DEMOCRATIC AND POPULAR REPUBLIC
OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND
SCIENTIFIC RESEARCH

Mohamed Boudiaf University of M'sila
Faculty of Mathématics and Computer Sciences
Departement of Mathématics

Master memory

Field: Mathematics and Computer Sciences
Branch: Mathematics
Option: Algebra and Discrete Mathematics

Theme

Some properties of LCD cyclic codes over finite fields

Presented by :
Attallah seddik
Gherabi abdelhafid

Before the juru composed of :

D. MIHOUBI	**Prof,**	**University of M'sila**	**President**
L. HEBOUB	**M.C.B,**	**University of M'sila**	**Supervisor**
N. GHADBANE	**M.C.A,**	**University of M'sila**	**Examiner**

University year 2023/2024.

To the soul of my dear father, may God have mercy on him and make him dwell in his spacious paradise.

To my dear mother, may God prolong her life,

To my wife and to my beloved children, Akram, Alaa, Yahya and Khadija may God protect them and prolong their lives.

To my colleague Haj GHERABI Abdel Hafid, and to everyone who contributed to this humble research, whether from near or far.

To the soul of my dear parents,

To all my entire family members from the youngest to the oldest, my classmates, our esteemed teachers, my honorable colleague and partner in preparing this document Mr ATTALLAH Seddik without forgetting our supervisor Mr Lakhdar HEBOUB.

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.

$\gcd(a, b)$: 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

Coding theory originated with the 1948 publication of the paper "A mathematical theory of communication" by Claude Shannon. For the past half century, coding theory has grown into a discipline intersecting mathematics and engineering with applications to almost every area of communication such as satellite and cellular telephone transmission, compact disc recording, and data storage.

Cyclic codes over finite fields indeed play an important 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.

This document is divided into three chapters. The first chapter is about coding theory which serves as a recall of the essential concepts and notation that will be used in the subsequent chapters and will cover some generalities the code like, hamming distance, hamming weight, distance of a code, linear codes and generator and parity-check matrix, dual codes.

Chapter 2 is about cyclic codes which is a special classes of linear codes. We present some algebraic description of cycl codes.

Chapter 3 is about some properiete of LCD cyclic codes over finite fields of length $N = 2p$ with p is an odd prime. More precsely,is about the minimal and maximal LCD 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., $q^{p-1} \equiv 1 (\mathrm{mod}\, 2p)$.

Chapter 1

Coding theory

1.1 Preliminaries

We begin with some basic definitions.

Definition 1.1.1 *Let $A = \{a_1, a_2, ..., a_q\}$ be a set of size q, which we refer to as a code alphabet and whose elements are called code symbols.*

(i) A q-ary word of length n over A is a sequence $w = w_1 w_2 ... w_n$ with each $w_i \in A$ for all i. Equivalently, w may also be regarded as the vector $(w_1, ..., w_n)$.

(ii) A q-ary block code of length n over A is a nonempty set C of $q-$ary words having the same length n.

(iii) An element of C is called a codeword in C.

(iv) The number of codewords in C, denoted by $|C|$, is called the size of C.

(v) The (information) rate of a code C of length n is defined to be $(log_q|C|)/n$.

(vi) A code of length n and size M is called an $(n, M)-$code.

Example 1.1.1 *A code over the code alphabet $\mathbb{F}_2 = \{0, 1\}$ is called a binary code; i.e., the code symbols for a binary code are 0 and 1. Some examples of binary codes are:*

(i) $C_1 = \{00, 01, 10, 11\}$ is a $(2, 4)$-code;

(ii) $C_2 = \{000, 011, 101, 110\}$ is a $(3, 4)$-code;

(iii) $C_3 = \{0011, 0101, 1010, 1100, 1001, 0110\}$ is a $(4, 6)$-code.

A code over the code alphabet $\mathbb{F}_3 = \{0, 1, 2\}$ is called a ternary code, while the term quaternary code is sometimes used for a code over the code alphabet $\mathbb{F}_4$. However, a code over the code alphabet $\mathbb{Z}_4 = \{0, 1, 2, 3\}$is also some times referred to as a quaternary code .

1.1.1 Hamming distance

Definition 1.1.2 *Let x and y be words of length n over an alphabet A. The (Hamming) distance from x to y, denoted by $d(x, y)$, is defined to be the number of places at which x and y differ. If $x = x_1...x_n$ and $y = y_1...y_n$, then*

$$d(x, y) = d(x_1, y_1) + ... + d(x_n, y_n).$$

where x_i and.y_i.are regarded as words of length 1, and

$$d(x_i, y_i) = \begin{cases} 1 \text{ if } x_i \neq y_i \\ 0 \text{ if } x_i = y_i. \end{cases}$$

Example 1.1.2 *(i) Let $A = \{0, 1\}$ and let $x = 01010$, $y = 01101$, $z = 11101$. Then*

$$\begin{aligned} d(x, y) &= 3, \\ d(y, z) &= 1, \\ d(z, x) &= 4. \end{aligned}$$

(ii) Let $A = \{0, 1, 2, 3, 4\}$ and let $x = 1234, y = 1423, z = 3214$. Then

$$\begin{aligned} d(x, y) &= 3, \\ d(y, z) &= 4, \\ d(z, x) &= 2. \end{aligned}$$

Proposition 1.1.1 *Let x, y, z be words of length n over A. Then we have*

(i) $0 \leq d(x, y) \leq n$,

(ii) $d(x, y) = 0$ if and only if $x = y$,

(iii) $d(x, y) = d(y, x)$,

(iv) (Triangle inequality) $d(x, z) \leq d(x, y) + d(y, z)$.

