $\mathbb{F}_q[x]/I$.
Soit $I + p(x) \in \mathbb{F}_q[x]$ diférent de zéro ($c..d$ différent de I), donc $p(x) \notin I$, ce qui montre que $p(x)$ n'est pas multiple de $f(x)$, comme $f(x)$ est irréductible, alors $f(x)$ et $p(x)$ sont premiers entre eux et donc d'aprés le théorème de bézout
$\exists, u(x), v(x) \in \mathbb{F}_q[x]/\big(f(x)\big)$ tel que

$$f(x)u(x) + p(x)v(x) = e$$

alors on a :

$$e - p(x)v(x) = f(x)u(x) \in I$$

et par conséquent

$$I + e = I + p(x)v(x) = (I + p(x))(I + v(x)) = e$$

$c.à.d$ $I + v(x)$ est l'élément inverse de $I + p(x)$. □

Exemple 1.2.3.
$\mathbb{F}_{3^2} \simeq \mathbb{F}_3[x]/(g)$, *où* $g = x^2 + x + 2$, *comme* g *est irréductible sur* $\mathbb{F}_3$, *on a* $\mathbb{F}_3[x]/(g) = \{a + b\alpha : a, b \in \mathbb{F}_3\}$ *et* $\alpha^2 + \alpha + 2 = 0$, *donc les éléments de* $\mathbb{F}_3$ *sont :*

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 lineaires et cycliques

contenu

Nous allons dans ce chapitre rappeler un ensemble des définitions et propriétés concernant les codes, et plus particuliérement les codes linéaires et les codes linéaires cycliques.

2.1 Les codes

Définition 2.1.1.
Un code sur l'ensemble A de longueur n est un sous-ensemble C de A^n, l'ensemble A est appelé l'alphabet, n la longeur du code C, un code $C \subset A^n$ est de cardinalité M si $M = |C|$ et les éléments de C sont appelés les mots du code.
où l'alphabet est un ensemble quelconque finie et non vide.

Exemple 2.1.1.

1. *Le code $C = \{1100, 0011, 1010, 0001\}$*
   un code de longeur 4 sur l'alphabet
   $A = \{0, 1\}$
2. *$C = \{abc, mmm, bbc, aaa\}$*
   est un code longeur 3 et de cardinal 4 sur l'alphab language francais.

Distance de Hamming

Définition 2.1.2.
Soient $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_q^n$ et $y = (y_1, y_2, ..., y_n) \in \mathbb{F}_q^n$, La distance de hamming de x et y est le nombre $d_H(x, y)$ défini par :

$$d_H(x, y) = |\{\overline{1, i} : x_i \neq y_i\}|$$

On remarque que la distance de hamming sur $\mathbb{F}_q^n$ est une vrie distance au sens numérique de terme. Rappelons briévement les propriétés d'un distance $d_H(x, y)$:

1. $d_H(x, y) = 0 \Longleftrightarrow x = y$;
2. $d_H(x, y) = d_H(y, x) \geq 0$;
3. $d_H(x, y) = d_H(x, z) + d_H(z, y) \forall x, y, z \in \mathbb{F}_q^n$.

Exemple 2.1.2.
$d_H(001, 010) = 2$, $d_H(000, 001) = 1$

La distance minimal d'un code

La distance minimale du code C est la distance minimum entre deux mots distincts de code défini par :

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

Définition 2.1.3.
Un code $[n, M, d]$ sur $\mathbb{F}_q$ est un code de longueur n, de taille M et de distance minimal d. $[n, M, d]$ sont les paramètre de C.

Le poids de Hamming

Définition 2.1.4.
Le poids de Hamming d'un mot $x = (x_1, x_2, ..., x_n)$, noté $w(x)$, est le nombre d'indice i telle que $x_i \neq 0$.

$$w_H(x) = |\{i/x_i \neq 0\}|d(x, 0)$$

Exemple 2.1.3.
$w(110) = 2$ *et* $w(100) = 1$

2.2 Codes Linéaires

Définition 2.2.1.
Un code linéaire de dimension $\mathbb{K}$ de longeur n sur $\mathbb{F}_q$ est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension $\mathbb{K}$.

Matrice génératrice

Définition 2.2.2.
Une matrice génératrice du code C est une matrice G à k lignes et n colonnes, dont les lignes formet une base de C, tels que

$$C = \{c \in \mathbb{F}_q^n / \exists x \in \mathbb{F}_q^k : c = xG\}$$

Définition 2.2.3.
La matrice G est appelée la matrice génératrice de C et tout les vecteurs de C sont appelés les mots code de C.

