RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ MOHAMED BOUDIAF - M'SILA
FACULTÉ DE MATHÉMATIQUES ET DE L'INFORMATIQUE
DÉPARTEMENT DE MATHÉMATIQUES

N° d'ordre : .....

T H È S E

Présentée pour l'obtention du diplôme
de Doctorat en sciences

Spécialité

Mathématiques

Option

Mathématiques discrètes

Par

Lakhdar Heboub

Thème

Sur les codes cycliques maximaux de longueur n

Soutenue le 21/12/2023 devant le jury composé de :

A. Boudaoud	Prof	Université de M'sila	Président
D. Mihoubi	Prof	Université de M'sila	Encadreur
K. Saadaoui	M.C.A	Université de M'sila	Examinateur
L. Noui	Prof	Université de Batna	Examinateur
S. Milles	M.C.A	Centre universitaire de Barika	Examinateur
D. Bellaouar	M.C.A	Université de Guelma	Examinateur
N. Ghadbane	M.C.A	Université de M'sila	Invité

Année Universitaire : 2023/2024

PEOPL'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY OF MOHAMED BOUDIAF / M'SILA
FACULTY OF MATHEMATICS AND COMPUTER SCIENCES
DEPARTMENT OF MATHEMATICS

THESIS

Presented for obtaining the degree of Doctor of Science

Speciality: Mathematics
Option: Discrete Mathematics

Heboub Lakhdar

On maximal cyclic codes of length n

Thesis defended publicly on : 21 / 12 / 2023, before a jury composed of :

A. Boudaoud	Prof	University of M'sila	Chair
D. Mihoubi	Prof	University of M'sila	Supervisor
K. Saadaoui	Dr	University of M'sila	Examiner
L. Noui	Prof	University of Batna	Examiner
S. Milles	Dr	University Center of Barika	Examiner
D. Bellaouar	Dr	University of Guelma	Examiner
N. Ghadbane	Dr	University of M'sila	Invite

Abstract

This work focuses on the theory of error-correcting codes, specifically the investigation of maximal cyclic codes. A cyclic code of length n over the finite field $\mathbb{F}_q$ can be defined as a principal ideal of the quotient ring $R_n = \mathbb{F}_q[x]/(x^n - 1)$ where $\mathbb{F}_q[x]$ represents the ring of polynomials with coefficients in the finite field $\mathbb{F}_q$ and $(x^n - 1)$ denotes the principal ideal generated by the polynomial $x^n - 1$.

The main objective of this thesis is to explore maximal ideals within the quotient ring R_n, as these ideals correspond to maximal cyclic codes of R_n.

Keywords: Linear and cyclic codes, Minimal and maximal cyclic codes, LCD cyclic codes.

Résumé

Ce travail se concentre sur la théorie des codes correcteurs d'erreurs, et plus particulièrement sur l'étude des codes cycliques maximaux. Un code cyclique de longueur n sur le corps fini $\mathbb{F}_q$ peut être défini comme un idéal principal de l'anneau quotient $R_n = \mathbb{F}_q[x]/(x^n - 1)$ où $\mathbb{F}_q[x]$ représente l'anneau des polynômes à coefficients dans le corps fini $\mathbb{F}_q$ et $(x^n - 1)$ désigne l'idéal principal engendré par le polynôme $x^n - 1$.

L'objectif principal de cette thèse est d'explorer les idéaux maximaux dans l'anneau quotient R_n, car ces idéaux correspondent aux codes cycliques maximaux de R_n.

Mots clés: Codes linéaires et cycliques, Codes cycliques minimaux et maximaux, Codes cycliques LCD.

Acknowledgements

I would first like to thank Mr Mihoubi Douadi, my supervisor, for having accepted to direct this work as well as for his advices.

I thank the members of the jury who accepted to judge my work. Mr A. BOUDAOUD, who did chairing this jury, Mr. L. NOUI, Mr.S. Milles, Mr.D. Bellaouar, Mr.K. Saadaoui and Mr. N. Ghadbane for having accepted to be examiners of this thesis and for the interest they have shown in it.

I cannot forget to thank Professors of the Institute of Mathematics for their support.

I would like to express here my gratitude to all those who were involved in this work, directly or indirectly.

Finally, i would like to thank my family and friends for their support during these years.

Notations

$\mathbb{N}$: Set of natural numbers.

$\mathbb{Z}$: Set of integer numbers.

$\mathbb{Z}/n\mathbb{Z}$: Quotient group of $\mathbb{Z}$ modulo n.

$\mathbb{F}_q$: The finite field of order q.

$K(M)$: The extension of K obtained by adjoining M.

$[L : K]$: The degree of the field L over K.

$\gcd(a, b)$: The greatest common divisor of a and b.

$\operatorname{lcm}(a, b)$: The least common multiple of a and b.

$d(x, y)$: The Hamming distance between x and y.

$w(x)$: The Hamming weight of x.

$C^{\perp}$: The dual code of C.

LCD : Linear codes with complementary duals.

$\mathbb{F}_q^*$: The multiplicativc group of nonzero elements of $\mathbb{F}_q$.

(a) : The principal ideal generated by a.

$\mathbb{F}_q[x]$: The polynomial ring over the finite field $\mathbb{F}_q$.

$\varphi(n)$: Euler's function of n.

A^T : The transpose of the matrix A.

$\det(A)$: The determinant of the matrix A.

$a \equiv b (\operatorname{mod} n)$: a is congruent to b modulo n.

$a \mid b$: a divides b.

$\deg(f)$: The degree of the polynomial f.

f^* : The reciprocal polynomial of f.

Table of contents

Introduction

In his paper "A Mathematical Theory of Communication" published in 1948, Claude Shannon introduced the field of coding theory and made significant contributions to the understanding of reliable communication in the presence of noise.
Error-correcting codes play an important role in improving reliability of transmissions over noisy channels. Since an important problem in coding theory revolves around the construction of error-correcting codes, it is necessary to study cyclic codes, which are a class of codes with desirable properties.

Let $\mathbb{F}_q$ be a finite field of order q and n be a positive integer coprime to q. The minimal cyclic codes of length n over $\mathbb{F}_q$ are viewed as minimal ideals of the principal quotient ring $R_n = \mathbb{F}_q[x]/(x^n - 1)$, also the maximal cyclic codes of length n over $\mathbb{F}_q$ are viewed as maximal ideals of the principal quotient ring R_n.
The construction of minimal cyclic codes involves finding generator polynomials that satisfy specific properties, such as having roots that are primitive.
On the other hand, maximal cyclic codes are characterized by having generator polynomials that are irreducible over the finite field.

In the paper [3], the authors S.K. Arora and M. Pruthi investigated in the computation of the minimal cyclic codes of length $2p^n$ with $n \geq 1$ is integer over the finite fields $\mathbb{F}_q$ where q is a power of an odd prime number and $\gcd(p, q) = 1$. The authors obtains $2n + 2$ q-cyclotomic cosets modulo $2p^n$. In this work, we determine in the special case $n = 1$ and q is an odd prime, the minimal cyclic codes and the maximal cyclic codes of length $2p$ over $\mathbb{F}_q$, whith $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$.
We show every cyclic code is a direct sum of some minimal cyclic codes.

Linear code with a complementary-dual (LCD) over finite fields was defined in [10] to be a linear code C satisfying $C_1 \cap C^{\perp} = \{0\}$ were first introduced and studied by Massey in 1964 and they were called reversible codes, Yang and Massey [41] gave a necessary and sufficient condition for a cyclic code to have a complementary dual.is that the generator polynomial $g(x)$ is self-reciprocal and any irreducible factor of $g(x)$ has the same multiplicity in $g(x)$ as in $x^n - 1$, Our work focuses on the determination of LCD cyclic codes over the finite field $\mathbb{F}_q$ in certain cases.

This document is structured into four chapters. The first chapter serves as a review and recall of the essential concepts and notations that will be used throughout the subsequent chapters. It covers some generalities about number theory, provides a foundation in abstract algebra, and introduces the concepts of finite fields and polynomials.

Chapter 2 we briefly present the theory of error-correcting codes, and we describe the cyclic linear codes, we delves into the briefly study of two significant families of cyclic codes: BCH codes and quadratic residue codes.
Then we describe a special kind of idempotents, called primitive idempotents, that, once known, will produce all the idempotents in R_n and therefore all the cyclic codes, they play a fundamental role in the theory and construction of cyclic codes, enabling us to explore their properties.

Chapter 3 is about some classes of cyclic codes over finite fields of length $N = 2p$ with p is an odd prime. More precsely,is about the minimal and maximal cyclic codes of length $2p$ over the finite field $\mathbb{F}_q$ whith p is an odd prime, over the finite fields $\mathbb{F}_q$ of q elements, where q is an odd prime distinct from p and $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$, i.e., $q^{p-1} \equiv 1 (\mathrm{mod}\, 2p)$.
At the end of this chapter, we focus into the relationship between the maximal and minimal cyclic codes, where we saw in particular every maximal cyclic code of length $2p$ over $\mathbb{F}_q$, is a direct sum of three minimal cyclic codes.

Chapter 4 focuses on the structure of LCD cyclic codes over the finite field $\mathbb{F}_q$. Specifically, we aim to determine two classes of LCD cyclic codes of length $2p$ over $\mathbb{F}_q$, where p and q are distinct odd primes and $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$. Additionally, we explore the relationship between these classes of codes.

Chapter 1

Preliminaries

1.1 Introduction

In this chapter we recall the essential concepts and notations that will be used throughout the subsequent chapters. It covers some generalities about number theory, provides a foundation in abstract algebra, and introduces the concepts of finite fields and polynomials. For more information see for example, [10], [21] and [37].

1.2 Notions of number theory

1.2.1 Definitions and recalls

For more details, we refer the reader to references on the subject, such as [1].

Definition 1.2.1 *Let $n \geq 1$, The Euler function $\varphi(n)$ is defined as the number of positive integers not exceeding n that are relatively prime to n, i.e.,*

$$\varphi(n) = |\{i \mid 1 \leq i \leq n, \gcd(i, n) = 1\}|.$$

Notice that $\varphi(1) = 1$.
Every integer less than the prime number n is relatively prime to it, then

$$\varphi(n) = n - 1.$$

Example 1.2.1

n :	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$:	1	1	2	2	4	2	6	4	6	4

Table 1.1: Some values of $\varphi(n)$.

We recall some properties of $\varphi(n)$.

Theorem 1.2.1 *Euler's function φ has the following properties:*

(1) *If p is a prime and $k \geq 1$, then*

$$\varphi(p^k) = p^k - p^{k-1}.$$

(2) *The function φ is a multiplicative function, i.e., if $\gcd(p,q) = 1$, then*

$$\varphi(pq) = \varphi(p)\varphi(q).$$

(3) *For each positive integer $n \geq 1$*

$$\varphi(n) = n \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

(4) *For each positive integer*

$$n \geq 1, \ \sum_{d|n} \varphi(d) = n.$$

Example 1.2.2 *a) The decomposition of* 360 *is* $2^3 \cdot 3^2 \cdot 5$, *then according to the Theorem* 1.2.1

$$\begin{aligned} \varphi(360) &= 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) \\ &= 360.\frac{1}{2}.\frac{2}{3}.\frac{4}{5} = 96. \end{aligned}$$

b) $\sum_{d|8} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(8) = 1 + 1 + 2 + 4 = 8.$

Theorem 1.2.2 ***(Euler-Fermat)*** *Let a and n be two nonzero positive integers.*
If $\gcd(a,n) = 1$, *then* $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$.

1.2.2 Primitive roots

Let a and n be two positive nonzero integers.

Definition 1.2.2 *Let $n \in \mathbb{N}^*$ and $\gcd(a,n) = 1$. The order of a modulo n is the smallest positive integer k such that*

$$a^k \equiv 1 (\mathrm{mod}\, n)$$

and is noted $ord_n(a)$.

Remark 1.2.1 *If $n > 1$, the order $ord_n(a)$ of a modulo n is the order in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$.*

Example 1.2.3 *$ord_7(2) = 3$ since $2^3 \equiv 1(\mathrm{mod}\, 7)$ while $2^1 \equiv 2(\mathrm{mod}\, 7)$ and $2^2 \equiv 4(\mathrm{mod}\, 7)$.*

Definition 1.2.3 *If $\gcd(a,n) = 1$ and a is of order $\varphi(n)$ modulo n, then a is a primitive root of the integer n.*

Example 1.2.4 *It is easy to see that 3 is a primitive root of 7, for*

$$3 \equiv 3 \quad 3^2 \equiv 2 \quad 3^3 \equiv 6 \quad 3^4 \equiv 4 \quad 3^5 \equiv 5 \quad 3^6 \equiv 1 (\mathrm{mod}\, 7).$$

Corollary 1.2.1 *If n has a primitive root, then it has exactly $\varphi(\varphi(n))$ of them.*

Theorem 1.2.3 *There exists a primitive root modulo m $(m > 1)$ if and only*

$$m = 2, 4, p^k \text{ or } 2p^k,$$

where p is an odd prime.

1.2.3 Quadratic Residues

Definition 1.2.4 *Let p be an odd prime coprime to the integer a. If the quadratic congruence $x^2 \equiv a(\mathrm{mod}\ p)$ has a solution, then a is said to be a quadratic residue of p. Otherwise, a is called a quadratic nonresidue of p.*

Example 1.2.5 *Let* $p = 11$. *To find the integers* $1, 2, ..., 10$ *are quadratic residues of* 11, *we must know which of the congruences*

$$x^2 \equiv a(\mathrm{mod}\, p)$$

has a solution when a runs through the set $\{1, 2, ..., 10\}$. *Modulo*11, *the squares of the integers* $1, 2, 3, ..., 10$ *are*

$$\begin{aligned} 1^2 &\equiv 10^2 \equiv 1; \\ 2^2 &\equiv 9^2 \equiv 4; \\ 3^2 &\equiv 8^2 \equiv 9; \\ 4^2 &\equiv 7^2 \equiv 5; \\ 5^2 &\equiv 6^2 \equiv 3. \end{aligned}$$

Then, the quadratic residues of 11 *are* $1, 3, 4, 5, 9$, *and the nonresidues are* $2, 6, 7, 8, 10$.

Theorem 1.2.4 *Let* p *be an odd prime. Then every reduced residue systeme* $\mathrm{mod}\, p$ *contains exaxtly* $(p-1)/2$ *quadratic residues and exaxtly* $(p-1)/2$ *quadratic nonresidues* $\mathrm{mod}\, p$. *The quadratic residues belong to the residue classes containing the numbers* $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$.

Euler devised a simple criterion for deciding whether an integer a is a quadratic residue of a given prime p.

Theorem 1.2.5 ***Euler's criterion***. *Let* p *be an odd prime and* $\gcd(a, p) = 1$. *Then* a *is a quadratic residue of* p *if and only if* $a^{(p-1)/2} \equiv 1(\mathrm{mod}\, p)$.

Corollary 1.2.2 *Let* p *an odd prime and* $\gcd(a, p) = 1$. *Then* a *is a quadratic residue or nonresidue of* p *according to whether*

$$a^{(p-1)/2} \equiv 1(\mathrm{mod}\, p) \text{ or } a^{(p-1)/2} \equiv -1(\mathrm{mod}\, p).$$

Example 1.2.6 *If* $p = 11$, *we find that*

$$2^{(11-1)/2} = 2^5 \equiv -1(\mathrm{mod}\, 11).$$

Hence, by the last corollary the integer 2 *is a quadratic nonresidue of* 11.

1.3 Some basis of abstract algebra

1.3.1 Maximal elements of a family

In this part, we consider a finite field $\mathbb{F}_q$ (not necessarily $\mathbb{F}_2$ or an extension) and an integer $n \geq 1$. Let $\mathcal{L}$ be a family of subsets of $\mathbb{F}_q^n$, we impose that $\mathbb{F}_q^n \in \mathcal{L}$.
We define in this family the most natural order relation, the relation of inclusion $\subset$. We thus obtain a partially ordered family $(\mathcal{L}, \subset)$.

Definition 1.3.1 *Let C be an element of $\mathcal{L} \setminus \{\mathbb{F}_q^n\}$. The element C is called a maximal element of $\mathcal{L}$ if:*

$$(C \subset D \text{ et } D \in \mathcal{L}) \Rightarrow (D = C \text{ ou } D = \mathbb{F}_q^n).$$

In the other words, C is a maximal element of $\mathcal{L}$ if there is no element between C and $\mathbb{F}_q^n$ in $(\mathcal{L}, \subset)$.

Example 1.3.1 *Let C_i be a subset of $\mathbb{F}_q^n$ for $1 \leq i \leq 6$, according to the definition of maximal elements, these are exactly those which are framed (C_1, C_2, C_3). They are on the last level before $\mathbb{F}_q^n$*

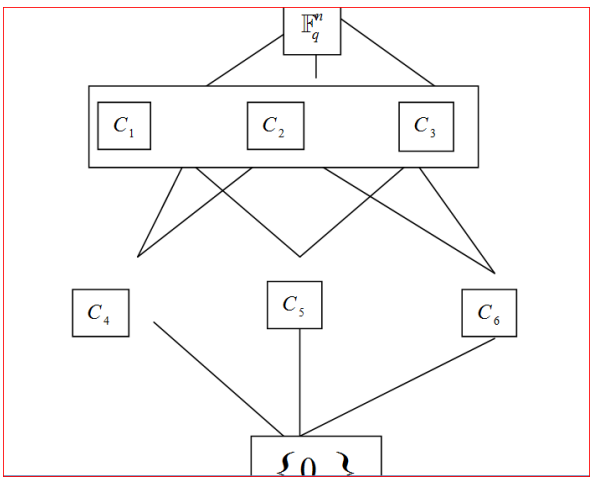

Figure 1.1: Example of a family structure.

