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

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

Theme

Some weights of linear codes over finite fields

Presented by : *Benia Nihal*

Publicly presented on : June 9, 2024.

In front of the jury :

MIHOUBI Dawadi	Prof,	University of M'sila	**Presedent**.
LEBED Khawla	M.C.B,	University of M'sila	**Supervisor**.
HEBOUB Lakhdar	M.C.B,	University of M'sila	**Examinator**.

University years 2023/2024

Abstract

Linear codes can have different weights, which are measures of the distance between codewords. The most common weights are Hamming, Lee, and Distribution weights, in which Hamming and Lee weight counts the number of nonzero positions in a codeword, as they determine the error-correcting capability of the code. The weight distribution of a code, which specifies how many codewords have each possible weight, it can be used to compute the error probability of the code under various decoding algorithms. They are utilized in various applications within coding theory, and one of its most important uses is detecting and correcting errors. In this work, we study some weights of linear codes over finite fields and their results.

Key words

Finite fields, Linear codes, Weights.

Résumé

Les codes linéaires peuvent avoir des poids différents, qui sont des mesures de la distance entre les mots de code. Les poids les plus courants sont les poids Hamming, Lee et Distribution, dans lesquels Hamming et Lee comptent le nombre de positions non zéro dans un mot de code, car ils déterminent la capacité de correction d'erreur du code. La répartition du poids d'un code, qui spécifie combien de mots de code ont chaque poids possible, il peut être utilisé pour calculer la probabilité d'erreur du code sous divers algorithmes de décodage. Ils sont utilisés dans diverses applications au sein de la théorie du codage, et l'un de ses usages les plus importants est la détection et la correction des erreurs. Dans ce travail, nous étudions quelques poids de codes linéaires sur des corps finis et leurs résultats.

Les mot-clés

Les corps fini, Les codes linéaires, Poids.

Acknowledgements

I cannot begin and finish my work without thanking the greatest and the most powerful "Allah" for blessing me to complete this memory. I would like to express my sincere gratitude to my supervisor :

the professor Lebed khawla for the continuous support, for her patience, for her guidance helped me the whole time of research and writing of this memory.

All the gratitude to the president of the jury professor Mihoubi Douadi and the examiners professor Heboub Lakhdar for devoting thier time and thier effort to read and examine my work. I am very grateful to my mother and father. Their prayers, passionate, encouragements, and generosities have followed me everywhere to give me a lot of power. My sincere thanks to my dear sisters and brother.

you were the main supporters of me along my study.

My thanks to all the members of family for their encouraging during my studies.

Nihal Benia

Contents

Notations

- $|\mathbf{C}|$: Number of elements in $\mathbf{C}$.
- $\mathbb{N}$: Natural numbers.
- $\mathbb{Z}$: Integer numbers.
- $\mathbb{R}$: Real numbers .
- $\mathbb{C}$: Complex numbers.
- $\mathbb{Q}$: Rational numbers.
- $\mathbb{Z}/p\mathbb{Z}$: Integers modulo n.
- $\mathbb{F}_q$: Finite field with q elements.
- $\mathbf{R}/\mathbf{I}$: Quotient ring.
- $\mathbf{F}[X]$: The set of polynomials in X with coefficients in $\mathbf{F}$.
- wt: Hamming weight.
- $\mathrm{w}_{\mathbf{C}}$: Distribution weight.
- wt_L : Lee weight.
- d_H : Hamming distance.
- d_{min} : Minimum distance.
- deg : Degree of a polynomial.
- $\mathbf{C}^{\perp}$: Dual code of $\mathbf{C}$.
- MDS : Maximum Distance Separable.
- $\mathbb{RS}$: Reed-Solomon codes .

Introduction

Coding theory is a traditional area of research that addresses the question of how to build, evaluate, and utilize the codes for successful and bandwidth efficient transmission and storage of data, this involves the construction of error-correcting codes, coding and decoding algorithms design, and performance study. In [1], coding theory began by the mathematician Claude Shannon in 1948. Error correcting codes are remarkably indispensable in guaranteeing trustworthy in numerous communication systems. This last one is used in every digital system : Computer memory, satellites, Deep Space and Satellite Communications, Bar code, QR code, and so forth. The most studied type of codes are the linear codes, whose algebraic properties make their description, construction, encoding and decoding particularly simple.