1.1.2 *Hamming weight*

Recall that the Hamming distance $d(x, y)$ between two words x, $y \in \mathbb{F}_q^n$,

where 0 is the zero word.

Definition 1.1.3 *Let x be a word in $\mathbb{F}_q^n$. The (Hamming) weight of x, denoted by $wt(x)$, is defined to be the number of nonzero coordinates in x; i.e.,*

$$wt(x) = d(x, 0).$$

Remark 1.1.1 *For every element x of $\mathbb{F}_q^n$, we can define the Hamming weightas follows:*

$$wt(x) = d(x, 0) = \begin{cases} 1 \text{ if } x \neq 0 \\ 0 \text{ if } x = 0. \end{cases}$$

Then, writing $x \in \mathbb{F}_q^n$ as $x = (x_1, x_2, ..., x_n)$, the Hamming weight of x can also be equivalently defined as

$$wt(x) = wt(x_1) + wt(x_2) + ... + wt(x_n). \textit{(1.1)}$$

Lemma 1.1.1 *If x, $y \in \mathbb{F}_q^n$, then $d(x, y) = wt(x - y)$.*

Proof. For x, $y \in \mathbb{F}_q^n$, $d(x, y) = 0$ if and only if $x = y$, which is true if and only if $x - y = 0$ or, equivalently, $wt(x - y) = 0$. ■

Corollary 1.1.1 *Let q be even. If x, $y \in \mathbb{F}_q^n$, then $d(x, y) = wt(x + y)$.*

For $x = (x_1, x_2, ..., x_n)$ and $y = (y_1, y_2, ..., y_n)$ in $\mathbb{F}_q^n$, let

$$x * y = (x_1y_1, x_2y_2, ..., x_ny_n).$$

Lemma 1.1.2 *If x, $y \in \mathbb{F}_2^n$, then*

$$wt(x + y) = wt(x) + wt(y) - 2wt(x * y). \quad (1.2)$$

Lemma 1.1.3 *For any prime power q and x, $y \in \mathbb{F}_q^n$, we have*

$$wt(x) + wt(y) \geq wt(x + y) \geq wt(x) - wt(y). \quad (1.3)$$

Definition 1.1.4 *Let C be a code (not necessarily linear). The minimum (Hamming) weight of C, denoted $wt(C)$, is the smallest of the weights of the nonzero codewords of C.*

1.1.3 Distance of a code

Apart from the length and size of a code, another important and useful characteristic of a code is its distance.

Definition 1.1.5 *For a code C containing at least two words, the (minimum)distance of C, denoted by $d(C)$, is $d(C) = min\{d(x, y) : x, y \in C, x \neq y\}$.*

Definition 1.1.6 *A code of length n, size M and distance d is referred to as an (n, M, d)-code. The numbers n, M and d are called the parameters of the code.*

Example 1.1.3 *Let $C = \{00000, 00111, 11111\}$ be a binary code Then $d(C) = 2$ since*

$$\begin{aligned} d(00000, 00111) &= 3 \\ d(00000, 11111) &= 5 \\ d(00111, 11111) &= 2 \end{aligned}$$

Hence, C is a binary $(5, 3, 2)$-*code*.

Example 1.1.4 *Let $C = \{000000, 000111, 111222\}$ be a ternary code (i.e. with code alphabet $\{0, 1, 2\}$). Then $d(C) = 3$ since*

$$\begin{aligned} d(000000, 000111) &= 3, \\ d(000000, 111222) &= 6, \\ d(000111, 111222) &= 6. \end{aligned}$$

Hence, C is a ternary $(6, 3, 3) - code$.

Since the distance of a code is related to the error detecting and error-correcting capabilities of the code we have.

Definition 1.1.7 *Let u be a positive integer. A code C is u-error-detecting if, whenever a codeword incurs at least one but at most u errors, the resulting word.is not a codeword. A code C is exactly u -error-detecting if it is u-error-detecting.but not $(u + 1)$-error-detecting.*

Example 1.1.5 *The binary code* $C = \{00000, 00111, 11111\}$ *is* 1*-error detecting since changing any codeword in one position does not result in another.codeword. In other words,*

$$00000 \longrightarrow 00111 \text{ needs to change three bits,}$$
$$00000 \longrightarrow 11111 \text{ needs to change five bits,}$$
$$00111 \longrightarrow 11111 \text{ needs to change two bits.}$$

In fact, C *is exactly* 1*-error-detecting, as changing the first two positions of* 00111 *will result in another codeword* 11111 *(so* C *is not a* 2*-error-detecting code).*