This diagram can be read as follows: an element C is related to an element D placed higher up if and only if $C \subset D$. In this example, we see that

$$\{0\} \subset C_4 \subset C_1 \subset \mathbb{F}_q^n.$$

1.3.2 Maximal and prime ideals

Let R be a commutative ring.

Definition 1.3.2 *An ideal in R is maximal if it is a maximal element in the set of ideals in R distinct from R is ordered by inclusion. In other words, I is a maximal ideal if $I \neq R$, and if J is an ideal in R with $I \subset J$, then $I = J$, or $J = R$.*

Definition 1.3.3 *An ideal P in R with $P \neq R$ is a prime ideal if whenever $ab \in P$ with a, $b \in R$ then either $a \in P$ or $b \in P$.*

Definition 1.3.4 *An element $a \in R$ is prime if it is nonzero, non-invertible and satisfies*

$$a \mid bc \Rightarrow a \mid b \text{ or } a \mid c.$$

Theorem 1.3.1 *A nonzero element a of in R is prime if and only if the ideal (a) is prime.*

Definition 1.3.5 *Let R be an integral ring. An element a in R is irreducible if it is nonzero, non-invertible and if its only divisors are the trivial divisors.*

Theorem 1.3.2 *Let I be an ideal of a commutative ring R. Then.*

1) *The ring R/I is an integral if and only if is I a prime ideal.*

2) *The ring R/I is a field if and only if I is a maximal ideal.*

3) *Every maximal ideal is prime.*

Proposition 1.3.1 *Let R be a principal ring. If a is a nonzero element, then following conditions are equivalent;*

1) *The element a is irreducible.*

2) *The ideal (a) is prime.*

3) *The ideal (a) is maximal.*

1.4 Finite fields and polynomials

Finite fields indeed play a fundamental role in the application of modern algebra to various domains, including telecommunications. A finite field, also known as a Galois field, is a

mathematical structure that consists of a finite set of elements along with operations such as addition, subtraction, multiplication, and division. These fields have a wide range of applications, and their use in telecommunications is particularly significant.

For more information see for example [14], [20] and [37].

1.4.1 Finite fields as vector spaces

Definition 1.4.1 *Let K be a field and $\mathbb{F}$ be a subfield of K. Then K is called an extension of the field $\mathbb{F}$, we write $\mathbb{F} < K$.*

We can regarded K as a vector space over $\mathbb{F}$. The dimension of the vector space K over $\mathbb{F}$ is called the degree of the extension K of $\mathbb{F}$ and is denoted by $[K : \mathbb{F}]$. The extension $\mathbb{F} < K$ is called a finite extension if the degree $[K : \mathbb{F}]$ is finite.

Lemma 1.4.1 *Let K be a finite extension of finite field $\mathbb{F}$ with $d = [K : \mathbb{F}]$.*
Then $|K| = |\mathbb{F}|^d$.

Theorem 1.4.1 *Suppose $\mathbb{F}$ is a finite field of characteristic p. Then $\mathbb{F}$ contains p^n elements:*

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

Corollary 1.4.1 *The group $\mathbb{F}^*$ of nonzero elements of a fiinite field $\mathbb{F}$ is cyclic.*

A finite field is called a Galois field and if $\mathbb{F}$ is a field of order q, we write $\mathbb{F} = \mathbb{F}_q$.

Definition 1.4.2 *A generator of the cyclic group $\mathbb{F}_q^*$ of the finite field $\mathbb{F}_q$ is called a primitive element of $\mathbb{F}_q$.*

Definition 1.4.3 *An element α in a finite field $\mathbb{F}_q$ is called a primitive element (or generator) of $\mathbb{F}_q$ if*

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

Proposition 1.4.1 *Let F_i be a subspace of the vector space $\mathbb{F}_q^n$ for $i = 1$ and 2. Then the sum $F_1 + F_2$ is direct, if and only if*

$$F_1 \cap F_2 = \{0\}.$$

Proposition 1.4.2 *Let F_i be a subspace of the vector space $\mathbb{F}_q^n$ for $i \in \{1,2,3\}$. Then $F_1 + F_2 + F_3$ is a direct sum if and only if*

$$\dim(F_1 + F_2 + F_3) = \dim(F_1) + \dim(F_2) + \dim(F_3).$$

1.4.2 Polynomials over a finite field

Definition 1.4.4 *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial over $\mathbb{F}_q$ with a_n and a_0 are nonzero. The reciprocal $f^*(x)$ of $f(x)$ is defined by*

$$f^*(x)) = a_0^{-1} x^n f(x^{-1}).$$

Proposition 1.4.3 *Let $h(x), f(x) \in \mathbb{F}_q[x]$. Then*

$$(h(x)f(x))^* = h^*(x)f^*(x).$$

Definition 1.4.5 *(**Irreducible Polynomials**) A polynomial $f(x)$ is irreducible in $\mathbb{F}_q[x]$ if $f(x)$ cannot be factored into a product of lower degree polynomials in $\mathbb{F}_q[x]$.*

Theorem 1.4.2 *Let $p(x)$ be a polynomial over a field $\mathbb{F}$ of degree ≥ 1. Then $\mathbb{F}[x] \diagup (p(x))$ is a field if and only if $p(x)$ is irreducible.*

Definition 1.4.6 *Any extension field of $\mathbb{F}_q$ in which $f(x)$, a polynomial over $\mathbb{F}_q$, factors into linear and constant terms is called a splitting field of $f(x)$.*

Theorem 1.4.3 *(**Fundamental Theorem of Algebra**). A polynomial $f(x)$ of degree n over $\mathbb{F}_q$ has at most n zeros.*

Minimal polynomials

In this part we are interested in nonzero polynomials $f(x) \in \mathbb{F}_q[x]$ of the least degree such that $f(\alpha) = 0$, where $\mathbb{F}_q$ be a subfield of $\mathbb{F}_r$, for an element α of $\mathbb{F}_r$.
Let $\mathbb{F}_r$ be a finite extension field of $\mathbb{F}_q$. Then $\mathbb{F}_r$ is a vector space over $\mathbb{F}_q$ and so $\mathbb{F}_r = \mathbb{F}_{q^m}$ for some positive integer m.

Definition 1.4.7 *A minimal polynomial of an element $\alpha \in \mathbb{F}_{q^m}$ is a nonzero monic polynomial $f(x)$ of the least degree in $\mathbb{F}_q[x]$ such that $f(\alpha) = 0$.*

Theorem 1.4.4 *Let $p(x)$ be a polynomial in $\mathbb{F}_q[x]$ and let α be a root of $p(x)$ in some extension field $\mathbb{F}_{q^m}$. Then:*
(1) $p(x^q) = p(x)^q$, *and*
(2) α^q *is also a root of* $p(x)$ *in* $\mathbb{F}_q$.

Proof. For the proof of this theorem, one can see $[14, p.114]$ ■

If we apply this theorem repeatedly, we find that $\alpha, \alpha^q, \alpha^{q^2}, ...$ are all roots of minimal polynomial of α. The sequence $\alpha, \alpha^q, \alpha^{q^2}, ...$ will stop after d terms, where $\alpha^{q^d} = \alpha$.
Based on this, we define the equivalence relation on the set

$$S = \{0, 1, 2..., n-1\}$$

as follows

$$\text{for } a, b \in S, a \sim b \Leftrightarrow a \equiv bq^i (\text{mod}\, n)$$

for some integer $i \geq 0$, this is an equivalence relation on the set S and partitions S into q-cyclotomic cosets.

Definition 1.4.8 *The q-cyclotomic cosets modulo n is the set*

$$C_s := \{s, sq, sq^2, ..., sq^{n_s-1}\} \ \text{mod}\, n,$$

where n_s is the smallest positive integer such that $sq^{n_s} \equiv s (\text{mod}\, n)$.

1.4.3 Factorization of $x^n - 1$ over finite field $\mathbb{F}_q$

The following result will be useful when we study cyclic codes.
Let $\mathbb{F}_q$ be a finite field and n be a positive integer with $\gcd(n, q) = 1$. To factor $x^n - 1$ over $\mathbb{F}_q$, it is necessary to find an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ that contains all of its roots where m be a positive non-zero integer such that $n \mid q^m - 1$. In other words, $\mathbb{F}_{q^m}$ must contain a primitive $n - th$ root of unity.

Definition 1.4.9 *An element of $\mathbb{F}_{q^m}$ whose order divides n is called an $n-th$ root of unity over $\mathbb{F}_q$, and an element of $\mathbb{F}_{q^m}$ of order n is called a primitive $n-th$ root of unity over $\mathbb{F}_q$.*

In particular, if $n = q^m - 1$, a primitive $n - th$ root of unity over $\mathbb{F}_q$ is a primitive element of $\mathbb{F}_{q^m}$.

The $n-th$ roots of unity over $\mathbb{F}_q$ form a subgroup of $\mathbb{F}_{q^m}^*$. Since $\mathbb{F}_{q^m}^*$ is cyclic, this subgroup is also cyclic. If β is a generator of this subgroup which is of order n, this subgroup consists of all the roots of $x^n - 1$, *i.e.* the factorization of $x^n - 1$ over $\mathbb{F}_{q^m}$ is

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

Theorem 1.4.5 *Let $\mathbb{F}_q$ be a finite field and n be a positive integer with $\gcd(n, q) = 1$. Let $m = ord_n(q)$. Let α be a primitive $n - th$ root of unity in $\mathbb{F}_{q^m}$.*

(1) *For each integer s with $0 \leq s < n$, the minimal polynomial of α^s over $\mathbb{F}_q$ is*

$$m_s(x) = \prod_{j \in C_s} \left(x - \alpha^j\right)$$

where C_s is the q-cyclotomic coset of s modulo n.

(2) *Furthermore,*

$$x^n - 1 = \prod_s m_s(x)$$

is the decomposition of $x^n - 1$ into irreducibles over $\mathbb{F}_q$, where s runs through a set of representatives of the q-cyclotomic cosets modulo n.

Example 1.4.1 *Consider the polynomial $x^7 - 1$ over finite field $\mathbb{F}_2$. Snce $7 = 2^3 - 1$, the splitting field for $x^n - 1$ is $\mathbb{F}_{q^m} = \mathbb{F}_{2^3} = \mathbb{F}_8$, the cyclotomic cosets of 2 modulo 7are:*

$$C_0 = \{0\},\ C_1 = \{1, 2, 4\} = C_2,\ C_3 = \{3, 5, 6\}.$$

Then the three minimal pylonomials are:

$$\begin{aligned} m_0(x) &= x - 1, \\ m_1(x) &= \prod_{j \in C_1} \left(x - \alpha^j\right) = (x - \alpha)\left(x - \alpha^2\right)\left(x - \alpha^4\right), \\ m_2(x) &= \prod_{j \in C_3} \left(x - \alpha^j\right) = \left(x - \alpha^3\right)\left(x - \alpha^5\right)\left(x - \alpha^6\right). \end{aligned}$$

To find the coefficients of $m_1(x)$ et $m_2(x)$ we calculate in $\mathbb{F}_8$. Since $8 = 2^3$, we consider an irreducible binary polynomial of degree 3, for example $f(x) = x^3 + x + 1$.If α is a primitive

root of $f(x) = x^3 + x + 1$, *then* $f(\alpha) = 0$.

So we have:

$$\begin{aligned}
\alpha^3 &= \alpha + 1, \\
\alpha^4 &= \alpha^2 + \alpha, \\
\alpha^4 &= \alpha^2 + \alpha, \\
\alpha^5 &= \alpha^2 + \alpha + 1, \\
\alpha^6 &= \alpha^2 + 1, \\
\alpha^7 &= 1.
\end{aligned}$$

Then

$$m_1(x) = (x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right) = x^3 + \left(\alpha+\alpha^2+\alpha^4\right)x^2 + \left(\alpha^3+\alpha^5+\alpha^6\right)x + \alpha^7 = x^3 + x + 1,$$

and in the same way we find

$$m_2(x) = x^3 + x^2 + 1.$$

So

$$\begin{aligned}
x^7 - 1 &= \prod_{s\in\{0,1,2\}} m_s(x) = (x-1)\, m_1(x) m_2(x) \\
&= (x-1)\left(x^3+x+1\right)\left(x^3+x^2+1\right).
\end{aligned}$$

Chapter 2

On coding theory

2.1 Introduction

Coding theory, also known as the theory of error-correcting codes, exemplifies the practical application of abstract algebra. It has a many applications, from ensuring the clear transmission. Abstract algebra provides a framework for understanding codes and their properties, employing concepts such as matrices, polynomials, their roots, and shift registers.
The theory of error-correcting codes originated in 1948 with the paper of Claude Shannon, and it has since developed into a variant field.

This chapter serves as an introduction to the fundamental concepts of block codes. It discusses the properties of linear codes, introduces the concept of cyclic codes, and includes material on special cyclic codes.
This chapter help also to study the properties and characteristics of primitive idempotents and their role in generating cyclic codes. It discusses methods for determining and utilizing these idempotents in the context of coding theory. For more details, we refer the reader to references on the subject such as [27], [37] , [38] and [14].

2.2 General information on the theory of codes

In a communication process, we have three entities involved: the sender, the receiver and the transmission channel.

To send a message, it must first be encoded. Encoding is the process of converting the information into another acceptable format for transmission. Decoding is the reverse process; it allows the information to be interpreted.

Let Q be an alphabet with q distinct symbols. A code is called a block code if the coded information can be divided into blocks of n symbols. These blocks are the codewords of length n, generally we take Q the finite field $\mathbb{F}_q$ with q elements.

Let $n \in \mathbb{N}^*$, and q a power of a prime number p. Let $\mathbb{F}_q$ the finite field with q elements then $\mathbb{F}_q^n$ denote of all vectors or sequences of length n over $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(a_1, a_2, ..., a_n) \mid a_i \in \mathbb{F}_q,\ i = 1, ..., n\}.$$

Definition 2.2.1 *Let $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_q^n$ and $y = (y_1, y_2, ..., y_n) \in \mathbb{F}_q^n$. The Hamming-distance $d(x, y)$ of x and y is defined by*

$$d(x, y) = |\{i \mid 1 \leq i \leq n, x_i \neq y_i\}|.$$

The Hamming weight $\omega(x)$ of x is defined by

$$\omega(x) = d(x, 0).$$

(We always denote $(0, 0, ..., 0)$ by 0).
A code C over $\mathbb{F}_q$ is a part of $\mathbb{F}_q^n$, n is called length of C, code elements are called code words.

Definition 2.2.2 *The minimum distance of a code C is the smallest distance between distinct codewords, i.e.*

$$d = min\{d(x, y) | x, y \in C, x \neq y\}.$$

The minimum distance of a code is an important quantity as it characterises the code's correction capacity.

Theorem 2.2.1 *A code C with minimum distance d can detect $d - 1$ errors and correct $t = \left[\frac{d-1}{2}\right]$ errors.*

Example 2.2.1 *Consider the parity code where each word* $(c_1, c_2, ..., c_n)$ *is such that*

$$c_n = -\sum_{i=1}^{n-1} c_i.$$

For example, the binary parity code of length 4 *is given by*

$$C = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}.$$

2.3 Some concepts of linear codes

Let $\mathbb{F}_q$ the finite field with q elements where q is a prime power. Recall that $\mathbb{F}_q^n$ is a vector space over the field $\mathbb{F}_q$ characterized by their dimension n. In this section, we will consider that the messages we wish to transmit are an elements of $\mathbb{F}_q^k$ for some $k > 1$.

Definition 2.3.1 *A linear block code of length* n *and dimension* k *is a vector subspace of* $\mathbb{F}_q^n$.

Notation 2.3.1 *A linear code of length* n *and dimension* k *will be denoted as an* $[n, k]$ *code.*

Let C be an $[n, k]$ linear code. Since C is a vector subspace of $\mathbb{F}_q^n$ of dimension k over $\mathbb{F}_q$, then it can be represented by a base.
The linear code C has q^k codewords.

Example 2.3.1 *The binary code* $C = \{000, 001, 010, 011\}$ *is linear.*

The two most common ways to present a linear code are with either a generator matrix or a parity check matrix.

Definition 2.3.2 *If* C *is a linear code, then the minimum distance* d *of* C *is defined as*

$$d = min\{d(x, y)|x, y \in C, x \neq y\} = min\{\omega(x)|x \in C, x \neq 0\}.$$

This distance is usually denoted by d and so we speak of a $[n, k, d]$-code.

Example 2.3.2 *Consider the binary linear code* $C = \{0000, 1000, 0100, 1100\}$. *Because*

$$\begin{aligned} \omega(1000) &= 1; \\ \omega(0100) &= 1; \\ \omega(1100) &= 2. \end{aligned}$$

Then, $d = 1$.

Definition 2.3.3 *A generator matrix for an* $[n, k]$ *code* C *is any* $k \times n$ *matrix* G *whose rows form a basis for* C.

If $(c_1, c_2, ..., c_k)$ *is a basis of* C, *then* $G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$.

In general there are many generator matrices for a code.

Example 2.3.3 *Let* C *be a binary* $[3, 2]$ *code with generator matrix*

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

The codewords of C *are* $00.G = 000$, $01.G = 101$, $10.G = 011$, $11.G = 110$.

Definition 2.3.4 *A linear code of length* n, *dimension* k, *and minimum distance* d *is called an* (n, k, d)*code.*

In the following A^T is the transpose of the matrix A.

