PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

Mohamed Boudiaf University of M'sila

Faculty of Mathematics and Informatics

Departement of Mathematics

Master of Mathematics

Field : Mathematics and Informatics

Specialty: Mathematics

Option : Algebra and Discrete Mathematics

Theme

LCD cyclic codes over finite fields

Presented by :

BELOUADAH Ahamd - LATRECHE Saad

Publicly presented on : June 26, 2025.

In front of the jury :

MIHOUBI Douadi	Prof,	University of M'sila	**President**.
HEBOUB Lakhdar	M.C.B,	University of M'sila	**Supervisor**.
GHEDBANE Nacer	M.C.A,	University of M'sila	**Examiner**.

University years: 2024/2025.

Dedications

.... To my esteemed thesis supervisor,

I hope this letter finds you in the best of health and spirits. I would like to express my sincere and profound apologies for the neglect that occurred during the process of writing my thesis. Your guidance and assistance have always been of immense value to me, and there should be no lapse on my part in making the most of this invaluable opportunity.

I fully realize that dedication and commitment were crucial for the successful completion of this task. Unfortunately, the circumstances were not always favorable. Various personal and academic obligations piled up during this period, which affected my ability to engage fully in thesis writing.

There are no acceptable excuses for the neglect that occurred, and I understand that it tarnishes the image of my effort and diligence. I want to assure you that this situation will not be repeated in the future, and I will work even harder to compensate for this shortcoming.

★★★

Ahmed

Dedications

.... To my dearest people in my life,

My parents, my beloved siblings, my respected professor.

To my parents: First and foremost, I would like to express my deep gratitude for everything you have given me. Thanks to your boundless love and support, I was able to achieve this milestone. You are not only my parents but also my friends and the closest people to my heart. I owe you everything, and I love you very much.

To my siblings: To my dear siblings, the years of growth and sharing with you have been unforgettable. You have always been here for fun and support, and you have always been an integral part of my journey. Thank you for the beautiful moments and continuous motivation.

To my professor: I thank my great professor for the wonderful guidance and education you provided me. You have deeply impacted my academic journey and contributed to the development of my skills and understanding. I am sincerely grateful to you and appreciate your boundless efforts.

★★★

Saad

Table of contents

Notations

- $|G|$: Number of elements in G.
- $\mathbb{N}$: Natural numbers.
- $\mathbb{Z}$: Integer numbers.
- $\mathbb{R}$: Real numbers .
- $\mathbb{C}$: Complex numbers.
- $\mathbb{Q}$: Rational numbers.
- $\cong$: Isomorphism .
- $\mathbb{Z}/p\mathbb{Z}$: Integers modulo p.
- $\mathbb{F}_q$: Finite field with q elements and $\mathbb{F}_q^* = \mathbb{F} - \{0\}$.
- $char(\mathbb{F})$: Characteristic of $\mathbb{F}$.
- R/I : Quotient ring.
- $\mathbb{F}[X]$: The set of polynomials with coefficients in $\mathbb{F}$.
- w_H: Hamming weight.
- d_H: Hamming distance.

- d_{min} : Minimum distance.
- deg() : Degree of polynomial.
- $\langle \cdot, \cdot \rangle$: The Euclidean inner product .
- c^T : Transpose of c.
- $C^{\perp}$: Dual code of C.
- LCD : Linear Complementary Dual.
- $\lfloor x \rfloor$: The greatest integer less than or equal to the real number x.

Introduction

Error-correcting codes are a fundamental part of mathematics and computer science, developed to detect and correct errors in data transmission and storage. The field was established by Claude Shannon in 1948 and has since become essential in applications.

Linear symbols are among the most studied types of symbols for their algebraic properties, which make encoding and decoding easier. A linear code is typically denoted by $[n, k, d]$, where n is the length, k is the dimension, and d is the minimum Hamming distance.

A notable subclass of linear codes is the Linear Complementary Dual codes. These codes are defined by their property of having a trivial intersection with their dual codes, i.e., $C \cap C^{\perp} = \{0\}$. LCD codes are valued for their robustness in error correction and their broad applications in communications, consumer electronics, data storage, and cryptography.

The objective of this work is to study some specific linear complementary dual (LCD) cyclic codes over finite fields, focusing on their theoretical foundations and properties. The work is structured into three main chapters to achieve this goal:

Chapter 1, presents the fundamental mathematical concepts necessary for understanding the subsequent chapters. It begins with an overview of algebraic structures, followed by an introduction to finite fields, with a particular focus on their multiplicative structure. The chapter also covers polynomials over finite fields and how finite fields can be represented using polynomial representations. It concludes by addressing the existence and uniqueness of finite fields, as well as their construction via irreducible polynomials.

Chapter 2 focuses on linear and cyclic codes, beginning with essential concepts such as

weights and distances, followed by definitions of linear codes over finite fields. It also introduces generator and parity-check matrices, as well as dual codes. The chapter then turns to cyclic codes, covering their definitions, generator polynomials, and associated matrices.

Chapter 3 is dedicated to the study of linear complementary dual (LCD) cyclic codes over finite fields. It begins with general notions related to these codes, then explores q-cyclotomic cosets modulo n and related auxiliary tools, and concludes with detailed characterizations of LCD cyclic codes.

Chapter 1

Preliminaries

1.1 Algebraic Structure

The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure. In this chapter, we will define three common algebraic structures: groups, rings, and fields.

Definition 1.1 (Groups)**.**
A group is a set G together with a binary operation
$o : G \times G \to G$*, with the following properties. We write go h instead of o(g, h).*

(i) o *is associative, i.e.,* $fo(goh) = (fog)oh$ *for all* $f, g, h \in G$*;*

(ii) There exists a neutral elements $n \in G$*, i.e.,* $nog = gon = g$ *for all* $g \in G$*;*

(iii) For every $g \in G$ *there is some* $h \in G$ *with* $goh = hog = n$*, where* n *is the neutral element.*

If(G, o) also fulfills the law

(iv) $goh = hog$ *for all* $g, h \in G$*,*
then (G, o) is called a commutative or abelian group, $\mid G \mid$ *Abel the number of elements of G is called the order of the group G.*

Example 1.1.

We define a set $G = \{a, b, c, d\}$*, and the operation as shown in*

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

A very interesting group is the permutation group. The set is the set of all permutations, and the operation is composition: applying one permutation after another.

Definition 1.2 (Rings)**.**

A ring $(R, +, \cdot)$ *is a non-empty set* R *with two binary operations addition* $(+)$ *and multiplication* $(\cdot)$*, such that* :

(i) $(R, +)$ *is an abelian group;*

(ii) Associative of multiplication $(\cdot)$*, i.e.,* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *for all* $x, y, z \in R$*;*

(iii) The distributive laws hold; that is, for all $x, y, z \in R$ *we have*

$$x \cdot (y + z) = x \cdot y + x \cdot z,$$

and

$$(y + z) \cdot x = (y \cdot x) + (z \cdot x).$$

A ring is said to be commutative (or abelian) , if $x \cdot y = y \cdot x$ *for all* $x, y \in R$*, then* $(R, +, \cdot)$ *is called a commutative ring.*

Example 1.2.

$(\mathbb{Z}, +, \times)$*,* $(\mathbb{Q}, +, \times)$*,* $(\mathbb{R}, +, \times)$ *and* $(\mathbb{C}, +, \times)$ *are commutative rings.*

Definition 1.3.

