PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESERACH

Mohamed Boudiaf University of M'sila
Faculty of Mathematics and Informatics
Departement of Mathematics

Master of Mathematics

Mathematics and Informatics
Specialty: Mathematics
Option : Algebra and Discrete Mathematics

Theme

MDS Codes with Complementary Duals over Finite Fields

Persented by :
M^s ABASSI Nour El Houda - ALIANE Khira Soulef

Publicly presented on : 18/06/2023.

In front of the jury :

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

University years: 2022/2023.

Contents

Introduction **V**

1 Preliminaries **1**
1.1 Basic definitions and results 1
1.2 Finite fields 7
1.2.1 Some properties of finite fields 8
1.3 Background of coding theory 11
1.3.1 Codes 11
1.3.2 Linear codes 12

2 Generalized Reed-Solomon codes **16**
2.1 Generalized Reed-Solomon codes 17
2.2 Dual of Generalized Reed-Solomon codes 18

3 MDS codes with complementary duals over finite fields **21**
3.1 Some constructions of LCD MDS codes 22
3.1.1 Examples 23
3.1.2 Examples 25

Conclusion **27**
Bibliography 1

Notations

- $|G|$: Number of elements in G.
- $\mathbb{N}$: Natural numbers.
- $\mathbb{Z}$: Integers numbers.
- $\mathbb{R}$: Reel 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.
- $F[X]$: The set of polynomials with coefficients in 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.
- G : Generator matrix.
- H : Parity cheek matrix.
- $C^\perp$: Dual code of C.
- MDS : Maximum Distance Separable.

- LCD : Linear Complementary Dual.
- GRS : Generalized Reed-Solomon Codes .
- $\lfloor x \rfloor$: The greatest integer less than or equal to the real number x.

Acknowledgements

.

In the Name of Allah, the most Gracious, the most Merciful.

"Say work, and God will see your work, and his Messenger, and the true believers."

Great truth of God.

Thanks to Allah who doesn't make the night good except if we thank him, and dosen't make the day good except if obey him, and all the moments are good only when we remember him.

To the one who conveyed the message and fulfilled the trust . . . our prophet Mohamed may Allah′ peace and blessings be upon him .

We would like th express our deepest gratitude to our supervisor LEBED Khawla for her useful guidance and help. We would like also to thank the committee members and all the teachers of the faculty of Mathematics especially Saad ABDELKEBIR .

The journey is over, it has not been easy and it will never be so. no matter how long it takes, it will be go with its sweetness and bitterness moments and now thanks to Allah we have completed this work.

I dedicate my graduation, the culmination of my efforts, and the joy I have been anticipating throughout my life, to those who paved the way for me in the realm of knowledge, my parents.

To my beloved brothers and sisters, who have been my support and pillars in my life, I also dedicate it to you.

Lastly, I would like to dedicate my graduation to myself, for working hard and striving throughout these years to achieve this accomplishment. I hope that my graduation marks the beginning of a promising future, where knowledge and understanding play a significant role in my life and in serving the community.

Soulaf Khira and Nour El Houda.

Introduction

Coding theory is a branch of mathematics and computer science, that deal with the study of error-correcting code. It was initiated in 1948 by the mathematician Claude Shannon [1]. Coding theory has applications in many different fields, including telecommunications, computer networking, digital storage, cryptography, wireless networks, satellite, communication systems and internet protocols and more. Error-correcting codes (ECC) are techniques used in computer science and telecommunications to detect and correct errors that may occur during data transmission or storage. These codes are commonly employed in various applications, including digital communication systems, storage devices, and error-resilient data transmission protocols. Linear code is one of the most important type of error-correcting code. Because of their algebraic structure, they are easier to describe, encode and decode.

A linear $[n, k, d]$ code C over $\mathbb{F}_q$ is defined as subspace of $\mathbb{F}_q^n$ of length n, dimension k and minimal distance $d = d_{min}(C)$, where $\mathbb{F}_q$ is the finite field of q elements. The Hamming weight $w_H(c)$ of a code-word $c \in C$ is the number of its elements that are non-zero and the distance between two code-words is the Hamming distance d_H between them, that is the number of elements in which they differ. For a linear code C, we have Singleton Bound $d \leq n - k + 1$, if $d = n - k + 1$, then the code C is called Maximum Distance Separable (MDS) code.

MDS codes are a class of error correcting codes that achieve the maximum possible distance between code-words. MDS codes have important application, such as communication, data storage, and secret sharing. The most well-know family of MDS codes are Generalized Reed-Solomon (GRS for short) codes, which not only have nice theoretic properties, but also have been extensively application in engineering due to their easy encoding and efficient decoding algorithm.

Linear complementary dual (LCD) codes are whose intersections with their dual codes are trivial ($C \bigcap C^{\perp} = \{0\}$). These codes introduced by Massey in 1992 [3]. It is well known that LCD code have been widely used in communications systems, consumer electronics, application data storage, and cryptography. These application of LCD codes renewed the interest in the construction of LCD having a large minimum distance. Besides, MDS codes are of particular interest from both practical and theoretical points of view. Hence, it is significant to construct LCD MDS codes. As we know, GRS codes are the class of probably best known MDS codes. Thus, it is natural to construct LCD MDS codes through GRS codes. In [13] , Jin constructed some classes of LCD MDS codes by two disjoint classes of GRS codes. The problem of the existence of q-ary Euclidean LCD MDS codes for various lengths and dimensions was completely solved in [13] when q is even. In [14], Chen and Liu improved some results of LCD MDS codes in [13] when q is odd. In [15], Carlet et al showed that an LCD code is equivalent to an arbitrary linear code for $q > 3$ in the Euclidean case. Linear codes yield MDS codes. So the existence of LCD MDS codes is finished for $q > 3$.

To be clear, the majority of this thesis work is not new.

My thesis organized as follows :

The first chapter is chapter of introduction, we presented initially preliminaries, basic definitions and results from abstract algebra and coding theory.

The second chapter, we study the structure of Generalized Reed-Solomon codes and its dual.

Finally the third chapter is the last part of this thesis, we study some results about $LCD\ MDS$ codes from GRS codes over finite fields, that are given by Bocong Chen and Hongwei Liu [14].

Chapter 1

Preliminaries

In this chapter, we summarize the background and some known results of abstract algebra, and coding theory. The definitions, theorems, lemmas, corollaries and their proofs that are used in the following chapter can be found in [6], [2] ,[11],[10],[4],[7] and [5].

1.1 Basic definitions and results

We give definition of Groups, Rings, Fields and some important Theorems.

Definition 1.1 (Groups)**.**
A group $(G, \cdot)$ is a set with a binary operation $(\cdot)$ satisfying the following axioms :

(i) G is closed under the operation $(\cdot)$, i.e., $x \cdot y = xy \in G$ for all $x, y \in G$;

(ii) The operation $(\cdot)$ is associative, i.e., $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in G$;

(iii) There is an identity element $1 \in G$ such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in G$;

(iv) For each $x \in G$, there exists an inverse element $x^{-1} \in G$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

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

Example 1.1.
The following are examples of abelian groups :

1. $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ *are all abelian groups under addition.*
2. $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$ *are all abelian groups under multiplication.*

Definition 1.2 (Cyclic group)**.**
Let $(G, \cdot)$ be a group, then G is called cyclic, if there exists an element $g \in G$, such that $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ and g is called a generator of the group G.

Example 1.2.

1. *The group* $(\mathbb{Z}, +)$ *is an infinite cyclic group with generator* 1 *or* -1.
2. *The group* $G = \{1, -1, i, -i\}$ *is a cyclic group under multiplication generator by* i.

Definition 1.3 (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 1.3.
$(\mathbb{Z}, +, \times)$*,* $(\mathbb{Q}, +, \times)$*,* $(\mathbb{R}, +, \times)$ *and* $(\mathbb{C}, +, \times)$ *are commutative rings.*

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) $\forall a \in I, \forall x \in R \Rightarrow a \cdot x \in I, x \cdot a \in I$.

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.

Remark 1.1.
Let I be an ideal of a ring R then :

(i) $1 + I$ *is the multiplicative identity of* R/I *and* $0 + I = I$ *is the additive identity of* R/I;

(ii) If R is a commutative ring with unity then R/I is also a commutative ring with unity.

Definition 1.7 (Field)**.**
A field is a set F with binary operations addition $(+)$ and multiplication $(\cdot)$, for which the following axioms are satisfied :

(i) $(F, +)$ *is an abelin group (whose identity is* 0*) under the operation* $(+)$;

(ii) The set $F^* = F - \{0\} = \{a \in F, a \neq 0\}$ *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* $a, b, c \in F$.

Theorem 1.1.
$\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p = \{0, 1, \cdots, p - 1\}$ *is a field if and only if p is a prime number.*

Example 1.6.

1. *Let* $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. *The addition and multiplication tables are given by*

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

2. *Let* $\mathbb{Z}_3 = \{0, 1, 2\}$ *be a field, here p equals* 3. *The addition and multiplication defined by the two tables below*

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Definition 1.8 (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.

1. *The characteristic of $\mathbb{R}, \mathbb{Q}$ are 0.*
2. *The characteristic of $\mathbb{Z}_2$ is 2.*

Definition 1.9 (Subfield)**.**
A subfield S of a field F is a subset of F which is itself a field with the same operations as F.