Definition 2.3.5 *Let* C *be a linear* $[n, k]$ *code over* $\mathbb{F}_q$. *An* $(n - k) \times n$ *matrix* H *with coefficients in* $\mathbb{F}_q$ *is called a parity check matrix of* C *if*

$$C = \left\{ x \in \mathbb{F}_q^n \mid Hx^T = 0 \right\}.$$

Thus, if G is a generator matrix of C, we have:

$$GH^T = 0.$$

It is then easy to construct a parity check matrix of a code from a generator matrix of that code.

Proposition 2.3.1 *If $G = [I_K \mid A]$ is a generator matrix for the $[n, k]$ code C in standard form, then $H = \left[-A^T \mid I_{n-k}\right]$ is a parity check matrix for C.*

Example 2.3.4 *Let C be a binary $[7, 4]$ code with generator matrix*

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

which is of course in standard form. The corresponding parity check matrix is

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

Let $b = (b_1, ..., b_n)$ and $c = (c_1, ..., c_n)$ be vectors in $\mathbb{F}_q^n$ the quantity

$$b.c^T = b_1 c_1 ... b_n c_n$$

denote the dot product of b and c over $\mathbb{F}_q^n$. If $b.c^T = 0$, then b and c are called orthogonal.

Definition 2.3.6 *Let C be a linear $[n, k]$ code over $\mathbb{F}_q$. The dual (orthogonal) code $C^\perp$ of C is defined by*

$$C^\perp = \{b \in \mathbb{F}_q^n : bc^T = 0 \ \forall c \in C\}.$$

Remark 2.3.1 1) *If G and H are generator and parity check matrices, respectively,for C, then H and G are generator and parity check matrices, respectively, for $C^\perp$.*
2) *$C^\perp$ est un $[n, n-k]-$code over $\mathbb{F}_q$.*

Proposition 2.3.2 ***(Singleton Bound).*** *For any linear $[n, k, d]$-code over $\mathbb{F}_q$, we have*

$$d \leq n - k + 1.$$

Proof. Let H be a parity-check matrix of a given linear $[n, k, d]$ code over $\mathbb{F}_q$. Then $n - k$ is the rank of H, and so any $n - k + 1$ columns of H are linearly dependent. Thus $d \leq n - k + 1$. ■

Remark 2.3.2 *A linear $[n, k, d]-$code over $\mathbb{F}_q$ with $d = n - k + 1$ is called an MDS code. Here MDS stands for "maximum distance separable".*

2.4 Algebraic coding theory

2.4.1 Cyclic codes

Cyclic codes over finite fields indeed play a vital role in the theory of error-correcting codes and have practical applications. These codes possess rich algebraic structures, which allow for efficient encoding and decoding operations.
In the context of coding theory, a linear code is defined as a subspace of a vector space. However, cyclic codes go one step further by introducing multiplication within the vector space. This is achieved by considering the elements of each vector as coefficients of polynomials. By treating the code vectors as polynomials, we can exploit the properties of polynomials with coefficients in a finite field to construct and analyze cyclic codes.

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power and $n \in \mathbb{N}^*$.

Definition 2.4.1 *The linear code C of length n over the finite field $\mathbb{F}_q$ is said to be cyclic if $(c_0, c_1, c_2, ..., c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_2, ..., c_{n-2}) \in C$.*

We can regard C as an ideal in the principal quotient ring $R_n := \mathbb{F}_q[x]/(x^n - 1)$. By identifying any vector $(c_0, c_1, c_2, ..., c_{n-1}) \in \mathbb{F}_q^n$ with

$$c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in R_n,$$

we note that since $x^n = 1$ in this factor ring, the shifted vector $(c_{n-1}, c_0, c_2, ..., c_{n-2})$ corresponds to the polynomial

$$x\left(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}\right) = c_{n-1} + c_0x + c_1x^2 \cdots + c_{n-2}x^{n-2}.$$

Under the correspondence between vectors and polynomials, as mentioned earlier, cyclic codes can be viewed as ideals of the quotient ring R_n. Conversely, ideals of R_n can be regarded as cyclic codes. Therefore, studying cyclic codes over $\mathbb{F}_q^n$ is equivalent to studying ideals in R_n.

Theorem 2.4.1 *A linear code C in $\mathbb{F}_q^n$ is cyclic if and only if C is an ideal in $R_n = \mathbb{F}_q[x]/\left(x^n - 1\right)$.*

Proof. If C is an ideal in $\mathbb{F}_q[x]/\left(x^n - 1\right)$ and $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ is any codeword, then $xc(x)$ is also a codeword, i.e., $(c_{n-1}, c_0, c_2, ..., c_{n-2}) \in C$.

Conversely, if C is cyclic, then for every codeword $c(x)$ the word $xc(x)$ is also in C. Therefore $x^ic(x)$ is in C for every i, and since C is linear $a(x)c(x)$ is in C for every polynomial $a(x)$. Hence, C is an ideal. ■

Since $\mathbb{F}_q[x]/\left(x^n - 1\right)$ is a principal ring every cyclic code C consists of the multiples of a polynomial $g(x)$ which is the monic polynomial of lowest degree (,i.e., not the zero polynomial) in the ideal.

Theorem 2.4.2 *Let C be a cyclic code of length n over $\mathbb{F}_q$. Then*
(1) *There exists a unique monic polynomial $g(x)$ of smallest degree in C.*
(2) *C generated by $g(x)$ and can be discribed by*

$$C = \{g(x)f(x) \mid f(x) \in R_n\}.$$

(3) *The dimension of C is $k = n - r$, where $r = deg(g(x))$.*
(4) *$g(x)$ divides $x^n - 1$ in $\mathbb{F}_q[x]$.*
(5) *Any element $c(x) \in C$ can be written uniquely as $c(x) = g(x)f(x)$ in $\mathbb{F}_q[x]$.*

Definition 2.4.2 *Let $C = \langle g(x) \rangle$ be a cyclic code of length n . Then $g(x)$ called the generator polynomial of C and $h(x) = \frac{(x^n-1)}{g(x)}$ is called the parity check polynomial of C.*

Since $g(x)$ is monic of degree $n-k$, the control polynomial $h(x)$ is monic of degree k. The cyclic codes of a given length n over $\mathbb{F}_q$ can be obtained by factoring x^n-1 over $\mathbb{F}_q$.

Example 2.4.1 *Let C_i be the cyclic code of length 7 ovr $\mathbb{F}_2$.*
Since x^7-1 over $\mathbb{F}_2$ have the factorization

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

The eight binary cyclic codes C_i of length 7 with generator polynomial $g_i(x)$ given in the following table

i	dim	$g_i(x)$
0	0	x^7-1
1	1	$(x^3+x+1)(x^3+x^2+1)=x^6+x^5+x^4+x^3+x^2+x+1$
2	3	$(x+1)(x^3+x+1)=x^4+x^3+x^2+1$
3	3	$(x+1)(x^3+x^2+1)=x^4+x^2+x+1$
4	4	x^3+x+1
5	4	x^3+x^2+1
6	6	$x+1$
7	7	1

Table 2.1

When constructing generator and parity-check matrices for cyclic linear codes, we can directly utilize polynomials over the finite field $\mathbb{F}_q$. Here's an overview of the process.

Theorem 2.4.3 *Let $g(x)$ be the generator polynomial of a cyclic code C of length n. If the degree of $g(x)$ is r, then the dimension of $C=\langle g(x)\rangle$ is $k=n-r$ and C has generator matrix*

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

Let

$$h(x) = h_0 + h_1 x + ... + h_k x^k$$

be the check polynomial of degree k for a cyclic codes C in R_n. Then

1) *A parity check for C is given by*

$$H = \begin{pmatrix} h_k & \dots & h_1 & h_0 & 0 & ... & 0 & 0 & 0 \\ 0 & h_k & ... & h_1 & h_0 & 0 & ... & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & 0 & h_k & \dots & h_1 & h_0 \end{pmatrix}.$$

2) *The dual code $C^{\perp}$ of C is a cyclic code of dimension r with a generator polynomial*

$$h^{\perp}(x) = x^k h(\frac{1}{x}) = h_k + h_{k-1}x + \ldots + h_0 x^k.$$

Example 2.4.2 *Consider the binary $[7,4]-$cyclic code with generator polynomial $g(x) = 1 + x + x^3$. Then this code has a generator matrix*

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ x^3 g(x) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Let $h(x)$ be the check polynomial of C. Then

$$h(x) = \frac{(x^7 - 1)}{g(x)} = x^4 + x^2 + x + 1$$

and the parity check for C is

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

To encode 0111 *using the polynomial product, we must multiply the polynomial*

$m(x) = x^3 + x^2 + x$ *by* $g(x) = 1 + x + x^3$. *We obtain*

$$\begin{aligned} c(x) &= m(x)\, g(x) = \left(x^3 + x^2 + x\right)\left(1 + x + x^3\right) \\ &= x^6 + x^5 + x = c_6 x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_5 x^5 + c_1 x + c_0, \end{aligned}$$

which corresponds to the code word

$$c_0 c_1 c_2 c_3 c_4 c_5 c_6 = 0100011.$$

Assume that $\gcd(n, q) = 1$ and denote $m = ord_n(q)$, i.e., m is the smallest positive integer such that $q^m \equiv 1 (\mathrm{mod}\, n)$. Let α be a generator of $\mathbb{F}_{q^m}^*$ and put $\beta = \alpha^{\frac{q^m - 1}{n}}$. Then β is a primitive $n - th$ root of unity.

Definition 2.4.3 *If C is cyclic code with generator polynomia $g(x)$, $Z = \left\{\beta^i \mid g\left(\beta^i\right) = 0\right\}$ is called the zero of C and $T = \left\{0 \le i \le n-1 \mid g\left(\beta^i\right) = 0\right\}$ is called the defining set of C, respectively.*

Property 1 *The dimension of C is $n - |T|$ as $|T|$ is the degree of $g(x)$.*

Property 2 *Let C is cyclic code with defining set T, then*

$$C = \left\{f(x) \bmod (x^n - 1) \mid f\left(\beta^i\right) = 0 \ \forall i \in T\right\}.$$

Proposition 2.4.1 *Let C_i be cyclic codes of length n over $\mathbb{F}_q$ with defining sets T_{C_i} for $i = 1, 2$.*

(a) The code $C_1 \cap C_2$ has defining set $T_{C_1} \cup T_{C_2}$.

(b) The code $C_1 + C_2$ has defining set $T_{C_1} \cap T_{C_2}$.

Proof. Let $g_{C_1}(x)$, $g_{C_2}(x)$ the generator polynomial of C_1, C_2 respectively, then we have

$$\begin{aligned} T_{C_1} \cup T_{C_2} &= \left\{i \mid g_{C_1}\left(\beta^i\right) = 0 \text{ or } g_{C_2}\left(\beta^i\right) = 0\right\} \\ &= \left\{i \mid \mathrm{lcm}\left(g_{C_1}(x), g_{C_2}(x)\right)\left(\beta^i\right) = 0\right\} \\ &= \left\{i \mid g_{C_1 \cap C_2}\left(\beta^i\right) = 0\right\} \\ &= T_{C_1 \cap C_2}. \end{aligned}$$

and

$$\begin{aligned} T_{C_1} \cap T_{C_2} &= \left\{ i \mid g_{C_1}\left(\beta^i\right) = 0 \text{ and } g_{C_2}\left(\beta^i\right) = 0 \right\} \\ &= \left\{ i \mid \gcd\left(g_{C_1}(x), g_{C_2}(x)\right)\left(\beta^i\right) = 0 \right\} \\ &= \left\{ i \mid g_{C_1+C_2}\left(\beta^i\right) = 0 \right\} \\ &= T_{C_1+C_2}. \end{aligned}$$

The proof is finished. ■

Let C be an$[n,k]$ cyclic code over $\mathbb{F}_q$ with defining set T. Denote $T^{-1} = \{n-t : t \in T\}$. Then we have

Proposition 2.4.2 *Let C be an $[n,k]$ cyclic code over $\mathbb{F}_q$ with defining set T and $C^\perp$ the dual code of C.*
(1) *$C \cap C^\perp = \{0\}$ if and only if $T = T^{-1}$.*
(2) *$C \subseteq C^\perp$ if and only if $T \cup T^{-1} = \mathbb{Z}_n$.*
(3) *$C^\perp \subseteq C$ if and only if $T \cap T^{-1} = \phi$.*

Some special cyclic codes

This subsection focuses on a brief study of two important families of cyclic codes: BCH codes and quadratic residue codes.

BCH codes

The binary BCH codes were discovered around 1960 by Hocquenghem and independently by Bose and Ray-Chaudhuri and were generalized to all finite fields by Gorenstein and Zierler. They are described by the roots of the polynomial $g(x)$ generating the code.

Let $n \in \mathbb{N}^*$, throughout this part we take q as a power of a prime and n coprime to q. Let α be a primitive n-th root of unity in some extension field of $\mathbb{F}_q$ and

$$m_s(x) = \prod_{j \in C_s} \left(x - \alpha^j\right)$$

is the minimal polynomial of α^s over $\mathbb{F}_q$, where C_s the q-cyclotomic cosets containing s modulo n. Then

$$x^n - 1 = \prod_s m_s(x).$$

The set

$$T = \left\{0 \leq i \leq n-1 \mid g(\alpha^i) = 0\right\}$$

is referred to as the defining set of the cyclic code $C = \langle g(x) \rangle$.

Let δ be an integer with $2 \leq \delta \leq n$. A BCH code C over $\mathbb{F}_q$ of length n and designed distance δ is a cyclic code with defining set

$$T = C_b \cup C_{b+1} \cup ... \cup C_{b+\delta-}2,$$

where C_i is the q-cyclotomic coset modulo n containing i . By the BCH Bound this code has minimum distance at least δ.

Theorem 2.4.4 *The minimum distance of a BCH code with designed distance δ is at least δ.*

Definition 2.4.4 *A cyclic code of length n over $\mathbb{F}_q$ is called a BCH code of designed distance δ if its generator $g(x)$ is the least common multiple of the minimal polynomials of $\alpha^b, \alpha^{b+1}, ..., \alpha^{b+\delta-2}$, $g(x) = \operatorname{lcm}\left(m_b(x), m_{b+1}(x), ..., m_{b+\delta-2}(x)\right)$ for some b, where α is a primitive $n-$th root of unity. Usually we shall take $b = 1$ (sometimes called a narrow-sense BCH code). If $n = q^m - 1$, i.e. α is a primitive element of $\mathbb{F}_{q^m}$, then the BCH code is called primitive.*

Example 2.4.3 *Let $n = 7$ and $q = 2$, we have $n = 7 = q^m - 1 = 2^3 - 1$. Then*

$$C_0 = \{0\}, C_1 = \{1, 2, 4\}, C_3 = \{3, 6, 5\}$$

and

$$m_0(x) = x - 1,\ m_1(x) = x^3 + x + 1,\ m_3(x) = x^3 + x^2 + 1.$$

Also we have:

1) *A narrow-sense binary BCH code of length 7 with designed distance 2 is a cyclic code generated by $m_1(x)$.*

2) *A narrow-sense binary BCH code of length 7 with designed distance 4 is a cyclic code*

generated by

$$\begin{aligned} g(x) &= \operatorname{lcm}\left(m_1(x), m_2(x), m_5(x)\right) \\ &= \operatorname{lcm}\left(m_1(x), m_5(x)\right) \\ &= m_1(x)\, m_5(x) \\ &= \left(x^3+x+1\right)\left(x^3+x^2+1\right) \\ &= x^6+x^5+x^4+x^3+x^2+x+1. \end{aligned}$$

Quadratic residue codes

Quadratic residue codes (QR codes) were first defined in 1964 by Andrew Gleason who demonstrated many of their important properties in a brief letter.

Let Q be the set of quadratic residues modulo p, p a prime, and N the set of corresponding nonresidues, we take q as a power of a prime and p an prime, coprime to q which is a quadratic residue mod p. Then Q is partitioned as a disjoint union of cyclotomic cosets modulo p under multiplication by q. Similarly, N is partitioned as a union of cyclotomic cosets modulo p under multiplication by q a quadratic residue mod p.

Let α be a generator of $\mathbb{F}_{q^m}^*$, where $m = ord_p(q)$, then the element $\beta = \alpha^{\frac{q^m-1}{p}}$ is a primitive $p-th$ root of unity in $\mathbb{F}_{q^m}$. Then since $q \in Q$, the set Q is closed under multiplication by q. Thus, Q is a disjoint union of cyclotomic cosets mod p.
Hence,

$$q(x) = \prod_{j \in Q}\left(x-\beta^j\right) \text{ and } \eta(x) = \prod_{j \in N}\left(x-\beta^j\right)$$

have coefficients from $\mathbb{F}_q$. Also

$$x^p - 1 = (x-1)q(x)\eta(x).$$

Definition 2.4.5 *The quadratic-residue codes of length p over $\mathbb{F}_q$ are cyclic codes with generator polynomials*

$$q(x),\ (x-1)q(x),\ \eta(x) \text{ and } (x-1)\eta(x).$$

Remark 2.4.1 *As*

$$\text{degree of } q(x) = \text{degree of } \eta(x) = \frac{p-1}{2}$$

both $\langle q(x)\rangle$ *and* $\langle \eta(x)\rangle$ *are linear codes over* $\mathbb{F}_q$ *of dimension*

$$p - \frac{p-1}{2} = \frac{p+1}{2},$$

and similarly, $\langle (x-1)q(x)\rangle$ *and* $\langle (x-1)\eta(x)\rangle$ *are linear codes over* $\mathbb{F}_q$ *of dimension* $\frac{p-1}{2}$.