Let R *be a ring.* R *is said to be commutative if this applies to multiplication. If there is an element* 1 *in* R *such that* $r \cdot 1 = 1 \cdot r = r$ *for any* $r \in R$*, then* 1 *is called an identity (or unit) element. As for groups (see the lines after 10.1), we easily see that the identity*

is unique if it exists. If $r \neq 0, s \neq 0$ *but* $rs = 0$*, then* r *is called a left divisor and* s *a right divisor of zero. If* R *has no zero divisors, i.e., if* $r \cdot s = 0$ *implies* $r = 0$ *or* $s = 0$ *for all* $r, s \in R$*, then* R *is called integral. A commutative integral ring with identity* $1 \neq 0$ *is called an integral domain. If* $(\mathbb{R}^*, \cdot)$ *is a group, then* R *is called a skew field or a division ring. If, moreover,* R *is commutative, we speak of a field. Hence a field is a ring* $(\mathbb{R}^*, +, \cdot)$ *in which both* $(\mathbb{R}, +)$ *and* $(\mathbb{R}^*, \cdot)$ *are abelian groups. The characteristic of* R *is the smallest natural number* k *with* $k \cdot r = \underbrace{r + r + \cdots + r}_{k-times} = 0$*, for all* $r \in R$*. We then write* $k = charR$*. If no such* k *exists, we put char* $R = 0$*. So if* $k = charR$*, all elements in the group* $(\mathbb{R}, +)$ *have an order dividing* k*.*

Now we list a series of examples of rings. Let R *be a ring and let* $S \subseteq R$*.* S *is called a sub ring of* R *(denoted by* $S \leq R$*) if* S *is a ring with respect to the operations of* R*.*

Example 1.3.

1. *The characteristic of* $\mathbb{R}, \mathbb{Q}$ *is* 0*.*
2. *The characteristic of* $\mathbb{Z}_p$ *is* p *for any prime* p*.*

Theorem 1.1.

(i) Every finite integral domain is a field.

(ii) If R *is an integral domain, then char* R *is prime.*

(iii) Every field is an integral domain.

Definition 1.4 (Ideals)**.**

A non-empty set I *of a ring* R*, is called an ideal on* R *if*

(i) $(I, +)$ *is a subgroup of a group* $(R, +)$*;*

(ii) $\forall a \in I, \forall x \in R$*, then* $a \cdot x \in I, x \cdot a \in I$*.*

Example 1.4.

Consider the ring $(\mathbb{Z}, +, \times)$*. Let* $n \in \mathbb{N}$*. Then* $I = \{a \cdot n \colon a \in \mathbb{Z}\}$ *is an ideal of* $\mathbb{Z}$*.*

Definition 1.5 (Principal ideal)**.**

An ideal $(I, +, \cdot)$ *of the ring* $(R, +, \cdot)$ *generated by a single element* $a \in R$ *is called a principal ideal, and is denoted by* $\langle a \rangle$ *such that*

$$I = \langle a \rangle = \{a \cdot r : r \in R\}.$$

Example 1.5.

1. *The principal ideal of the ring* $(\mathbb{Z}, +, \cdot)$ *generated by* n *is* :

   $I = \langle n \rangle = n\mathbb{Z}$ *, for some* $n \in \mathbb{N}$.

2. *Here are some examples of principal ideals in the ring* $(\mathbb{R}, +, \cdot)$:

   $I = \langle 0 \rangle = \{0\}$.

   $I = \langle 1 \rangle = \mathbb{R}$.

Definition 1.6 (Quotient ring)**.**

Let I *be an ideal of a ring* R*, then the set* $R/I = \{a + I : a \in R\}$ *is a ring for addition and multiplication are defined as* :

(i) $(a + I) + (b + I) = (a + b) + I$, $a, b \in R$;

(ii) $(a + I) \cdot (b + I) = a \cdot b + I$, $a, b \in R$.

This ring is called the quotient ring of R *with respect to the ideal* I *or ring of residue classes modulo* I.

Definition 1.7 (Field)**.**

A field is a set $\mathbb{F}$ *with binary operations addition* $(+)$ *and multiplication* $(\cdot)$*, for which the following axioms are satisfied* :

(i) $(\mathbb{F}, +)$ *is an abelian group (whose identity is* 0*) under the operation* $(+)$;

(ii) The set $\mathbb{F}^* = \mathbb{F} - \{0\} = \{a \in \mathbb{F}, a \neq 0\}$ *forms an abelian group (whose identity is* 1*) under the operation*$(\cdot)$;

(iii) Distributive law holds : $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$*, for all* $a, b, c \in \mathbb{F}$.

Theorem 1.2.

$\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p = \{0, 1, \cdots, p - 1\}$ *is a field if and only if* p *is a prime number.*

Lemma 1.1. F *is a field.* $\forall a, b \in F$

(i) $(-1) \cdot a = a$

(ii) $a \cdot b = 0$ *implies* $a = 0$ *or* $b = 0$.

Example 1.6.

1. $\mathbb{Z}_2$ *is a ring also a field.*

2. $\mathbb{Z}_4$ *is a ring but not a field since* 2^{-1} *does not exist.*

1.2 Finite Fields

Finite fields are one of the essential building blocks in coding theory and cryptography and thus appear in many areas in IT security. This section introduces finite fields systematically stating for which orders finite fields exist, shows how to construct them and how to compute in them efficiently.

Definition 1.8 (Finite fields)**.**
A field with finitely many elements is called a finite field.We denote a finite field with q elements by $\mathbb{F}_q$.
Finite fields are also called Galois fields, named after Evariste Galois, and several books and scientific papers thus use$GF(q)$ to denote a finite field with q elements.

Definition 1.9 (Characteristic)**.**
Let F be a field. The smallest natural number $n > 0$ such that

$$n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n-times} = 0,$$

is called the characteristic of F, denoted by $char(F) = n$. If no such n exists, we say $char(F) = 0$.

Example 1.7.
The ring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a finite field of characteristic p. Obviously $\mathbb{F}_p$ has exactly p elements and is thus finite, we have seen that it is a field and every element vanishes under multiplication by p, thus the characteristic is p. The following lemma gives useful properties of the characteristic.

Lemma 1.2.
Let K be a field.

(i) If the characteristic of K is positive, $char(K)$ is prime.

(ii) Finite fields have $char(K) > 0$. By the first part of this lemma we even have that a finite field has prime characteristic.

Corollary 1.1.
Let p be a prime. Up to isomorphism there is only one finite field with p elements, denoted by $\mathbb{F}_p$.

Lemma 1.3.

Let L be a finite field with $|L| = P^n$ and let$K$ be a subfield of L.

There exists an integer $n > 1$ so that $|L| = P^m$ and m/n.

The extension degree of$L$ over K is $[L : K] = n = m$.

Definition 1.10 (Primitive element)**.**

Let K be a finite field. A generator of K^* is called primitive element.

Corollary 1.2.

Every finite field contains at least one primitive element. More precisely there are exactly $\varphi(q-1)$ primitive elements.

This gives a second possibility of representing finite fields. Let g be a primitive element of K then

$$K = \{0, 1, g, g^2, \cdots, g^{q-2}\} = \{0\} \cup < g > .$$

Definition 1.11 (Polynomials)**.**

Let F be a field. A polynomial over F with the variable X is a polynomial of the form $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, where $a_0, a_1, \cdots, a_n \in F$ and $a_n \neq 0$, $n \geq 0$, where $\deg(f) = n$. The polynomial ring over F is

$$\mathbb{F}[X] = \left\{ \sum_{i=0}^{n} a_i X^i : a_i \in \mathbb{F}, n \geq 0 \right\}.$$

Example 1.8.

Let $f(X) = 2X^3 + 3X + 1$ and $g(X) = 1 + 2X$ be polynomials over $\mathbb{Z}_5$, where $\deg(f) = 3$ and $\deg(g) = 1$.

Definition 1.12 (Minimal polynomial)**.**

A minimal polynomial of an element $\alpha \in \mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ is a non-zero monic polynomial $f(x)$ of the least degree in $\mathbb{F}_q[x]$ such that $f(\alpha) = 0$.