Example 1.1.6 *The ternary code* $C = \{000000, 000111, 111222\}$ *is* 2*-error-detecting.*

since changing any codeword in one or two positions does not result in another codeword. In other words,

$$000000 \longrightarrow 000111 \text{ needs to change three positions,}$$
$$000000 \longrightarrow 111222. \text{ needs to change six positions,}$$
$$000111 \longrightarrow 111222 \text{ needs to change six positions.}$$

In fact, C *is exactly* 2*-error-detecting, as changing each of the last three positions of* 000000 *to* 1 *will result in the codeword* 000111 *(so* C *is not* 3*-error-detecting).*

Theorem 1.1.1 *A code* C *is* u*-error-detecting if and only if* $d(C) \geq u + 1$*; i.e.,a code with distance* d *is an exactly* $(d-1)$*-error-detecting code.*

Proof. Suppose $d(C) \geq u+1$. If $c \in C$ and x are such that $1 \leq d(c, x) \leq u < d(C)$, then $x \notin C$; hence, C is u-error-detecting. On the other hand, if $d(C) < u + 1$, i.e., $d(C) \leq u$, then.there exist $c_1, c_2 \in C$. such that $1 \leq d(c_1, c_2) = d(C) \leq u$. It is therefore possible that we begin with c_1 and $d(C)$ errors (where $1 \leq d(C) \leq u$) are incurred such that the resulting word is c_2, another codeword in C. Hence, C is not a u-error-detecting code. ■

Definition 1.1.8 *Let* v *be a positive integer. A code* C *is* v*-error-correcting if minimum distance decoding is able to correct* v *or fewer errors, assuming that the incomplete decoding rule is used. A code* C *is exactly* v*-error-correcting if it is* v*-error-correcting but not* $(v+1)$*-error–correcting.*

Example 1.1.7 *Consider the binary code* $C = \{000, 111\}$*. By using the minimum distance decoding rule, we see that:*

·*if* 000 *is sent and one error occurs in the transmission, then the received word* (100, 010 *or* 001) *will be decoded to* 000*;*

·*if* 111 *is sent and one error occurs in the transmission, then the received word* (110, 101 *or* 011) *will be decoded to* 111*.*

In all cases, the single error has been corrected. Hence, C *is* 1*-error-correcting.*

If at least two errors occur, the decoding rule may produce the wrong code word. For instance, if 000 *is sent and* 011 *is received, then* 011 *will be decoded to* 111 *using the minimum distance decoding rule. Hence,* C *is exactly* 1*-error-correcting.*

Theorem 1.1.2 *A code* C *is* v*-error-correcting if and only if* $d(C) \geq 2v + 1$*;.i.e., a code with distance* d *is an exactly* $(d-1)/2$*-error-correcting code.*

1.2 Linear codes

We are now ready to introduce linear codes and discuss some of their elementary properties

Definition 1.2.1 *A linear code* C *of length* n *over* $\mathbb{F}_q$ *is a subspace of* $\mathbb{F}_q^n$

Example 1.2.1 *The following are linear codes:*
(i) $C = \{(\lambda, \lambda, ..., \lambda) : \lambda \in \mathbb{F}_q\}$*. This code is often called a repetition code.*
(ii) $(q = 2)$ $C = \{000, 001, 010, 011\}$*.*
(iii) $(q = 3)$ $C = \{0000, 1100, 2200, 0001, 0002, 1101, 1102, 2201, 2202\}$.
(iv) $(q = 2)$ $C = \{000, 001, 010, 011, 100, 101, 110, 111\}$.
(iv) $(q = 2)$ $C = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

Definition 1.2.2 *Let* C *be a linear code in* $\mathbb{F}_q^n$*. The dimension of the linear code* C *is the dimension of* C *as a vector space over* $\mathbb{F}_q$ *, i.e.,* $dim(C)$*.*

Definition 1.2.3 *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.

Theorem 1.2.1 *Let C be a linear code over $\mathbb{F}_q$. Then $d(C) = wt(C)$.*

Proof. Recall that for any words x, y we have $d(x, y) = wt(x - y)$ By definition, there exist $x^{/}, y^{/} \in C$ such that $d(x^{/}, y^{/}) = d(C)$, so

$$d(C) = d(x^{/}, y^{/}) = wt(x^{/} - y^{/}) \geq wt(C).$$

Since $x^{/} - y^{/} \in C$.

Conversely, there is a $z \in C\backslash\{0\}$ such that $wt(C) = wt(z)$, so

$$wt(C) = wt(z) = d(z, 0) \geq d(C).$$

■

Example 1.2.2 *Consider the binary linear code $C = \{0000, 1000, 0100, 1100\}$.*
Because

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

Then, the minimum distance $d = 1$.

Remark 1.2.1 *A linear code C of length n and dimension k over $\mathbb{F}_q$ is often called a $q-ary$ $[n, k]$-code or, if q is clear from the context, an $[n, k]-code$. It is also an (n, q^k)-linear code. If the distance d of C is known, it is also sometimes referred to as an $[n, k, d]$-linear code.*

Remark 1.2.2 *(Some advantages of linear codes) The following are some of the reasons why it may be preferable to use linear codes over nonlinear ones:*
(i) As a linear code is a vector space, it can be described completely by using a basis.
(ii) The distancode are faster and sice of a linear code is equal to the smallest weight of its nonzero codewords.
(iii) The encoding and decoding procedures for a linear mpler than those for arbitrary non-linear codes.