Proposition 2.4.3 *The QR codes have defining sets,* Q, N, $Q \cup \{0\}$ *and* $N \cup \{0\}$.

Theorem 2.4.5 *Quadratic residue codes of odd prime length* p *exist over* $\mathbb{F}_q$ *if and only if* $q \in Q$.

Example 2.4.4 *Let* $p = 13$ *and* $q = 3$. *Then* $Q = \{1, 4, 9, 3, 12, 10\}$ *and* $N = \{2, 5, 6, 7, 8, 11\}$. *Let* α *be a generator of* $\mathbb{F}^*_{q^m} = \mathbb{F}^*_{3^3}$, *where* $m = ord_p(q) = ord_{13}(3) = 3$, *then the element* $\beta = \alpha^{\frac{q^m-1}{p}} = \alpha^{\frac{3^3-1}{13}} = \alpha^2$ *is a primitive* $13-th$ *root of unity in* $\mathbb{F}_{27}$.
Here the cyclotomic classes modulo 13 *relative to* 3 *are:*

$$C_0 = \{0\}\ C_1 = \{1, 3, 9\}\ C_2 = \{2, 6, 5\}\ C_4 = \{4, 12, 10\}\ C_7 = \{7, 8, 11\}.$$

Hence,

$$\begin{aligned} q(x) &= \prod_{j \in Q} \left(x - \beta^j\right) \\ &= (x-\beta)\left(x-\beta^3\right)\left(x-\beta^4\right)\left(x-\beta^9\right)\left(x-\beta^{10}\right)\left(x-\beta^{12}\right) \\ &= M_1(x)\, M_2(x) \\ &= (x^3 + 2x^2 + 2x + 2)(x^3 + x^2 + x + 2) \\ &= x^6 + x^5 + 2x^4 + 2x^2 + x + 1. \end{aligned}$$

and

$$\begin{aligned} \eta(x) &= \prod_{j \in N} \left(x - \beta^j\right) \\ &= \left(x-\beta^2\right)\left(x-\beta^5\right)\left(x-\beta^6\right)\left(x-\beta^7\right)\left(x-\beta^8\right)\left(x-\beta^{11}\right) \\ &= M_4(x)\, M_7(x) \\ &= \left(x^3 + x^2 + 2\right)(x^3 + 2x + 2) \\ &= x^6 + 2x^4 + 2x^3 + 2x^2 + 1. \end{aligned}$$

Also

$$\begin{aligned} x^{13}-1 &= (x-1)q(x)\eta(x) \\ &= (x+2)\left(x^6+x^5+2x^4+2x^2+x+1\right)\left(x^6+2x^4+2x^3+2x^2+1\right). \end{aligned}$$

Then the quadratic-residue codes of length 13 *over* $\mathbb{F}_3$ *are*

$$\langle q(x)\rangle, \langle \eta(x)\rangle, \langle (x+2)q(x)\rangle \text{ and } \langle (x+2)\eta(x)\rangle.$$

2.4.2 The idempotent of a cyclic code

The generator polynomial of a cyclic code possesses a useful property: its degree provides information about the dimension of the code.

However, determining generator polynomials often involves a decomposition process, which can be challenging. Decomposing the polynomial x^n-1 is particularly difficult in many cases. There are other generators that can be found without factoring x^n-1. These are called idempotent generators.

Let $g(x)$ be the minimal generator polynomial of a cyclic code C of length n over the field $\mathbb{F}_q$, and let $R_n = \mathbb{F}_q[x]/\left(x^n-1\right)$ be the principal quotient ring.

Definition 2.4.6 *A polynomial* $e(x) \in R_n$ *is said to be idempotent in* R_n *if*

$$e^2(x) = e(x).$$

Each cyclic code C in R_n contains a unique idempotent which generates the ideal C. This idempotent is called the generating idempotent of C.

Example 2.4.5 *The polynomial* $e(x) = x^6+x^5+x^3$ *is an idempotent in* R_7 *since*

$$\left(x^6+x^5+x^3\right)^2 \equiv \left(x^6+x^5+x^3\right)\left(\mathrm{mod}\left(x^7-1\right)\right).$$

Theorem 2.4.6 *Let* C *be a cyclic code in* R_n*. Then:*

(1) *there exists a unique idempotent* $e(x) \in C$ *such that* $C = (e(x))$ *, and*

(2) *if* $e(x)$ *is a nonzero idempotent in* C*, then* $C = (e(x))$ *if and only if* $e(x)$ *is a unity of* C*.*

Theorem 2.4.7 *Let C be a cyclic code over $\mathbb{F}_q$ with generating idempotent $e(x)$. Then the generator polynomial of C is $g(x) = \gcd(e(x), x^n - 1)$ computed in $\mathbb{F}_q[x]$.*

If C_1 and C_2 are codes of length n over $\mathbb{F}_q$, then

$$C_1 + C_2 = \{c_1 + c_2 \mid c_1 \in C_1 \text{ and } c_2 \in C_2\}$$

is the sum of C_1 and C_2. Both the intersection and the sum of two cyclic codes are cyclic, and their generator polynomials and generating idempotents are determined in the next theorem.

Theorem 2.4.8 *Let C_i be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g_i(x)$ and generating idempotent $e_i(x)$ for $i = 1$ and 2. Then:*
(1) $C_1 \cap C_2$ has generator polynomial $\operatorname{lcm}(g_1(x), g_2(x))$ and generating idempotent $e_1(x)e_2(x)$;
(2) $C_1 + C$ has generator polynomial $\gcd(g_1(x), g_2(x))$ and generating idempotent $e_1(x) + e_2(x) - e_1(x)e_2(x)$.

Minimal and maximal cyclic codes

Let $\mathbb{F}_q$ be a finite field with q elements and $n \in \mathbb{N}^*$, where $(n, q) = 1$.
Let $x^n - 1 = m_1(x)\, m_2(x) \ldots m_t(x)$ is the complete factorization of $x^n - 1$ over $\mathbb{F}_q$ into different irreducible polynomials.

Definition 2.4.7 *The cyclic code generated by $m_i(x)$ is called a maximal cyclic code (since it is a maximal ideal) and denoted by M_i. The code generated by $(x^n - 1)/m_i(x)$ is called a minimal cyclic code and denoted by $\widehat{m_i}$. Minimal cyclic codes are also called irreducible cyclic codes.*

Example 2.4.6 *The polynomial $x^7 - 1$ factorize over the finite field $\mathbb{F}_2$ into different irreducible polynomials as:*

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

Then the maximal cyclic codes of length 7 over $\mathbb{F}_2$ are exactly
$\langle m_1(x)\rangle, \langle m_2(x)\rangle$ and $\langle m_3(x)\rangle$ with

$m_1(x) = (x+1)$.

$m_2(x) = x^3 + x + 1$.

and $m_3(x) = x^3 + x^2 + 1$.

The minimal cyclic codes of length 7 *over* $\mathbb{F}_2$ *are exactly*

$\left\langle \frac{x^7-1}{m_1(x)} \right\rangle$, $\left\langle \frac{x^7-1}{m_2(x)} \right\rangle$ *and* $\left\langle \frac{x^7-1}{m_3(x)} \right\rangle$ *with*

$\frac{x^7-1}{m_1(x)} = (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1.$

$\frac{x^7-1}{m_2(x)} = (x+1)(x^3+x^2+1) = x^4+x^2+x+1.$

and $\frac{x^7-1}{m_3(x)} = (x+1)(x^3+x+1) = x^4+x^3+x^2+1.$

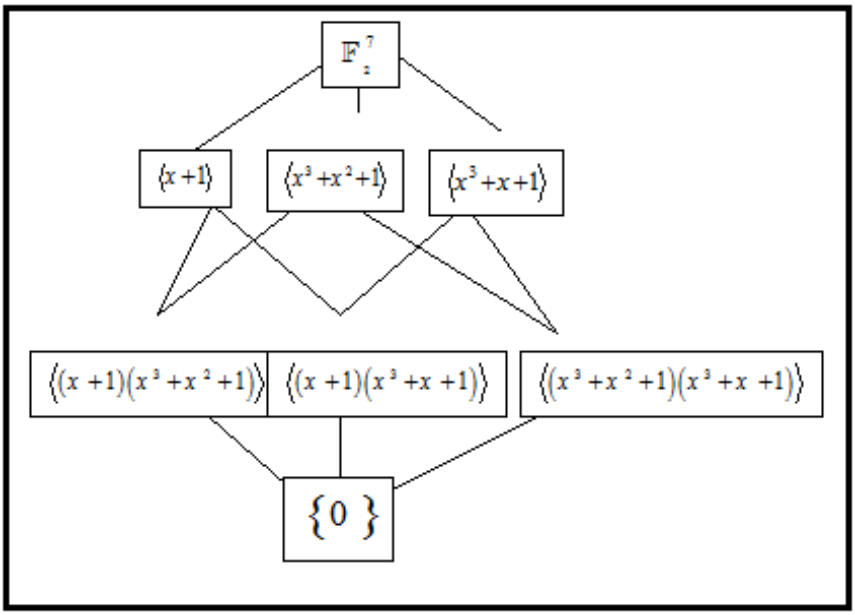

Figure 2.1: Structure of the family of cyclic codes of length 7 over $\mathbb{F}_2$.

Proposition 2.4.4 *Every cyclic code over a finite field is a direct sum of minimal cyclic codes.*

(This an example of a well known structure theorem for ideals).

Example 2.4.7 *In the previous example*

$$\langle m_1(x) \rangle = \left\langle \frac{x^7-1}{m_2(x)} \right\rangle \oplus \left\langle \frac{x^7-1}{m_3(x)} \right\rangle,$$

since

$$\begin{aligned}\left\langle \frac{x^7-1}{m_2(x)} \right\rangle + \left\langle \frac{x^7-1}{m_3(x)} \right\rangle &= \left\langle (x+1)\left(x^3+x^2+1\right)\right\rangle + \left\langle (x+1)\left(x^3+x+1\right)\right\rangle \\ &= \left\langle \gcd\left((x+1)\left(x^3+x^2+1\right),(x+1)\left(x^3+x+1\right)\right)\right\rangle \\ &= \left\langle (x+1)\gcd\left(\left(x^3+x^2+1\right),\left(x^3+x+1\right)\right)\right\rangle = \langle (x+1)\rangle = \langle m_1(x)\rangle .\end{aligned}$$

and

$$\begin{aligned}\left\langle \frac{x^7-1}{m_2(x)} \right\rangle \cap \left\langle \frac{x^7-1}{m_3(x)} \right\rangle &= \left\langle \mathrm{lcm}\left((x+1)\left(x^3+x^2+1\right),(x+1)\left(x^3+x+1\right)\right)\right\rangle \\ &= \left\langle (x+1)\left(x^3+x^2+1\right)\left(x^3+x+1\right)\right\rangle = \left\langle \left(x^7-1\right)\right\rangle = \{0\}.\end{aligned}$$

Primitive idempotents in $R_n = \mathbb{F}_q[x]/\left(x^n-1\right)$

In the context of cyclic codes and the ring R_n, there exists a special set of idempotents known as primitive idempotents. These primitive idempotents have the remarkable property that once we know them, we can generate all the idempotents in R_n and, consequently, all the cyclic codes.

Let $x^n-1 = m_1(x)\, m_2(x) \ldots m_t(x)$ is the complete factorization of x^n-1 into different irreducible polynomials, we show that the ideals $\widehat{m_i}$ of R_n generated by $(x^n-1)/m_i(x)$ for $1 \leq i \leq t$ are the minimal ideals of R_n. We denote the generating idempotent of $\widehat{m_i}$ by $\theta_i(x)$. The idempotents $\theta_1(x), \ldots, \theta_t(x)$ are called the primitive idempotents of R_n.

Theorem 2.4.9 *We have the following:*

(1) *The ideals* $\widehat{m_i}$ *for* $1 \leq i \leq t$ *are all the minimal ideals of* R_n.

(2) *The ring* R_n *is the vector space direct sum of* $\widehat{m_i}$ *for* $\leq i \leq t$.

(3) *If* $i \neq j$, *then* $\theta_i(x)\theta_j(x) = 0$ *in* R_n.

(4) $\sum_{i=1}^{t} \theta_i(x) = 1$ *in* R_n.

(5) *The only idempotents in* $\widehat{m_i}$ *are* 0 *and* $\theta_i(x)$.

(6) *If* $e(x)$ *is a nonzero idempotent in* R_n, *then there is a subset* T *of* $\{1, 2, \ldots, t\}$ *such* $e(x) = \sum_{i \in T} \theta_i(x)$ *and* $\langle e(x)\rangle = \sum_{i \in T} \widehat{m_i}$.

If C is a cyclic code of length n over $\mathbb{F}_q$, then a complement of C is a unique cyclic code C^c such that $C + C^c = \mathbb{F}_q^n$ and $C \cap C^c = \{0\}$. We call this code the cyclic complement of

C. In the following theorem we give the generator polynomial and generating idempotent of the cyclic complement.

Theorem 2.4.10 *Let C be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g(x)$, generating idempotent $e(x)$, and*
defining set T. Let C^c be the cyclic complement of C. The following hold.
(1) *$h(x) = (x^n - 1)/g(x)$ is the generator polynomial for C^c and $1 - e(x)$ is its generating idempotent.*
(2) *C^c is the sum of the minimal ideals of R_n not contained in C.*
(3) *If $N = \{0, 1, ..., n-1\}$, then $N \setminus T$ is the defining set of C^c.*

Theorem 2.4.11 *Let C be an $[n, k]$ cyclic code over $\mathbb{F}_q$ with generator polynomial $g(x)$ generating idempotent $e(x)$, and*
defining set T. Let $h(x) = (x^n - 1)/g(x)$. Then.
(1) *The dual $C^\perp$ of a cyclic code C is also cyclic.*
(2) *$C^\perp$ has generating idempotent $1 - e(x^{-1})$ and generator polynomial $\frac{x^k}{h(0)} h(\frac{1}{x})$.*
(3) *If $N = \{0, 1, ..., n-1\}$, then $N \setminus (-1)\, T$ is the defining set of $C^\perp$.*

Finding generator idempotent

We know that by multiplying the generator polynomials of maximal cyclic codes, we can find the generator polynomial of a cyclic code. Similarly, by addition the generating idempotents of the minimal cyclic codes, the generating idempotent of a cyclic code can be obtained.

Let $\mathbb{F}_q$ be a field of prime order q. Let n be an integer with $gcd(q, n) = 1$. If α denotes a primitive $n - th$ root of unity in some extension field of $\mathbb{F}_q$, the follows that

$$x^n - 1 = \prod_{s \in C_s} m_s(x)$$

gives the decomposition of $x^n - 1$ into irreducible factors over $\mathbb{F}_q$, where C_s the $q-$cyclotomic coset *modulo* n containing s. Let $\widehat{m_s}$ be the minimal ideal in R_n generated by $(x^n - 1)/m_s(x)$ and $\theta_s(x)$ be the primitive idempotent of $\widehat{m_s}$.

Proposition 2.4.5 *Let C be a cyclic code of length n over $\mathbb{F}_q$ with generating idempotent $e(x) = \sum_{i=0}^{n-1} e_i x^i$. Then:*

(1) $e_i = e_j$ *if* i *and* j *are in the same* q*-cyclotomic coset modulo* n,

(2) *if* $q = 2$,

$$e(x) = \sum_{j \in J} \sum_{i \in C_j} x^i,$$

where J *is some subset of representatives of* $2-$*cyclotomic cosets modulo* n.

Lemma 2.4.1 *Let* $\theta_s(x)$ *be a primitive idempotents of* $\widehat{m_s}$. *Then*

$$\theta_s(\alpha^j) = \begin{cases} 1 \text{ if } j \in C_s \\ 0 \text{ if } j \notin C_s \end{cases}$$

Theorem 2.4.12 *Let* $\theta_s(x)$ *be a primitive idempotents of* $\widehat{m_s}$. *Then*

$$\theta_s(x) = \sum_{i=0}^{n-1} \varepsilon_i x^i,$$

where

$$\varepsilon_i = \frac{1}{n} \sum_{j \in C_s} \alpha^{-ij}, \text{ for all } i \geq 0.$$

Proof. We have

$$\sum_{i=0}^{n-1} \theta_s(\alpha^j)\alpha^{-ij} = \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} \varepsilon_k \alpha^{jk} \alpha^{-ij} = \sum_{k=0}^{n-1} \varepsilon_k \sum_{j=0}^{n-1} \alpha^{j(k-i)} = n\varepsilon_i.$$

Then

$$\varepsilon_i = \frac{1}{n} \sum_{i=0}^{n-1} \theta_s(\alpha^j)\alpha^{-ij} = \frac{1}{n} \sum_{j \in C_s} \alpha^{-ij}.$$

The proof is finished. ■

Example 2.4.8 *Let* $n = 7$,. *The* $2-$*cyclotomic cosets modulo* n *are*

$$C_0 = \{0\}, \ C_1 = \{1, 2, 4\}, \ C_3 = \{3, 6, 5\}.$$

Then the following table gives all the cyclic codes C_i *of length* 7 *over* $\mathbb{F}_2$ *with their generating idempotents* $e_i(x)$, *and the code's dimension.*

i	dim	$e_i(x)$
1	0	$e_1(x) = 0$
2	7	$e_2(x) = x^0 = 1$
3	4	$e_3(x) = x + x^2 + x^4$
4	4	$e_4(x) = x^3 + x^5 + x^6$
5	3	$e_5(x) = e_2(x) + e_3(x) = 1 + x + x^2 + x^4$
6	3	$e_6(x) = e_2(x) + e_4(x) = 1 + x^3 + x^5 + x^6$
7	6	$e_7(x) = e_3(x) + e_4(x) = x + x^2 + x^3 + x^5 + x^6$
8	1	$e_8(x) = e_2(x) + e_3(x) + e_4(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$

Table 2.2

Chapter 3

Minimal and maximal cyclic codes of length $N = 2p$

3.1 Introduction

This chapter includes our publication entitled minimal and maximal cyclic codes of length $2p$ whish was appeared in the international journal Journal of Discrete Mathematical Sciences and Cryptography.