Example 1.9.

Let α be a root of the polynomial $1 + x + x^2 \in \mathbb{F}_2[x]$. It is clear that the two linear polynomials x and $1 + x$ are not minimal polynomials of α. Therefore, $1 + x + x^2$ is a minimal polynomial of α. Since $1+(1+\alpha)+(1+\alpha)^2 = 1+1+\alpha+1+\alpha^2 = 1+\alpha+\alpha^2 = 0$ and $1 + \alpha$ is not a root of x or $1 + x, 1 + x + x^2$ is also a minimal polynomial of $1 + \alpha$.

Definition 1.13 (Irreducible polynomial)**.**

A polynomial $h \in \mathbb{F}[X]$ is said to be irreducible over F (or irreducible in $\mathbb{F}[X]$, or prime in $\mathbb{F}[X]$) if h has positive degree and $h = f \cdot g$, with $f, g \in \mathbb{F}[X]$ implies that either f or g is a constant polynomial.

Theorem 1.3.

Let K be a finite field and let $L = K[x]/f$. $K[x]$ be the residue classes modulo a polynomial $f \in L[x]$. L is a field if and only if f is irreducible.

Example 1.10.

1. Consider the ring $\mathbb{R}[x]/(1+x^2) = \{a + bx : a, b \in R\}$. It is a field since $1 + x^2$ is irreducible over $\mathbb{R}$. In fact, it is the complex field $\mathbb{C}$. To see this, we just replace x in $\mathbb{R}[x]/(1+x^2)$ by the imaginary unit i.

2. Consider the ring $\mathbb{Z}_2[x]/(1+x+x^2) = \{0, 1, x, 1+x\}$. As $1+x+x^2$ is irreducible over $\mathbb{Z}_2$, the ring $\mathbb{Z}_2[x]/(1+x+x^2)$ is in fact a field. This can also be verified by the addition and multiplication tables in

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

1.3 Polynomials over finite fields

This section studies polynomials over finite fields. In this Section we introduced many properties of polynomials over a field.

We recall the definition of an irreducible polynomial. A polynomial $f(x) \in K[x]$ is irreducible if it cannot be written as a product of polynomials of lower degree over the same field, i.e. $u(x)|f(x)$ implies u is constant or $u(x) = f(x)$. Otherwise it is called reducible.

Example 1.11. *Consider the following polynomials in $F_2[x]$: $f_1(x) = x$, $f_2(x) = x^2 + 1$, $f_3(x) = x^2 + x + 1$, and $f_4(x) = x^4 + x^2 + 1$.*

a) Apparently f_1 is irreducible.

b) A non-trivial factor of f_2 must be linear, one sees that $(x+1)|f_2(x)$, actually $f_2(x) = (x+1)^2$.

c) There are only two linear polynomials, x and $x+1$, over F_2 . One easily checks that none of them divides f_3 , so f_3 is irreducible.

d) The last polynomial is not divisible by a linear factor. However, it is not irreducible since $f_4(x) = (x2+x+1)^2 = (f_3(x))^2$. which cannot be factored further since f_3 is irreducible.

For functions over the reals, the derivative gives information about the slope of the tangent in a point. In the discrete setting of finite fields we lose this interpretation but we can still define the derivative of a polynomial.

1.4 Polynomial representation of finite fields

In this section we show how to construct finite fields with $p^n, n > 1$, elements by using an irreducible polynomial of degree n over F_p. The same considerations can be used to construct an extension field of K with $|K| = p^m$ in which case the polynomial must be irreducible over K.
We start by investigating relations between a finite field and a subfield of it.

Lemma 1.4. *Let $K; L$ be finite fields with $K \subset L, |K| = q, |L| = q^n$.*
Every element $\alpha \in L$ is a root of a uniquely defined monic polynomial $m_\alpha \in K[x], degm_\alpha \leq n$. This polynomial m_α satisfies that if α is a root of some polynomial $f \in K[x]$ then $m_\alpha|f$.

Proof. We start by considering L as a vector space over K. Since the dimension $dimK(L : K)$ is n, any $n+1$ or more elements are linearly dependent. So the elements $1; \alpha; \alpha^2; \ldots; \alpha^n$ are linearly dependent and there exist coefficients $c_0; \ldots; c_n \in K$ so that $c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0$.
We just constructed a polynomial $f(x) = \sum_{i=0}^{n} c_i x^i \in K[x]$ of degree n such that $f(\alpha) = 0$. This proves the existence part of the lemma.
Now that we know that there is at least one polynomial of degree $\leq n$ over K which has α as root and since we can make each polynomial monic as K is a field, let m_α be the

monic polynomial of minimal degree so that $m_\alpha(\alpha) = 0$. From the first part we know $deg(m_\alpha) \leq deg(f) \leq n$.
We first note that m_α must be irreducible because if it would split as $m_\alpha = a.b$ with $deg(a); deg(b) > 1$ would give $0 = m_\alpha(\alpha) = a(\alpha).b(\alpha)$ and because there are no zero divisors either $a(\alpha) = 0 \text{or} b(\alpha) = 0$ which contradicts the minimality of the degree of $m\alpha$. Let $f(\alpha) = 0$, and let $r(x); deg(r) < deg(m_\alpha)$ be the remainder of f by division by m_α, i.e. $f(x) = q(x)m_\alpha(x) + r(x)$. Evaluating both sides at α gives the identity.

$$0 = f(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) = q(\alpha).0 + r(\alpha) = r(\alpha).$$

so $r(\alpha) = 0$. Again by the minimality of $deg(m_\alpha)$ we obtain $r(x) = 0$ which means $m_\alpha | f$. □

Definition 1.14 (Minimal polynomial)**.** *Let K be a field, L be a finite extension field of K and $\alpha \in L$. The polynomial $m_\alpha \in K[x]$ constructed in Lemma1.4 is called the minimal polynomial of α over K.*

The prime fields F_p are constructed as residue classes of the integers modulo a prime p. We have seen that the ring of polynomials over a field shares many similarities with the ring of integers and so we consider the polynomial ring modulo an irreducible polynomial.

Theorem 1.4. *Let K be a finite field and let $L = K[x]/fK[x]$ be the residue classes modulo a polynomial $f \in L[x]$.*
L is a field if and only if f is irreducible.

Proof. In Example ?? we considered the case $K = F_2$ and $f(x) = x^n + 1$ in detail and showed that $F_2[x]/(x^n + 1)F_2$ is a commutative ring with unity. The same proof works for any field K and any polynomial f.
Let $deg(f) = n$. Like in the example we represent each residue class in L by the polynomial of smallest degree in it $L = \{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \ \ | a_i \in K\}$. Given that L is a commutative ring with unity for any field K and any polynomial f it remains to show the equivalence.

$$L \text{is a field} \iff f \text{is irreducible.}$$

Let f be irreducible and let $0 \neq a(x) \in K[x]$ be a polynomial of degree $deg(a) < n$. In

$K[x]$ we have $gcd(a(x); f(x)) = 1$ and Bézout's identity leads to a representation.

$$1 = a(x)u(x) + f(x)v(x); \text{with} deg(u) < n.$$

This implies $(a(x))^{-1} \equiv u(x)\ modf(x)$ and because of the degrees, a and u are both representatives of classes in L and we obtain the identity of classes $(a(x))^{-1} = u(x)$.
To prove the other implication assume on the contrary that f splits as $f(x) = g(x).h(x)$, with $1 \leq deg(g); deg(h) < n$. Because of the degrees, g and h are representatives of their respective classes in L and they both do not represent the class of 0. However, we have $g.h = f \equiv 0 modf$ and thus $g.h = 0$ in L which contradicts that fields do not have zero divisors.