Finite fields $\mathbb{F}_q$, also know as Galois fields $GF(q)$, provide a finite set of elements on which arthmetic operations (addition, multiplication) are defined. This finite nature makes them particulary suitable for digital applications where data is represented in descret form, a linear code $\mathbf{C}$ of length n, dimension k and minimum distance $d = d_{min}$ is called an $[n, k, d]$ linear code (or precisely $[n, k, d]_q$ code), and it is a subspace of $\mathbb{F}_q^n$, with q is a prime power. As the first class of linear codes devloped for error correction purpose, Hamming codes. They were introduced by Richard Hamming in 1947. Another class of linear codes is Reed-Solomon codes, Reed-Solomon codes were introduced by Irving S. Reed and Gustave Solomon in 1960 [2]. Both play an important role to guarantee the correctness of data and the security while it transmitted and stored in the contemporary communication and storage system.

In linear codes, weights play a crucial role in determing the error-correcting capability of the code. The weight of a codewords refers to the number of non-zero elements it contains differnt weights, like Hamming weight, Lee weight, Disrtribution weights.

This memory is organized as follows :

Chapter 1 : we give the necessary difinitions and notations are introduced in chapter 2 and chapter 3 .

Chapter 2 : we provide some linear codes. Precisely, we introduce Hamming codes, and detect and correct the message with Hamming codes. Then, we give some basis knowlege and results on $\mathbb{RS}$ codes.

Chapter 3: we study some weights, and their results (Hamming, Lee and Distribution weights) .

Chapter 1

Preliminaries

This chapter contains the basic concepts from coding theory and algebraic structures. We recall some definitions, propositions, theorems and corollary, they can be found in [2], [5], [6], [7], [8].

1.1 Background

Definition 1.1 (Groups)**.**
A group is a non-empty set together with a binary operation

$$\mathbf{G} \times \mathbf{G} \to \mathbf{G}$$
$$(a, b) \longmapsto a \cdot b$$

Satisfying the following condtions:

(i) Associativity : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, $c \in \mathbf{G}$;

(ii) Identity element : there exists $e \in \mathbf{G}$ such that $a \cdot e = e \cdot a = a$ for all $a \in \mathbf{G}$;

(iii) Inverses : for any $a \in \mathbf{G}$ there exists $a^{-1} \in \mathbf{G}$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.
We usually abbreviate $(\mathbf{G}, \cdot)$ to $\mathbf{G}$. Also, we usually write ab for $a \cdot b$ and 1 for e. The group $\mathbf{G}$ is said to be abelian (or commutative) if $a \cdot b = b \cdot a$ for all elements a and $b \in \mathbf{G}$.

Remark 1.1.
If the set $\mathbf{G}$ is finite, we define the order of G to be the number of elements in $\mathbf{G}$, and denote it $\mid \mathbf{G} \mid$.

Example 1.1.

1. Let $\mathbf{G}_1 = \{e\}$ be a one element set, and let $\cdot$ be the binary operation on $\mathbf{G}_1$ defined by $e \cdot e = e$. Then $(\mathbf{G}_1, \cdot)$ is a group called the trivial group.

2. Let $\mathbf{G}_2 = \{1, -1, i, -i\} \subset \mathbb{C}$ and let $\cdot$ be the multiplication of complex numbers on $\mathbf{G}_2$. Then $(\mathbf{G}_2, \cdot)$ is a group.

Example 1.2.
The following are examples of abelian groups :

1. $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are abelian groups.