Remarque 2.2.1.

1. *Le rang de la matrice génératrice G est k.*
2. *À partir de la matrice génératrice G, on peut aussi considérer la code linéaire $C = C(n, k)$ comme l'image d'un application linéaire f telle que*

$$\begin{aligned} f : \mathbb{F}^k &\to \mathbb{F}^n \\ a &\longmapsto f(a) = aG \end{aligned}$$

L'application f est appelée la fonction de codage et a la mot d'information.

Exemple 2.2.1.
Soit G la matrice génératrice du $[3, 2]$ code binaire C telle que :

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

Matrice de contrôle

On peut aussi se donner un sous -espace vectoriel par un système d'équations indépendants. Une matrice de contrôle d'un code linéaire C est la matrice d'un système d'équations linéaires homogénes indépendantes dont l'éspace des solutions est C.

Définition 2.2.4.
Une matrice de contrôle H d'un code linéaire C est une matrice de taille $n \times (n-k)$ et de rang $(n-k)$ vérifiant :

$$C = \{c \in \mathbb{F}_q^n \backslash H^t c = 0\}$$

Exemple 2.2.2.

Pour obtenir le code C a partir de la matrice de contrôle H on calcul tout d'abord l'espace nul de $G, y \in \mathbb{F}_2^4$. Alors $y \in$ l'espace nul de G ssi $Gy^t = 0$

$$Gy^t = 0 \Leftrightarrow \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = 0 \Leftrightarrow \begin{cases} y_1 + y_2 = 0 \\ y_2 + y_3 + y_4 = 0 = 0 \\ y_1 + y_3 = 0 \end{cases}$$

Les solutions du système sont $\{0000, 1110\}$.
Donc la base est $\{1110\}$ *et la matrice* $H = [1110]$
Soit

$$\varphi_H : \mathbb{F}_2^4 \to \mathbb{F}_2$$

$$(x_1, x_2, x_3, x_4) \to (1110) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$\varphi_H(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3$$

et par conséquent, on a
$C = \ker \varphi_H = \{x \in \mathbb{F}_2^4 : x_1 + x_2 + x_3 = 0\}$ *on a par exemple*
$1111 \notin C$ *car* $1 + 1 + 1 \neq 0, 0111 \in C$ *car* $0 + 1 + 1 = 0$

Proposition 2.2.1.
La distance minimale d'un code linéaire $C = C(n, k)$ est le plus petit poids des mots code non nul

$$d = \min_{u \in C - \{0\}} w(u)$$

Code Dual

Définition 2.2.5.
Soit C un $[n, k, d]$-code linéaire. Soit $\langle ., . \rangle$ le produit scalaire euclidien usuel :
$\langle u, v \rangle = \sum_{i=1}^{n} c_i v_i$. *Le code dual note $C^\perp$ est donc un code linéaire de la même longueur. Sa dimension est $n - k$*

$$C^\perp = \{v \in \mathbb{F}_q^n : \forall c \in C : \langle u, v \rangle = 0\}$$

Il découle directement des définitions que si H est une matrice génératrice de $C^{\perp}$, elle est communément appelée matrice de contrôle du code C. De même, une matrice génératrice de C est une matrice de contrôle de $C^{\perp}$.

Définition 2.2.6.
le code dual de C noté par $C^{\perp}$ est :

$$C^{\perp} = \{y \in \mathbb{F}_q^n : \forall x \in C, \langle x, y\rangle = 0\}$$

où $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$ est le produit scalaire de x par y .

Exemple 2.2.3.
Soit le code $C = \{000, 011, 101, 110\}$ de longueur 3 sur $\mathbb{F}_2$ le dual $C^{\perp}$ de C est

$$C^{\perp} = \{y \in \mathbb{F}_2^3 : y = abc, \forall c \in C : \langle u, v\rangle = 0\}$$

donc $y = 111$ OU $y = 000$ d'ou $C = \{000, 111\}$

2.3 Codes Cycliques

Définition 2.3.1.
Un code linéaire $C \subset \mathbb{F}_q^n$ est dit cyclique s'il vérifie la propriété suivante :
si $x_1...x_n \in C$, alors $x_n x_1...x_{n-1} \in C$