Example 1.8.

1. *$(\mathbb{Q}, +, \cdot)$ is a subfield of the field $\mathbb{R}$.*
2. *$(\mathbb{R}, +, \cdot)$ is a subfield of the field $\mathbb{C}$.*

Definition 1.10 (Extension of field)**.**
If $(E, +, \cdot)$ is a subfield of a field $(F, +, \cdot)$. Then F is called an extension field of E.

Definition 1.11.
A field F is a finite extension of K if $K \subseteq F$ and F is a finite dimensional vector space over K. In this case we refer to the dimension m of F over K as the degree of the extension, and we write $[F : K] = m$.

Example 1.9.
The field of complex numbers $\mathbb{C}$ is an extension field of the field of reel numbers $\mathbb{R}$, and $\mathbb{R}$ in turn is an extension field of the field of rational numbers $\mathbb{Q}$. Clearly then, $\mathbb{C}/\mathbb{Q}$ is also a field extension. we have $[\mathbb{C} \colon \mathbb{Q}] = 2$ because $\{1, i\}$ is a basis, so the extension $\mathbb{C}/\mathbb{Q}$ is finite.

Definition 1.12 (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

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

Example 1.10.
Let $f(X) = 2X^3 + 3X + 1$ and $g(X) = 1 + 2X$ be polynomials over $\mathbb{Z}_5$, where $\deg(f) = 3$ and $\deg(g) = 1$.

Remark 1.2.
Let k be a non-negative integer and let F be a field. Then $F[X]_k$ denotes all polynomials of $F[X]$ of degree less than k with the convention that the zero polynomial has degree -1. Notice that $F[X]$ is an infinite dimensional vector space over F and $F[X]_k$ is a subspace of $F[X]$ of k-dimension.

Corollary 1.1.
If F is a field and if $g \in F[X]$ has degree n, then g has at most n roots (even if we count the roots with their multiplicities).

Theorem 1.2 (Lagrange Interpolation Formula)**.**
For $n \geq 0$, let $\alpha_0, \alpha_1, \cdots, \alpha_n$ be $n+1$ distinct elements of F, and let $b_0, b_1, \cdots, b_n$ be $n+1$ arbitrary elements of F. Then there exists exactly one polynomial $f(X) \in F[X]$ of degree $\leq n$ such that $f(\alpha_i) = b_i$ for $i = 0, \cdots, n$. This polynomial is given by

$$P(X) = \sum_{i=0}^{n} b_i L_i(X),$$

where

$$L_i(X) = \prod_{j=0, i\neq j}^{n} \frac{(X - \alpha_j)}{(\alpha_i - \alpha_j)}.$$

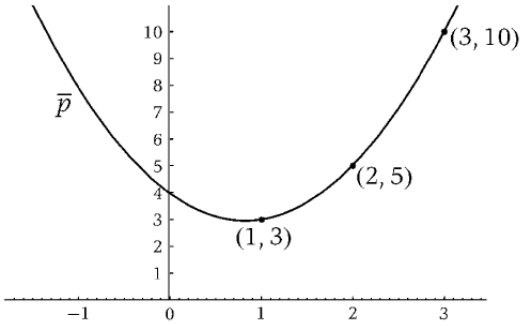
Example 1.11.
To find a polynomial function passing through the points $(1,3), (2,5), (3,10) \in \mathbb{R}^2$, we compute L_0, L_1, L_2 according to 1.2
Solution :

$$L_0 = \frac{(X-2)(X-3)}{(1-2)(1-3)} = \frac{1}{2}(X^2 - 5X + 6),$$

$$L_1 = \frac{(X-1)(X-3)}{(2-1)(2-3)} = -1(X^2 - 4X + 3),$$

$$L_2 = \frac{(X-1)(X-3)}{(3-1)(3-2)} = \frac{1}{2}(X^2 - 3X + 2).$$

So, $P(X) = 3L_0 + 5L_1 + 10L_2 = \frac{3}{2}X^2 - \frac{5}{2}X + 4$ determines a polynomial function f which passes through the given points.



Definition 1.13 (Irreducible polynomial)**.**
A polynomial $h \in F[X]$ is said to be irreducible over F (or irreducible in $F[X]$, or prime in $F[X]$) if h has positive degree and $h = f \cdot g$, with $f, g \in F[X]$ implies that either f or g is a constant polynomial.

Theorem 1.3.
The polynomial $f \in F[X]$ of degree 2 or 3 is irreducible in $F[X]$ if and only if f has no root in F.

Example 1.12.
Consider the polynomial $X^2 + 1$ in $\mathbb{Z}_3[X]$. This polynomial has no roots in $\mathbb{Z}_3$, so it is irreducible over $\mathbb{Z}_3$.

Example 1.13.

1. *The polynomial $g(X) = X^2 + X + 1$ is irreducible in $\mathbb{Z}_2[X]$.*
2. *The polynomial $f(X) = X^3 + 2X^2 + 1$ is irreducible in $\mathbb{Z}_3[X]$.*
3. *The polynomial $h(X) = X^2 + 1$ is irreducible over $\mathbb{R}$.*
4. *The polynomial $p(X) = X^2 + X + 2$ is irreducible over $\mathbb{Z}_5$.*

Theorem 1.4.
Let F be a field and $\deg(f) = k$. Then $F[X]/\langle f \rangle$ is a k-dimensional vector space over F with basis $\{1, \alpha, \cdots, \alpha^{k-1}\}$, where $\alpha = \overline{x} = x + \langle f \rangle$, and $F[\alpha]/\langle f \rangle$ is a field if and only if f is irreducible.

Example 1.14.
Let F be the field $\mathbb{Z}_2 = \{0, 1\}$; then $f(X) = X^2 + X + 1$ is an irreducible polynomial of degree 2 over $\mathbb{Z}_2$. Hence $\mathbb{Z}_2[X]/\langle X^2 + X + 1 \rangle$ is a field whose elements can be represented in the form $a + b\alpha$, $a, b \in \mathbb{Z}_2$, where α satisfies $f(\alpha) = 0$, i,e., $\alpha^2 + \alpha + 1 = 0$, which means that $\alpha^2 = \alpha + 1$, due to $-1 = 1$ in $\mathbb{Z}_2$. Hence, $\mathbb{Z}_2[X]/\langle X^2 + X + 1 \rangle$ is a field with four elements:

$$\mathbb{Z}_2[X]/\left\langle X^2 + X + 1 \right\rangle = \{0, 1, \alpha, 1 + \alpha\}.$$

The addition and multiplication tables as follows

$+$	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

1.2 Finite fields

Definition 1.14 (Finite fields)**.**
A finite field is a field with a finite number of elements. Denoted a finite field with q elements by $\mathbb{F}_q$.

Remark 1.3.
Another common notation for a finite field of order q is $GF(q)$, where GF stands for Galois field. This name is used in honor of Evariste Galois $(1811-1832)$, who in 1830 was the first person to seriously study properties of general finite fields.

Remark 1.4.
When p is a prime number, $\mathbb{Z}_p$ is a finite field with p elements. It is also denoted by $\mathbb{F}_p$.

Lemma 1.1.
The finite field $\mathbb{F}_q$ has characteristic p, where p is a prime number.

Example 1.15.
The characteristic of $\mathbb{Z}_p$ is p, where p is a prime number.

Theorem 1.5.
Let $\mathbb{F}_q$ be a finite field of characteristic p. Then $|\mathbb{F}_q| = p^n$, where $n \geq 1$.

Theorem 1.6.

(i) For any prime p and any $n \in \mathbb{N}$, there is a finite field of order p^n;

(ii) Any finite field of order p^n is (up to isomorphism) the splitting finite field of $X^{p^n} - X$ and also of $X^{p^n-1} - 1 \in \mathbb{F}_p[X]$;

(iii) Any two finite fields of order p^n are isomorphic.

Corollary 1.2.
For every finite field $\mathbb{F}_q$ and every positive integer n, there exists an irreducible polynomial in $\mathbb{F}_q[X]$ of degree n.

Theorem 1.7.
If $f(X) \in \mathbb{F}_p[X]$ is an irreducible polynomial of degree n, then $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/\langle f(X)\rangle$ is a field.

Example 1.16.

1. *The polynomial* $X^3 + X + 1 \in \mathbb{F}_2[X]$ *is irreducible. Then* $\mathbb{F}_2[X]/\langle X^3 + X + 1\rangle \cong \mathbb{F}_{2^3}$.
2. *The polynomial* $X^2 + X + 2 \in \mathbb{F}_5[X]$ *is irreducible. Then* $\mathbb{F}_5[X]/\langle X^2 + X + 2\rangle \cong \mathbb{F}_{5^2}$.
3. *The polynomial* $X^2 + 1 \in \mathbb{F}_3[X]$ *is irreducible. Then* $\mathbb{F}_3[X]/\langle X^2 + 2X + 1\rangle \cong \mathbb{F}_{3^2}$.
4 *The polynomial* $X^3+2X^2+1 \in \mathbb{F}_3[X]$ *is irreducible. Then* $\mathbb{F}_3[X]/\langle X^3 + 2X^2 + 1\rangle \cong \mathbb{F}_{3^3}$.

1.2.1 Some properties of finite fields

In this subsection, we list some important properties of finite fields.