1.2.1 Generator and parity-check matrix

Knowing a basis for a linear code enables us to describe its codewords explicitly. In coding theory, a basis for a linear code is often represented in the form of a matrix, called a generator matrix, while a matrix that represents a basis for the dual code is called a parity-check matrix. These matrices play an important role in coding theory.

Definition 1.2.4 *(i) A generator matrix for a linear code C is a matrix G whose rows form a basis for C.*

(ii) A parity-check matrix H for a linear code C is a generator matrix for the.dual code $C^{\perp}$.

We clearly have $GH^T = 0$.

Theorem 1.2.2 *If $G = [I_K|A]$ is a generator matrix for the $[n, k]$ code C in standard form,then $H = [-A^T|I_{n-k}]$ is a parity check matrix for C.*

Proof. : We clearly have $HG^T = -A^T + A^T = O$. Thus C is contained in the kernel of the linear transformation $x \mapsto Hx^T$. As H has rank $n - k$, this linear transformation has kernel of dimension k, which is also the dimension of C. The result follows ■

Example 1.2.3 *The matrix $G = [I_4|A]$, where*

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

is a generator matrix in standard form for a $[7, 4]$ binary code that we denote by H a parity check matrix for H is

$$H = [-A^T|I_{n-k}] = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

This code is called the $[7, 4]$ Hamming code.

Lemma 1.2.1 *Let C be an $[n,k]$-linear code over $\mathbb{F}_q$, with generator matrix G Then $v \in \mathbb{F}_q^n$ belongs to $C^\perp$ if and only if v is orthogonal to every row of G; i.e., $v \in C^\perp \Leftrightarrow vG^t = 0$. In particular, given an $(n-k) \times n$ matrix H, then H is a parity-check matrix for C if and only if the rows of H are linearly independent and $HG^T = O$.*

Proof. Let r_i denote the ith row of G. In particular, $r_i \in C$ for all $1 \leq i \leq k$, and every $c \in C$ may be written as.

$$c = \lambda_1 r_1 + ... + \lambda_k r_k$$

where $\lambda_1, ..., \lambda_k \in \mathbb{F}_q$. If $v \in C^\perp$, then $v \cdot c = 0$ for all $c \in C$. In particular, v is orthogonal to r_i, for all $1 \leq i \leq k$; i.e., $vG^T = 0$. Conversely, if $v \cdot r_i = 0$ for all $1 \leq i \leq k$, then clearly, for any

$$c = \lambda_1 r_1 + ... + \lambda_k r_k \in C,$$

$$v \cdot c = \lambda_1 (v \cdot r_1) + ... + \lambda_k (v \cdot r_k) = 0.$$

For the last statement, if H is a parity-check matrix for C, then the rows of H are linearly independent by definition. Since the rows of H are codewords.in $C^\perp$, it follows from the earlier statement that $HG^T = O$. Conversely, if $HG^T = O$, then the earlier statement shows that the rows of H, and hence the row space of H, are contained in $C^\perp$. Since the rows.of H are linearly independent, the row space of H has dimension $n-k$, so the row space of H is indeed $C^\perp$. In other words, H is a parity-check matrix for C. ■

Remark 1.2.3 *An alternative but equivalent formulation for* Lemma 1.2.1 *is the following:*

Let C be an $[n,k]$-linear code over $\mathbb{F}_q$, with parity-check matrix H. Then.$v \in \mathbb{F}_q^n$ belongs to C if and only if v is orthogonal to every row of H; i.e.,

$v \in C \Leftrightarrow vH^T = 0$. In particular, given a $k \times n$ matrix G, then G is a generator matrix for C if and only if the rows of G are linearly independent and $HG^T = O$.

One of the consequences of Lemma 1.2.1 *is the following theorem relating the distance d of a linear code C to properties of a parity-check matrix of C.*

Theorem 1.2.3 *Let C be a linear code with parity-check matrix H. Then*

(i) C has distance $\geq d$ if and only if any $d-1$ columns of H are linearly.independent; and

(ii) C has distance $\leq d$ if and only if H has d columns that are linearly.dependent.

Corollary 1.2.1 *Let C be a linear code and let H be a parity-check matrix for C. Then the following statements are equivalent:*

(i) C has distance d;

(ii) any $d-1$ columns of H are linearly independent and H has d columns that are linearly dependent.

Example 1.2.4 *: Determine the set of code words for the $(7,4)$-code with the generator matrix*

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

Solution 1.2.1 *: First, we consider all the 16 possible message words $(0000), (1000), (0100), \ldots, (1111)$. Substituting G and $u = (1000)$ gives the code word as follows:*

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

Similarly, substituting all other values of u, we may find out the other code words. Just to illustrate the process, we find out another code word by substituting $u = (1111)$ which gives