□

This theorem is the most important tool to construct finite fields of cardinality p^n with $n > 1$. All we need is to find is an irreducible polynomial of degree n over $\mathbb{F}_p$. Let us first consider some examples.

Example 1.12. *Let $K = \mathbb{F}_2$.*

a) The polynomial $f(x) = x$ is obviously irreducible but the residue class field $\mathbb{F}_2[x]/(x) = \{a_0 \in \mathbb{F}_2\}$ is isomorphic to the field $\mathbb{F}_2$ itself.

b) Consider $f(x) = x^2 + 1$. We know from Example 19 that $f(x) = (x + 1)^2$ is not irreducible. Consider the addition and multiplication tables modulo f.

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	1	$1+x$
$1+x$	0	$1+x$	$1+x$	0

Since $(x + 1) \cdot (x + 1) = 0$ this is not a field but only a ring.

c) Let $f(x) = x^2 + x + 1$; f is irreducible. By the previous lemma, $F_2[x]/f$ is a field.

Given that the number of elements in

$$L = F_2[x]/(x^2 + x + 1) = \{a_0 + a_1 x | a_i \in F_2; 0 \leq i \leq 1\}.$$

is 4 we have that L is a finite field with 4 elements. In Example 12 we investigated what the field F_4 would look like. Note that the addition and multiplication tables we presented there apply directly to L with a representing the class of x and so we have now established that they define addition and multiplication in F_4.

Chapter 2

Linear codes and cyclic codes

Linear codes are a type of error-correcting code where any linear combination of codewords is also a valid codeword. Cyclic codes are a special subclass of linear codes with an additional property: if a codeword is part of the code then any cyclic shift of that codeword is also a valid codeword In this chapter, we will provide some fundamental notions Codes over Finite Fields, Dual Code and Cyclic codes over finite fields.

2.1 Basic Concepts of Codes over Finite Fields

In this section, we shall briefly recall some fundamental definitions in Coding Theory and give some examples of codes over $\mathbb{F}_q$, the finite field of order q.

Definition 2.1. *Let A be any finite set. A code C over A of length n is a subset of A^n.*

Coding theory is concerned with the following problem. Consider an information in the form of sequences $a_1, a_2, ..., a_m$ over a q-element set A. We wish to find a function f encoding $a_1, a_2, ..., a_m$ as another sequence $b_1, b_2, ..., b_n$ such that, if an error of specified type occurs in the sequence (b_i), the sequence (a_i) can still be recovered. There should also be a readily computable function g giving $a_1, a_2, ..., a_m$ from $b_1, b_2, ..., b_n$ with possible errors.

In terms of classical coding theory, the elements of the code are called codewords and the underlying set A is called an alphabet.

2.1.1 Weights and Distances

An important invariant of a code is the minimum distance between codewords. The principal distance used in coding theory is known as the Hamming distance.

Definition 2.2. *Let $v = (v_1, v_2, ..., v_n), w = (w_1, w_2, ..., w_n)$ in A^n where A is any set. Then the Hamming distance $d_H(v, w)$ is defined to be the number of coordinates in which v and w differ.*

$$d_H(v, w) = |\{i, |v_i \neq w_i\}|$$

The minimum Hamming distance of a code C defined over A is the smallest distance between distinct code words of C

$$d_H(C) = min\,\{d_H(v, w)|v, w \in C, v \neq w\}$$

.

Definition 2.3. *The Hamming weight $wt_H(v)$ of a vector v of A^n is the number of nonzero coordinates in v.*

$$wt_H(v) = |\{i, |v_i \neq 0\}|$$

.

Example 2.1. *Consider the code $C = \{c_0, c_1, c_2, c_3\}$ where $c_0 = (00000), c_1 = (10110), c_2 = (01011), c_3 = (11101)$. Then*

$$d(c_0, c_1) = 3, d(c_0, c_2) = 3, d(c_0, c_3) = 4, d(c_1; c_2) = 4, d(c_1, c_3) = 3, d(c_2, c_3) = 3$$

Hence, the minimum distance of C is $d = 3$.

During coding the channel, some sensitive letters of the received word can be badly transmitted. The number of errors is the number of those letters and decoding the channel consists of associating the received word to a word of C in order to find the initial submitted word.

Theorem 2.1. *Let C be a code over A of length n and minimum distance d, then*

1. *C has detection capability $l = d - 1$;*
2. *C has correction capability $t = [\frac{d-1}{2}]$.*

2.1.2 Linear Codes over Finite Fields

A general code might have no structure and not admit any representation other than listing the entire code book. We now focus on an important subclass of codes with additional structure called linear codes. Many of the important and widely used codes are linear. Throughout, we will denote by $\mathbb{F}_q$ the finite field with q elements, where q is a prime power.

Definition 2.4. *A linear code of length n and dimension k is a linear subspace C with dimension k of the vector space $\mathbb{F}_q^n$. Such a code is called a q-ary code.*
If $q = 2$ or $q = 3$, the code is described as a binary code, or a ternary code respectively. The size of a code is the number of code words and equals q^k.

In general, finding the minimum distance of a code requires comparing every pair of distinct elements. For a linear code however this is not necessary.

Theorem 2.2. *For $v, w \in \mathbb{F}_q^n$, we have $d_H(v; w) = wt_H(v - w)$. Hence, if C is a linear code over $\mathbb{F}_q$, the minimum distance d is the same as the minimum weight of the nonzero code words of C.*

As a result of this theorem, for linear codes, the minimum distance is also called the minimum weight of the code. If the minimum weight d of a code C is known, then we refer to the code as an $[n, k, d]$ code.

Example 2.2. *Consider*

$$C_1 = \{0000, 1000, 0100, 1100\}$$

and

$$C_2 = \{0000, 1100, 0011, 1111\}$$

C_1 and C_2 are both 2-dimensional subspaces of $\mathbb{F}_2^4$. The Hamming distance and weight of C_1 are both 1, whereas for C_2 they are both 2.

There is an important bound on the linear codes parameters, the Gilbert-Varshamov bound which give condition on the existence of a linear code.

Proposition 2.1. *There exist an $[n, k, d]$ linear code over $\mathbb{F}_q$ if the following inequality holds:*

$$q^{n-k} - 1 > \sum_{i=1}^{d-1} \binom{n-1}{i} (q-1)^i$$

Definition 2.5. *Two linear codes are said to be equivalent if one can be obtained from the other by a series of operations of the following two types:*

i. An arbitrary permutation of the coordinate positions, and;

ii. In any coordinate position, multiplication by any non-zero scalar.

In such case we say that the codes are monomially equivalent and so, they have the same parameters.

2.1.3 Generator and Parity Check Matrices

Definition 2.6. *A generator matrix for an [n; k; d] linear code C is any $k \times n$ matrix G whose rows form a basis for C. The matrix G completely defines the code C :*

$$C = xG; x \in \mathbb{F}_q^k$$

.

Since the basis of a $k-$ dimensional vector space is not unique, neither is the generator matrix G of a linear code C. For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an information set for C. The remaining $r = n - k$ coordinates are termed a redundancy set and r is called the redundancy of C. If the first k coordinates form an information set, the code has a unique generator matrix of the form $[I_k|A]$ where I_k is the $k \times k$ identity matrix and A is a $k \times (n - k)$ matrix. Such a generator matrix is in standard form. If a generator matrix in standard form exists for a linear code C, it is unique, and any other generator matrix can be brought to the standard from by the following operations:

- Permutation of the rows;
- Multiplication of a row by a non-zero element in $\mathbb{F}q$;
- Addition of a scalar multiple of one row to another.

Example 2.3. *Let the code C defined over $\mathbb{F}_2$ by matrix*

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

apply row operations to find the generator matrix of C in standard form .