Theorem 1.8.
Let $\mathbb{F}_q$ *be a finite field with* q *elements.*

(i) The multiplicative group $(\mathbb{F}_q^*, \cdot)$ *of the non-zero elements of* $\mathbb{F}_q$ *is cyclic of order* $q - 1$;

(ii) All elements α *of* $\mathbb{F}_q$ *satisfies* $\alpha^q - \alpha = 0$.

Definition 1.15 (Order)**.**
The order of a non-zero element $\alpha \in \mathbb{F}_q$*, denoted by* $ord(\alpha)$*, is the smallest positive integer* k *such that* $\alpha^k = 1$.

Example 1.17.
Since there are no linear factors for the polynomial $1 + X^2$ *over* $\mathbb{F}_3$*,* $1 + X^2$ *is irreducible over* $\mathbb{F}_3$*. Consider the element* α *in the field* $\mathbb{F}_9 = \mathbb{F}_3[\alpha]$*, where* α *is a root of* $1+X^2$*. Then* $\alpha^2 = -1, \alpha^3 = \alpha(\alpha^2) = -\alpha$ *and* $\alpha^4 = (\alpha^2)^2 = (-1)^2 = 1$*. This means that* $ord(\alpha) = 4$.

Lemma 1.2.

(i) The order $ord(\alpha)$ *divides* $q - 1$ *for every* $\alpha \in \mathbb{F}_q^*$.

(ii) For two non-zero elements $\alpha, \beta \in \mathbb{F}_q^*$*, if* $gcd(ord(\alpha), ord(\beta)) = 1$*, then* $ord(\alpha\beta) = ord(\alpha) \times ord(\beta)$.

Definition 1.16.
A generator of the cyclic group $\mathbb{F}_q^*$ *is called a primitive element of* $\mathbb{F}_q$.

Remark 1.5.
If α *is a root of an irreducible polynomial* $f(X)$ *of degree* n *over* $\mathbb{F}_p$*, and it is also a primitive element of* $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/f(X) \cong \mathbb{F}_p[\alpha]$*, then every element in* $\mathbb{F}_{p^n}$ *can be represented both as a polynomial in* α *and as a power of* α*, since*

$$\mathbb{F}_{p^n} = \{a_0 + a_1 + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{F}_p\} = \{1, \alpha, \alpha^2, \cdots .\alpha^{p^n-1}\}.$$

Addition for the elements of $\mathbb{F}_{p^n}$ *is easily carried out if the elements are represented as polynomials in* α*, whilst multiplication is easily done if the elements are represented as powers of* α.

Example 1.18.
Consider the field $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, *where* α *is a root of an irreducible polynomial* $f(X) = X^3 + X + 1 \in \mathbb{Z}_2[X]$. *Then we have*
$\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha(\alpha^3) = \alpha^2 + \alpha$, $\alpha^5 = \alpha(\alpha^4) = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha(\alpha^5) = \alpha^2 + 1$. *Thus,* $\mathbb{Z}_8 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. *So* α *is a primitive element.*

Proposition 1.1.

(i) A non-zero element of $\mathbb{F}_q$ *is a primitive element if and only if its order is* $q - 1$;

(ii) Every finite field has at least one primitive element.

Example 1.19.
Let α *be a root of* $X^3 + X + 1 \in \mathbb{F}_2[X]$. *Hence,* $\mathbb{F}_{2^3} = \mathbb{F}_2[\alpha]$, *the order of* α *is a divisor of* $8 - 1 = 7$. *Thus,* $ord(\alpha) = 7$ *and* α *is a primitive element.*

Theorem 1.9.
Let $\mathbb{F}_{p^n}$ *be a finite extension of* $\mathbb{F}_p$ *and let* $\mathbb{F}_{p^n}$ *be a finite extension of* $\mathbb{F}_{p^m}$. *Then* $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \cdot [\mathbb{F}_{p^m} : \mathbb{F}_p]$.

Lemma 1.3.
Let F *be a field and let* p *be a prime number. The following are equivalent* :

(i) $m \mid n$;

(ii) $p^m - 1 \mid p^n - 1$;

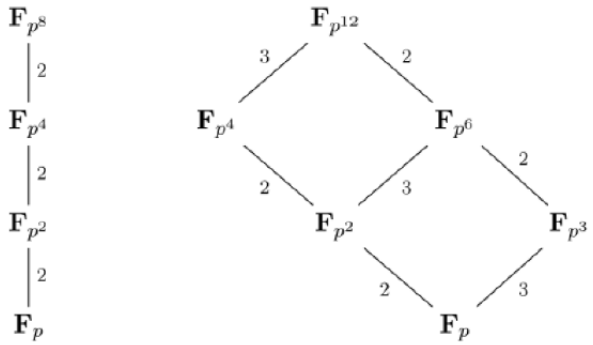
(iii) $x^m - 1 \mid x^n - 1$.

Theorem 1.10 (Subfield Criterion)**.**
Let p *be a prime and let* m, n *be natural numbers.*

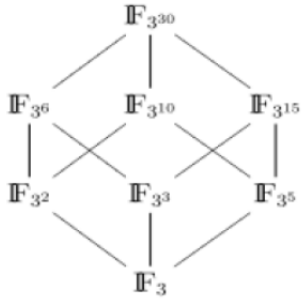
(i) If $\mathbb{F}_{p^m}$ *is a subfield of* $\mathbb{F}_{p^n}$, *then* $m \mid n$;

(ii) If $m \mid n$, *then* $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$. *There is exactly one subfield of* $\mathbb{F}_{p^m}$ *with* p^m *elements.*

Example 1.20.
In the diagram below are the subfields of $\mathbb{F}_{p^8}$ *and* $\mathbb{F}_{p^{12}}$.



Example 1.21.
Consider the finite field $\mathbb{F}_{3^{30}}$*. By Theorem* 1.10 *any subfield* $\mathbb{F}_{3^m}$ *must satisfy* $m \mid 30$ *and thus there are only the following subfields:* $\mathbb{F}_3, \mathbb{F}_{3^2}, \mathbb{F}_{3^3}, \mathbb{F}_{3^5}, \mathbb{F}_{3^6}, \mathbb{F}_{3^{10}}, \mathbb{F}_{3^{15}}$*; and* $\mathbb{F}_{3^{30}}$*. This leads to the following Hasse-diagram:*



Lemma 1.4.
Let p *be a prime number and let* F *be a field (finite or not) of characteristic* p*. Then*

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

for all positive integer n*.*

Example 1.22.
In a field of characteristic 2*, we have*

1. $(a+b)^2 = a^2 + b^2$.
2. $(a+b)^{2^2} = a^{2^2} + b^{2^2}$.
3. $(a+b)^{2^3} = a^{2^3} + b^{2^3}$.

1.3 Background of coding theory

1.3.1 Codes

We now look at some simple codes and give the basic definitions concerning codes.

Definition 1.17 (Codes)**.**
Let A be a finite set and $n \geqslant 1$ be an integer, we define

$$A^n = \{(a_1, a_2, \cdots, a_n) : a_i \in A\}.$$

A code C is a subset of A^n, where A^n is called a code space and the elements of a code C are called code-words. The cardinal or the size of C is M .i,e., $|C| = M$.

Example 1.23.

1. *Let $A = \{0, 1\}$. Then $C = \{1111, 1010, 1110, 0001\}$ is a code of length 4 over A.*
2. *Let $C = \{aaa, bbb, ccc, ddd\}$ be a code of length 3 and cardinal 4 from the English alphabets.*

Definition 1.18 (Hamming distance)**.**
Let $c_1 = (x_1, x_2, \cdots, x_n)$ and $c_2 = (y_1, y_2, \cdots, y_n)$, where $c_1, c_2 \in A^n$. A Hamming distance between c_1 and c_2 is the number of position, in which c_1 and c_2 are different, denoted $d_H(c_1, c_2)$

$$d_H(c_1, c_2) = \mid \{i : 1 \leq i \leq n, x_i \neq y_i\} \mid .$$

Example 1.24.
Let $C = \{0000, 1010, 1110, 0001, 1111\}$ be a code of length 4 over $A = \{0, 1\}$. Take $c_1 = (1111)$ and $c_2 = (1010)$. Then $d_H(c_1, c_2) = 2$.

Definition 1.19 (Hamming weight)**.**
Let $c = (c_1, \cdots, c_n) \in A^n$. We defined the Hamming weight of c to be the number of non-zero entries in c. More formally, the Hamming weight of c is

$$w_H(c) = \mid \{i : c_i \neq 0\} \mid,$$

and

$$w_H(c) = d_H(c, 0).$$

Example 1.25.
Let $C = \{0000, 1010, 1110, 0001, 1111\}$ be a code of length 4 over $A = \{0, 1\}$.

1. *Take $c = (1010)$. Then $w_H(1010) = 2$.*
2. *Take $c = (1111)$. Then $w_H(1111) = 4$.*

Remark 1.6.
A minimum weight of the code C is the minimum non-zero weight among all code-words of C,

$$w_{\min}(C) = \{\min(w_H(c)), 0 \neq c \in C\}.$$

Definition 1.20 (Minimum distance)**.**
The minimum distance of a code C, denoted $d_{\min}(C)$ is defined to be the minimum Hamming distance between tow distinct code-words of C

$$d_{\min}(C) = \min\{d_H(c_1, c_2) \colon c_1, c_2 \in C, c_1 \neq c_2\}.$$

Example 1.26.