Exemple 2.3.1.
le code $C = \{0000, 1100, 0011, 1010\}$ est un cod cyclique

Représentation polynomiale

Nous supposons que $pgcd(n, q) = 1$ et on notera (x^n-1) l'idéal de $\mathbb{F}_q[x]$ engendré par (x^n-1). Alors, tout élément de $R_n = \mathbb{F}_q[x]/(x^n-1)$ 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. L'isomorphisme est donné par

$$c_0 c_1 ... c_{n-1} \rightarrow c_0 + c_1 x + ... + c_{n-1} x^{n-1}$$

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

Exemple 2.3.2.
le code $C = \{000, 101, 110, 010\}$ correspond ausc polynômes
$0, 1 + x^2, 1 + x, x$ pris modulo $x^3 - 1$ sa representation polynômiale.
est donc $C = \{0, 1 + x^2, 1 + x, x\}$

Polynôme générateur d'un code cyclique

Théorème 2.3.1.
Code linéaire C de longueur n sur le corps $\mathbb{F}_q$ est cyclique si et seulement si C est un idéal de $\mathbb{F}_q[x]/(x^n-1)$.

Preuve.
C est un idéal de $\mathbb{F}_q[x]/(x^n-1)$ 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 $\mathbb{F}_q[x]/(x^n-1)$ sont principaux. En particulier, tout idéal non nul est engendré par un polynôme $g(x)$ de plus bas degré qu'il contient :

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

□

Théorème 2.3.2.
Soit C un idéal dans R_n, c'est-à-dire un code cyclique de longueur n.

1. *Il existe un polynôme unique $g(x)$ de degré minimum dans C .*
   Ce polynôme engendré C, c'est-à-dire $C = \langle g(x)\rangle$, et il appelé polynôme générateur pour C.

2. *Le polynôme générateur $g(x)$ divise x^n-1.*

3. *Si deg $(g(x)) = r$, alors C a la dimension $n-r$ et*

$$C = \langle g(x)\rangle = \{r(x)g(x) | \deg(r(x)) < n - r\}.$$

Preuve.

1. Supposons que C contienne deux polynômes distincts $g_1(x)$ et $g_2(x)$ de degré minimum r. Alors leur différence $g_1(x)-g_2(x)$ serait un polynôme non nul en C de degré inférieur à r, qui n'est pas possible. Par conséquent, il existe un polynôme unique $g(x)$ de degré r dans C. Puisque $g(x) \in C$ et C est un idéal, nous avons $\langle g(x) \subset C\rangle$. Par contre, supposons que $p(x) \in C$, et soit

   $$p(x) = q(x)g(x) + r(x)$$

   où $\deg(r(x)) < r$. Alors $r(x) = p(x) - q(x)g(x) \in C$ a un degré inférieur à r, ce qui n'est possible que si $r(x) = 0$. Par conséquent, $p(x) = q(x)g(x) \in \langle g(x)\rangle$, et donc $C \subset \langle g(x)\rangle$. Ainsi, $C = \langle g(x)\rangle$.

2. Diviser x^n-1 par $g(x)$ donne

   $$x^n-1 = q(x)g(x) + r(x)$$

   où $\deg(r(x)) < r$. Puisque dans $R_n = x^n-1 = 0 \in C$, nous voyons que $r(x) \in C$, et donc $r(x) = 0$, qui montre que $g(x)|x^n-1$.

3. L'idéal généré par $g(x)$ est

   $$\langle g(x)\rangle = \{f(x)g(x) | f(x) \in R_n\}$$

   avec le modulo de réduction habituel x^n-1, et nous devons montrer qu'il suffit de restreindre $f(x)$ à des polynômes de degré inférieur à $n-r$. Nous avons vu que $g(x)|x^n-1$, et donc $x^n-1 = h(x)g(x)$.
   Pour un polynôme $h(x)$ de degré $n-r$. Divisons $f(x)$ par $h(x)$

$$f(x) = q(x)h(x) + r(x)$$

où $\deg(r(x)) < n - r$. Alors
$f(x)g(x) = q(x)h(x)g(x) + r(x)g(x) = q(x)(x^n - 1) + r(x)g(x)$
et donc $f(x)g(x) = r(x)g(x)$ dans R_n qui est ce que nous voulions montrer. Cela montre également que l'ensemble

$$\{g(x), xg(x), ..., x^{n-r-1}g(x)\}$$

s'étend sur C, et comme il est linéairement indépendant, il forme une base pour C. Par conséquent $\dim(C) = n - r$.