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

*The total linear block code for the given generator matrix is shown in Table **

*Table * The* $(7,4)$ *Linear Block Code*

Messages (u)	*Code Words* (c)
$(0\ 0\ 0\ 0)$	$(0\ 0\ 0\ 0\ 0\ 0\ 0)$
$(1\ 0\ 0\ 0)$	$(1\ 1\ 0\ 1\ 0\ 0\ 0)$
$(0\ 1\ 0\ 0)$	$(0\ 1\ 1\ 0\ 1\ 0\ 0)$
$(1\ 1\ 0\ 0)$	$(1\ 0\ 1\ 1\ 1\ 0\ 0)$
$(0\ 0\ 1\ 0)$	$(1\ 1\ 1\ 0\ 0\ 1\ 0)$
$(1\ 0\ 1\ 0)$	$(0\ 0\ 1\ 1\ 0\ 1\ 0)$
$(0\ 1\ 1\ 0)$	$(1\ 0\ 0\ 0\ 1\ 1\ 0)$
$(1\ 1\ 1\ 0)$	$(0\ 1\ 0\ 1\ 1\ 1\ 0)$
$(0\ 0\ 0\ 1)$	$(1\ 0\ 1\ 0\ 0\ 0\ 1)$
$(1\ 0\ 0\ 1)$	$(0\ 1\ 1\ 1\ 0\ 0\ 1)$
$(0\ 1\ 0\ 1)$	$(1\ 1\ 0\ 0\ 1\ 0\ 1)$
$(1\ 1\ 0\ 1)$	$(0\ 0\ 0\ 1\ 1\ 0\ 1)$
$(0\ 0\ 1\ 1)$	$(0\ 1\ 0\ 0\ 0\ 1\ 1)$
$(1\ 0\ 1\ 1)$	$(1\ 0\ 0\ 1\ 0\ 1\ 1)$
$(0\ 1\ 1\ 1)$	$(0\ 0\ 1\ 0\ 1\ 1\ 1)$
$(1\ 1\ 1\ 1)$	$(1\ 1\ 1\ 1\ 1\ 1\ 1)$

Theorem 1.2.4 *Let G be a generator matrix of a linear code C. Then the rows of G form a basis of C.*

Proof. *The k rows of G are clearly linearly independent by the definition of G. If r is a row vector of G, then $rH^T = 0$, so $Hr^T = 0$, whence $r \in C$.* ■

1.2.2 Dual codes

Definition 1.2.5 *Let $u = u_1...u_n$ and $v = v_1...v_n$ be vectors in $\mathbb{F}_q^n$ and let $u.v = u_1v_1+\cdots+u_nv_n$ denote the dot product of u and v over $\mathbb{F}_q^n$. If $u.v = 0$, then u and v are called* orthogonal.

Definition 1.2.6 *Let $x = (x_1x_2...x_n)$ and $y = (y_1y_2...y_n)$ be two vectors of length n over a field $\mathbb{F}_q$ Then, by the intersection $x * y$ of x and y, we mean the vector*

$$x * y = (x_1y_1 \quad x_2y_2.....x_ny_n)$$

while by their scalar product $x.y$ we mean the element

$$x.y = x_1y_1 + x_2y_2 + ... + x_ny_n \text{ of } \mathbb{F}_q^n$$

Thus

$$x.y = x.y^T = y.x = y.x^T.$$

Example 1.2.5 *Let X, Y Z T be for vectors of length n over a field $\mathbb{F}_2$ where*

$X = (1101)$ $\qquad$ $Y = (1111)$

$Z = (101011)$ $\qquad$ $T = (110101)$

then $X * Y = (1\ 1\ 0\ 1)$ $\qquad$ $X.Y = 1 + 1 + 0 + 1 = 1$

and $Z * T = (1\ 0\ 0\ 0\ 0\ 1)$ $\qquad$ $Z.T = 1+0+0+0+0+1 = 0$

Definition 1.2.7 *Two vectors x and y of the same length n over $\mathbb{F}_q$ are called* orthogonal *if $x.y = 0$*

or equivalently $x.y^T = y.x = y.x^T = 0$

Definition 1.2.8 *Let C be a linear (n, k) code over $\mathbb{F}_q$ The* dual *(or* orthogonal*)* code *$C^\perp$ of C is defined by*

$C^\perp = \{u \in \mathbb{F}_q^n / u.v = 0 \text{ for all } v \in C\}$.

Theorem 1.2.5 *Let C be a linear code of length n over $\mathbb{F}_q$ Then,*

(i) $|C| = q^{dim(C)}$ *, i.e.,*$dim(C) = log_q|C|$;

(ii) $C^\perp$ *is a linear code and* $dim(C) + dim(C^\perp) = n$;

(iii) $(C^\perp)^\perp = C$.