1. *Let $C = \{000, 110, 011, 101\}$ be a code of length 3 over $A = \{0, 1\}$. Hence, $d_{min}(C) = 2$.*
2. *Let $D = \{0001, 0011, 0101, 1100\}$ be a code of length 4 over $B = \{0, 1, 2\}$. Hence, $d_{min}(D) = 1$.*

1.3.2 Linear codes

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.

Definition 1.21 (Linear codes)**.**
Let $\mathbb{F}_q$ be a finite field. If the code C is a subspace of $\mathbb{F}_q^n$. Then the code C is said to be a linear code of k-dimension, minimum distance d and length n. The cardinal of C is $|C| = M = q^k$. A q-ary linear code will be referred as an $[n, k, d]_q$ code or $[n, k, d]$ code.

Example 1.27.
Let C be a linear code over $\mathbb{F}_3$ with parameters $[5, 2, 3]$

$$C = \{00000, 11100, 22200, 00111, 00222, 11211, 22011, 11022, 22122\}.$$

Proposition 1.2.
For an $[n, k, d]_q$ code C, the minimum distance is the same as minimum weight for linear codes.

$$d_{\min}(C) = w_{\min}(C).$$

Definition 1.22 (Generator matrix)**.**
A generator matrix of a linear code C is a $(k \times n)$ matrix G whose rows form a basis of C. There are many generator matrices of a linear code .

$$C = \left\{c \in C, \exists x \in \mathbb{F}_q^k : c = xG\right\}.$$

Example 1.28.

1. *Let $C_1 = \{00, 01, 10, 11\}$ be a binary $[2, 2]$code with generator matrix*

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

2. *Let $C_2 = \{000, 011, 101, 110\}$ be a binary $[3, 2]$ code with generator matrix*

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

Example 1.29.
Let G be a generator matrix of a linear code C over $\mathbb{F}_2 = \{0, 1\}$ with parameters $[3, 2]$, giving

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

Then, we have

$$\begin{aligned} C &= \{x_1(101), x_2(011) : x_1, x_2 \in \mathbb{F}_2\} \\ &= \{000, 101, 011, 110\}. \end{aligned}$$

So, C is the $[3, 2, 2]$ linear code over $\mathbb{F}_2$.

Definition 1.23. *(Inner product)*
Let $c = (c_1, \cdots, c_n)$, $\tilde{c} = (\tilde{c_1}, \cdots, \tilde{c_n}) \in \mathbb{F}_q^n$. The inner product of tow vectors $\tilde{c}$ and c is defined by

$$\langle \tilde{c}, c \rangle = \left\{ \sum_{i=1}^{n} \tilde{c}_i \cdot c_i : c_i, \tilde{c}_i \in \mathbb{F}_q \right\}.$$

If $\langle \tilde{c}, c \rangle = 0$, the vectors are orthogonal.

Definition 1.24 (The dual code)**.**
Let C be a linear code. The dual code of C, denoted $C^\perp$ is the code $[n, n-k]_q$ over $\mathbb{F}_q$.

$$C^\perp = \left\{ \tilde{c} \in \mathbb{F}_q^n \colon \langle \tilde{c}, c \rangle = 0, \forall c \in C \right\},$$

where $\langle \tilde{c}, c \rangle$ is the inner product.

Example 1.30.
Consider the linear code $C = \{0000, 1000, 0100, 1100\}$ over $\mathbb{F}_2$ with parameters $[4, 2, 1]$. Then the dual code of C is

$$C^\perp = \{0000, 0010, 0001, 0011\}.$$

Theorem 1.11.
If C is an $[n, k]_q$ linear code, then $(C^\perp)^\perp = C$.

Definition 1.25 (Parity check matrix)**.**
A parity check matrix H for an $[n, k]$ linear code C is an $(n-k) \times n$ matrix which is a generator matrix of $C^\perp$.

$$C = \left\{ c \in \mathbb{F}_q^n \colon Hc^T = \boldsymbol{0} \right\}.$$

Example 1.31.
Let H be a parity check matrix of a linear code C over $\mathbb{F}_2$ with parameters $[5, 2]$

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

For any code-word $c \in C$ the equation $Hc^T = \mathbf{0}$ holds. In other words, any code-words in C is valid a solution of the following set of equation. Let $c = (c_1, c_2, c_3, c_4, c_5) \in C$, we have $Hc^T = \mathbf{0}$

$$\begin{cases} c_1 + c_2 = 0 \\ c_1 + c_3 + c_4 = 0 \\ c_1 + c_3 + c_5 = 0 \end{cases} \Leftrightarrow \begin{cases} c_2 = -c_1 \\ c_4 = -c_1 - c_3 = c_1 + c_3 \\ c_5 = c_1 + c_3 = c_4 \end{cases}.$$

Then $c = (c_1, c_1, c_3, c_1 + c_3, c_1 + c_3) \Leftrightarrow c = c_1(1, 1, 0, 1, 1) + c_3(0, 0, 1, 1, 1)$.
The code C have $q^k = 2^2$ code-words, then

$$C = \{00000, 11011, 00111, 11100\}.$$

Proposition 1.3.
There is a unique generator matrix of the form $G = [I_k|A]$ where I_k is the identity matrix. The code is said to be in systematic form. If $G = [I_k|A]$ is a generator matrix for the $[n, k]$ code C, then $H = \left[-A^T|I_{n-k}\right]$ is a parity check matrix.

Remark 1.7.
We clearly have $GH^T = \mathbf{0}$.

Example 1.32.
Let $C = \{00000, 01101, 10110, 11011\}$ be the $[5, 2]$ linear code given by the generator matrix $G = [I_k|A]$ with corresponding parity check matrix $H = \left[-A^T|I_{n-k}\right]$

$$G = \left(\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right) \qquad H = \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right).$$

Theorem 1.12 (Singleton Bound)**.**
If C is an $[n, k]$ linear code over the finite field $\mathbb{F}_q$, then

$$d_{min}(C) \leq n - k + 1.$$

Definition 1.26 (Maximum Distance Separable)**.**
A linear code that meets the Singleton Bound with equality is called maximum distance separable for short MDS, such that $d = n - k + 1$.

Example 1.33.
Consider the $[4, 3, 2]$ binary linear code whose generator matrix G is :

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

The rows of G are chosen in such away that any two rows have a minimum Hamming distance of at least 2. Since $d = n - k + 1 = 4 - 3 + 1 = 2$. Then this code is an MDS code over $\mathbb{F}_2$.

Definition 1.27 (Linear complementary dual)**.**
A linear complementary dual ($LCD for short$) *is a linear code* C *that intersects with its dual* $C^{\perp}$ *trivially, i.e.,* $C \bigcap C^{\perp} = \{0\}$.

Corollary 1.3. *[12]*
Let C *be a linear code and let* G *and* H *be respectively a generator matrix and a parity-check matrix of* C*. Then the following statements are equivalent* :

(i) C *is an* LCD *code;*

(ii) $\det(GG^T) \neq 0$*;*

(iii) $\det(HH^T) \neq 0$.

Example 1.34.
Let G *be a generator matrix and* H *parity check matrix of a linear code* C *over* $\mathbb{F}_2$ *with parameters* $[4, 2]$

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

We calculate

$$G \cdot G^T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad H \cdot H^T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and $\det(G \cdot G^T) = 1 \neq 0$, $\det(H \cdot H^T) = 1 \neq 0$. *According to Corollary* 1.3, C *is an* LCD *code.*

Definition 1.28.
Linear codes that are both MDS *and* LCD *are called* LCD MDS *codes.*

Chapter 2

Generalized Reed-Solomon codes

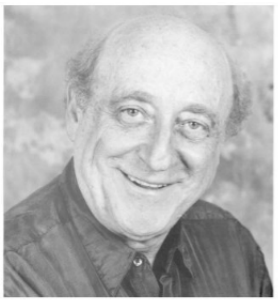
The Generalized Reed-Solomon (GRS) code is an extension of the classic Reed-Solomon code, which is a type of error-correcting code. RS codes were developed by Irving S. Reed and Gustave Solomon in 1960. This type of code is widely used in various applications that require error-correction, such as data storage systems and wireless communications.

The GRS code excels in handling more complex error patterns compared to the classic code. Instead of solely focusing on correcting errors caused by data loss or noise, the GRS code can handle more sophisticated errors like timing deviations or variations in signal strength.

Enhanced performance of the GRS code is achieved through the utilization of interpolation and symbol-level processing techniques in the error-correction process. These techniques involve leveraging available data to recover lost or damaged information and improving the code's ability to recover lost or damaged data by individually processing symbols.

The GRS code finds applications in a wide range of fields. For example, it is used in data storage systems such as hard drives and memory cards, where it helps protect data from errors and corruption. It is also employed in wireless communication applications such as mobile phones and wireless networks, where it enhances the reliability and quality of data transmission by mitigating errors.

Irving Reed



Gus Solomon

In this chapter, we review some basic notations and results about generalized Reed-Solomon codes and its dual. For more details, we refer the reader to see [6],[2],[8],[9], [14] and [7].