□

Exemple 2.3.3.
Soit $C(n, k)$ un code linéaire sur $\mathbb{F}_2$ tel que :
$\theta(x) = \{0, 1 + X, X + X^2, 1 + X^2\}$, $g(X) = 1 + X$ *est un générateur de C.*

Exemple 2.3.4.
Les codes cycliques non nuls de longueur $n = 9$ sur le corps des racines 9^{me} de l'unité $\mathbb{K} = F_{64}$. La décomposition de $X^9 - 1$ en produit de polynômes irréductibles sur F_2 est donnée par :
$X^9 - 1 = (X - 1)(X^2 + X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$.
Le tableau ci-dessous nous donne les di¤érentes valeurs possibles du polynôme générateur $g(X)$ des codes cycliques de longueur $n = 9$.

Le générateur $g(X)$	*Le Code* C
1	$<1>=\mathbb{k}^9(trivial)$
X^2+X+1	$<X^2+X+1>$
X^3+X^2+1	$<X^3+X^2+1>$
$(X-1)(X^3+X+1)$	$<X^4+X^3+X^2+1>$
$(X^2+X+1)(\ X^3+X+1)$	$<X^2+X+1(X-1)(\ X^3+X^2+1)>$
$(X^3+X+1)(X^3+X^2+1)$	$<(X^3+X+1)(X^3+X^2+1)>$
$(X-1)(\ X^2+X+1)(X^3+X^2+1)$	$<(X-1)(\ X^2+X+1)(X^3+X^2+1)>$
$(\ X^2+X+1)(X^3+X+1)(X^3+X^2+1)$	$<(\ X^2+X+1)(X^3+X+1)(X^3+X^2+1)>$
$X-1$	$<X-1>$

Le générateur $g(X)$	*Le Code* C
X^3+X+1	$<X^3+X+1>$
$(X-1)(X^2+X+1)$	$<X^3+1>$
$(X-1)(X^3+X^2+1)$	$<X^4+X^2+X+1>$
$(X^2+X+1)(X^3+X^2+1)$	$<(X^2+X+1)(X^3+X^2+1)>$
$(X-1)(\ X^2+X+1)(X^3+X+1)$	$<(X-1)(\ X^2+X+1)(X^3+X+1)>$
$(X-1)(X^3+X+1)(X^3+X^2+1)$	$<(X-1)(X^3+X+1)(X^3+X^2+1)>$
$X^9-1=0$	$\{0\}$

Exemple 2.3.5.
Sur $\mathbb{F}_2$ *on* $ax^7-1=(x+1)(x^3+x^2+1)(x^3+x+1)$
alors les codes cycliques de longueur 7 *sur* $\mathbb{F}_q$ *sont :*
$\langle 1\rangle = R_n$,
$\langle (x+1)\rangle$,
$\langle (x^3+x+1)\rangle$,
$\langle (x^3+x^2+1)\rangle$,
$\langle (x+1)(x^3+x+1)\rangle$,
$\langle (x+1)(x^3+x^2+1)\rangle$,
$\langle (x^3+x+1)(x^3+x^2+1)\rangle$,
$\langle 0\rangle = \{0\}$.

Chapitre 3

Quelques codes cycliques de longeur 2p

contenu

3.1 Introduction

Soit $\mathbb{F}_q$ le corps fini à q éléments et p un nombre premier impair où p et q sont premier entre eux et $p-1$ est l'ordre multiplicatif de q modulo $2p$
Dans ce chapitre on s'itrésse aux quelques codes cycliques de longeur $2p$ sur $\mathbb{F}_q$.

3.2 Structure des codes cycliques

Les codes cycliques se sont les codes les plus utilisés car admettent de bons algorithmes de dècodage

3.2.1 Polynôme générateur et polynôme de contrôle

Proposition 3.2.1.
Tout mot d'un code cyclique C est multiple du polynôme générateur $g(x)$ on note $C = \langle g(x) \rangle$

Définition 3.2.1.
Soit C un code cyclique de longeur n et de dimension K sur $\mathbb{F}_q$, de polynôme générateur appelle polynôme de contrôle de C le polynôme

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

Comme g est unitaire de degré $n-k$, le polynôme h est unitaire de degré k.