2. $(\mathbb{R}, \times)$ *is an abelian group under multiplication.*

3. $M_2(\mathbb{R})$ *is an abelian group under the addition of matrices.*

Corollary 1.1.
Let $\mathbf{G}$ *and* H *be groups. Define an operation* $(\cdot)$ *on the Cartesian product* $\mathbf{G} \times H$ *by*

$$(g, h) \cdot (g', h') = (g \cdot g', h \cdot h'),$$

where $g, g' \in \mathbf{G}$*, and* $h, h' \in H$*. Then* $\mathbf{G} \times H$ *is a group.*

Definition 1.2 (Cyclic groups)**.**
Let $(\mathbf{G}, \cdot)$ *be a group and let* g *be an element of the group* $\mathbf{G}$ *such that* $\mathbf{G} =< g >= \{g^n : n \in \mathbb{Z}\}$*, then* $\mathbf{G}$ *is called a cyclic group, and* g *is called a generator of the groupe* $\mathbf{G}$*.*

Example 1.3.

1. *The group* $(\mathbb{Z}, +)$ *is a cyclic group,* $\mathbb{Z} =< 1 >=< -1 >$.

2. *The group* $(\mathbb{Q}, +)$ *is not a cyclic group.*

Definition 1.3 (Rings)**.**
A structure $(\mathbf{R}, +, \cdot)$ *is a ring, if* $\mathbf{R}$ *is a non-empty set and* $(+)$ *and* $(\cdot)$ *are binary operations:*

$$+ : \mathbf{R} \times \mathbf{R} \to \mathbf{R}, (a, b) \hookrightarrow a + b = b + a$$

$$\cdot : \mathbf{R} \times \mathbf{R} \to \mathbf{R}, (a, b) \hookrightarrow a \cdot b = ab$$

such that

(i) $(\mathbf{R}, +)$ *is an abelian group;*

(ii) The multiplication $(\cdot)$ *is associative on* $\mathbf{R}$*;*

(iii) The multiplication $(\cdot)$ *is distributive over addition that is for all* $a, b, c \in \mathbf{R}$*, the left distributive law is* $a \cdot (b + c) = a \cdot b + a \cdot c$*, and the right distributive law is* $(b + c) \cdot a = b \cdot a + c \cdot a$*.*

A commutative ring is also known as an abelian ring is characterized by the property that the multiplication of any two elements is commutative i.e., $a \cdot b = b \cdot a$ *for all* $a, b \in \mathbf{R}$*. In such a ring denoted as* $(\mathbf{R}, +, \cdot)$*, the order of multiplication does not affect the result.*

Example 1.4.
Consider the set of all even integers $2\mathbb{Z}$ *is a commutative ring without an identity.*

Example 1.5.
$(\mathbb{Z}, +, \times)$ *,*$(\mathbb{R}, +, \times)$ *and* $(\mathbb{C}, +, \times)$ *are commutative rings.*

Definition 1.4 (Subring)**.**
Let $\mathbf{R}$ *be a ring. A subset* $\mathbf{R}_1 \subseteq \mathbf{R}$ *is called a subring, if* $(\mathbf{R}_1, +)$ *is a subgroup of* $\mathbf{R}$*, closed under the multiplication and the additon. It follows immediately that a subring is a ring.*

Example 1.6.

i. Let $(\mathbb{Z}, +, \cdot)$ *be a subring of* $(\mathbb{Q}, +, \cdot)$.

ii. Let $(2\mathbb{Z}, +, \cdot)$ *be a subring of* $(\mathbb{Z}, +, \cdot)$.

Definition 1.5 (Ideals)**.**
Let $\mathbf{I}$ *be a nonempty subset of a ring* $\mathbf{R}$. *Then* $\mathbf{I}$ *is a two-sided ideal of* $\mathbf{R}$ *if*

(i) $a, b \in \mathbf{I}$ *imply* $a - b \in \mathbf{I}$;

(ii) $r \in \mathbf{R}$ *and* $a \in \mathbf{I} \Rightarrow r \cdot a \in \mathbf{I}, a \cdot r \in \mathbf{I}$.

Example 1.7.
For any $n \in \mathbb{Z}$, $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$ *is an ideal of* $\mathbb{Z}$.