This chapter is about some classes of cyclic codes of over finite fields of length $N = 2p$ with p is an odd prime. More precsely, we copute the minimal and maximal cyclic codes of length $2p$ over the finite field $\mathbb{F}_q$ whith p is an odd prime, over the finite fields $\mathbb{F}_q$ of q elements, where q is an odd prime distinct from p and $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$, i,e., $q^{p-1} \equiv 1 (\mathrm{mod}\, 2p)$.

Finaly, we study the relationship btween the maximal and minimal cyclic codes.

3.2 Minimal and maximal cylic codes

Recall that a cyclic code C of length N over the finite field $\mathbb{F}_q$, is an ideal C in the principal ring $\mathbb{F}_q[x]/\left(x^N - 1\right)$. That is $C = \langle g(x) \rangle$ with $g(x)$ is the nonzero monic polynomial of minimal degree in C that divides the polynomial $x^N - 1$. see [18] If $x^N - 1 = g_1 ... g_t$ is the

complete factorization of $x^N - 1$ into different irreducible polynomials, then the cyclic codes $\langle g_i(x)\rangle$ generated by polynomials $g_i(x)$ are called maximal cyclic codes. In the other side $\left(x^N - 1\right)/g_i(x)$ is a generator polynomial of a so called minimal or irreducible code.

3.2.1 The Minimal and maximal cylic codes of length $2p^n$

In the paper [3], the authors S.K. Arora and M. Pruthi investigated in the computation of the minimal cyclic codes of length $2p^n$. In this work, we are interested in the computation of all maximal and minimal cyclic codes of length $2p$ with $n \geq 1$ is integer, over the finite fields $\mathbb{F}_q$ where q is a power of an odd prime number. The authors obtains $2n+2$ q-cyclotomic cosets modulo $2p^n$

3.2.2 The q-cyclotomic cosets modulo $2p^n$

Consider the set

$$S = \{0, 1, 2, ..., 2p^n - 1\}.$$

For $a, b \in S$, we say that

$$a \sim b \text{ if } a \equiv bq^i \pmod{2p^n}$$

for some integer $i \geq 0$. This equivalence relation partitions the set S into disjoint equivalence classes called the q-cyclotomic cosets modulo $2p^n$, the q-cyclotomic coset containing $s \in S$ is

$$C_s := \{s, sq, sq^2, ..., sq^{n_s - 1}\},$$

where n_s is the smallest positive integer such that

$$sq^{n_s} \equiv s (\bmod n).$$

The authors obtains $2n+2$ q-cyclotomic cosets modulo $2p^n$ of the forms given by:

$$\begin{aligned} C_{p^{i-1}} &= \{p^{i-1}, p^{i-1}q, ..., p^{i-1}q^{\phi(p^{n-i+1})-1}\}, \\ C_{2p^{i-1}} &= \{2p^{i-1}, 2p^{i-1}q, ..., 2p^{i-1}q^{\phi(n-i+1)-1}\} \end{aligned}$$

where $1 \leq i \leq n+1$ and

$$C_{2p^n} = \{0\}.$$

For more details see [3] and [31] .

3.2.3 Cyclotomic cosets in case $n = 1$ and and auxiliaries

To give the complte factorization of $x^{2p} - 1$, we compute in first the q-cyclotomic cosets modulo $2p$. In the special case $n = 1$ and q is an odd prime, we determine the q-cyclotomic cosets modulo $2p$.

Proposition 3.2.1 *Given the set of integers $S = \{0, 1, 2, ..., 2p-1\}$ and $\varphi(p)$ is the multiplicative order of q modulo $2p$. Then S, can be partitioned into 4 q-cyclotomic cosets given by*

$$C_0 = \{0\}, C_p = \{p\}, C_1 = \{1, q, q^2, ..., q^{p-2}\}, C_2 = \{2, 2q, 2q^2, ..., 2q^{p-2}\}.$$

Proof. *For $s \in S$, the class of s denoted by C_s is given by*

$$C_s = \{s, sq, sq^2, ..., sq^{n_s-1}\} modulo 2p.$$

For $s = 0$, we have

$$C_0 = \{0, 0q, 0q^2, ..., 0q^{n_s-1}\} = \{0\}.$$

And for $s = 1$, we will show that we have

$$C_1 = \{1, 1 \times q, 1 \times q^2, ..., 1 \times q^{n_s-1}\} = \{1, q, q^2, ..., q^{p-2}\}$$

with $n_s = p - 1$.
Suppose in the contrary, there is an integers i, j with $0 \leq i < j \leq p-2$ and $q^i = q^j$. Multiplying both sides by q^{-j}, we obtain

$$q^i q^{-j} (\mathrm{mod}\, 2p) \equiv q^j q^{-j} (\mathrm{mod}\, 2p) \equiv q^0 (\mathrm{mod}\, 2p) \equiv 1 (\mathrm{mod}\, 2p).$$

But we have $1 \leq j - i \leq p - 2$ and this contradict the fact that the order of q is $p - 1$ modulo $2p$.
Then necessary, $q^i \neq q^j$ for all $i, j \in \{1, 2, ..., p-2\}$ with $i \neq j$. Since the integer 2 is not in the classes C_0 and C_1 then

$$C_2 = \{2, 2q, 2q^2, ..., 2q^{p-2}\}.$$

The same argument as above, shows that we have $2q^i \neq 2q^j$ *for all* $i, j \in \{1, 2, ..., p-2\}$ *with* $i \neq j$. *Since the prime* p *is an odd prime then* p *is not in the classes* C_0, C_1, C_2; *then we have*

$$C_p = \{p, pq, pq^2, ..., pq^{n_s-1}\} = \{p\} \text{ modulo } 2p.$$

Firstly, $p \equiv p(\mathrm{mod}\, 2p)$ *because* $p < 2p$ *then, and so* $p \in C_p$. *We have also,* $pq \equiv p(\mathrm{mod}\, 2p)$ *because* q *is an odd prime greater or equal to* 3, *and in this case we can write* $q = 2t+1$ *and consequently, we have*

$$pq = p\,(2t+1) = 2pt + p \equiv p(\mathrm{mod}\, 2p).$$

The same argument holds for pq^i, *i.e.,* $pq^i \equiv p(\mathrm{mod}\, 2p)$.
Since

$$|C_0| = |C_p| = 1$$

and

$$|C_1| = |C_2| = p - 1,$$

hen we have

$$|C_0 \cup C_1 \cup C_2 \cup C_p| = |C_0| + |C_1| + |C_2| + |C_p| = 1 + 1 + (p-1) + (p-1) = 2p,$$

wihch is the cardinal of S. *And this confirms that we have:*

$$C_0 \cup C_1 \cup C_2 \cup C_p = S.$$

The proof is finished. ■

Theorem 3.2.1 *The number of monic irreducible factors of* $x^{2p} - 1$ *over* $\mathbb{F}_q$ *is equal to the number of cyclotomic cosets of* q *modulo* $2p$.

Proof. For the proof of this theorem, one can see [18],[20]. ■

In this section, we consider the complete factorization of $x^{2p} - 1$ over $\mathbb{F}_q$, with p and q are distinct odd primes and $\phi(p) = p - 1$ is the multiplicative order of q modulo $2p$.
The unique complete factorization of $x^{2p} - 1$ over $\mathbb{F}_q$ into irreducible polynomials is

$$x^{2p} - 1 = \prod m_s\,(x)\,,$$

where s runs over the complete set of representatives from distinct q-cyclotomic cosets modulo $2p$.

Since

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

And we have:

$$(x^p - 1) = (x - 1)\left(x^{p-1} + x^{p-2} + ... + x + 1\right);$$

and

$$(x^p + 1) = (x + 1)\left(x^{p-1} - x^{p-2} + ... - x + 1\right).$$

Then,

$$x^{2p} - 1 = (x - 1)\left(x^{p-1} + x^{p-2} + ... + x + 1\right)(x + 1)\left(x^{p-1} - x^{p-2} + ... - x + 1\right)$$

$$= (x - 1)(x + 1)\left(x^{p-1} - x^{p-2} + ... - x + 1\right)\left(x^{p-1} + x^{p-2} + ... + x + 1\right).$$

The polynomials

$$x^{p-1} + x^{p-2} + ... + x + 1, x^{p-1} + x^{p-2} + ... + x + 1$$

are shown to be irreducible in $\mathbb{F}_q$, with q is an odd prime and $\phi(p) = p-1$ is the multiplicative order of q modulo $2p$, see [13], [15] and [25].

The minimal polynomials corresponding to each cyclotomic coset are obtained below:

$$m_0(x) = x - 1,$$

$$m_p(x) = x + 1,$$

$$m_1(x) = x^{p-1} - x^{p-2} + ... - x + 1,$$

$$m_2(x) = x^{p-1} + x^{p-2} + ... + x + 1.$$

And we have:

$$x^{2p} - 1 = \prod_{s \in \{0,\, 1,\, 2,\, p\}} m_s(x).$$

3.2.4 The minimal and maximal cyclic codes of length $2p$

Since the classes C_0, C_p, C_1, C_2 are all the distinct q-cyclotomic cosets modulo $2p$, then

$$M_0 = \langle m_0(x) \rangle, M_p = \langle m_p(x) \rangle, M_1 = \langle m_1(x) \rangle, M_2 = \langle m_2(x) \rangle$$

are precisely all the distinct maximal cyclic codes of length $2p$ over $\mathbb{F}_q$. And we have

$$\widehat{m_0} = \langle \frac{(x^{2p}-1)}{m_0(x)} \rangle, \widehat{m_p} = \langle \frac{(x^{2p}-1)}{m_p(x)} \rangle, \widehat{m_1} = \langle \frac{(x^{2p}-1)}{m_1(x)} \rangle, \widehat{m_2} = \langle \frac{(x^{2p}-1)}{m_2(x)} \rangle,$$

are precisely all the distinct minimal cyclic codes of length $2p$ over $\mathbb{F}_q$. See [18], for the definitions of minimal and maximal cyclic codes. The following tables, gives the generating polynomial and the corresponding dimension of the above maximal and minimal codes. The maximal codes of length $2p$ over $\mathbb{F}_q$ are given by:

Codes	Generating polynomial	Dimension
M_0	$m_0(x)$	$2p-1$
M_p	$m_p(x)$	$2p-1$
M_1	$m_1(x)$	$p+1$
M_2	$m_2(x)$	$p+1$

Table 3.1

The minimal codes of length $2p$ over $\mathbb{F}_q$ are given by:

Codes	Generating polynomial	Dimension
$\widehat{m_0} = \langle \frac{(x^n-1)}{m_0(x)} \rangle$	$m_p(x) \times m_1(x) \times m_2(x)$	1
$\widehat{m_p} = \langle \frac{(x^n-1)}{m_p(x)} \rangle$	$m_0(x) \times m_1(x) \times m_2(x)$	1
$\widehat{m_1} = \langle \frac{(x^n-1)}{m_1(x)} \rangle$	$m_0(x) \times m_p(x) \times m_2(x)$	$p-1$
$\widehat{m_2} = \langle \frac{(x^n-1)}{m_2(x)} \rangle$	$m_0(x) \times m_p(x) \times m_1(x)$	$p-1$

Table 3.2

3.3 The relationship between the maximal and the minimal cyclic codes

In this section, we show that every maximal cyclic code of length $2p$ over $\mathbb{F}_q$, with p and q are distinct odd primes and $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$, can be written as an unique direct sum of three minimal cyclic codes. Finally, we show that each cyclic code of length $2p$ generated by the product of two distinct minimal polynomials, is the direct sum of two minimal cyclic codes.

Proposition 3.3.1 *As any cyclic code of length n over the finite field $\mathbb{F}_q$ is simply a subspace of the vector space $\mathbb{F}_q^n$, we have : if C_1 and C_2 are cyclic codes of length n over $\mathbb{F}_q$, then sum $C_1 + C_2 = \{c_1 + c_2 | c_1 \in C_1$ and $c_2 \in C_2\}$ and the intersection $C_1 \cap C_2$ are also a cyclic codes.*

Proposition 3.3.2 *Let C_i be a cyclic code of length n over $\mathbb{F}_q$ for $i = 1$ and 2. Then the sum $C_1 + C_2$ is direct, if and only if $C_1 \cap C_2 = \{0\}$.*

The dimension of the cyclic code C is the dimension of C as a vector space over $\mathbb{F}_q$.

Proposition 3.3.3 *Let C_i be a cyclic code of length n over $\mathbb{F}_q$ for $i \in \{1, 2, 3\}$. Then $C_1 + C_2 + C_3$ is a direct sum if and only if*
$\dim(C_1 + C_2 + C_3) = \dim(C_1) + \dim(C_2) + \dim(C_3)$.

Now we prove our main results.

Proposition 3.3.4 *Every maximal cyclic code of length $2p$ over $\mathbb{F}_q$, is a direct sum of three minimal cyclic codes with p and q are distinct odd primes and $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$.*

Proof. Using the Theorem 2.4.8 and properties of gcd of polynomials, we find:
$\widehat{m_0} + \widehat{m_p} + \widehat{m_1} =$
$$\langle \gcd \begin{pmatrix} m_p(x) \times m_1(x) \times m_2(x),\ m_0(x) \times m_1(x) \times m_2(x), \\ m_0(x) \times m_p(x) \times m_2(x) \end{pmatrix} \rangle$$

$$= \langle \gcd \begin{pmatrix} \gcd\left(m_p(x) \times m_1(x) \times m_2(x),\ m_0(x) \times m_1(x) \times m_2(x)\right), \\ m_0(x) \times m_p(x) \times m_2(x) \end{pmatrix} \rangle$$

$$= \langle \gcd\left(m_1(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_2(x)\right) \rangle$$

$$= \langle m_2(x) \times \gcd\left(m_1(x),\ m_0(x) \times m_p(x)\right)$$

$$= \langle m_2(x) \rangle$$

Also, using Proposition 3.3.3 we find:

$\dim(\widehat{m_0} + \widehat{m_p} + \widehat{m_1}) = \dim(\langle m_2(x) \rangle) = p + 1 = \dim(\widehat{m_0}) + \dim(\widehat{m_p}) + \dim(\widehat{m_1})$.

then $M_2 = \widehat{m_0} \oplus \widehat{m_p} \oplus \widehat{m_1}$.

In a similar way, we find:

$\widehat{m_0} + \widehat{m_p} + \widehat{m_2} =$

$$\langle \gcd \begin{pmatrix} m_p(x) \times m_1(x) \times m_2(x),\ m_0(x) \times m_1(x) \times m_2(x), \\ m_0(x) \times m_p(x) \times m_1(x) \end{pmatrix} \rangle$$

$$= \langle \gcd \begin{pmatrix} \gcd\left(m_p(x) \times m_1(x) \times m_2(x),\ m_0(x) \times m_1(x) \times m_2(x)\right), \\ m_0(x) \times m_p(x) \times m_1(x) \end{pmatrix} \rangle$$

$$= \langle \gcd\left(m_1(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_1(x)\right) \rangle$$

$$= \langle m_1(x) \times \gcd\left(m_2(x),\ m_0(x) \times m_p(x)\right) \rangle$$

$$= \langle m_1(x) \rangle.$$

$\dim(\widehat{m_0} + \widehat{m_p} + \widehat{m_2}) = \dim(\langle m_1(x) \rangle) = p + 1 = \dim(\widehat{m_0}) + \dim(\widehat{m_p}) + \dim(\widehat{m_2})$.

$M_1 = \widehat{m_0} \oplus \widehat{m_p} \oplus \widehat{m_2}$.

$$\widehat{m_0} + \widehat{m_1} + \widehat{m_2} = \langle \gcd \begin{pmatrix} m_p(x) \times m_1(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_2(x), \\ m_0(x) \times m_p(x) \times m_1(x) \end{pmatrix} \rangle$$

$$= \langle \gcd \begin{pmatrix} \gcd\left(m_p(x) \times m_1(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_2(x)\right), \\ m_0(x) \times m_p(x) \times m_1(x) \end{pmatrix} \rangle$$

$$= \langle \gcd\left(m_p(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_1(x)\right) \rangle$$

$$= \langle m_p(x) \times \gcd\left(m_2(x),\ m_0(x) \times m_1(x)\right) \rangle$$

$$= \langle m_p(x) \rangle.$$

$\dim(\widehat{m_0} + \widehat{m_1} + \widehat{m_2}) = \dim(\langle m_p(x) \rangle) = 2p - 1 = \dim(\widehat{m_0}) + \dim(\widehat{m_1}) + \dim(\widehat{m_2}))$.

$M_p = \widehat{m_0} \oplus \widehat{m_1} \oplus \widehat{m_2}$.

$$\widehat{m_p} + \widehat{m_1} + \widehat{m_2} = \langle \gcd \begin{pmatrix} m_0(x) \times m_1(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_2(x), \\ m_0(x) \times m_p(x) \times m_1(x) \end{pmatrix} \rangle$$

$$= \langle \gcd \begin{pmatrix} \gcd\left(m_0(x) \times m_1(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_2(x)\right), \\ m_0(x) \times m_p(x) \times m_1(x) \end{pmatrix} \rangle$$

$= \langle \gcd\left(m_0(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_1(x)\right)$

$= \langle m_0(x) \times \gcd\left(m_2(x),\ m_p(x) \times m_1(x)\right) \rangle$

$= \langle m_0(x) \rangle$.