3.2.2 Représentation matricielle

Soit C un code cyclique de longeur n et de dimension k sur $\mathbb{F}_q$.
Soit $g = \sum_{i=0}^{k} g_i x^i$ et $h = \sum_{i=0}^{k} h_i x^i (r = n-1)$ respectivement le polynôme générateur et de contrôle de C.

Théorème 3.2.1.
Soit C un code cyclique de longeur n sur Q un corps fini $\mathbb{F}_q$ de polynôme générateur $g(x)$. Alors dim $(C) = n - r$ et le matrice génératrice G de C

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

Exemple 3.2.1.
Considérons les codes ternaires longeur 4. Nous avons alors le factorisation en facteur irréductibles suivante

$$X^4 - 1 = (x-1)(x+1)(x^2+1)$$

Comme il ya 3 facteurs irréductibles, il y a $2^3 = 8$ codes cycliques

polynôme générateur	*matrice générateur*
1	I_4
$x-1$	$\begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & -1 \end{bmatrix}$
$x+1$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
x^2+1	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
x^2-1	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x-1)(x^2+1) = x^3-x^2+x-1$	$\begin{bmatrix} -1 & 1 & -1 & 1 \end{bmatrix}$
$(x+1)(x^2+1) = x^3+x^2+x+1$	$\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$
$(x^4-1) = 0$	$\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$

Une matrice de contrôle du code C de polynôme de contrôle $h(x)$ est donnée par :

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

Exemple 3.2.2.
Soit C le code binaire de paramétre $(7,4)$ de polynôme générateur $g(x) = x^3+x+1$
Le polynôme de contrôle de C est

$h(x) = \dfrac{x^7 - 1}{g(x)} = x^4 + x^2 + x + 1.$
La matrice de contrôle du code c est

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

3.2.3 Dual d'un code cyclique

Définition 3.2.2. *(polynôme réciproque)*
Soit $f(x)$ un polynôme de degré n, on définit son polynôme réciproque par :

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

Proposition 3.2.2.
Soit C un code cyclique de dimension K engendré par le polynôme $g(x)$ de degré r, le code $C^\perp$ dual de C est un code cyclique engendré par

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

avec

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

Si $C(n.k)$ un code cyclique de polynôme générateur $g(x)$. Le code dual $C^\perp$ de C est un $(n.n-k)$ code cyclique de polynôme générateur

$$h^\perp = x^{\deg h}(h \circ x^{-1}) = x^{\deg h} h(x^{-1})$$

Exemple 3.2.3.
Considérons le code binaire $C(7,4)$ généré par $g(x) = x^3 + x + 1$ sa matrice génératrice est composée à partir du polynôme générateur
$g(x) = g_0 + g_1 x + g_2 x^2 + ... + g_k x^k$

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

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

Calculer la matrice de contrôle à partir de la matrice générateur n'est pas en général aisé, par contre, on peut facilement trouver le polynôme de contrôle $h(x)$, qui est
Tel que :

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

et donc

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

et la matrice de contrôle correspondant est

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

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

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

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

Qui correspondant au mot code $c_0c_1c_2c_3c_4c_5c_6 = 0100011$.

Exemple 3.2.4.
Soit C *un code cyclique de polynôme générateur*
$g(x) = x^3+x+1$ *et de longeur* 7
$h(x) = \dfrac{x^7-1}{g(x)} = x^4+x^2+x+1$
Le code dual $C^\perp$ *de* C *est un.* $(7, 7-4)$ *code cyclique de polynôme générateur.*
$h^\perp = x^{\deg h}h(x^{-1}) = x^4+x^3+x^2+1$.

3.3 Factorisation de $x^{2p}-1$ sur $\mathbb{F}_q$

Pour traiter les codes cycliques de longeur $2p$ sur un corps fini $\mathbb{F}_q$, nous devons étudier la factorisation de $x^{2p}-1$ sur $\mathbb{F}_q$
Dans [11] les auteurs étudient la factorisation de $x^{2p^n}-1$ sur $\mathbb{F}_q$ où p et q sont des nombres premiers impairs distincts et $p-1$ l'ordre multiplication de q modulo $2p^n$. Dans cette section, nous considérons la factorisation compléte de $x^{2p}-1$ sur $\mathbb{F}_q$