2.1 Generalized Reed-Solomon codes

Definition 2.1.
Let $\mathbb{F}_q$ be a finite field of order q. Let n and k be positive integers such that $1 \leq k \leq n \leq q$. Take $\mathbf{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$, where α_i $(1 \leq i \leq n)$ are distinct elements of $\mathbb{F}_q^n$.
For $1 \leq i \leq n$, we introduce

$$L_i(X) = \prod_{j=1, i \neq j}^{n} (X - \alpha_j).$$

It will be used throughout this chapter.
Choosing $\mathbf{v} = (v_1, v_2, \cdots, v_n)$, where $v_i \in (\mathbb{F}_q^*)^n$. Then k-dimensional generalized Reed-Solomon code (GRS code for short) of length n associated with $\mathbf{a}$ and $\mathbf{v}$ is defined as follows :

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{(v_1 f(\alpha_1), \cdots, v_n f(\alpha_n)) : f(X) \in \mathbb{F}_q[X], \deg(f(X)) \leq k-1\}. \tag{2.1}$$

Remark 2.1.
Let $\mathbf{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ be distinct and $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_q^*)^n$, we define the evaluation map :

$$\begin{array}{rccl} \mathbf{ev}_{\mathbf{a},\mathbf{v}}(.) : \mathbb{F}_q[X]_k & \longrightarrow & \mathbb{F}_q^n \\ f(X) & \longmapsto & v_i \cdot f(\alpha_i) = (v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)) \end{array}$$

Note that $\mathbf{ev}_{\mathbf{a},\mathbf{v}}(.)$ is an $\mathbb{F}_q$-linear map. The corresponding generalized Reed-Solomon code of dimension k as

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{\mathbf{ev}_{\mathbf{a},\mathbf{v}}(f) : f(X) \in \mathbb{F}_q[X]_k\}.$$

Proposition 2.1.
One basic $\mathbb{F}_q[X]_k$ is $\{1, X, \cdots, X^{k-1}\}$. Thus, $\{\mathbf{ev}_{\mathbf{a},\mathbf{v}}(1), \mathbf{ev}_{\mathbf{a},\mathbf{v}}(X), \cdots, \mathbf{ev}_{\mathbf{a},\mathbf{v}}(X^{k-1})\}$ gives a generator matrix of $GRS_k(\mathbf{a}, \mathbf{v})$.

$$\begin{aligned} G &= \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \ldots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \ldots & v_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \ldots & v_n\alpha_n^{k-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix} \begin{pmatrix} v_1 & 0 & \cdots & 0 \\ 0 & v_2 & \cdots & 0 \\ & & \cdots & \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & v_n \end{pmatrix}. \end{aligned} \tag{2.2}$$

Remark 2.2. *[6]*
In the case where $\mathbf{v} = (1, 1, \cdots, 1)$ *and* $n \leqslant q-1$*, the generalized Reed-Solomon code constructed is often called a punctured Reed-Solomon code, as it can be obtained by puncturing an RS code at suitable coordinates.*

Example 2.1.

1. *Let 's consider the* $GRS_3(\mathbf{a}, \mathbf{v})$ *code over* $\mathbb{F}_7$ *with parameters* $[6, 3]$*, evaluated at* $\mathbf{a} = (2, 4, 6, 1, 3, 5)$ *with* $\mathbf{v} = (1, 1, 1, 1, 1, 1)$*. Then, this code has a generator matrix* :

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 4 & 6 & 1 & 3 & 5 \\ 4 & 2 & 1 & 1 & 2 & 4 \end{pmatrix}.$$

2. *Consider the* $GRS_4(\mathbf{a}, \mathbf{v})$ *code over* $\mathbb{F}_{11}$*, let* $\mathbf{a} = (1, 2, 3, 4, 5, 6, 7, 8)$ *and* $\mathbf{v} = (1, 3, 5, 7, 9, 2, 6, 4)$*. Then, the generator matrix of* $GRS_4(\mathbf{a}, \mathbf{v})$ *is given by* :

$$G = \begin{pmatrix} 1 & 3 & 5 & 7 & 9 & 2 & 6 & 4 \\ 1 & 6 & 4 & 6 & 1 & 1 & 9 & 10 \\ 1 & 1 & 1 & 2 & 5 & 6 & 8 & 3 \\ 1 & 2 & 3 & 8 & 3 & 3 & 1 & 2 \end{pmatrix}.$$

Theorem 2.1. *[7]*
$GRS_k(\mathbf{a}, \mathbf{v})$ *is an* $[n, k]$ *linear code. Moreover, it is an* MDS *code.*

Proof. [7]
By Definition 2.1, α_i are distinct, we must have $n \leq q$. If $a \in \mathbb{F}_q$ and $f(X), g(X) \in \mathbb{F}_q[X]_k$. Then $a \cdot f(X) + g(X)$ is also in $\mathbb{F}_q[X]_k$; and

$$\mathbf{ev}_{\mathbf{a},\mathbf{v}}(a \cdot f(X) + g(X)) = a \cdot \mathbf{ev}_{\mathbf{a},\mathbf{v}}(f(X)) + \mathbf{ev}_{\mathbf{a},\mathbf{v}}(g(X)) = a \cdot f + g.$$

Then, $GRS_k(\mathbf{a}, \mathbf{v})$ is linear of length n over $\mathbb{F}_q$.

Let $f(X), g(X) \in \mathbb{F}_q[X]_k$ be distinct polynomials. Set $h = f - g \neq 0$. Then $w_H(h) = d_H(f, g)$. But the weight of h is n minus the number of 0's in h. As all the v_i are non-zero, this equals n minus the number of roots that $h(X)$ has among $\alpha_1, \cdots, \alpha_n$. As $h(X)$ has at most $k-1$ roots, the weight of h is at least $n - (k-1) = n - k + 1$. Therefore $d_H \geqslant n - k + 1$, and we get equality from the Singleton bound Shaw that $d_H \leq n - k + 1$, so $d_H = n - k + 1$. Hence, $GRS_k(\mathbf{a}, \mathbf{v})$ is an MDS code. □

2.2 Dual of Generalized Reed-Solomon codes

Theorem 2.2. *[7]*
Let $\mathbf{a} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{F}_q^n$*, where* $\alpha_1, \cdots, \alpha_n$ *are distinct elements, and let* $\mathbf{v} = (v_1, \cdots, v_n) \in (\mathbb{F}_q^*)^n$*. The dual code of* $GRS_k(\mathbf{a}, \mathbf{v})$ *is* $GRS_{n-k}(\mathbf{a}, \boldsymbol{u})$*, where* $u_i = (u_1, \cdots, u_n)$ *with* $u_i = v_i^{-1}(L_i(\alpha_i))^{-1}$*, for all* $(1 \leq i \leq n)$*.*

Proof. [7]
Let $c = \mathbf{ev}_{\mathbf{a},\mathbf{v}}(f(X))$, where $\deg f(X) \leq k-1$, and $\tilde{c} = \mathbf{ev}_{\mathbf{a},\mathbf{u}}(g(X))$, where $\deg g(X) \leq n-k-1$. Therefore, $\deg f(X)g(X) \leq n-2 \leq n-1$. By Lagrange interpolation 1.2, we have

$$f(X)g(X) = \sum_{i=1}^{n} \frac{L_i(X)}{L_i(\alpha_i)} f(\alpha_i)g(\alpha_i).$$

Equating the coefficient of X^{n-1} from the two sides gives :

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \frac{1}{L_{i(\alpha_i)}} f(\alpha_i)g(\alpha_i) \\ &= \sum_{i=1}^{n} (v_i f(\alpha_i)) \frac{v_i^{-1}}{L_i(\alpha_1)} g(\alpha_i) \\ &= \sum_{i=1}^{n} (v_i f(\alpha_i))(u_i g(\alpha_i)) \\ &= c \cdot \tilde{c}. \end{aligned}$$

This implies that, $GRS_{n-k}(\mathbf{a},\mathbf{u}) \subseteq GRS_k(\mathbf{a},\mathbf{v})^{\perp}$. Comparing the dimensions of both codes, the theorem follows.

□

Corollary 2.1. *[7]*
The following matrix is a parity check matrix of $GRS_k(\mathbf{a},\mathbf{v})$ *as in Definition* 2.1.

$$H = \begin{pmatrix} u_1 & u_2 & \cdots & u_n \\ u_1\alpha_1 & u_2\alpha_2 & \cdots & u_n\alpha_n \\ u_1\alpha_1^2 & u_2\alpha_2^2 & \cdots & u_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ u_1\alpha_1^{n-k-1} & u_2\alpha_2^{n-k-1} & \cdots & u_n\alpha_n^{n-k-1} \end{pmatrix}, \tag{2.3}$$

where $u_i = (u_1, \cdots, u_n)$ *and* $u_i = v_i^{-1}(L_i(\alpha_i))^{-1}$, *for all* $(1 \leq i \leq n)$.

Remark 2.3. *[14]*
Let $\mathbf{1} = (1, \cdots, 1)$ *denote the all-one row vector with appropriate length. The dual of* $GRS_k(\mathbf{a},\mathbf{1})$ *is* $GRS_{n-k}(\mathbf{a},\mathbf{u})$, *where* $u_i = (u_1, \cdots, u_n)$ *with* $u_i = L_i(\alpha_i)^{-1}$*for* $1 \leq i \leq n$.