Example 1.2.6 *Consider the* $(4, 7)$*binary Hamming code*

$$C = \left\{ \begin{array}{c} 0000000, 0001011, 1110100, 1000101, 0111010, 1100010, 0011101, 0110001, \\ 1001110, 1011000, 0100111, 0101100, 1010011, 0010110, 1101001, 1111111 \end{array} \right\}$$

It is a $[7,4,3]$*linear code with the basis* $\{111010, 0111010, 0011101, 0001011\}$*. As a consequence of this, it follows that the code words of the* $(4,7)$ *Hamming code are in one-to-one correspondence with the code words of the code generated by the matrix*

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

A vector $(x_1x_2x_3x_4x_5x_6)$*is orthogonal to* C *iff it is orthogonal to the basis vectors. For this, we have These imply*

$$\begin{aligned} x_1 + x_2 + x_3 + x_5 &= 0 \\ x_2 + x_3 + x_4 + x_6 &= 0 \\ x_3 + x_4 + x_5 + x_7 &= 0 \\ x_4 + x_6 + x_1 &= 0 \end{aligned}$$

These imply

$$\begin{aligned} x_5 &= x_1 + x_2 + x_3 \\ x_7 &= x_2 + x_3 \\ x_4 &= x_1 + x_3 \\ x_6 &= x_1 + x_2 \end{aligned}$$

In matrix form, these equations can be rewritten as

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ ... \\ x_7 \end{pmatrix} = 0.$$

Thus the generator matrix of the dual code $C^{\perp}$ *is*

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

In view of this, it follows that $C^{\perp}$ *is a linear code of dimension* 3. *All the code words of* $C^{\perp}$ *are:*

$$\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & ..... & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & ..... & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & ..... & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & ..... & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array}$$

Example 1.2.7 (i) $(q = 2)$ *Let* $C = \{0000, 1010, 0101, 1111\}$, *so* $dim(C) = log_2|C| = log_2 4 = 2$. *It is easy to see that* $C^{\perp} = \{0000, 1010, 0101, 1111\} = C$,*so* $dim(C^{\perp}) = 2$.

(ii) $(q = 3)$ *Let* $C = \{000, 001, 002, 010, 020, 011, 012, 021, 022\}$, *so* $dim(C) = log_3|C| = log_3 9 = 2$. *One checks readily that* $C^{\perp} = \{000, 100, 200\}$, *so* $dim(C^{\perp}) = 1$.

Definition 1.2.9 *Let* C *be a linear code.*

(i) C *is self-orthogonal if* $C \subseteq C^{\perp}$.

(ii) C *is self-dual if* $C = C^{\perp}$

Example 1.2.8 *Let* C *be a binary self dual code of length* 4. *Then its dimension is clearly* 2. *The vectors* (1100) *and* (1010) *are linearly independent over* $\mathbb{F}_2$ *and so generate a space of dimension* 2. *But*

$$(1100)(1010)^{\perp} \neq 0$$

and so the space generated by these two vectors is not a self dual code.

However, the code

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

generated by 1100 *and* 0011 *is self dual. Following are the other self dual codes of length* 4 :

$$\{0000, 0101, 1010, 1111\}.....\{0000, 1001, 0110, 1111\}.$$

Chapter 2

Cyclic Codes

2.1 Introduction

We now turn to special classes of linear codes C for which $(a_0, ..., a_{n-1}) \in C$ implies that $(a_{n-1}, a_o, ..., a_{n-2}) \in C$. Let again $\mathbb{F}_q^n$, $n \geqslant 2$, be the $n - dimensional$ vector space of $n - tuples$ $(a_0, ..., a_{n-1})$, with the usual operations of addition of $n - tuples$ and scalar multiplication of $n - tuples$ by elements in $\mathbb{F}_q$.

The mapping

$$\begin{array}{rcl} \tau & : & \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n; \\ (a_o, ..., a_{n-1}) & \longmapsto & (a_{n-1}, a_o, ..., a_{n-2}) \end{array}$$

is a linear mapping, called a "cyclic shift."

We shall also consider the polynomial ring $\mathbb{F}_q[x]$. Now $\mathbb{F}_q[x]$ is not only a commutative ring with identity but also a vector space over $\mathbb{F}_q$ with countable basis $1, x, x^2, ...$ in the natural way. This is often expressed by calling $\mathbb{F}_q[x]$ an $\mathbb{F}_q - algebra$. We define a subspace $\mathbb{F}_q[x]$ of this vector space by

$$\mathbb{V}_n = \{a_0 + a_1 x + ... + a_{n-1} x^{n-1} / a_i \in F_q, 0 \leq i \leq n-1\}.$$

We can identify the two spaces $\mathbb{V}_n$ and $\mathbb{F}_q^n$ by the isomorphism

$$\begin{array}{rcl} \theta & : & \mathbb{F}_q^n \longrightarrow \mathbb{V}_n \\ (a_o, ..., a_{n-1}) & \longmapsto & (a_o + a_1 x + ... + a_{n-1} x^{n-1}). \end{array}$$

Definition 2.1.1 *A linear code C of length n over $\mathbb{F}_q$ is called cyclic if any cyclic shift of a code word is again a code word, i.e., if $(a_o, ..., a_{n-1})$ is in C then so is $(a_{n-1}, a_o, ..., a_{n-2})$.*

Example 2.1.1 *1) The binary linear code $C = \{000, 110, 101, 011\}$ is cyclic since $110 \in C \Longrightarrow 011 \in C$; $101 \in C \Longrightarrow 110 \in C$; $011 \in C \Longrightarrow 101 \in C$.*
2) The binary code $C = \{000, 110, 101\}$ is not cyclic becouse $110 + 101 = 011 \notin C$.