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \xrightarrow{r_2 \leftrightarrow r_1} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\xrightarrow[r_4 \to r_4 + r_1]{r_3 \to r_3 + r_1} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{r_3 \to r_3 + r_2} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{r_4 \to r_4 + r_3} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \xrightarrow[r_3 \to r_3 + r_4]{\substack{r_1 \to r_1 + r_4 \\ r_2 \to r_2 + r_3}} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Definition 2.7. *A monomial matrix P is a square matrix with exactly one nonzero entry in each row and column. If all of its no zero elements are equal to 1, then P is said to be a permutation matrix.*

Thus two codes C_1 and C_2 are monomially equivalent provided that there exists a monomial matrix P such that if G_1 is a generator matrix of C_1 then G_1P is a generator matrix of C_2.

Theorem 2.3. *Let C be a linear code. Then C is permutation equivalent to a code which has generator matrix in standard form.*

Example 2.4. *Let C and C0 be the binary codes with generator matrices respectively*

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

We will show that C and C' are equivalent codes as follows. By row operations on G (add row 1 to rows 2 and 3), another generating matrix for C is

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

Now, if we select the permutation matrix

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

then $G' = \widehat{G}P$, P interchanges columns 1 and 3 of $\widehat{G}$, and hence interchanges coordinates 1 and 3 in each codeword of C. Thus the two codes are equivalent. Note, however, that these codes are not identical.

Since a linear code is a subspace of $\mathbb{F}_q^n$, it is the kernel of some linear application. In particular, there is an $(n-k) \times n$ matrix H, called a parity check matrix for the $[n, k, d]$ code C, defined by

$$C = ker\ H = \{x \in \mathbb{F}_q^n | Hx^T = 0\}$$

In general, there are also several possible parity check matrices for C. The next theorem gives one of them when C has a generator matrix in standard form.

Theorem 2.4. *If $G = [I_k|A]$ is a generator matrix for the $[n, k, d]$ code C in standard form, then $H = [-A^T|I_{n-k}]$ is a parity check matrix for C.*

Example 2.5. *The matrix*

$$G = [I_4|A] = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

is a generator matrix in standard form for a $[7, 4, 3]$ binary code C. By Theorem 2.4, a parity check matrix for C is

$$H = \left[A^T|I_3\right] = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

There is an elementary relationship between the weight of a codeword and a parity check matrix for a linear code. This is presented by the following theorem.

Theorem 2.5. *Let C be a linear code with parity check matrix H. If c is in C, the columns of H corresponding to the nonzero coordinates of c are linearly dependent. Conversely, if a linear dependence relation with nonzero coefficients exists among m columns of H, then there is a codeword in C of weight m whose nonzero coordinates correspond to these columns.*

One way to find the minimum weight d of a linear code is to examine all the nonzero codewords. The following corollary shows how to use the parity check matrix to find d.

Corollary 2.1. *A linear code has minimum weight d if and only if its parity check matrix H has a set of d linearly dependent columns but no set of $d-1$ linearly dependent columns.*

2.1.4 Dual Codes

Definition 2.8. *Let $C \subseteq \mathbb{F}_q^n$ be a linear code over a finite field $\mathbb{F}_q$. The **dual code** of C, denoted by $C^\perp$, is defined as:*

$$C^\perp = \left\{ \mathbf{v} \in \mathbb{F}_q^n \;\middle|\; \langle \mathbf{v}, \mathbf{c} \rangle = 0 \text{ for all } \mathbf{c} \in C \right\},$$

where $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{F}_q^n$, defined by:

$$\langle \mathbf{v}, \mathbf{c} \rangle = \sum_{i=1}^{n} v_i c_i.$$

The dual code $C^\perp$ is also a linear subspace of $\mathbb{F}_q^n$. Moreover, if $\dim(C) = k$, then:

$$\dim(C^\perp) = n - k.$$

Example 2.6. *A binary linear code of type $(n = 3, k = 2)$ is defined by the generator matrix:*

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

The code words generated by multiplying all binary messages $u \in \mathbb{F}_2^2$ with G are:

$$[0,0] \Rightarrow [0,0,0]$$
$$[1,0] \Rightarrow [1,0,1]$$
$$[0,1] \Rightarrow [0,1,1]$$
$$[1,1] \Rightarrow [1,1,0]$$

Thus, the linear code is:

$$C = \{000, 101, 011, 110\}.$$

The dual code $C^\perp$ consists of all vectors in $\mathbb{F}_2^3$ that are orthogonal to all codewords in C. The parity-check matrix is:

$$H = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Then the dual code is:

$$C^{\perp} = \{000, 111\}$$

Theorem 2.6. *If C is an $[n, k]$ code, then $C^{\perp}$ is an $[n, n-k]$ code.*

It is easy to show that 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 $C^{\perp}$.

A code C is said to be self dual if $C = C^{\perp}$ and it is isodual if C is equivalent to $C^{\perp}$. It is called LCD or linear complementary dual if $C \cap C^{\perp} = 0$.

For an $[n, k, d]$ linear code C with generator matrix G and a vector v in $\mathbb{F}_q^n$, we can easily show that v belongs to $C^{\perp}$ if and only if v is orthogonal to every row of G;

$$v \in C^{\perp} \Leftrightarrow Gv^T = 0$$

.

Example 2.7. *Let C be the ternary linear code C with generator matrix G, in standard form, given by*

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

Since $C = \langle v_1 = (1, 0, 1, 1), v_2 = (0, 1, 1, -1) \rangle$ and

$$Gv_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = Gv_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

This code is self-dual.

2.2 Cyclic codes over finite fields

Linear codes are nice to study and implement, because they have algebraic structures that ensure easy encoding and decoding. However, we can do more to simplify the implementation of codes if we require a cyclic shift of a codeword in C to still be a codeword. This requirement smells like a combinatorial structure, but we shall combine the works of the previous section to show that this has an algebraic structure.

2.2.1 Definitions

Definition 2.9. *Let $\mathbb{F}_q$ be a finite field with q elements, and let $C \subseteq \mathbb{F}_q^n$ be a linear code of length n. Then C is called a* ***cyclic code*** *if:*

$$\textit{For every } (c_0, c_1, \ldots, c_{n-1}) \in C, \textit{ the cyclic shift } (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

Example 2.8. *The sets*

$$\{0112, 2011, 1201, 1120)\} \subset \mathbb{F}_3^4, \quad \{11111\} \subset \mathbb{F}_2^5$$

are cyclic sets, but they are not cyclic codes since they are not linear spaces.

2.2.2 Generator polynomials

Since a cyclic code is invariant under a cyclic shift we conclude that a cyclic code contains all cyclic shifts of any code word. We can describe these codes in algebraic terms since any element $(c_0, c_1, \ldots, c_{n-1})$ of the vector space $\mathbb{F}_q^n$ can be identified by the residue class of the polynomial $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}(mod(x^n - 1))$ over $\mathbb{F}_q$, by the bijection

$$\begin{aligned} \mathbb{F}_q^n &\rightarrow \mathbb{F}_q[x]/\langle x^n - 1\rangle \\ (c_0, c_1, \ldots, c_{n-1}) &\rightarrow c_0 + c_1x + \cdots + c_{n-1}x^{n-1}mod(x_n - 1) \end{aligned}$$

Therefore, any code word is identified as a vector or as a polynomial. It is clear that if C is a cyclic code and $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ in C then

$$xc(x) = c_0x + c_1x^2 + \cdots + c_{n-1}x^n = c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} \in C$$

.

Hence, multiplying the polynomial $c(x)$ by x corresponds to a right shift of the vector c. It follows that cyclic codes over $\mathbb{F}_q$ are precisely the ideals of the ring $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$, and vice versa. Therefore, the study of cyclic codes over $\mathbb{F}_q$ is equivalent to the study of ideals in R_n. It is known that R_n is a principapl ideal ring and hence cyclic codes are the principal ideals of R_n. More precisely, C is generated by the monic polynomial of least degree $g(x)$ in C; called the generator polynomial. Then, $g(x)$ is a divisor of $x^n - 1$ in $\mathbb{F}_q$.