Remark 2.4. *[6]*
Recall that $u_i = (u_1, \cdots, u_n)$ *is any vector that generates the dual of* $GRS_{n-k}(\mathbf{a},\mathbf{u})$, *then it is not unique. In particular, the parity-check matrix is also not unique.*

Example 2.2.

1. *Consider the* 7*-ary* $[6,3]$*-GRS code as in Example* 2.1. *First we compute* $L_i(\alpha_i)$ *for all* $1 \leq i \leq n$*, we get*

$$\begin{array}{lccccccccc} L_1(2) = & & (-2) & (-4) & (1) & (-1) & (-3) & = & 24 & = & 3. \\ L_2(4) = & (2) & & (-2) & (3) & (1) & (-1) & = & 12 & = & 5. \\ L_3(6) = & (4) & (2) & & (5) & (3) & (1) & = & 120 & = & 1. \\ L_4(1) = & (-1) & (-3) & (-5) & & (-2) & (-4) & = & -120 & = & 6. \\ L_5(3) = & (1) & (-1) & (-3) & (2) & & (-2) & = & -12 & = & 2. \\ L_6(5) = & (3) & (1) & (-1) & (4) & (2) & & = & -24 & = & 4. \end{array}$$

By Remark 2.3*, the dual code of* $GRS_3(\mathbf{a},\mathbf{v})$ *is* $GRS_3(\mathbf{a},\mathbf{u})$*, where* $\boldsymbol{u} = (5,3,1,6,4,2)$ *with parity check matrix of* $GRS_3(\mathbf{a},\mathbf{u})$*:*

$$H = \begin{pmatrix} 5 & 3 & 1 & 6 & 4 & 2 \\ 3 & 5 & 6 & 6 & 5 & 3 \\ 6 & 6 & 1 & 6 & 1 & 1 \end{pmatrix}.$$

2. *Consider the* 11*-ary* $[8,4]$*-GRS code as in Example* 2.1. *By Theorem* 2.2*, the dual code of* $GRS_4(\mathbf{a},\mathbf{v})$ *is* $GRS_4(\mathbf{a},\mathbf{u})$*, where* $\boldsymbol{u} = (5,3,10,8,6,8,4,7)$ *with parity check matrix* :

$$H = \begin{pmatrix} 5 & 3 & 10 & 8 & 6 & 8 & 4 & 7 \\ 5 & 6 & 8 & 10 & 8 & 4 & 6 & 1 \\ 5 & 1 & 2 & 7 & 7 & 2 & 9 & 8 \\ 5 & 2 & 6 & 6 & 2 & 1 & 8 & 9 \end{pmatrix}.$$

Example 2.3.

Consider the 8*-ary* $[6,3]$*-GRS code, evaluated at* $\mathbf{a} = (\alpha^0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ *and* $\mathbf{v} = (\alpha^4, \alpha^2, \alpha^3, \alpha^0, \alpha^5, \alpha^6)$*, where* $\alpha^3 + \alpha + 1 = 0$ *in* $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$*. A generator matrix of* $GRS_3(\mathbf{a},\mathbf{v})$ *is given by* :

$$G = \begin{pmatrix} \alpha^4 & \alpha^2 & \alpha^3 & \alpha^0 & \alpha^5 & \alpha^6 \\ \alpha^4 & \alpha^3 & \alpha^5 & \alpha^3 & \alpha^2 & \alpha^4 \\ \alpha^4 & \alpha^4 & \alpha^0 & \alpha^6 & \alpha^6 & \alpha^2 \end{pmatrix}.$$

First we compute $L_i(\alpha_i)$ *for all* $1 \leq i \leq n$*,*

$$\begin{array}{rccccc} L_1(1) = (\alpha^0 - \alpha) & (\alpha^0 - \alpha^2) & (\alpha^0 - \alpha^3) & (\alpha^0 - \alpha^4) & (\alpha^0 - \alpha^5) & = \alpha^5. \\ L_2(\alpha) = (\alpha - \alpha^0) & (\alpha - \alpha^2) & (\alpha - \alpha^3) & (\alpha - \alpha^4) & (\alpha - \alpha^5) & = \alpha. \\ L_3(\alpha^2) = (\alpha^2 - \alpha^0) & (\alpha^2 - \alpha) & (\alpha^2 - \alpha^3) & (\alpha^2 - \alpha^4) & (\alpha^2 - \alpha^5) & = \alpha^5. \\ L_4(\alpha^3) = (\alpha^3 - \alpha^0) & (\alpha^3 - \alpha) & (\alpha^3 - \alpha^2) & (\alpha^3 - \alpha^4) & (\alpha^3 - \alpha^5) & = \alpha^0. \\ L_5(\alpha^4) = (\alpha^4 - \alpha^0) & (\alpha^4 - \alpha) & (\alpha^4 - \alpha^2) & (\alpha^4 - \alpha^3) & (\alpha^4 - \alpha^5) & = \alpha^0. \\ L_6(\alpha^5) = (\alpha^5 - \alpha^0) & (\alpha^5 - \alpha) & (\alpha^5 - \alpha^2) & (\alpha^5 - \alpha^3) & (\alpha^5 - \alpha^4) & = \alpha. \end{array}$$

By Theorem 2.2*, the dual code of* $GRS_3(\mathbf{a},\mathbf{v})$ *is* $GRS_3(\mathbf{a},\mathbf{u})$*, where* $\boldsymbol{u} = (\alpha^5, \alpha^4, \alpha^6, \alpha^0, \alpha^2, \alpha^0)$ *with parity check matrix* :

$$H = \begin{pmatrix} \alpha^5 & \alpha^4 & \alpha^6 & \alpha^0 & \alpha^2 & \alpha^0 \\ \alpha^5 & \alpha^5 & \alpha & \alpha^3 & \alpha^6 & \alpha^5 \\ \alpha^5 & \alpha^6 & \alpha^3 & \alpha^6 & \alpha^3 & \alpha^3 \end{pmatrix}.$$

Chapter 3

MDS codes with complementary duals over finite fields

In this chapter, we list some results about *LCD MDS* code, which are given by Bocong Chen and Hongwei Liu in [14].
Throughout this chapter, let $\mathbf{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$, where α_i $(1 \leq i \leq n)$ are distinct elements of $\mathbb{F}_q^n$, and $\mathbf{v} = (v_1, v_2, \cdots, v_n) \in (\mathbb{F}_q^*)^n$. For $1 \leq i \leq n$, we denote

$$L_i(X) = \prod_{j=1, i \neq j}^{n} (X - \alpha_j).$$

We begin with the following lemma, which is useful for building *LCD GRS* codes over finite fields .

Lemma 3.1. *[14]*
Assume that $GRS_k(\mathbf{a}, \mathbf{v})$ is the GRS code associated with $\mathbf{a}$ and $\mathbf{v}$ as in (2.1). A codeword $\boldsymbol{c} = (v_1 f(\alpha_1), v_2 f(\alpha_2), \cdots, v_n f(\alpha_n))$ of $GRS_k(\mathbf{a}, \mathbf{v}) \subseteq GRS_k(\mathbf{a}, \mathbf{v})^{\perp}$ if and only if a polynomial $g(X) \in \mathbb{F}_q[X]$ with $\deg g(X) \leq n - k - 1$, such that

$$\left(v_1^2 f(\alpha_1), v_2^2 f(\alpha_2), \cdots, v_n^2 f(\alpha_n)\right) = \left(u_1 g(\alpha_1), u_2 g(\alpha_2), \cdots, u_n g(\alpha_n)\right), \tag{3.1}$$

where $u_i = L_i(\alpha_i)^{-1}$ for $1 \leq i \leq n$.

Proof. [14]
Let G be a generator matrix of $GRS_k(\mathbf{a}, \mathbf{v})$ given by (2.2). We have

$$G = \underbrace{\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}}_{G_1} \underbrace{\begin{pmatrix} v_1 & & & \\ & v_2 & & \\ & & \ddots & \\ & & & v_n \end{pmatrix}}_{\Delta}.$$

Since $\mathbf{c} = (v_1 f(\alpha_1), v_2 f(\alpha_2), \cdots, v_n f(\alpha_n))$ is contained in $GRS_k(\mathbf{a}, \mathbf{v})^\perp$ if and only if

$$G\mathbf{c}^T = (G_1\Delta)\mathbf{c}^T = G_1(\Delta\mathbf{c}^T) = G_1\left(v_1^2 f(\alpha_1), v_2^2 f(\alpha_2), \cdots, v_n^2 f(\alpha_n)\right)^T = \mathbf{0},$$

where $\mathbf{c}^T$ denotes the transpose of $\mathbf{c}$. It follows that

$$\left(v_1^2 f(\alpha_1), v_2^2 f(\alpha_2), \cdots, v_n^2 f(\alpha_n)\right) \in GRS_k(\mathbf{a}, \mathbf{1})^\perp.$$

□

3.1 Some constructions of LCD MDS codes

Throughout this section, we assume that $1 < k \leq \lfloor n/2 \rfloor$, where $\lfloor \mathbf{a} \rfloor$ denotes the integer part of $\mathbf{a}$.

In the following, we list some *LCD MDS* codes from *GRS* codes of length $1 < n \leq q$.

Theorem 3.1. *[14]*
Let $q > 3$ be an odd prime power. If $n > 1$, with $n \mid q-1$, then there exists a k-dimensional LCD GRS code of length n over $\mathbb{F}_q$.