2.2 Algebraic description of cyclic codes

There is a beautiful algebraic description of cyclic codes. To obtain this we define a map

$$\theta : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/(x^n - 1)$$

where $(x^n - 1)$ denotes the ideal of the polynomial ring $\mathbb{F}_q[x]$ generated by $x^n - 1$, by

$$\theta(a_o, ..., a_{n-1}) = (a_o + a_1 x + ... + a_{n-1}x^{n-1}) \forall a_i \in \mathbb{F}_q, 0 \leq i \leq n-1.$$

Observe that $\mathbb{F}_q[x]/(x^n - 1)$ is also a vector space over $\mathbb{F}_q$ and θ is a vector space isomorphism. Let C be a linear code of length n over $\mathbb{F}_q$, i.e. C is a subspace of $\mathbb{F}_q^n$. Then $\theta(C)$ is a subspace of $\mathbb{F}_q[x]/(x^n-1)$. Let $a = (a_0, a_1, ..., a_{n-1}) \in C$. Then $(a_{n-1}, a_o, ..., a_{n-2}) \in C$ iff

$$a_{n-1} + a_0 x + ... + a_{n-2}x^{n-1} = x(a_o + a_1 x + ... + a_{n-1}x^{n-1})$$

is in $\theta(C)$ From this it follows that C is a cyclic code iff $\theta(C)$ is an ideal in the quotient ring $\mathbb{F}_q[x]/(x^n-1)$. Identifying the element $(a_o, ..., a_{n-1})$ in C with the corresponding element $(a_o + a_1 x + ... + a_{n-1}x^{n-1})$ or with the polynomial $(a_o + a_1 x + ... + a_{n-1}x^{n-1})$ of degree at most $n - 1$, we may regard a cyclic code C of length n as an ideal of the quotient ring $\mathbb{F}_q[x]/(x^n - 1)$.

Theorem 2.2.1 *A linear code C in $\mathbb{F}_q^n$ is cyclic if and only if C is an ideal in $R_n := \mathbb{F}_q[x]/(x^n - 1)$.*

Proof. If C is an ideal in $\mathbb{F}_q[x]/(x^n-1)$ 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. ■

Example 2.2.1 *In the ring $\mathbb{F}_2[x]/(x^3-1)$, the subset $I = \{0, 1+x, x+x^2, 1+x^2\}$ is an ideal.*

Theorem 2.2.2 *The rings $\mathbb{Z}$, $\mathbb{F}_q[x]$ and $\mathbb{F}_q[x]/(x^n-1)$ are all principal ideal rings.*

Proof. Let I be an ideal of $\mathbb{Z}$. If $I = \{0\}$, then $I =< 0 >$ is a principal ideal. Assume that $I \neq \{0\}$ and let m be the smallest positive integer in I. Let a be any element of I. By the division algorithm, we have

$$a = qm + r \tag{2.1}$$

for some integers q and $0 \leq r \leq m-1$. The equality (2.1) implies that r is also an element of I since $r = a - qm$. This forces $r = 0$ by the choice of m. Hence, $I =< m >$. This shows that $\mathbb{Z}$ is a principal ideal ring.

Using the same arguments, we can easily show that $\mathbb{F}_q[x]$ is also a principal ideal ring. Essentially the same method can be employed for the case $\mathbb{F}_q[x]/(x^n-1)$. Since this case is crucial for this chapter, we repeat the arguments. The zero ideal is obviously principal. We choose a nonzero polynomial $g(x)$ of a nonzero ideal J with the lowest degree. For any polynomial $f(x)$ of J, we have

$$f(x) = s(x)g(x) + r(x)$$

for some polynomials $s(x), r(x) \in \mathbb{F}_q[x]$ with $deg(r(x)) < deg(g(x))$. This forces $r(x) = 0$, since $r(x) = f(x) - s(x)g(x) \in J$ and $g(x)$ has the lowest degree among the nonzero polynomials of J. Hence, $J =< g(x) >$. ■

Example 2.2.2 *let* $I = \{0\,, 1+x, x+x^2, 1+x^2\}$*, the ideal* I *is principal.*
In fact, $I =< 1+x >$ *. Note that*

$$\begin{aligned} 0(1+x) &= 1+x^3 = 0 = (1+x+x^2)(1+x) \\ 1(1+x) &= 1+x = (x+x^2)(1+x) \\ x(1+x) &= x+x^2 = (1+x^2)(1+x) \\ x^2(1+x) &= 1+x^2 = (1+x)(1+x) \end{aligned}$$

Theorem 2.2.3 *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 2.2.3 $(7, 4)$ *Cyclic Code Generated by the Polynomial* $g(x) = 1 + x + x^3$

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

Example 2.2.4 *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 cyclic codes of length 7*over* $\mathbb{F}_2$ *are*

$\langle 1\rangle = R_7$.

$\langle (x+1)\rangle$.

$\langle (x^3+x+1)\rangle$.

$\langle (x^3+x^2+1)\rangle$.

$\langle (x+1)(x^3+x+1)\rangle$.

$\langle (x+1)(x^3+x^2+1)\rangle$.

$\langle (x^3+x+1)\,(x^3+x^2+1)\rangle$.