Definition 2.10. *Let $C = \langle g(x)\rangle$ be a cyclic code of length n over $\mathbb{F}_q$. Then $g(x)$ is called the generator polynomial of C.*
Since $g(x)$ is monic of degree $n - k$, the parity-check 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 $\mathbb{F}_q$.

Any code word $c(x)$ in C can be uniquely written as $c(x) = \lambda(x)g(x)$, where $\lambda(x)$ has degree less than $n\ deg(g(x))$ and the dimension of C is $k = n - deg(g(x))$. This discussion gives the following theorem.

Theorem 2.7. *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 $\mathbb{F}_q[x]$.*

Example 2.9. *Table of Binary Cyclic Code of length 7, Generated by the Polynomial $g(x) = 1 + x + x^3$.*

Messages	*Message Poly* $\mathbf{u}(x)$	*Code Polynomial* $c(x) = \mathbf{u}(x) \cdot g(x)$	*Code Vector*
0000	*0*	$0\left(1+x+x^3\right) = 0$	*0000000*
0001	x^3	$x^3\left(1+x+x^3\right) = x^3+x^4+x^6$	*0001101*
0010	x^2	$x^2\left(1+x+x^3\right) = x^2+x^3+x^5$	*0011010*
0011	x^2+x^3	$\left(x^2+x^3\right)\left(1+x+x^3\right) = x^2+x^4+x^5+x^6$	*0010111*
0100	x	$x\left(1+x+x^3\right) = x+x^2+x^4$	*0110100*
0101	$x+x^3$	$\left(x+x^3\right)\left(1+x+x^3\right) = x+x^2+x^3+x^6$	*0111001*
0110	$x+x^2$	$\left(x+x^2\right)\left(1+x+x^3\right) = x+x^3+x^4+x^5$	*0101110*
0111	$x+x^2+x^3$	$\left(x+x^2+x^3\right)\left(1+x+x^3\right) = x+x^5+x^6$	*0100011*
1000	*1*	$1\left(1+x+x^3\right) = 1+x+x^3$	*1101000*
1001	$1+x^3$	$\left(1+x^3\right)\left(1+x+x^3\right) = 1+x+x^4+x^6$	*1100101*
1010	$1+x^2$	$\left(1+x^2\right)\left(1+x+x^3\right) = 1+x+x^2+x^5$	*1110010*
1011	$1+x^2+x^3$	$\left(1+x^2+x^3\right)\left(1+x+x^3\right) = 1+x+x^2+x^3+x^4+x^5+x^6$	*1111111*
1100	$1+x$	$(1+x)\left(1+x+x^3\right) = 1+x^2+x^3+x^4$	*1011100*
1101	$1+x+x^3$	$\left(1+x+x^3\right)\left(1+x+x^3\right) = 1+x^2+x^6$	*1010001*
1110	$1+x+x^2$	$\left(1+x+x^2\right)\left(1+x+x^3\right) = 1+x^4+x^5$	*1000110*
1111	$1+x+x^2+x^3$	$\left(1+x+x^2+x^3\right)\left(1+x+x^3\right) = 1+x^3+x^5+x^6$	*1001011*

Theorem 2.8. *The dual code of a cyclic code is cyclic.*

Definition 2.11. *Let* $f(x) = a_0 + a_1x + \cdots + a_rx^r$ *be a polynomial of* $R[x]$ *of degree* r *such that* $f(0) = a_0$ *is a unit in* R *(where* R *is a finite commutative ring). The monic reciprocal polynomial of* $f(x)$ *is defined by*

$$f^* = f(0)^{-1}x^r f\left(x^{-1}\right)$$

If $f^*(x) = f(x)$*, the polynomial* $f(x)$ *is called self reciprocal.*

The following Lemma is easily deduced.

Lemma 2.1. *Let* $f(x)$ *and* $g(x)$ *be two polynomials in* $R[x]$ *with* $\deg f(x) \geq \deg g(x)$ *and with constants terms are units. Then the following holds.*

i. $[f(x)g(x)]^* = f(x)^*g(x)^*$

ii. $[f(x)+g(x)]^* = f(x)^* + x^{\deg f - \deg g}g(x)^*$

2.2.3 Generator and parity-check matrices

In the previous section, we showed that a cyclic code is totally determined by its generator polynomial. Hence, such a code should also have generator matrices determined by this polynomial. Indeed, we have the following result.

Theorem 2.9. *Let $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ be the generator polynomial of a cyclic code C in $\mathbf{F}_q^n$ with $\deg(g(x)) = n - k$. Then the matrix.*

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

is a generator matrix of C (note that we identify a vector with a polynomial).

Proof. It is sufficient to show that $g(x), xg(x), \ldots, x^{k-1}g(x)$ form a basis of C. It is clear that they are linearly independent over $\mathbb{F}_q$. By Theorem 7.2.14, we know that $\dim(C) = k$. The desired result follows.

Example 2.10. *Consider the binary $[7, 4]$-cyclic code with generator polynomial $g(x) = 1 + x^2 + x^3$. Then this code has a generator matrix*

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

Definition 2.12. *Let C be a q-ary cyclic code of length n. Put $h(x) = (x^n - 1)/g(x)$. Then, $h_0^{-1}h_{\mathrm{R}}(x)$ is called the parity-check polynomial of C, where h_0 is the constant term of $h(x)$.*

Corollary 2.2. *Let C be a q-ary $[n, k]$-cyclic code with generator polynomial $g(x)$. Put $h(x) = (x^n - 1)/g(x)$. Let $h(x) = h_0 + h_1x + \cdots + h_kx^k$. Then the matrix*

$$H = \begin{pmatrix} h_{\mathrm{R}}(x) \\ xh_{\mathrm{R}}(x) \\ \cdot \\ \cdot \\ \cdot \\ x^{n-k-1}h_{\mathrm{R}}(x) \end{pmatrix} = \begin{pmatrix} h_k & h_{k-1} & \cdot & \cdot & \cdot & h_0 & 0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & h_k & h_{k-1} & \cdot & \cdot & \cdot & h_0 & 0 & 0 & \cdot & \cdot & 0 \\ \cdot & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & h_k & h_{k-1} & \cdot & \cdot & \cdot & h_0 & \end{pmatrix}$$

is a parity-check matrix of C.

Proof. The result immediately follows from Theorems 7.3.1 and 7.3.7.

Example 2.11. *Let C be the binary [7,4]-cyclic code generated by $g(x) = 1 + x^2 + x^3$ as in previous Example. Put $h(x) = \left(x^7 - 1\right)/g(x) = 1 + x^2 + x^3 + x^4$. Then $h_{\mathrm{R}}(x) = 1 + x + x^2 + x^4$ is the parity-check polynomial of C. Hence,*

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

is a parity-check matrix of C.

Chapter 3

LCD cyclic codes over finite fields

Introduction

Linear codes with complements, also known as binary complementary codes, are important concepts in encryption theory and data communication. These codes were developed to provide an effective solution for secure and reliable transmission of information, especially in environments prone to interference or noise.

The unique feature of these codes is that each code has an orthogonal complementary binary code. This means that the combination of the original code and its complementary code spans the entire vector space without any overlap. These codes are based on principles of mathematics and linear algebra, where data is encoded into sequences of numbers or symbols, allowing it to be transmitted through various communication channels with minimal impact from noise or data loss.

3.1 Generalities on LCD Codes over Finite Fields

Definition LCD Code : A linear code C over a field $\mathbb{F}_q$ is called an LCD code (linear code with complementary dual) if $C \cap C^{\perp} = \{0\}$, which is equivalent to $C \oplus C^{\perp} = \mathbb{F}_q^n$.