$\dim(\widehat{m_p} + \widehat{m_1} + \widehat{m_2}) = \dim(\langle m_0(x) \rangle) = 2p - 1 = \dim(\widehat{m_p}) + \dim(\widehat{m_1}) + \dim(\widehat{m_2}))$.

$M_0 = \widehat{m_p} \oplus \widehat{m_1} \oplus \widehat{m_2}$. ■

Proposition 3.3.5 *Every cyclic code of length $2p$ over $\mathbb{F}_q$ generated by product of two minmal polynomials is a direct sum of two minimal cyclic codes with p and q are distinct odd primes and $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$.*

Proof. Using the Theorem 2.4.8 and properties of gcd we find:

$\widehat{m_0} + \widehat{m_p} = \langle \gcd\left(m_p(x) \times m_1(x) \times m_2(x),\ m_0(x) \times m_1(x) \times m_2(x)\right) \rangle$

$= \langle m_1(x) \times m_2(x) \gcd\left(m_p(x),\ m_0(x)\right) \rangle$

$= \langle m_1(x) \times m_2(x) \rangle$.

Also, using Proposition 3.3.2 and properties of of lcm we find:

$\widehat{m_0} \cap \widehat{m_p} = \langle \mathrm{lcm}\left(m_p(x) \times m_1(x) \times m_2(x),\ m_0(x) \times m_1(x) \times m_2(x)\right) \rangle$

$= \langle m_0(x) \times m_p(x) \times m_1(x) \times m_2(x) \rangle$

$= \langle x^{2p} - 1 \rangle = \{0\}$.

so $\langle\ m_1(x) \times m_2(x) \rangle = \widehat{m_0} \oplus \widehat{m_p}$.

In a similar way, we find: $\langle m_p(x) \times m_2(x) \rangle\ = \widehat{m_0} \oplus \widehat{m_{1,}}$

$\langle\ m_p(x) \times m_1(x) \rangle = \widehat{m_0} \oplus \widehat{m_2}$,

$\langle\ m_0(x) \times m_2(x) \rangle = \widehat{m_p} \oplus \widehat{m_1}$,

$\langle\ m_0(x) \times m_1(x) \rangle = \widehat{m_p} \oplus \widehat{m_2}$,

$\langle\ m_0(x) \times m_p(x) \rangle = \widehat{m_1} \oplus \widehat{m_2}$. ■

Example 3.3.1 *Take $q = 3$, $p = 17$. The maximal ternary cyclic codes M_0, M_p, M_1, M_2 of length 34 and the minimal ternary cyclic codes*

$\widehat{m_0}$, $\widehat{m_p}$, $\widehat{m_1}$, $\widehat{m_2}$ of length 34 have the following parameters:

(a) The minimal polynomial corresponding to each cyclotomic coset is obtained below:

$m_0(x) = x - 1$, $m_{17}(x) = x + 1$,

$m_1(x) = x^{17}-x^{16}+x^{15}-x^{14}+x^{13}-x^{12}+x^{11}-x^{10}+x^9-x^8+x^7-x^6+x^5-x^4+x^3-x^2+x-1,$

$m_2(x) = x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1.$

(b) If $g_s(x)$ is the generating polynomial of $\widehat{m_s}$ then we have $g_0(x) = \frac{(x^{34}-1)}{m_0(x)} = x^{33}+x^{32}+x^{31}+$
$x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}$
$+ x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$

$g_{17}(x) = \frac{(x^{34}-1)}{m_{17}(x)} = x^{33} - x^{32} + x^{31} - x^{30} + x^{29} - x^{28} + x^{27} - x^{26} + x^{25} - x^{24} + x^{23} - x^{22} + x^{21} -$
$x^{20} + x^{19} - x^{18} + x^{17} - x^{16} + x^{15} - x^{14} + x^{13} - x^{12}$
$+ x^{11} - x^{10} + x^9 - x^8 + x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1,$

$g_1(x) = \frac{(x^{34}-1)}{m_1(x)} = x^{18} + x^{17} - x - 1,$

$g_2(x) = \frac{(x^{34}-1)}{m_2(x)} = x^{18} - x^{17} + x - 1.$

(c) Table 3.3: The generating polynomial and dimension of the maximal ternary cyclic codes of length 34 *are given by:*

Codes	M_0	M_{17}	M_1	M_2
Generating polynomial	$m_0(x)$	$m_{17}(x)$	$m_1(x)$	$m_2(x)$
Dimension	33	33	18	18

d) Table 3.4: The generating polynomial and dimension of the minimal ternary cyclic codes of length 34 *are given by:*

Codes	$\widehat{m_0}$	$\widehat{m_p}$	$\widehat{m_1}$	$\widehat{m_2}$
Generating polynomial	$g_0(x)$	$g_{17}(x)$	$g_1(x)$	$g_2(x)$
Dimension	1	1	16	16

3.4 Primitive idempotents in $R_{2p} = \mathbb{F}_q[x]/\left(x^{2p}-1\right)$

Let M_s be the minimal cyclic codes in R_{2p} generated by $\frac{(x^{2p}-1)}{m_s(x)}$, where

$$x^{2p}-1 = \prod_{s\in\{0,\,1,\,2,\,p\}} m_s(x)$$

is the unique complete factorization of $x^{2p}-1$ over $\mathbb{F}_q$ into irreducible polynomials.Let θ_s be the primitive idempotent of M_s we know by (Theorem 2.4.12)
the primitive idempotent θ_s corresponding to the cyclotomic coset C_s containing s in R_{2p} is given by

$$\theta_s = \sum_{i=0}^{2p} \varepsilon_i x^i,$$

where

$$\varepsilon_i = \frac{1}{2p} \sum_{j \in C_s} \alpha^{-ij} \ \forall i \geq 0.$$

The authors Arora and Pruthi in [3] obtains the primitive idempotents in R_{2p^n}.In this section, we determine in the special case $n = 1$ and q is an odd prime, the primitive idempotents in R_{2p}, with $\varphi(p) = p-1$ is the multiplicative order of q modulo $2p$.

For $1 \leq i \leq 2$, the elements $X_i(x)$, $X_i^*(x)$ of R_{2p} are defined as

$$X_i(x) = \sum_{s \in C_{p^{i-1}}} x^s \text{ and } X_i^*(x) = \sum_{s \in C_{2p^{i-1}}} x^s.$$

Theorem 3.4.1 *The ring R_{2p} has 4 primitive idempotents given by*

$$\begin{aligned}
e_0 &= \frac{1}{2p} \sum_{j=1}^{2} \left(X_j^* + X_j\right)(x), \\
\eta_0 &= \frac{1}{2p} \sum_{j=1}^{2} \left(X_j^* - X_j\right)(x), \\
e_1 &= \frac{1}{2p} \left[(p-1)\left(X_2^* + X_2\right)(x) - \left(X_1^* + X_1\right)(x)\right], \\
\eta_1 &= \frac{1}{2p} \left[(p-1)\left(X_2^* - X_2\right)(x) - \left(X_1^* - X_1\right)(x)\right].
\end{aligned}$$

Example 3.4.1 *Take $q = 3$, $p = 17$. Then the q cyclotomic cosets modulo 34 are:*

$$\begin{aligned}
C_0 &= \{0\}, \\
C_1 &= \{1, 3, 9, 27, 13, 5, 15, 11, 33, 31, 25, 7, 21, 29, 19, 23\}, \\
C_2 &= \{2, 6, 18, 20, 26, 10, 30, 22, 32, 28, 16, 14, 8, 24, 4, 12\}, \\
C_{17} &= \{17\}.
\end{aligned}$$

Then the four primitive idempotents are:

$$
\begin{aligned}
e_0 &= \frac{1}{34}\left[(X_1^* + X_1) + (X_2^* + X_2)\right], \\
&= x^{33}+x^{32}+x^{31}+x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+ \\
&\quad x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1, \\
\eta_0 &= \frac{1}{34}\left[(X_1^* - X_1) + (X_2^* - X_2)\right], \\
&= -x^{33}+x^{32}-x^{31}+x^{30}-x^{29}+x^{28}-x^{27}+x^{26}-x^{25}+x^{24}-x^{23}+x^{22}-x^{21}+x^{20}-x^{19}+x^{18} \\
&\quad -x^{17}+x^{16}-x^{15}+x^{14}-x^{13}+x^{12}-x^{11}+x^{10}-x^9+x^8-x^7+x^6-x^5+x^4-x^3+x^2-x+1, \\
e_1 &= \frac{1}{34}\left[16\left(X_2^* + X_2\right) - (X_1^* + X_1)\right], \\
&= -x^{33}-x^{32}-x^{31}-x^{30}-x^{29}-x^{28}-x^{27}-x^{26}-x^{25}-x^{24}-x^{23}-x^{22}-x^{21}-x^{20}-x^{19}-x^{18} \\
&\quad +x^{17}-x^{16}-x^{15}-x^{14}-x^{13}-x^{12}-x^{11}-x^{10}-x^9-x^8-x^7-x^6-x^5-x^4-x^3-x^2-x+1, \\
\eta_1 &= \frac{1}{34}\left[16\left(X_2^* - X_2\right) - (X_1^* - X_1)\right], \\
&= x^{33}-x^{32}+x^{31}-x^{30}+x^{29}-x^{28}+x^{27}-x^{26}+x^{25}-x^{24}+x^{23}-x^{22}+x^{21}-x^{20}+x^{19}-x^{18} \\
&\quad -x^{17}-x^{16}+x^{15}-x^{14}+x^{13}-x^{12}+x^{11}-x^{10}+x^9-x^8+x^7-x^6+x^5-x^4+x^3-x^2+x+1.
\end{aligned}
$$

Chapter 4

Some LCD cyclic codes of length $2p$ over finite fields

4.1 Introduction

This chapter includes our publication entitled Some LCD cyclic codes of length $2p$ over finite fields whish was appeared in the international journal Discussiones Mathematicae - General Algebra and Applications.

LCD cyclic codes over finite fields called also reversible cyclic codes were first introduced and studied by Massey [22] in 1964. Yang and Massey gave a necessary and sufficient condition for a cyclic code to have a complementary dual [41]. In this chapter, we are intersted to construct two classes of LCD cyclic codes of length $2p$ over $\mathbb{F}_q$, with p and q are distinct odd primes where $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$. (φ denotes Euler's phi-function). In the same conditions as above, we show that every LCD maximal cyclic code can be represented as an unique direct sum of three LCD minimal cyclic codes.

The objective of this chapter is to determine two classes of LCD cyclic codes of length $2p$ over $\mathbb{F}_q$ and the relationship between them with p and q are distinct odd primes, where $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$.

4.2 On LCD cyclic codes of length n over finite fields

Preliminaries

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. An $[n,k]$ linear code C over $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$ with dimension k. Let C be an $[n,k]$ linear code over $\mathbb{F}_q$. Then the dual code of C is defined as:

$$C^{\perp} = \{b \in \mathbb{F}_q^n : bc^T = 0 \ \forall c \in C\},$$

where bc^T denotes the standard inner product of the two vectors b and c.
The code $C^{\perp}$ is an $[n, n-k]$ linear code, and we have

$$\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp}) = n.$$

A generator matrix of C is a $k \times n$ matrix whose rows are a set of basis vectors of C.
A parity-check matrix of C is a generator matrix of $C^{\perp}$

Definition 4.2.1 *A linear code with a complementary dual (an LCD code) was defined to be a linear code C whose dual code $C^{\perp}$ satisfies(see[23])$C_1 \cap C^{\perp} = \{0\}$.*

Proposition 4.2.1 *Let C be a linear code of length n over $\mathbb{F}_q$. Then C is LCD if and only if $\mathbb{F}_q^n = C \oplus C^{\perp}$, i.e., $\mathbb{F}_q^n$ is the direct sum of C and $C^{\perp}$.*

Proof. Directly follows from the Definition 4.2.1 and the fact $\dim_{\mathbb{F}_q}(C)+\dim_{\mathbb{F}_q}(C^{\perp}) = n$.

The proof is finished. ■

Let Π_C be the orthogonal projector from $\mathbb{F}_q^n$ onto C, i.e., the linear mapping from $\mathbb{F}_q^n$ onto $\mathbb{F}_q^n$ defined by

$$v\Pi_C = \begin{cases} v \text{ if } v \in C \\ 0 \text{ if } v \notin C^{\perp} \end{cases}$$

Let A^T denote the transpose of a matrix A.

The following theorem gives a complete characterization of LCD codes.

Theorem 4.2.1 $(Massey, 1992)$ *If G is a generator matrix for the linear code C, then C is an LCD code if and only if the $k \times k$ matrix GG^T is nonsingular. Moreover, if C is an LCD code, then $\Pi_C = G^T(GG^T)^{-1}G$ is the orthogonal projector from $\mathbb{F}_q^n$ onto C.*

Proof. Suppose that GG^T is nonsingular. Then if $v \in C$, i.e., if $v = uG$ for some u, it follows that

$$vG^T(GG^T)^{-1}G = uGG^T(GG^T)^{-1}G = uG = v.$$

Moreover, if $v \in C^\perp$, i.e., if $vG^T = 0$, it follows that

$$vG^T(GG^T)^{-1}G = 0(GG^T)^{-1}G = 0.$$

Thus $G^T(GG^T)^{-1}$ is indeed the orthogonal projector Π_C and hence C must be an LCD code.

Conversely, suppose that GG^T is singular. Then there is a nonzero vector u in $\mathbb{F}_q^k$ such that $uGG^T = 0$. Now uG is a nonzero vector in C. But an arbitrary vector v in C can be written as $v = u'G$ for some u' in $\mathbb{F}_q^k$ so that

$$uGv^T = (uG)\,(u'G)^T = uGG^T\,(u')^T = 0\,(u')^T = 0$$

and hence uG is also a vector in $C^\perp$. It follows that $C \cap C^\perp \neq \{0\}$, i.e., that C is not an LCD code. ■

The following characterization is due to Massey [23].

Proposition 4.2.2 *Let C be an (n, k) linear code with generator matrix G and parity-check matrix H. Then the following conditions are equivalent*
(1) *C is an LCD code,*
(2) *The $k \times k$ matrix GG^T is nonsingular,*
(3) *The $(n-k) \times (n-k)$ matrix HH^T is nonsingular.*

Example 4.2.1 *Let C be a binary $[3, 2]$ code. If*

$$C = \{000, 001, 100, 101\},$$

then

$$C^{\perp} = \{000, 010, 110, 111\}.$$

Since $C \cap C^{\perp} = \{0\}$ *we deduce that* C *is an LCD code.*

The linear code C of length n over the finite field $\mathbb{F}_q$ is said to be cyclic if C is an ideal in the principal quotient ring $R_n := \mathbb{F}_q[x]/\left(x^n - 1\right)$.

Let $C = \langle g\left(x\right)\rangle$ be a cyclic code of length n over $\mathbb{F}_q$, the dual code of C is $C^{\perp} = \langle h^*\left(x\right)\rangle$, where $x^n - 1 = g(x)h(x)$

and

$$h^*\left(x\right) = h(0)^{-1}x^{deg(h)}h(\frac{1}{x}).$$

The integer $k = n - \deg g(x)$ is the dimension of C and $|C| = q^k$.

Let $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ denote the ring of integers modulo n.

For $s \in \mathbb{Z}_n$, the q-cyclotomic cosets of s modulo n denoted by C_s is given by

$$C_s := \left\{s, sq, sq^2, ..., sq^{n_s - 1}\right\} \bmod n,$$

where n_s is the smallest positive integer such that $sq^{n_s} \equiv s(\bmod n)$.

The smallest nonnegative integer in C_s is called the coset leader of C_s.

Let $\Gamma_{(n,q)}$ be the set of all the coset leaders. Then we have

$$\bigcup_{s \in \Gamma_{(n,q)}} C_s = \mathbb{Z}_n.$$

Definition 4.2.2 *Let* $s \in \mathbb{Z}_n$ *and let* C_s *be the* q*-cyclotomic cosets of* s *modulo* n *over* $\mathbb{F}_q$*. If* $C_s = C_{-s}$ *we will say that* C_s *is reversible.*

Lemma 4.2.1 *If* C_1 *is reversible, then* C_s *is reversible for all* s *in* $\Gamma_{(n,q)}$.

Proof. Since $q^i \equiv -1(\bmod n)$, we get $sq^i \equiv -s(\bmod n)$ for all s in $\Gamma_{(n,q)}$. Thus $-s \in C_s$. The proof is finished. ■

The cyclotomic coset C_s is said to be reversible if and only if $C_{n-s} = C_s$ if and only if $n - s$ is in C_s.

Let α be a generator of $\mathbb{F}_{q^m}^*$, where $m = ord_n(q)$, then the element $\beta = \alpha^{\frac{q^m-1}{n}}$ is a primitive $n-th$ root of unity in $\mathbb{F}_{q^m}$, then for each integer s, the polynomial (see for example [20])

$$m_s(x) = \prod_{j \in C_s} \left(x - \beta^j\right)$$

is the minimal polynomial of β^s over $\mathbb{F}_q$, which is irreducible over $\mathbb{F}_q$. It then follows that

$$x^n - 1 = \prod_{s \in \Gamma_{(n,q)}} m_s(x)$$

gives the decomposition of $x^n - 1$ into irreducible factors over $\mathbb{F}_q$.