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

2.2.1 Generator and parity-check polynomials

Definition 2.2.1 *Let $g(x)$ be a generator polynomial of a cyclic code C. Then $h(x) = (x^n-1)/g(x)$ is called a* check polynomial *of C.*

Theorem 2.2.4 *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*

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

Let

$$h(x) = h_0 + h_1x + ... + h_kx^k$$

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*

$$h^\perp(x) = x^k h(\frac{1}{x}) = h_k + h_{k-1}x + \ldots + h_0x^k.$$

Example 2.2.5 *Consider the binary* $[7,4]-$*cyclic code with generator polynomial* $g(x) = 1 + x^2 + x^3$ *Then this code has a generator matrix*

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

Example 2.2.6 *Let* C *be the binary* $[7,4]-$*cyclic code generated by* $g(x) = 1 + x^2 + x^3$. *Put* $h(x) = (x^7 - 1)/g(x) = 1 + x^2 + x^3 + x^4$.

Then $h^{\perp}(x) = 1 + x + x^2 + x^4$ *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

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

3.1 Introduction

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).

The objective of this chapter is to determine 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 $2p$.

3.2 Preliminaries

3.2.1 Polynomials over a finite field

Definition 3.2.1 *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 3.2.1 *Let $h(x), f(x) \in \mathbb{F}_q[x]$. Then*

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

Definition 3.2.2 ***(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 $\mathbb{F}_q[x]$.*

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 3.2.3 *The cyclic code generated by $m_i(x)$ is called a maximal cyclic code 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 3.2.1 *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 $\frac{x^7-1}{m_3(x)} = (x+1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1.$

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.

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

Proposition 3.2.2 *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 3.2.1 and the fact $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp}) = n$.

The proof is finished. ■

Example 3.2.2 *Let C be a binary $[3, 2]$ code. If*

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

then

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

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

and

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

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

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 cyclic code $C = \langle f(x) \rangle$ of length n over $\mathbb{F}_q$ is LCD cyclic codes if $f(x)$ is a self-reciprocal polynomial.

3.2.2 The structure of LCD cyclic codes

A necessary and sufficient condition for the existence of LCD cyclic codes of length n over $\mathbb{F}_q$ is given.

Theorem 3.2.1 *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., $g^*(x) = g(x)$.*

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)).
The proof is finished. ■

3.3 LCD cyclic codes of length $2p$

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

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 3.3.1 *Let $\mathbb{F}_q$ be a finite field with q elements and p be an odd prime coprime to q, then $x^{2p} - 1 = \prod_{s\in\{0,1,2,p\}} m_s(x)$, where*

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

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 $\mathbb{F}_q$.

3.3.2 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 3.1: 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 3.2: 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 3.3.2 *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 3.3.3 *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 3.2.1, the code C is an LCD cyclic code. ■

3.4 Some LCD cyclic codes of length $2p$

In this section we determine the generating polynomial of the dual of maximal and minimal 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 $2p$.

Table 3.3: 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 3.4: 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 $C^{\perp}$
$\widehat{m_0} = \langle \frac{(x^{2p}-1)}{m_0(x)} \rangle$	$m_p(x) \times m_1(x) \times m_2(x)$	$m_0(x)$
$\widehat{m_p} = \langle \frac{(x^{2p}-1)}{m_p(x)} \rangle$	$m_0(x) \times m_1(x) \times m_2(x)$	$m_p(x)$
$\widehat{m_1} = \langle \frac{(x^{2p}-1)}{m_1(x)} \rangle$	$m_0(x) \times m_p(x) \times m_2(x)$	$m_1(x)$
$\widehat{m_2} = \langle \frac{(x^{2p}-1)}{m_2(x)} \rangle$	$m_0(x) \times m_p(x) \times m_1(x)$	$m_2(x)$

Example 3.4.1 *Take $q = 7$, $p = 11$. Then $x^{2p} - 1 = \prod_{s \in \{0,1,2,11\}} m_s(x)$, 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 3.5: 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 3.6: 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

This work,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 LCD 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., $q^{p-1} \equiv 1 (\mathrm{mod}\, 2p)$.

Bibliography

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

[2] 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.

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

[4] L. Heboub, *Sur les codes cycliques maximaux de longueuer* n, Thèse de doctorat .Université de M'sila, 2023.

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

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

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

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

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

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

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

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

[13] A. Saha, N. Manna, S. Mandal, Information theory coding and cryptography,Dorling Kindersley (India) Pvt. Ltd. , 2013.

خلاصة

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

$$.R_N = \mathbb{F}_q[x] \Big/ \left(x^N - 1\right)$$

الهدف الأساسي من هذه الرسالة هو دراسة متممة الشفرات الدورية المصححة للأخطاء.
الكلمات المفتاحية : الشفرات الخطية الدورية، متممة الشفرات الدورية.

Abstract

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

$$R_N = \mathbb{F}_q[x] \Big/ \left(x^N - 1\right).$$

The main objective of this memory is the study of LCD cyclic codes.

Keywords: Linear and 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.

Un code cyclique de longueur N sur le corps fini $\mathbb{F}_q$ peut être défini comme un idéal principal de l'anneau quotient $R_N = \mathbb{F}_q[x] \Big/ \left(x^N - 1\right)$.

L'objectif principal de ce mémoire est l'étude des codes cycliques *LCD.*

Mots clés: Codes linéaires et cycliques, codes cycliques *LCD.*