Proposition 3.3.1.
Soit $\mathbb{F}_q$ *le corps fini à* q *éléments et* p *un nombre premier impair premier avec* q. *Soit* $2p = q^m-1$, *avec* $m = ord_{2p}(q)$, *alors*
$x^{2p}-1 = \prod_{s\in\{0,1,2,p\}} m_s(x)$
avec

$$\begin{aligned} m_0(x) =& x-1 \\ m_p(x) =& x+1 \\ m_1(x) =& x^{p-1}-x^{p-2}+\ldots-x+1 \\ m_2(x) =& x^{p-1}+x^{p-2}+\ldots+x+1 \end{aligned}$$

Exemple 3.3.1.
Prendre $q = 7$, $p = 11$, *alors*
$x^{22} - 1 = \prod_{s\in\{0,1,2,11\}} m_s(x)$
avec

$$\begin{aligned} m_0(x) =& x - 1 \\ m_{11}(x) =& x + 1 \\ m_1(x) =& x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ m_2(x) =& x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 \end{aligned}$$

Le polynôme générateur et la dimension de quelques codes cycliques de longeur 22.

Code	C_0	C_{11}	C_1	C_2
Polynôme génerateur	$m_0(x)$	$m_{11}(x)$	$m_1(x)$	$m_2(x)$
Dimension	21	21	12	12

CONCLUSION

Nous avons présenté dans ce travail une étude sur les codes cycliques de longeur $2p$ sur un corps fini $\mathbb{F}_q$ où p et q sont des nombres premiers impairs distincts et $p-1$ l'ordre multiplicatif de q modulo $2p$.

ملخص

ليكن $\mathbb{F}_q$ الحقل المنتهي ذو q عنصرا ، في هذا العمل نهتم بالمثاليات لحلقة حاصل القسمة

$$R_{2p} = \frac{\mathbb{F}_q[x]}{(x^{2p}-1)}$$

هذه المثاليات تمثل الشفرة الدورية التي طولها $2p$.

RESUMÉ

Soit $\mathbb{F}_q$ le corps fini à q éléments , dans ce travail on s'ntéresse aux idéaux de l'anneau quotient

$$R_{2p} = \frac{\mathbb{F}_q[x]}{(x^{2p}-1)}$$

ces idéaux repésentent les codes cycliques de longeur $2p$.

ABSTRACT

Let $\mathbb{F}_q$ be the finite field with q elements , in this work we are intersted with the ideals of the quotient ring

$$R_{2p} = \frac{\mathbb{F}_q[x]}{(x^{2p}-1)}$$

these ideals represent cyclic codes of length $2p$.

Bibliographie

[1] **F.Z.Benhamed :** Les polynômes en cryptographie,These de Doctorat , *université de Alger* 2019.

[2] **S.Damma et A.Lia :** Sur les décodage d'un code cyclique, Mémoire de master, *université de* M^{ed} *Boudiaf m'sila,* 2018-2019.

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

[4] **L.Heboub :** Etude de techniques décodage des codes lineaires, Mémoire présente pour l'obtention du diplôme du magistér, *université* M^{ed} *Boudiaf m'sila,* 2009.

[5] **L . Houchi :** Sur les polynômes irréductibles, Mémoire de master, *université de* M^{ed} *Boudiaf m'sila,* 2017 - 2018.

[6] **M.Khalfa et S.Saai :** Sur les codes cycliques sur un corps fini, Mémoire de master, *université de* M^{ed} *Boudiaf m'sila,* 2020 - 2021.

[7] **C.Kouidri et K.Hamza :** Sur les idempotents primitifs des codes cycliques irréductibles, Mémoire de master, *université de* M^{ed} *Boudiaf m'sila,* 2019 - 2020.

[8] **S . Lahoula :** Sur le cryptosystéme asymetrique de Niederreiter basé sur les codes cycliques, Mémoire de master, *université de jijle,* 2017.

[9] **C. Mihoubi :** Classifcation 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.

[10] **O.Moussai :** Codes cycliques optimaux de rendement $1/2$ sur F_2, Mémoire de master, *université de* M^{ed} *Boudiaf m'sila,* 2012-2013.

[11] **M.Pruthi et S.K.Arora :** Minimal cyclic codes of length $2p^n$, Finite Fields App.5 (2)(1999) 177-187.

[12] **A.Regouid et M.Bahache :** Sur les codes cycliques minimaux .Mémoire de Master, *université de* M^{ed} *Boudiaf m'sila,* 2016 - 2017.