Definition 1.6 (Principle ideal)**.**
An ideal $\mathbf{I}$ *of a ring* $\mathbf{R}$ *is called principal if there is an element* a *of* $\mathbf{R}$ *such that*

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

Example 1.8.
All ideals in the ring $(\mathbb{Z}, +, \cdot)$ *are principal.*

Definition 1.7 (Quotient ring)**.**
Let $(\mathbf{R}, +, \cdot)$ *be a ring and* $\mathbf{I}$ *be an ideal of* $\mathbf{R}$. *The quotient ring* $\mathbf{R}/\mathbf{I}$ *is the set of distinct additive cosets* $a + \mathbf{I}$, *with the addition and the multiplication defined by*

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

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

Example 1.9.
Let $\mathbb{R} = \mathbb{Z}$ *and* $\mathbf{I} = n\mathbb{Z}$. *The quotient ring* $\mathbb{Z}/n\mathbb{Z} = \{k + n\mathbb{Z} \mid k \in \mathbb{Z}\}$.

Proposition 1.1.
Let $\mathbf{R}$ *be a ring, and let* $\mathbf{I}$ *be an ideal*

(i) If $\mathbf{R}$ *is a commutative ring, so is* $(\mathbf{R}/\mathbf{I})$;

(ii) If $\mathbf{R}$ *has a multiplicative identity 1, then* $1 + \mathbf{I}$ *is a multiplicative identity for* $\mathbf{R}/\mathbf{I}$. *In this case, if* $r \in \mathbf{R}$ *is a unit, then so is* $r + \mathbf{I}$, *and* $(r + \mathbf{I})^{-1} = r^{-1} + \mathbf{I}$.

Definition 1.8 (Fields)**.**
A nonempty set $\mathbf{F}$ *of elements having two operations is called a field, the terms* $(+)$ *(for addition) and* $(\cdot)$ *(for multiplication) meet the following requirements precepts. Given every* a, b *and* $c \in \mathbf{F}$*:*
(i) The group $(\mathbf{F}, +)$ *is an abelian group with identity element* 0 *with respect to the operation* $(+)$;
(ii) The set $\mathbf{F}^* = \mathbf{F} - \{0\} = \{a \in \mathbf{F}, a \neq 0\}$ *forms an abelian group with identity element* 1 *under the operation* $(\cdot)$;
(iii) The distributive law is satisfied : $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Example 1.10.

1. *$\mathbb{Z}_2 = \{0, 1\}$ are a field. The addition and multiplication tables are given by*

$+$	0	1
0	0	1
1	1	0

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

2. *Let $\mathbb{Z}_3 = \{0, 1, 2\}$ be a field. The addition and multiplication tables are given by*

$+$	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 1.9 (Characteristic)**.**
Let $\mathbf{F}$ be a field. The characteristic of $\mathbf{F}$ is the least positive integer p such that $p \cdot 1 = 0$, where 1 is the multiplicative identity of $\mathbf{F}$. If no such p exists, we define the characteristic to be 0.

Example 1.11.

1. *The characteristics of $\mathbb{R}, \mathbb{C}$ are 0.*
2. *The characteristic of the field $\mathbb{Z}_5$ is 5 .*

Definition 1.10 (Subfield)**.**
A subfield $\mathbf{E}$ of a field $\mathbf{F}$ is a subset of $\mathbf{F}$ that behaves as a field under $\mathbf{F}$ field operations.

Example 1.12.

1. *Let $\mathbb{Q}$ be a subfield of $\mathbb{R}$.*
2. *Let $\{0, 1\}$ be a subfield of $\mathbb{R}$.*
3. *The set of integers $\mathbb{Z}$ is not a subfield of $\mathbb{R}$, since it is not closed under taking inverses ($2^{-1} \notin \mathbb{Z}$).*

Definition 1.11 (Vector spaces)**.**
A nonempty set $\mathbf{V}$, along with a certain operation of vector addition $(+)$ and scalar multiplication by elements from $\mathbf{V} \to \mathbf{V}$. The vector space (or linear space) over $\mathbf{F}$ if it satisfies all of the following conditions. For all $x, y, z \in \mathbf{V}$ and for all $\lambda, \mu \in \mathbf{F}$:

(i) $x + y \in \mathbf{V}$;

(ii) $(x + y) + z = x + (y + z)$;

(iii) There is an element $0 \in \mathbf{V}$ *with the property* $0 + y = y = y + 0$ *for all* $y \in \mathbf{V}$;

(iv) For each $x \in \mathbf{V}$ *there is an element of* $\mathbf{V}$*, called* $-x$*, such that* $x + (-x) = 0 = (-x) + x$;

(v) $x + y = y + x$;

(vi) $\lambda y \in \mathbf{V}$;

(vii) $\lambda(x + y) = \lambda x + \lambda y$, $(\lambda + \mu)x = \lambda x + \mu x$;

(viii) $(\lambda\mu)x = \lambda(\mu x)$;

(ix) If 1 is the multiplicative identity of $\mathbf{F}$*, then* $1.x = x$.