Example 3.1. *Let C be a binary $[3, 2]$ code. If*

$$C = \{000, 010, 001, 011\}.$$

then the dual code $C^{\perp}$ is given by

$$C^{\perp} = \{000, 100\}.$$

Since $C \cap C^{\perp} = \{0\}$, we deduce that C is an LCD (Linear Complementary Dual) code.

Proposition 3.1. *[7] Let C be a linear code with a generator matrix G and a parity-check matrix H. Then the three following properties are equivalent:*

i. C is an LCD code;

ii. $C^{\perp}$ is an LCD code

iii. The matrix GG^T is invertible;

iv. The matrix HH^T is invertible.

Corollary 3.1. *Let C be a linear code with generator matrix in standard form $G = [I_k|A]$. Then C is an LCD code if and only if -1 is not an eigenvalue of AA^T.*

Proof. By a simple calculation we have

$$GG^T = [I_k|A] \left[\frac{I_k}{T}\right] = AA^T + I_k$$

The matrix GG^T is invertible if and only if -1 is not an eigenvalue of AA^T. □

Example 3.2. *Let C be the binary code with generator matrix*

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

The parity-check matrix H of this code is

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

Since

$$det\ (GG^T) = det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \neq 0$$

Then this code is an LCD code. it follows that

$$det\ (HH^T) = det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq 0$$

3.2 q-Cyclotomic cosets modulo n and auxiliaries

To deal with cyclic codes of length n over $GF(q)$, we have to study the canonical factorization of $x^n - 1$ over $GF(q)$. To this end, we need to introduce q-cyclotomic cosets modulo n. Note that $x^n - 1$ has no repeated factors over $GF(q)$ if and only if $gcd(n, q) = 1$ Throughout this paper, we assume that $gcd(n, q) = 1$.

Let $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$, denoting the ring of integers modulo n. For any $s \in \mathbb{Z}_n$,

the q-cyclotomic coset of s modulo n is defined by

$$C_s = \{s, sq, sq^2, \ldots, sq^{\ell_s - 1}\} \; mod \; n \subseteq \mathbb{Z}_n.$$

where ℓ_s is the smallest positive integer such that $s \equiv sq^{\ell_s} \pmod{n}$, and is the size of the q-cyclotomic coset. The smallest integer in C_s is called the coset leader of C_s. Let $\Gamma(n, q)$ be the set of all the coset leaders. We have then $C_s \cap C_t = \emptyset$ for any two distinct elements s and t in $\Gamma(n, q)$, and

$$\bigcup_{s \in \Gamma_{n,q}} C_s = \mathbb{Z}_n. \tag{3.1}$$

Hence, the distinct q-cyclotomic cosets modulo n partition $\mathbb{Z}_n$.

Let $m = ord_n(q)$, and let α be a generator of $GF(q^m)^*$, which denotes the multiplicative group of $GF(q^m)$. Put $\beta = \alpha^{(q-1)/n}$. Then β is a primitive n-th root of unity in $GF(q^m)$. The minimal polynomial $m_s(x)$ of β_s over $GF(q)$ is the monic polynomial of the smallest degree over $GF(q)$ with β_s as a zero. It is now straightforward to prove that this polynomial is given by

$$m_s(x) = \prod_{i \in C_s} \left(x - \beta^i\right) \in GF(q)[x], \tag{3.2}$$

which is irreducible over $GF(q)$. It then follows from (3.1) that

$$x^n - 1 = \prod_{s \in \Gamma_{(n,q)}} m_s(x) \tag{3.3}$$

which is the factorization of $x^n - 1$ into irreducible factors over $GF(q)$. This canonical factorization of $x^n - 1$ over $GF(q)$ is crucial for the study of cyclic codes.

3.3 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 3.1. *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 3.3. *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*

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

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

and

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

Lemma 3.1. *The size* ℓ_s *of each q-cyclotomic coset* C_s *is a divisor of* $ord_n(q)$, *which is the size* ℓ_1 *of* C_1.

Lemma 3.2. *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 the sum*

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

and the intersection $C_1 \cap C_2$ *are also cyclic codes.*

Theorem 3.1. *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* $\gcd(g_1(x), g_2(x))$.

Theorem 3.2. *Let* C_1 *and* C_2 *be cyclic codes of length n over* $\mathbb{F}_q$ *with generator polynomial* $g_1(x), g_2(x)$. *Then* $C_1 \cap C_2$ *has generator polynomial* $Icm(g_1(x), g_2(x))$.

Lemma 3.3. *Let C_i be a cyclic code of length n over $\mathbb{F}_q$ for $i = 1, 2$. Then the sum $C_1 + C_2$ is a direct sum if and only if $C_1 \cap C_2 = \{0\}$.*

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

Lemma 3.4. *Let C_i be cyclic codes of length n over $\mathbb{F}_q$ for $i \in \{1, 2, 3\}$. Then the sum $C_1 + C_2 + C_3$ is a direct sum if and only if*

$$\dim(C_1 + C_2 + C_3) = \dim(C_1) + \dim(C_2) + \dim(C_3).$$

3.4 Characterisations of LCD cyclic codes over finite fields

Let $f(x) = f_h x^h + f_{h-1}x^{h-1} + \cdots + f_1 x + f_0$ be a polynomial over $GF(q)$ with $f_h \neq 0$ and $f_0 \neq 0$ The reciprocal $f^*(x)$ of $f(x)$ is defined by

$$f^* = f_0^{-1} x^h f\left(x^{-1}\right)$$

Definition 3.2 (Self-reciprocal)**.** *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 polynomial is self-reciprocal if it coincides with its reciprocal.

Definition 3.3. *A code C is called reversible if for each code word $(c_0, c_1, \ldots, c_{n-1}) \in C$, the reverse code word $(c_{n-1}, c_{n-2}, \ldots, c_0) \in C$. This means that reversing the order of the components of any codeword gives always again a codeword.*

Proposition 3.2. *[8] A cyclic code is reversible if and only if its generator polynomial is self reciprocal.*

Theorem 3.3. *Let C be a cyclic code of length n over $GF(q)$ with generator polynomial $g(x)$. Then the following statements are equivalent.*

i. C is an LCD code.

ii. g is self-reciprocal.

iii. β^{-1} is a root of g for every root β of $g(x)$ over the splitting field of $g(x)$.

Furthermore, if -1 is a power of q mod n, then every cyclic code over $GF(q)$ of length n is reversible.

3.5 LCD Cyclic Codes of Length $2p$

3.5.1 Factorization of $x^{2p}-1$ over $\mathbb{F}_q$ and Auxiliary Results

Proposition 3.3. *Let $\mathbb{F}_q$ be a finite field with q elements, and let p be an odd prime such that $\gcd(p,q)=1$. Suppose that $2p \mid (q^m-1)$, where $m = ord_{2p}(q)$. Then:*

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

where $m_0(x) = x-1$, denotes a complete set of representatives of the q-cyclotomic cosets modulo $2p$.

$$m_p(x) = x+1, \quad m_1(x) = x^{p-1}-x^{p-2}+\cdots-x+1, \quad m_2(x) = x^{p-1}+x^{p-2}+\cdots+x+1.$$

The cyclic codes

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

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

Furthermore, the cyclic codes
$\widehat{m_0} = \left\langle \dfrac{x^{2p}-1}{m_0(x)} \right\rangle, \quad \widehat{m_p} = \left\langle \dfrac{x^{2p}-1}{m_p(x)} \right\rangle, \quad \widehat{m_1} = \left\langle \dfrac{x^{2p}-1}{m_1(x)} \right\rangle, \quad \widehat{m_2} = \left\langle \dfrac{x^{2p}-1}{m_2(x)} \right\rangle$
are all the distinct minimal cyclic codes of length $2p$ over $\mathbb{F}_q$.