Proof. [14]
Since $n \mid q-1$, there exists a primitive nth root of unity w in $\mathbb{F}_q$. Choose $\mathbf{a} = (w^0, w^1, \cdots, w^{n-1})$ and let $\mathbf{v} = (v_1, \cdots, v_{n-k+1}, v_{n-k+2}, \cdots, v_n)$, where $v_i = 1$ for $1 \leq i \leq n-k+1$, $v_i^2 \neq 1$ and $v_i \neq 0$ for $n-k+2 \leq i \leq n$. Consider the q-ary GRS code of length n over $\mathbb{F}_q$ associated with $\mathbf{a}$ and $\mathbf{v}$ as follows :

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{(f(w^0), \cdots, f(w^{n-k}), v_{n-k+2} f(w^{n-k+1}), \cdots, v_n f(w^{n-1})) : \\ f(X) \in \mathbb{F}_q[X], \deg f(X) \leq k-1\}.$$

We claim that $GRS_k(\mathbf{a}, \mathbf{v}) \bigcap GRS_k(\mathbf{a}, \mathbf{v})^\perp = \{0\}$. Assume that,

$$(f(w^0), \cdots, f(w^{n-k}), v_{n-k+2} f(w^{n-k+1}), \cdots, v_n f(w^{n-1})) \subseteq GRS_k(\mathbf{a}, \mathbf{v}) \bigcap GRS_k(\mathbf{a}, \mathbf{v})^\perp.$$

It yields,

$$G_2\left(f(w^0), \cdots, f(w^{n-k}), v_{n-k+2}^2 f(w^{n-k+1}), \cdots, v_n^2 f(w^{n-1})\right)^T = \mathbf{0},$$

where G_2 is the $k \times n$ matrix

$$G_2 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & w & \cdots & w^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & w^{k-1} & \cdots & w^{(k-1)(n-1)} \end{pmatrix}.$$

It is easy to verify that

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & w & \cdots & w^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & w^{n-2} & \cdots & w^{(n-2)(n-1)} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ w \\ \vdots \\ w^{n-1} \end{pmatrix} = \mathbf{0}.$$

Then, a polynomial $g(X) \in \mathbb{F}_q[X]$ with $\deg g(X) \leq n-k-1$ by way of explanation

$$(f(w^0), \cdots, f(w^{n-k}), v_{n-k+2}^2 f(w^{n-k+1}), \cdots, v_n^2 f(w^{n-1})) = (g(w^0), wg(w^1), \cdots, w^{n-1}g(w^{n-1})). \tag{3.2}$$

Comparing the first $n-k+1$ coordinates of (3.2) give $f(w^i) = w^i g(w^i)$ for $0 \leq i \leq n-k$. By condition $k \leq \lfloor n/2 \rfloor, \deg f(X) \leq k-1 \leq n-k-1$ and $\deg g(X) \leq n-k-1$, we get $f(X) = Xg(X)$. In particular, $\deg g(X) \leq k-2$. By the last $k-1$ coordinates of (3.2), we have that for any $n-k+2 \leq j \leq n$,

$$v_j^2 f(w^{j-1}) = v_j^2 w^{j-1} g(w^{j-1}) = w^{j-1} g(w^{j-1}).$$

It follows from $v_j^2 \neq 1$ that $g(w^{j-1}) = 0$. That is to say, $g(X)$ has $k-1$ distinct roots, giving $g(X) = 0$. Thus, $f(X) = 0$. □

3.1.1 Examples

Example 3.1.
Let $q = 7$. Take $n = 6 \mid q-1$ and $k = 3 \leq \lfloor 6/2 \rfloor$. Then $w = 3$ is a primitive 6-th root of unity. Choose $\mathbf{a} = (1, 3, 2, 6, 4, 5)$ and $v = (1, 1, 1, 1, 3, 3)$. We define $GRS_3(\mathbf{a}, \mathbf{v})$ as fellows:

$$GRS_3(\mathbf{a}, \mathbf{v}) = \{f(1), f(3), f(2), f(6), 3f(4), 3f(5) : f(X) \in \mathbb{F}_7[X], \deg f(X) \leq k-1\}.$$

Hence, the generator matrix of $GRS_3(\mathbf{a}, \mathbf{v})$ is

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 3 & 3 \\ 1 & 3 & 2 & 6 & 5 & 1 \\ 1 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}.$$

It is easy to verify that

$$G \cdot G^T = \begin{pmatrix} 1 & 2 & 6 \\ 2 & 6 & 0 \\ 6 & 0 & 6 \end{pmatrix},$$

and $\det(G \cdot G^T) = 6 \neq 0$. According to Theorem 3.1 and Corollary 1.3, $GRS_3(\mathbf{a}, \mathbf{v})$ is the 7-ary $[6, 3, 4]$ LCD MDS code.

Example 3.2.
Let $q = 5$. Take $n = 4 \mid q-1$ and $k = 2 \leq \lfloor 4/2 \rfloor$. Then $w = 2$ is a primitive 4-th root of unity. Choosing $\mathbf{a} = (1, 2, 3, 4)$ and $v = (1, 1, 1, 2)$. We define $GRS_2(\mathbf{a}, \mathbf{v})$ as fellows :

$$GRS_2(\mathbf{a}, \mathbf{v}) = \{f(1), f(2), f(3), 2f(4) : f(X) \in \mathbb{F}_5[X], \deg f(X) \leq k-1\}.$$

Then, the generator matrix of $GRS_2(\mathbf{a}, \mathbf{v})$ is

$$G = \begin{pmatrix} 1 & 1 & 1 & 2 \\ 1 & 2 & 3 & 3 \end{pmatrix}.$$

The dual code of $GRS_2(\mathbf{a}, \mathbf{v})$ is $GRS_2(\mathbf{a}, \mathbf{u})$, where $u = (4, 3, 2, 3)$ with parity check matrix:

$$H = \begin{pmatrix} 4 & 3 & 2 & 3 \\ 4 & 1 & 1 & 2 \end{pmatrix}.$$

It is easy to verify that

$$G \cdot G^T = \begin{pmatrix} 2 & 2 \\ 2 & 3 \end{pmatrix}, \qquad H \cdot H^T = \begin{pmatrix} 3 & 2 \\ 2 & 0 \end{pmatrix},$$

and $\det(G \cdot G^T) = 2 \neq 0$, $\det(H \cdot H^T) = 1 \neq 0$. According to Corollary 1.3 and Theorem 3.1, $GRS_2(\mathbf{a}, \mathbf{v})$ is the 5-ary $[4, 2, 3]$ LCD MDS code.

Theorem 3.2. *[14]*
Assume $q = p^e > 3$, where p is an odd prime number and $e \geq 1$ is an integer. Then there exists a k-dimensional LCD GRS code of length $n = p^\ell$ over $\mathbb{F}_q$, where ℓ is a positive integer with $1 \leq \ell \leq e$.

Proof.
Let T be an additive subgroup of $\mathbb{F}_{p^e}$ of order $n = p^\ell$, say $T = \{\alpha_1, \cdots, \alpha_n\}$. Can be expressed as

$$t = \prod_{z \in T \setminus \{0\}} z.$$

Choosing $\gamma \in \mathbb{F}_q^*$ with $\gamma^2 \neq 1$. Let $\mathbf{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ and let $\mathbf{v} = (v_1, \cdots, v_{n-k}, v_{n-k+1}, \cdots, v_n)$, where $v_i = 1$ for $1 \leq i \leq n-k$ and $v_i = \gamma$ for $n-k+1 \leq i \leq n$. We define the q-ary GRS code $GRS_k(\mathbf{a}, \mathbf{v})$ of length n, as follows :

$$GRS_k(\mathbf{a}, \mathbf{v}) = \{(f(\alpha_1), \cdots, f(\alpha_{n-k}), \gamma f(\alpha_{n-k+1}), \cdots, \gamma f(\alpha_n)) \colon f(X) \in \mathbb{F}_q[X], \deg f(X) \leq k-1\}.$$

As in the proofs of the previous Theorems, we can show that $GRS_k(\mathbf{a}, \mathbf{v}) \bigcap GRS_k(\mathbf{a}, \mathbf{v})^\perp = \{0\}$. Suppose we have

$$\mathbf{c} = (f(\alpha_1), \cdots, f(\alpha_{n-k}), \gamma f(\alpha_{n-k+1}), \cdots, \gamma f(\alpha_n)) \subseteq GRS_k(\mathbf{a}, \mathbf{v}) \bigcap GRS_k(\mathbf{a}, \mathbf{v})^\perp.$$

By Lemma 3.1, we get a polynomial $g(X) \in \mathbb{F}_q[X]$ with $\deg g(X) \leq n-k-1$, such that

$$(f(\alpha_1), \ldots, f(\alpha_{n-k}), \gamma^2 f(\alpha_{n-k+1}), \ldots, \gamma^2 f(\alpha_n)) = (u_1 g(\alpha_1), u_2 g(\alpha_2), \ldots, u_n g(\alpha_n)),$$

where $u_i = L_i(\alpha_i)^{-1}$ for $1 \leq i \leq n$. However, for any $1 \leq i \leq n$ we have

$$u_i = L_i(\alpha_i)^{-1} = t^{-1}.$$

Then

$$(f(\alpha_1), \cdots, f(\alpha_{n-k}), \gamma^2 f(\alpha_{n-k+1}), \cdots, \gamma^2 f(\alpha_n)) = (t^{-1}g(\alpha_1), t^{-1}g(\alpha_2), \cdots, t^{-1}g(\alpha_n)). \tag{3.3}$$

The first $n-k+1$ coordinates of (3.3) give $f(\alpha_i) = t^{-1}g(\alpha_i)$ for $1 \leq i \leq n-k$. By condition $k \leq \lfloor n/2 \rfloor$, $\deg f(X) \leq k-1 \leq n-k-1$ and $\deg g(X) \leq n-k-1$, we get $f(X) = t^{-1}g(X)$. In particular, $\deg g(X) \leq k-1$. By the last k coordinates of (3.3), we get that for any $n-k+1 \leq j \leq n$,

$$\gamma^2 f(\alpha_j) = \gamma^2 t^{-1} g(\alpha_j) = t^{-1} g(\alpha_j).$$

We have $\gamma^2 \neq 1$ then $g(\alpha_j) = 0$. Thus, $g(X)$ has $k-1$ distinct roots, giving $g(X) = 0$. Thus, $f(X) = 0$.