Example 1.13.

1. *Let $\mathbb{R}^n$ be a real vector space.*
2. *Let $\mathbb{C}^n$ be a complex vector space.*

Definition 1.12.
If K is a field containing the subfield $\mathbf{F}$, then $\mathbf{K}$ is said to be an extension field of $\mathbf{F}$, denoted $\mathbf{K}/\mathbf{F}$. The degree of a field extension $\mathbf{K}/\mathbf{F}$, denoted $[\mathbf{K} : \mathbf{F}]$, is the dimension of $\mathbf{K}$ as a vector space over $\mathbf{F}$. The extension is said to be finite if $[\mathbf{K} : \mathbf{F}]$ is finite and is said to be infinite otherwise.

Example 1.14.

(i) Let $\mathbf{F} = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, and let $\mathbf{E} = \{\mathbb{Q}(\sqrt{2} + \sqrt{3})\}$ be the smallest fields containing both $\mathbb{Q}$ and $\sqrt{2} + \sqrt{3}$. Both $\mathbf{E}$ and $\mathbf{F}$ are extension fields of the rational numbers.

(ii) 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 1.13 (Polynomials)**.**
Let $(\mathbf{R}, +, \cdot)$ be a ring. A polynomial $f(X)$ over $\mathbf{R}$ is an expression of the form

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

Example 1.15.
Consider the field $(\mathbf{C}, +, \cdot)$. Let $f(X)$ be a polynomial over $\mathbf{C}$, with $i^2 = -1$,

$$f(X) = (2 + i) + (3 + i)X + 4X^2 + 2iX^3.$$

Definition 1.14 (Degree of polynomials)**.**
The degree of a polynomial is the highest power of the variable in a polynomial expression. To recall, a polynomial is defined as an expression of more than two algebraic terms, especially the sum (or difference) of several terms that contain different powers of the same or different variables.

Example 1.16.
Let $f(X) = X^2 + 1$ and $g(X) = 2X^4 + X$ be polynomials of $\mathbb{Z}_5[X]$, where $\deg(f(X)) = 2$ and $\deg(g(X)) = 4$.

Proposition 1.2.
Let $f(X)$ and $g(X)$ be polynomials of $\mathbf{F}[X]$,

1. *$deg(f(X)) + deg(g(X)) = deg(f(X)g(X))$;*
2. *$deg(f(X) + g(X)) \preceq Max\ \{deg(f(X)), deg(g(X))\}$.*

Remark 1.2.
Let k be a non-negative integer and $\mathbf{F}$ be a field. Then $\mathbf{F}[X]_k$ denotes all polynomials of $\mathbf{F}[X]$ of degree less than k with the convention that the zero polynomial has degree -1.

Corollary 1.2.
Let $\mathbf{F}$ *be a field*

1. *An element of* $\mathbf{F}[X]$ *has a multiplicative inverse if and only if it has degree 0;*
2. *If* $f(X) \cdot g(X) = 0$, *then* $f(X) = 0$ *or* $g(X) = 0$;
3. *If* $f(X)$ *is nonzero and* $f(X)g(X) = f(X)h(X)$ *in* $\mathbf{F}[X]$, *then* $g(X) = h(X)$.

Definition 1.15 (Irreducible polynomial)**.**
Let $\mathbf{F}$ *be a field. We say that a non-constant polynomial* $f(X)$ *is reducible over* $\mathbf{F}$ *or a reducible element of* $\mathbf{F}[X]$, *if we can factor* $f(X)$ *as the product of* $g(X)$ *and* $h(X) \in \mathbf{F}[X]$, *where the degree of* $g(X)$ *and the degree of* $h(X)$ *are both less than the degree of* $f(X)$, *we say that a non-constant polynomial* $f(X)$ *is irreducible if it is not reducible.*

Example 1.17.