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

Table 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 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 $g(x)$
$\widehat{m_0} = \left\langle \frac{(x^{2p}-1)}{m_0(x)} \right\rangle$	$m_p(x) \times m_1(x) \times m_2(x)$	$m_p(x) \times m_1(x) \times m_2(x)$
$\widehat{m_p} = \left\langle \frac{(x^{2p}-1)}{m_p(x)} \right\rangle$	$m_0(x) \times m_1(x) \times m_2(x)$	$m_0(x) \times m_1(x) \times m_2(x)$
$\widehat{m_1} = \left\langle \frac{(x^{2p}-1)}{m_1(x)} \right\rangle$	$m_0(x) \times m_p(x) \times m_2(x)$	$m_0(x) \times m_p(x) \times m_2(x)$
$\widehat{m_2} = \left\langle \frac{(x^{2p}-1)}{m_2(x)} \right\rangle$	$m_0(x) \times m_p(x) \times m_1(x)$	$m_0(x) \times m_p(x) \times m_1(x)$

Proposition 3.4. *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 and $\phi(p) = p-1$ 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 1, $g(x)$ is a self-reciprocal. By Theorem 4, the code C is an LCD cyclic code.

Proposition 3.5. *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 $\phi(p) = p-1$ 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 2, $g(x)$ is a self-reciprocal. By Theorem 4, the code C is an LCD cyclic code.

Proposition 3.6. *If C is an LCD maximal cyclic code 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 $2p$, then C can be represented as a direct sum of three LCD minimal cyclic codes of length $2p$ over $\mathbb{F}_q$, i.e.,*

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

Proof. Using Lemma 3.4, Theorem 3.1, and the properties of the greatest common divisor (gcd) of polynomials, we find that if

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

then

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

Since

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

we have

$$\dim(C) = \dim\left(\langle \gcd(m_1(x) \cdot m_2(x), m_0(x) \cdot m_p(x) \cdot m_2(x)) \rangle\right).$$

Thus,

$$\dim(C) = \dim\left(\langle m_2(x) \cdot \gcd(m_1(x), m_0(x) \cdot m_p(x)) \rangle\right) = \dim(\langle m_2(x) \rangle) = \dim(M_2).$$

Hence,

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

which implies

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

In a similar way, if $C_1 = \widehat{m_0}, C_2 = \widehat{m_p}, C_3 = \widehat{m_2}$
then

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

Hence,

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

In a similar way, if

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

then

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

Hence,

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

In a similar way, if

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

then

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

Hence,

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

□

Example 3.4. *Take* $q = 3, p = 17$. *Then the maximal ternary LCD cyclic codes* M_0, M_p, M_1, M_2 *of length 34 and the minimal ternary LCD cyclic codes* $\widehat{m_0}, \widehat{m_p}, \widehat{m_1}, \widehat{m_2}$ *of length 34 are given as follows:*

(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 $g_0(x) = \dfrac{(x^{34}-1)}{m_0(x)} = x^{33} +$
$x^{32} + x^{31} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} +$
$x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$

$$g_{17}(x) = \frac{(x^{34}-1)}{m_{17}(x)} = x^{33} - x^{32} + x^{31} - x^{30} + x^{29} - x^{28} + x^{27} - x^{26} + x^{25} - x^{24} + x^{23} - x^{22} + x^{21} -$$
$$x^{20} + x^{19} - x^{18} + x^{17} - x^{16} + x^{15} - x^{14} + x^{13} - x^{12}$$
$$+ x^{11} - x^{10} + x^9 - x^8 + x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1,$$
$$g_1(x) = \frac{(x^{34}-1)}{m_1(x)} = x^{18} + x^{17} - x - 1,$$
$$g_2(x) = \frac{(x^{34}-1)}{m_2(x)} = x^{18} - x^{17} + x - 1.$$

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

LCD Maximal cyclic code of length 34 over $\mathbb{F}_3$	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 LCD

cyclic codes of length 34 are given by:

LCD Minmal cyclic code of length 34 over $\mathbb{F}_3$	$\widehat{m_0}$	$\widehat{m_p}$	$\widehat{m_1}$	$\widehat{m_2}$
Generating polynomial	$g_0(x)$	$g_{17}(x)$	$g_1(x)$	$g_2(x)$
Dimension	1	1	16	16

Conclusion

In this work, we explored the theory and structure of error-correcting codes, with a particular focus on linear and cyclic codes over finite fields. We began by introducing essential algebraic foundations, including finite fields and polynomial representations, which are crucial for understanding the construction and behavior of such codes. We then delved into the properties and representations of linear and cyclic codes, highlighting the role of generator and parity-check matrices, as well as the concept of duality. The final chapter was devoted to Linear Complementary Dual (LCD) cyclic codes, where we examined their specific structures, characterizations, and the importance of cyclotomic cosets and factorization techniques in their study. These codes are of great theoretical and practical value due to their error-correcting capabilities and applications in modern communication systems and data security. The results presented here provide a solid foundation for further research into more advanced constructions and applications of LCD codes in cryptography and beyond.

Bibliography

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1981.

[2] S. T. Dougherty, *Algebraic Coding Theory Over Finite Commutative Rings*. SpringerBriefs in Mathematics, Springer, 2017.

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

[4] N. Sendrier, "Linear codes with complementary duals meet the gilbert-varshamov bound," *Discrete Mathematics*, vol. 285, pp. 345--347, 2004.

[5] S. A. Vanstone and P. V. Oorschot, *Introduction To Error Correcting Codes With Applications*. Library of Congress Cataloging-In-Publication Data, 1989.

[6] E. J. Cheon, "Equivalence of linear codes with the same weight enumerator," *Scientiae Mathematicae Japonicae Online*, vol. e-2006, pp. 567--576, 2006.

[7] J. L. Massey, "Linear codes with complementary duals," *Discrete Mathematics*, vol. 106/107, pp. 337--342, 1992.

[8] X. Yang and J. L. Massey, "The condition for a cyclic code to have a complementary dual," *Discrete Mathematics*, vol. 126, no. 1--3, pp. 391--393, 1994.

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

[10] L. Heboub, D. Mihoubi, Some LCD cyclic codes of length 2p over finite fields. Discussiones Mathematicae-General Algebra and Applications 44.2 (2024): 249-259.

[11] L. Heboub, D. Mihoubi, Minimal and maximal cyclic codes of length 2p, Journal of Discrete Mathematical Sciences and Cryptography, Vol. 27 (2024), No. 1, pp. 6374.

[12] L. Heboub, Sur les codes cycliques maximaux de longueur n, These Doctorat, University of M'sila, 2024.

[13] A. Saha, N. Manna and S. Mandal, Information Theory, Coding and Cryptography. Pearson Education India (2013).

ملخص

في هذه المذكرة، قمنا بدراسة مفهوم الرموز الخطية والرموز الخطية الدورية، ثم تطرقنا الى نوع خاص من الرموز وهو الرموز الخطية المكملة والمزدوجة الدورية.

كلمات مفتاحية

الرموز الخطية، الرموز الدورية، الرموز الخطية التكميلية المزدوجة الدورية.

Abstract

In this memory, we have studied the concept of linear codes and linear cyclic codes. We then examined a particular subclass of these codes, Linear Complemented Dual cyclic codes over finite fields.
.

Key words

Linear codes, cyclic codes, LCD cyclic codes.

Résumé

Dans ce mémoire, nous avons étudié le concept des codes linéaires et codes linéaires cycliques. Nous nous sommes ensuite intéressés à une classe particulière de ces codes, Codes cycliques duaux complémentés linéaires sur corps finis
.

Mot-clés

Codes linéaires, codes cycliques, LCD codes cycliques.