The cyclic code $\widehat{m_s}$ in R_n generated by $\frac{(x^n-1)}{m_s(x)}$ is called a minimal cyclic code of length n over $\mathbb{F}_q$ or irreducible cyclic codes and the cyclic code M_s in R_n, generated by $m_s(x)$, is called a maximal cyclic code of length n over $\mathbb{F}_q$.

We recall some definitions as below:

- A polynomial $f(x)$ is said to be self-reciprocal if $f(x) = f^*(x)$, where $f^*(x)$ is the reciprocal polynomial of $f(x)$.
- A linear code C of length n is said to be reversible if $(c_{n-1}, c_{n-2}, ..., c_1, c_0) \in C$ whenever $(c_0, c_1, ..., c_{n-1}) \in C$.
- A cyclic code $C = \langle f(x) \rangle$ of length n over $\mathbb{F}_q$ is reversible if $f(x)$ is a self-reciprocal polynomial.

Remark 4.2.1 *LCD cyclic codes are called reversible cyclic codes in the literature.*

4.2.1 The structure of LCD cyclic codes

In[41], a necessary and sufficient condition for the existence of LCD cyclic codes of length n over $\mathbb{F}_q$ is given.

Theorem 4.2.2 *[17] Let C be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g(x)$ and $\gcd(n, q) = 1$. Then the following statements are equivalent.*
(1) *C is an LCD cyclic code.*

(2) $g(x)$ *is self-reciprocal, i.e.,* $g^*(x) = g(x)$.

(3) *An element* β *in the splitting field of* $g(x)$ *over* $\mathbb{F}_q$*, if* $g(\beta) = 0$*, then* $g(\beta^{-1}) = 0$.

Proof. (1) is equivalent to $C + C^{\perp} = \mathbb{F}_q^n$, if and only if $C = \langle g(x) \rangle$ and $C^{\perp} = \langle h^*(x) \rangle$ where $h(x) = \frac{x^n - 1}{g(x)}$. We get that C and $C^{\perp}$ are both reversible.
It is equivalent to (2) and (3).
The proof is finished. ■

The goal in this subsection is to give an exact count of reversible cyclic codes of length n over $\mathbb{F}_q$.

Lemma 4.2.2 *The irreducible polynomial* $m_s(x)$ *is self-reciprocal if and only if* $n - s \in C_s$.

Lemma 4.2.3 *The least common multiple* $\operatorname{lcm}(m_s(x), m_{n-s}(x))$ *is self-reciprocal for every* $s \in \mathbb{Z}_n$.

From the above, we conclude

$$\operatorname{lcm}(m_s(x), m_{n-s}(x)) = \begin{cases} m_s(x) & \text{if } n - s \in C_s, \\ m_s(x)\, m_{n-s}(x) & \text{otherwhise} \end{cases}$$

Let $\prod_{(n,q)} = \Gamma_{(n,q)} \setminus \{\max\{(s, LD(n-s)\} : s \in \Gamma_{(n,q)}, \ : n - s \notin C_s\}$, where $LD(i)$ denotes the coset leader of C_i.
The conclusion follows directly from Lemmas 4.2.2, 4.2.3 and Theorem 4.2.2.

Theorem 4.2.3 *The total number of reversible cyclic codes of length* n *over* $\mathbb{F}_q$ *is given by* $2^{|\Pi_{(n,q)}|} - 1$.

Proposition 4.2.3 *Every reversible cyclic code of length* n *over* $\mathbb{F}_q$ *is generated by a polynomial*

$$g(x) = \prod_{s \in H} \operatorname{lcm}(m_s(x), m_{n-s}(x))$$

where H *is a nonempty subset of* $\prod_{(n,q)}$.

Example 4.2.2 *Let $(n, q) = (15, 2)$. The $2-$cyclotomic classes modulo 15 are*

$$\begin{aligned} C_0 &= \{0\}, \\ C_1 &= \{1, 2, 4, 8\}, \\ C_3 &= \{3, 6, 9, 12\}, \\ C_5 &= \{5, 10\}, \\ C_7 &= \{7, 11, 13, 14\}. \end{aligned}$$

It then follows that

$$x^{15} - 1 = m_0(x)m_1(x)m_3(x)m_5(x)m_7(x),$$

where

$$\begin{aligned} m_0(x) &= x + 1, \\ m_1(x) &= x^4 + x + 1, \\ m_3(x) &= x^4 + x^3 + x^2 + x + 1, \\ m_5(x) &= x^2 + x + 1, \\ m_7(x) &= x^4 + x^3 + 1. \end{aligned}$$

Except for $m_1(x)$ and $m_7(x)$, all $m_i(x)$ are self-reciprocal. In this case,

$$\Gamma_{(n,q)} = \{0, 1, 3, 5, 7\}$$

and

$$\prod{}_{(n,q)} = \{0, 1, 3, 5\}.$$

Then the number of reversible cyclic codes of length n over $\mathbb{F}_q$ is

$$2^{\left|\prod_{(n,q)}\right|} - 1 = 2^4 - 1 = 15.$$

In this paragraph, we explicitly determine all generator polynomial $g_i(x)$ of the reversible cyclic code of length n over $\mathbb{F}_q$. Since the nonempty subset of $\prod_{(n,q)}$ are

$$\begin{aligned} &\{\{0\}, \{1\}, \{3\}, \{5\}, \{0, 1\}, \{0, 3\}, \{0, 5\}, \{1, 3\}, \{1, 5\}, \{3, 5\}, \{0, 1, 3\}, \\ &\{0, 1, 5\}, \{1, 3, 5\}, \{0, 1, 3, 5\}\}. \end{aligned}$$

Then we have

$$\begin{aligned}
g_1(x) &= \prod_{s\in\{0\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right) \\
&= \operatorname{lcm}\left(m_0(x), m_0(x)\right) = m_0(x).\\
g_2(x) &= \prod_{s\in\{1\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right) \\
&= \operatorname{lcm}\left(m_1(x), m_7(x)\right) = m_1(x)\, m_7(x).\\
g_3(x) &= \prod_{s\in\{3\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right) \\
&= \operatorname{lcm}\left(m_3(x), m_3(x)\right) = m_3(x).\\
g_4(x) &= \prod_{s\in\{5\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right) \\
&= \operatorname{lcm}\left(m_5(x), m_5(x)\right) = m_5(x).\\
g_5(x) &= \prod_{s\in\{0,1\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
&= \operatorname{lcm}\left(m_0(x), m_0(x)\right) \operatorname{lcm}\left(m_1(x), m_7(x)\right), \\
&= m_0(x)\, m_1(x)\, m_7(x).\\
g_6(x) &= \prod_{s\in\{0,3\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
&= \operatorname{lcm}\left(m_0(x), m_0(x)\right) \operatorname{lcm}\left(m_3(x), m_3(x)\right), \\
&= m_0(x)\, m_3(x).\\
g_7(x) &= \prod_{s\in\{0,5\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
&= \operatorname{lcm}\left(m_0(x), m_0(x)\right) \operatorname{lcm}\left(m_5(x), m_5(x)\right), \\
&= m_0(x)\, m_5(x).\\
g_8(x) &= \prod_{s\in\{1,3\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
&= \operatorname{lcm}\left(m_1(x), m_7(x)\right) \operatorname{lcm}\left(m_3(x), m_3(x)\right), \\
&= m_1(x)\, m_7(x)\, m_3(x).\\
g_9(x) &= \prod_{s\in\{1,5\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
&= \operatorname{lcm}\left(m_1(x), m_7(x)\right) \operatorname{lcm}\left(m_5(x), m_5(x)\right), \\
&= m_1(x)\, m_7(x)\, m_5(x).
\end{aligned}$$

$$
\begin{aligned}
g_{10}(x) &= \prod_{s\in\{3,5\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
&= \operatorname{lcm}\left(m_3(x), m_3(x)\right) \operatorname{lcm}\left(m_5(x), m_5(x)\right), \\
&= m_3(x)\, m_5(x).
\end{aligned}
$$

$$
\begin{aligned}
g_{11}(x) &= \prod_{s\in\{0,1,3\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
&= \operatorname{lcm}\left(m_0(x), m_0(x)\right) \operatorname{lcm}\left(m_1(x), m_7(x)\right) \operatorname{lcm}\left(m_3(x), m_3(x)\right), \\
&= m_0(x)\, m_1(x)\, m_3(x).
\end{aligned}
$$

$$
\begin{aligned}
g_{12}(x) &= \prod_{s\in\{0,1,5\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
&= \operatorname{lcm}\left(m_0(x), m_0(x)\right) \operatorname{lcm}\left(m_1(x), m_7(x)\right) \operatorname{lcm}\left(m_5(x), m_5(x)\right), \\
& m_0(x)\, m_1(x)\, m_5(x).
\end{aligned}
$$

$$
\begin{aligned}
g_{13}(x) &= \prod_{s\in\{0,3,5\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
&= m_0(x)\, m_3(x)\, m_5(x).
\end{aligned}
$$

$$
\begin{aligned}
g_{14}(x) &= \prod_{s\in\{1,3,5\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
&= m_1(x)\, m_7(x)\, m_3(x)\, m_5(x).
\end{aligned}
$$

$$
\begin{aligned}
g_{15}(x) &= \prod_{s\in\{0,1,3,5\}} \operatorname{lcm}\left(m_s(x), m_{n-s}(x)\right), \\
& m_0(x)\, m_1(x)\, m_7(x)\, m_3(x)\, m_5(x).
\end{aligned}
$$

4.3 LCD cyclic codes of length $2p$

4.3.1 Factorization of $x^{2p} - 1$ over $\mathbb{F}_q$ and auxiliaries

In [2], the authors determined the q-cyclotomic cosets modulo $2p^n$ in their paper, with $n \geq 1$ is an integer, and p is an odd prime over the finite fields $\mathbb{F}_q$ where q is a power of an odd prime number, with $(p,\ q) = 1$ and$\varphi(p^n)$ is the multiplicative order of q modulo $2p^n$. In this work, we are intersted in the special case $n = 1$.

Proposition 4.3.1 *Let $\mathbb{Z}_{2p} = \{0, 1, 2, ..., 2p-1\}$ denote the ring of integers modulo $2p$ and $\varphi(p)$ is the multiplicative order of q modulo $2p$. Then $\mathbb{Z}_{2p}$, can be partitioned into 4 q-cyclotomic cosets.*

Proof. For $s \in \mathbb{Z}_{2p}$, the class of s denoted by C_s is given by

$$C_s := \{s, sq, sq^2, ..., sq^{n_s-1}\} \mod 2p.$$

Since q has order $\varphi(p) \bmod 2p$, so q also has order

$$\varphi(p^{2-i})(\mathrm{mod}\, 2p^{2-i}), 1 \leq \ i \leq 2.$$

Then

$$q^{\varphi(p^{2-i})} \ \equiv 1(\mathrm{mod}\, 2p^{2-i})$$

or

$$p^{i-1}q^{\varphi(p^{2-i})} \ \equiv p^{i-1}(\mathrm{mod}\, 2p)$$

and

$$2p^{i-1}q^{\varphi(p^{2-i})} \ \equiv 2p^{i-1}(\mathrm{mod}\, 2p).$$

Hence,

$$C_{p^{i-1}} = \ \{p^{i-1}, p^{i-1}q, ..., p^{i-1}q^{\varphi(p^{2-i})-1}\}$$

and so

$$C_{2p^{i-1}} = \ \{2p^{i-1}, 2p^{i-1}q, ..., 2p^{i-1}q^{\varphi(p^{2-i})-1}\}.$$

Because $|C_0| = |C_p| = 1$ and $|C_1| = |C_2| = p-1$, then we have:

$$C_0 \cup C_p \cup C_1 \cup C_2 = \mathbb{Z}_{2p}.$$

The proof is finished. ■

In this section, we consider the complete factorization of $x^{2p} - 1$ over $\mathbb{F}_q$, with p and q are distinct odd primes and $\phi(p) = p - 1$ is the multiplicative order of q modulo $2p$.

Proposition 4.3.2 *Let $\mathbb{F}_q$ be a finite field with q elements and p be an odd prime coprime to q. Let $2p|q^m - 1$, where $m = ord_{2p}(q)$, then $x^{2p} - 1 = \prod_{s \in \Gamma_{(2p,q)}} m_s(x)$, where*

$$m_0(x) = x - 1,$$

$$m_p(x) = x + 1,$$

$$m_1(x) = x^{p-1} - x^{p-2} + ... - x + 1,$$

$$m_2(x) = x^{p-1} + x^{p-2} + ... + x + 1.$$

The cyclic codes

$$M_0 = \langle m_0(x) \rangle, M_p = \langle m_p(x) \rangle, M_1 = \langle m_1(x) \rangle, M_2 = \langle m_2(x) \rangle,$$

are all the distinct maximal cyclic codes with length $2p$ over $\mathbb{F}_q$.We also have

$$\widehat{m_0} = \langle \frac{(x^{2p}-1)}{m_0(x)} \rangle, \widehat{m_p} = \langle \frac{(x^{2p}-1)}{m_p(x)} \rangle, \widehat{m_1} = \langle \frac{(x^{2p}-1)}{m_1(x)} \rangle, \widehat{m_2} = \langle \frac{(x^{2p}-1)}{m_2(x)} \rangle,$$

are all the distinct minimal cyclic codes with length $2p$ over $\mathbb{F}_q$.

4.3.2 Maximal and minimal LCD cyclic codes of length $2p$

In this paragraph we are intersted to determine two classes of LCD cyclic codes of length $2p$ over $\mathbb{F}_q$, with p and q are distinct odd primes and $\varphi(p) = p-1$ is the multiplicative order of q modulo $2p$.

The following tables, gives the generating polynomial and the corresponding reciprocal polynomial of the above maximal and minimal codes.

Table 4.1: The reciprocal polynomial of the generating polynomial of the maximal cyclic codes of length $2p$ over $\mathbb{F}_q$

Codes	Generating polynomial $g(x)$	The reciprocal polynomial $g^*(x)$ of $g(x)$
M_0	$m_0(x)$	$m_0(x)$
M_p	$m_p(x)$	$m_p(x)$
M_1	$m_1(x)$	$m_1(x)$
M_2	$m_2(x)$	$m_2(x)$

Table 4.2: The reciprocal polynomial of the generating polynomial of the minimal cyclic codes of length $2p$ over $\mathbb{F}_q$

Codes	Generating polynomial $g(x)$	The reciprocal polynomial $g^*(x)$ of $g(x)$
$\widehat{m_0} = \langle \frac{(x^{2p}-1)}{m_0(x)} \rangle$	$m_p(x) \times m_1(x) \times m_2(x)$	$m_p(x) \times m_1(x) \times m_2(x)$
$\widehat{m_p} = \langle \frac{(x^{2p}-1)}{m_p(x)} \rangle$	$m_0(x) \times m_1(x) \times m_2(x)$	$m_0(x) \times m_1(x) \times m_2(x)$
$\widehat{m_1} = \langle \frac{(x^{2p}-1)}{m_1(x)} \rangle$	$m_0(x) \times m_p(x) \times m_2(x)$	$m_0(x) \times m_p(x) \times m_2(x)$
$\widehat{m_2} = \langle \frac{(x^{2p}-1)}{m_2(x)} \rangle$	$m_0(x) \times m_p(x) \times m_1(x)$	$m_0(x) \times m_p(x) \times m_1(x)$

Proposition 4.3.3 *Every maximal cyclic code of length $2p$ over $\mathbb{F}_q$ is an LCD maximal cyclic code of length $2p$ over $\mathbb{F}_q$, where p and q are distinct odd primes with $\varphi(p) = p-1$ is the multiplicative order of q modulo $2p$.*

Proof. Let $C = \langle g(x) \rangle$ be a maximal cyclic code of length $2p$ over $\mathbb{F}_q$. Then, from Table 4.1, $g(x)$ is a self-reciprocal. By Theorem 4.2.2, the code C is an LCD cyclic code. ■

Proposition 4.3.4 *Every minimal cyclic code of length $2p$ over $\mathbb{F}_q$, is an LCD minimal cyclic code of length $2p$ over $\mathbb{F}_q$, p and q are distinct odd primes and $\varphi(p) = p-1$ is the multiplicative order of q modulo $2p$*

Proof. Let $C = \langle g(x) \rangle$ be a minimal cyclic code of length $2p$ over $\mathbb{F}_q$. Then, from Table 4.2, $g(x)$ is a self-reciprocal. By Theorem 4.2.2, the code C is an LCD cyclic code. ■

4.4 Results concerning some LCD cyclic codes of length $2p$

In this section we determine the relationship between theLCD maximal cyclic codes and the LCD minimal cyclic codes of length $2p$ over $\mathbb{F}_q$, with p and q are distinct odd primes and $\varphi(p) = p-1$ is the multiplicative order of q modulo $2p$, we show that every LCD maximal

cyclic code of length $2p$ can be represented as a direct sum of three LCD minimal cyclic codes.