□

3.1.2 Examples

Example 3.3.
Let $q = 3^3$. Take $n = 3^2 = 9$ and $k = 3 \leq \lfloor 9/2 \rfloor$. Choose $\gamma = \alpha, \gamma^2 \neq 1$. Choose $\mathbf{a} = (1, 2, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7)$ and $v = (1, 1, 1, 1, 1, 1, \alpha, \alpha, \alpha)$, where $\alpha^3 + 2\alpha^2 + 1 = 0$ in $\mathbb{F}_{3^3} = \mathbb{F}_3[\alpha]$. We define $GRS_3(\mathbf{a}, \mathbf{v})$ as fellows

$$GRS_3(\mathbf{a}, \mathbf{v}) = \{f(1), f(2), f(\alpha), f(\alpha^2), f(\alpha^3), f(\alpha^4), \alpha f(\alpha^5), \alpha f(\alpha^6), \alpha f(\alpha^7) : f(X) \in \mathbb{F}_{3^3}[X], \deg f(X) \leq k-1\},$$

then, the generator matrix of $GRS_3(\mathbf{a}, \mathbf{v})$ is

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & \alpha & \alpha & \alpha \\ 1 & 2 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^6 & \alpha^7 & \alpha^8 \\ 1 & 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{11} & \alpha^{13} & \alpha^{15} \end{pmatrix}.$$

we calculate

$$G \cdot G^T = \begin{pmatrix} 0 & \alpha^2 & \alpha^{16} \\ \alpha^2 & \alpha^{16} & \alpha^{14} \\ \alpha^{16} & \alpha^{14} & \alpha^4 \end{pmatrix},$$

and $\det(G \cdot G^T) = \alpha^6 \neq 0$. Applying to Theorem 3.2 and Corollary 1.3, we get $GRS_3(\mathbf{a}, \mathbf{v})$ is the 3^3-ary $[9, 3, 7]$ LCD MDS code.

Example 3.4.
Let $q = 5^2$. Take $n = 5$ and $k = 2 \leq \lfloor 5/2 \rfloor$. Choose $\gamma = \alpha^2, \gamma^2 \neq 1$. Take $\mathbf{a} =$

$(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ *and* $v = (1, 1, 1, \alpha^2, \alpha^2)$ *with* $\alpha^2 + \alpha + 2 = 0$ *in* $\mathbb{F}_{5^2} = \mathbb{F}_5[\alpha]$. *We define* $GRS_2(\mathbf{a}, \mathbf{v})$ *as fellows*

$$GRS_2(\mathbf{a}, \mathbf{v}) = \{f(1), f(\alpha), f(\alpha^2), \alpha^2 f(\alpha^3), \alpha^2 f(\alpha^4) : f(X) \in \mathbb{F}_{5^2}[X], \deg f(X) \leq k-1\}.$$

Hence, the generator matrix of $GRS_2(\mathbf{a}, \mathbf{v})$ *is*

$$G = \begin{pmatrix} 1 & 1 & 1 & \alpha^2 & \alpha^2 \\ 1 & \alpha & \alpha^2 & \alpha^5 & \alpha^6 \end{pmatrix}.$$

The dual code of $GRS_2(\mathbf{a}, \mathbf{v})$ *is* $GRS_2(\mathbf{a}, \mathbf{u})$, *where* $u = (\alpha^5, \alpha^{12}, \alpha^{17}, \alpha^7, \alpha^{21})$ *with parity check matrix* :

$$H = \begin{pmatrix} \alpha^5 & \alpha^{12} & \alpha^{17} & \alpha^7 & \alpha^{21} \\ \alpha^5 & \alpha^{13} & \alpha^{19} & \alpha^{10} & \alpha \end{pmatrix}.$$

We compute

$$H \cdot H^T = \begin{pmatrix} \alpha^9 & \alpha^7 \\ \alpha^7 & \alpha^{21} \end{pmatrix}, \qquad G \cdot G^T = \begin{pmatrix} \alpha^{14} & 0 \\ 0 & \alpha^9 \end{pmatrix},$$

and $\det(G \cdot G^T) = \alpha^{23} \neq 0$, $\det(H \cdot H^T) = \alpha^{13} \neq 0$. *Applying to Corollary* 1.3 *and Theorem* 3.2 *we get* $GRS_2(\mathbf{a}, \mathbf{v})$ *is the* 5^2*-ary* $[5, 2, 4]$ *LCD MDS code.*

Conclusion

In this conclusion, we summarize the main results obtained in this work, we presented initially : definitions and some results of abstract algebra (Groups, Rings, Fields, Finite fields) and coding theory (Codes, Linear codes, Dual codes, MDS codes, LCD codes). Then, we studied the structure of generalized Reed-Solomon code and same properties of GRS and its dual. Finally, we studied some results about $LCD\ MDS$ codes over finite fields.

Abstract

A linear complementary dual (LCD) code is a linear code C whose dual code $C^{\perp}$ satisfies $C \bigcap C^{\perp} = \{0\}$. LCD codes have been used in certain communication systems. This application of LCD codes renewed the interest in the construction of LCD codes having a large minimum distance. Maximum Distance Separable MDS codes are a class of error correcting codes that achieve the maximum possible distance between code-words. Maximum distance separable with complementary dual ($LCD\ MDS$) codes are very important in coding theory and practice. We focus in this work on $LCD\ MDS$ codes constructed from generalized Reed-Solomon (GRS) codes over finite fields.

keywords : Linear complementary dual (LCD), generalized Reed-Solomon (GRS) code , MDS code.

Résumé

Un code dual complémentaire linéaire (LCD) est un code linéaire C dont le code dual $C^{\perp}$ satisfait à la condition $C \bigcap C^{\perp} = \{0\}$. Les codes LCD ont été utilisés dans certains systèmes de communication. Cette application des codes LCD a renouvelé l'intérêt pour la construction de codes LCD ayant une grande distance minimale. Les codes MDS (Maximum Distance Separable) est une classe de codes de correction d'erreur qui atteignent la distance maximale possible entre les mots de code. Les codes MDS avec dual complémentaire ($LCD\ MDS$) sont très importants en théorie et pratique du codage. Dans ce travail, nous nous concentrons sur les codes $LCD\ MDS$ construits à partir de codes Reed-Solomon généralisés (GRS) sur un corps fini.

Mots clés : Code dual complémentaire linéaire LCD, code Reed-Solomon généralisé GRS, code MDS

Bibliography

[1] C.E. Shannon, A mathematical theory of communication, Bell Syst. Tech, J.,27(3), 379-423, 1948

[2] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, Elsevier, North-Holland, 1977.

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

[4] R. Lidl and H. Niederreiter, Introduction to finite fields and applications, Cambridge university press, 1994.

[5] V. Pless, Introduction to the Theory of Error-Correcting Codes, Vol.48, John wiley and Sons, 1998.

[6] S. Ling and C. Xing, Coding Theory: A First Course, Cambridge University Press, Cambridge, 2004.

[7] S. Loepp, and W.k. wootters, Protecting information : from classical error correction to quantum cryptography, Cambridge University press, 2006 .

[8] A. Dagnelies, ALgebraic Soft-decoding of Reed-Solomon codes, Universite catholique de Louvain Master′s Thesis, 57, 2007 .

[9] W.C. Huffman and V. Pless, Fundamentals of error-correcting codes, Cambridge University press, 2010.

[10] R. Lidl and G. Pilz, Applied abstract algebra, Springer Science and Business Media, 2012.

[11] G.L. Mullen and D. Panario, Handbook of finite fields, CRC press, 2013.

[12] E.R. Lina and E.G. Nocon, On the construction of some LCD codes over finite fields, Manila journal of Science,9,67-82, 2016.

[13] L. Jin, Construction of MDS codes with complementary duals, IEEE Trans. Inf. Theory, DOI 10.1109/TIT.2016.2644660, 2016.

[14] B. Chen and H . Liu , New constructions of MDS codes with complementary duals, IEE Transactions on Information Theory, 64(8), 5776-5782, 2017.

[15] C. Carlet, S Mesnager, C. Tang and Y. Qi, Euclidean and hermitian LCD MDS Codes, preprint, arXiv:1702.08033, 2017.