Table 4.3: The generating polynomial of the dual of maximal cyclic codes of length $2p$ over $\mathbb{F}_q$

Code C	Generating polynomial of C	Generating polynomial of $C^{\perp}$
M_0	$m_0(x)$	$m_p(x) \times m_1(x) \times m_2(x)$
M_p	$m_p(x)$	$m_0(x) \times m_1(x) \times m_2(x)$
M_1	$m_1(x)$	$m_0(x) \times m_p(x) \times m_2(x)$
M_2	$m_2(x)$	$m_0(x) \times m_p(x) \times m_1(x)$

Table 4.4: The generating polynomial of the dual of minimal cyclic codes of length $2p$ over $\mathbb{F}_q$

Codes C	Generating polynomial of C	Generating polynomial of $C^{\perp}$
$\widehat{m_0} = \langle \frac{(x^{2p}-1)}{m_0(x)} \rangle$	$m_p(x) \times m_1(x) \times m_2(x)$	$m_0(x)$
$\widehat{m_p} = \langle \frac{(x^{2p}-1)}{m_p(x)} \rangle$	$m_0(x) \times m_1(x) \times m_2(x)$	$m_p(x)$
$\widehat{m_1} = \langle \frac{(x^{2p}-1)}{m_1(x)} \rangle$	$m_0(x) \times m_p(x) \times m_2(x)$	$m_1(x)$
$\widehat{m_2} = \langle \frac{(x^{2p}-1)}{m_2(x)} \rangle$	$m_0(x) \times m_p(x) \times m_1(x)$	$m_2(x)$

Theorem 4.4.1 *Let C_i be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g_i(x)$ for $i = 1$ and 2. Then:*
the cyclic code $C_1 + C_2$ has generator polynomial $\gcd(g_1(x), g_2(x))$.

Now, we prove our main results.

Proposition 4.4.1 *If C is an LCD maximal cyclic code of length $2p$ over $\mathbb{F}_q$, with p and q are distinct odd primes and $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$, then C can be represented as a direct sum of three LCD minimal cyclic codes of length $2p$ over $\mathbb{F}_q$, $C = C_1 \oplus C_2 \oplus C_3$. Moreover, $|C| = |C_1|\,|C_2|\,|C_3|$.*

Proof. Using the Proposition 3.3.3, theorem 2.4.8 and properties of gcd of polynomials, we find, if

$$C_1 = \widehat{m_0},\ C_2 = \widehat{m_p},\ C_3 = \widehat{m_1},$$

then

$$\begin{aligned}
\dim(C) &= \dim\left(C_1 + C_2 + C_3\right) \\
&= \dim\left((C_1 + C_2) + C_3\right) \\
&= \dim\left(\langle \gcd\left(m_1(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_2(x)\right)\rangle\right), \\
\text{since } \widehat{m_0} + \widehat{m_p} &= \langle m_1(x) \times m_2(x)\rangle \\
&= \dim\left(\langle m_2(x) \times \gcd\left(m_1(x),\ m_0(x) \times m_p(x)\right)\right) \\
&= \dim\left(\langle m_2(x)\rangle\right) \\
&= \dim\left(M_2\right).
\end{aligned}$$

Hence,

$$\dim(C) = \dim(M_2) = p + 1 = \dim(C_1) + \dim(C_2) + \dim(C_3).$$

We find:

$$C = C_1 \oplus C_2 \oplus C_3.$$

On the other hand,

$$|C_1|\,|C_2|\,|C_3| = q.q.q^{p-1} = q^{p+1} = |C|\,.$$

Hence,

$$|C| = |C_1|\,|C_2|\,|C_3|\,.$$

In a similar way, if

$$C_1 = \widehat{m_0},\ C_2 = \widehat{m_p},\ C_3 = \widehat{m_2},$$

then

$$\begin{aligned}
\dim(C) &= \dim\left(C_1 + C_2 + C_3\right) \\
&= \dim\left((C_1 + C_2) + C_3\right) \\
&= \dim(\langle \gcd\left(m_1(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_1(x)\right)\rangle \\
&\quad (\text{since } \widehat{m_0} + \widehat{m_p} = \langle m_1(x) \times m_2(x)\rangle) \\
&= \dim\left(\langle m_1(x) \times \gcd\left(m_2(x),\ m_0(x) \times m_p(x)\right)\rangle\right) \\
&= \dim(\langle m_1(x)\rangle) \\
&= \dim(M_1) = p + 1 = \dim(C_1) + \dim(C_2) + \dim(C_3).
\end{aligned}$$

Hence,

$$C = C_1 \oplus C_2 \oplus C_3.$$

On the other hand,

$$|C_1|\,|C_2|\,|C_3| = q.q.q^{p-1} = q^{p+1} = |C|\,.$$

Hence,

$$|C| = |C_1|\,|C_2|\,|C_3|\,.$$

In a similar way, if

$$C_1 = \widehat{m_0},\ C_2 = \widehat{m_1},\ C_3 = \widehat{m_2},$$

then

$$\begin{aligned}
\dim(C) &= \dim\left(C_1 + C_2 + C_3\right) \\
&= \dim\left((C_1 + C_2) + C_3\right) \\
&= \dim(\langle \gcd\left(m_p(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_1(x)\right)\rangle), \\
&\quad (\text{since } \widehat{m_0} + \widehat{m_1} = \langle m_p(x) \times m_2(x)\rangle) \\
&= \dim\left(\langle \gcd\left(m_p(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_1(x)\right)\rangle\right) \\
&= \dim\left(\langle m_p(x) \times\ \gcd\left(m_2(x),\ m_0(x) \times m_1(x)\right)\rangle\right) \\
&= \dim\left(\langle m_p(x)\rangle\right) \\
&= \dim(M_p) = 2p - 1 = \dim(C_1) + \dim(C_2) + \dim(C_3).
\end{aligned}$$

Hence,

$$C = C_1 \oplus C_2 \oplus C_3.$$

On the other hand,

$$|C_1|\,|C_2|\,|C_3| = q.q^{p-1}.q^{p-1} = q^{2p-1} = |C|\,.$$

Hence,

$$|C| = |C_1|\,|C_2|\,|C_3|\,.$$

In a similar way, if

$$C_1 = \widehat{m_P},\ C_2 = \widehat{m_1},\ C_3 = \widehat{m_2},$$

then

$$\begin{aligned}
\dim(C) &= \dim\left(C_1 + C_2 + C_3\right) \\
&= \dim\left((C_1 + C_2) + C_3\right) \\
&= \dim(\langle \gcd\left(m_0(x) \times m_2(x),\ m_0(x) \times m_p(x) \times m_1(x)\right)\rangle), \\
&\quad (\text{since } \widehat{m_p} + \widehat{m_1} = \langle m_0(x) \times m_2(x)\rangle) \\
&= \dim\left(\langle m_0(x) \times \gcd\left(m_1(x),\, m_0(x) \times m_p(x)\right)\rangle\right) \\
&= \dim\left(\langle m_0(x)\rangle\right) \\
&= \dim(M_0) = 2p - 1 = \dim(C_1) + \dim(C_2) + \dim(C_3).
\end{aligned}$$

Hence,

$$C = C_1 \oplus C_2 \oplus C_3.$$

On the other hand,

$$|C_1|\,|C_2|\,|C_3| = q.q^{p-1}.q^{p-1} = q^{2p-1} = |C|\,.$$

Hence,

$$|C| = |C_1|\,|C_2|\,|C_3|\,.$$

The proof is finished. ■

Example 4.4.1 *Take $q = 7$, $p = 11$. Then $\Gamma_{(2p,q)} = \{0, 1, 2, 11\}$, hence the LCD maximal cyclic codes M_0, M_{11}, M_1, M_2 of length 22 over $\mathbb{F}_7$ and the LCD minimal cyclic codes $\widehat{m_0}$,*

$\widehat{m_{11}}$, $\widehat{m_1}$, $\widehat{m_2}$ *of length* 22 *over* $\mathbb{F}_7$ *are given below:*

(a) There are the following minimal polynomials

$m_0(x) = x - 1$, $m_{11}(x) = x + 1$,

$m_1(x) = x^{11} - x^{10} + x^9 - x^8 + x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1$,

$m_2(x) = x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

(b) If $g_s(x)$ *is the generating polynomial of* $\widehat{m_s}$ *then we have:*

$g_0(x) = \frac{(x^{22}-1)}{m_0(x)} = x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$,

$g_{11}(x) = \frac{(x^{34}-1)}{m_{17}(x)} = x^{21} - x^{20} + x^{19} - x^{18} + x^{17} - x^{16} + x^{15} - x^{14} + x^{13} - x^{12} + x^{11} - x^{10} + x^9 - x^8 + x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1$,

$g_1(x) = \frac{(x^{22}-1)}{m_1(x)} = x^{12} + x^{11} - x - 1$,

$g_2(x) = \frac{(x^{34}-1)}{m_2(x)} = x^{12} - x^{11} + x - 1$.

(c) Table 4.5: The generating polynomial and dimension of the LCD maximal cyclic codes of length 22 *are given by:*

LCD Maximal cyclic code of length 22 *over* $\mathbb{F}_7$	M_0	M_{11}	M_1	M_2
Generating polynomial	$m_0(x)$	$m_{11}(x)$	$m_1(x)$	$m_2(x)$
Dimension	21	21	12	12

(d) Table 4.6: The generating polynomial and dimension of the LCD minimal cyclic codes of length 22 *are given by:*

LCD Minimal cyclic code of length 22 *over* $\mathbb{F}_7$	$\widehat{m_0}$	$\widehat{m_{11}}$	$\widehat{m_1}$	$\widehat{m_2}$
Generating polynomial	$g_0(x)$	$g_{11}(x)$	$g_1(x)$	$g_2(x)$
Dimension	1	1	10	10

In this work, p is odd prime and $\mathbb{F}_q$ is the finite fields of q elements, where q is an odd prime distinct from p and $\varphi(p) = p - 1$ is the multiplicative order of q modulo $2p$. The explicit expressions for the generating polynomials of all minimal and maximal cyclic codes of length $2p$ over $\mathbb{F}_q$ are obtained.

In the same conditions as above we show that every LCD maximal cyclic code of length $N = 2p$ over the finite fields $\mathbb{F}_q$ can be represented as an unique direct sum of three LCD minimal cyclic codes.

Bibliography

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976.

[2] M. Araya, M. Harada, On the classification of linear complementary dual codes, *Discrete Mathematics*. 342 (2019) 270–278.

[3] S.K. Arora, M. Pruthi, Minimal cyclic codes of length $2p^n$, *Finite Fields Appl.* 5 (1999) 177–187.

[4] G.K. Bakshi, M. Raka, A class of constacyclic codes over a finite field, *Finite Fields Appl.* 18 (2) (2012) 362–377.

[5] G.K. Bakshi, M. Raka, Self-dual and self-orthogonal negacyclic codes of length $2p^n$ over a finite field, *Finite Fields Appl.* 19 (1) (2013) 39–54.

[6] S. Batra, S. K. Arora, *Some cyclic codes of length* $2p^n$, *Des. Codes Cryptogr.* 61(1), 41–69 (2011).

[7] N. L. Biggs, *Codes an introduction to information communicationand cryptography*, Springer-Verlag, 2008.

[8] P. Binbin, Z. Shixin, S. Zhonghua, On LCD negacyclic codes over finite fields, *J Syst Sci Complex* (2018) 31: 1065–1077.

[9] R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, 2003.

[10] D. M. Burton, *Elementary Number Theory(7th ed.)*, Tata McGraw–Hill, 2009.

[11] C. Chapot, *Reconnaissance de codes, structure des codes quasi-cycliques*, Thèse de doctorat .Université de Limoges, 2009.

[12] C. Carstensen, B. Fine, G Rosenberger, *Abstract Algebra: Applications to Galois Theory, Algebraic Geometry and Cryptography*, Walter de Gruyter, 2011.

[13] K. Conrad, Cyclotomic extension, http://www.math.uconn.edu/kconrad /math5211s13/handouts/ cyclotomic.pdf.

[14] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[15] N. Jacobson, Lectures in abstract algebra, vol. III, D. Van Nostrand Company, Inc. Princeton, 1964.

[16] Y. Lei, C. Li, Y. Wu, P. Zeng, More results on hulls of some primitive binary and ternary BCH codes, *Finite Fields Appl.* 82 (2022) 1071-5797.

[17] C. Li, C. Ding , S. Li, LCD cyclic codes over finite fields, *IEEE Trans. Inf. Theory* 63 (2017) 4344–4356.

[18] R. Lidl, G. Pilz, *Applied Abstract Algebra, Springer*-Verlag. Ney York, 1998.

[19] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1994.

[20] S. Ling, C. xing, *Coding Theory, A First Course*, Cambridge University Press, 2004.

[21] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, North-Holland,Amsterdam, 1977.

[22] J. L, Massey, Reversible codes, *Information and Control*, 7 (1964), 369-380.

[23] J. L, Massey, Linear codes with complementary duals, *Discrete Math.* 106/107 (1992) 337–342.

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

[25] C. Mihoubi, P. Solé, New class of isodual cyclic codes of rate 1/2 over $\mathbb{F}_p$, *Romanian Journal of Mathematics and Computer Science.* 6(1), 1–5 (2016).

[26] M. Ali. Mohammed, A. J. munshid, M Alaeiyan, (2021) Cyclic codes of length p^n over $(\mathbb{Z}p)^m$, *Journal of Discrete Mathematical Sciences and Cryptography*, 24:2, 579-588.

[27] G. L. Mullen, C. Mummert, *Finite fields and applications*, American Mathematical Soc, 2007.

[28] Pankaj, M. Pruthi, (2017) Cyclic codes from Whiteman's generalized cyclotomic sequences of order 2^r, $r \geq 2$, *Journal of Information and Optimization Sciences,* 38:3-4, 621-646.

[29] Pankaj, M. Pruthi, (2018) Cyclic codes of prime power length from generalized cyclotomic classes of order 2^r, *Journal of Information and Optimization Sciences,* 39:4, 965-971.

[30] V. Pless, *Introduction to the Theory of Error Correcting Codes*, Wiley, New York, 1998.

[31] M. Pruthi, S. K. Arora, Minimal cyclic codes of prime power length, *Finite Fields Appl.* 3 (1997) 99–113.

[32] M. Pruthi, S Kumar, (2019) Cyclic codes with generalized cyclotomic cubic classes, J*ournal of Discrete Mathematical Sciences and Cryptography,* 22:6, 923-933.

[33] M. Purser, Introduction to error-correcting Codes, Artech House. 1995.

[34] B. Sakkour, *Etude et amélioration du décodage des codes de reed-muller d'ordre deux*, Thèse de doctorat en science.école polytechnique, 2007.

[35] A. Sharma, G.K. Bakshi, V.C. Dumir, M. Raka, Cyclotomic numbers and primitive idempotents in the ring $GF\,(q)\,[x]/(x^{p^n}-1)$,*Finite Fields Appl.* 10 (4) (2004) 653–673.

[36] G. Skersys, *Calcul du groupe d'automorphismes des codes. Dertimination l'équivalence des codes,* Thèse de doctorat .Université de Limoges, 1999.

[37] S. Roman, *Coding and information thory,* Springer-Verlag, 1992.

[38] J.H. van Lint, *Introduction to Coding Theory*, 3rd ed., Springer-Verlag, 1999.

[39] J, H. van Lint, G. van der Geer, *Introduction to Coding Theory and algebraic geometry,* Birkhäuser Verlag, Basel, 1988.

[40] L. R. Vermani, *Elements of algebraic coding theory,* Chapman & Hall. 1996.

[41] X. Yang, J. L. Massey, The condition for a cyclic code to have a complementary dual, *Discrete Math.* 126 (1994) 391–393.

خلاصة

يندرج هذا العمل في إطار الشفرات المصححة للأخطاء أكثر دقة دراسة الشفرات الدورية الأعظمية.
على الحقل المنته $\mathbb{F}_q$ الشفرة الدورية الأعظمية ذات الطول n تمثل المثالي الأعظمي من حلقة حاصل القسمة

$$R_n = \mathbb{F}_q[x] \Big/ (x^n - 1).$$

الهدف الأساسي من هذه الأطروحة هو دراسة المثاليات الأعظمية في حلقة حاصل القسمة لأن هذه المثاليات تمثل الشفرات الدورية الأعظمية في حلقة حاصل القسمة R_n.

الكلمات المفتاحية : الشفرات الخطية الدورية، الشفرات الدورية الأعظمية و الأصغرية، متممة الشفرات الدورية.

Abstract

This work focuses on the theory of error-correcting codes, specifically the investigation of maximal cyclic codes.

A cyclic code of length n over the finite field $\mathbb{F}_q$ can be defined as a principal ideal of the quotient ring $R_n = \mathbb{F}_q[x] \Big/ (x^n - 1)$ where $\mathbb{F}_q[x]$ represents the ring of polynomials with coefficients in the finite $\mathbb{F}_q$ and $(x^n - 1)$ denotes the principal ideal generated by the polynomial $x^n - 1$.

The main objective of this thesis is to explore maximal ideals within the quotient ring R_n, as these ideals correspond to maximal cyclic codes of R_n.

Keywords: Linear and cyclic codes, Minimal and maximal cyclic codes, LCD cyclic codes.

Résumé

Ce travail se concentre sur la théorie des codes correcteurs d'erreurs, et plus particulièrement sur l'étude des codes cycliques maximaux.

Un code cyclique de longueur n sur le corps fini $\mathbb{F}_q$ peut être défini comme un idéal principal de l'anneau quotient $R_n = \mathbb{F}_q[x] \Big/ (x^n - 1)$ où $\mathbb{F}_q[x]$ est l'anneau des polynômes à coefficients dans le corps fini $\mathbb{F}_q$ et $\langle x^n - 1 \rangle$ est l'idéal principal engendré par le polynôme $(x^n - 1)$.

L'objectif principal de cette thèse est d'explorer les idéaux maximaux dans l'anneau quotient R_n, car ces idéaux correspondent aux codes cycliques maximaux de R_n.

Mots clés: Codes linéaires et cycliques, Codes cycliques minimaux et maximaux, Codes cycliques *LCD*.