1. *The polynomial* $f(X) = 1 + X + X^2$ *is irreducible of* $\mathbb{Z}_2[X]$.
2. *The polynomial* $g(X) = X^4 + 3X^2 - 7X + 1i$ *is irreducible over* $\mathbb{Q}$.
3. *The polynomial* $h(X) = X^2 - 2$ *is irreducible over* $\mathbb{Q}$.
4. *The polynomial* $L(X) = X^3 + 3X + 2$ *is irreducible of* $\mathbb{Z}_5[X]$.

Theorem 1.1.
Let $f(X)$ *be a polynomial over a field* $\mathbf{F}$ *of degree* $\succeq 1$. $\mathbf{F}[X]/\langle f(X)\rangle$ *is a field if and only if* $f(X)$ *is irreducible.*

Remark 1.3.
If $f(X)$ *is a linear polynomial, then the field* $\mathbf{F}[X]/\langle f(X)\rangle$ *is the field* $\mathbf{F}$ *itself.*

Example 1.18.
Let $\mathbf{F}$ *be the field* $\mathbb{Z}_2$ *then* $p(X) = 1 + X + X^3$ *is an irreducible polynomial of degree* 3 *over* $\mathbb{Z}_2$. *Hence* $\mathbb{Z}_2[X]/\langle 1 + X + X^3\rangle$ *is a field with 8 elements:*

$$\mathbb{Z}_2[X]/\langle X^3 + X + 1\rangle = \{0, 1, X, X^2, 1 + X, 1 + X^2, X + X^2, 1 + X + X^2\}.$$

The addition and multiplication tables as follows

$+$	0	1	X	$X+1$	X^2	X^2+1	X^2+X	X^2+X+1
0	0	1	X	$X+1$	X^2	X^2+1	X^2+X	X^2+X+1
1	1	0	$X+1$	X	X^2+1	X^2	X^2+X+1	X^2+X
X	X	$X+1$	0	1	X^2+X	X^2+X+1	X^2	X^2+1
$X+1$	$X+1$	X	1	0	X^2+X+1	X^2+X	X^2+1	X^2
X^2	X^2	X^2+1	X^2+X	X^2+X+1	0	1	X	$X+1$
X^2+1	X^2+1	X^2	X^2+X+1	X^2+X	1	0	$X+1$	X
X^2+X	X^2+X	X^2+X+1	X^2	X^2+1	X	$X+1$	0	1
X^2+X+1	X^2+X+1	X^2+X	X^2+1	X^2	$X+1$	X	1	0

$\times$	0	1	X	$X+1$	X^2	X^2+1	X^2+X	X^2+X+1
0	0	0	0	0	0	0	0	0
1	0	1	X	$X+1$	X^2	X^2+1	X^2+X	X^2+X+1
X	0	X	X^2	X^2+X	X^2+1	1	X^2+X+1	X^2+1
$X+1$	0	$X+1$	X^2+X	X^2+1	X^2+X+1	X^2	1	X
X^2	0	X^2	$X+1$	X^2+X+1	X^2+X	X	X^2+1	1
X^2+1	0	X^2+1	1	X^2	X	X^2+X+1	$X+1$	X^2+X
X^2+X	0	X^2+X	X^2+X+1	1	X^2+1	$X+1$	X	X^2
X^2+X+1	0	X^2+X+1	X^2+1	X	1	X^2+X	X^2	X^2+1

1.2 Finite fields

Definition 1.16 (Finite fields)**.**
A field with finite elements is called a finite field. $\mathbb{F}_q$ *or* $\mathbf{GF}(q)$ *denotes a finite field with* q *elements.*

Theorem 1.2.
For any prime number p, $\mathbb{Z}_p \simeq \mathbb{F}_p$ *is a finite field of order* p.

Example 1.19.
$\mathbb{Z}_2 \simeq \mathbb{F}_2$ *and* $\mathbb{Z}_3 \simeq \mathbb{F}_3$ *are two finite fields.*

Corollary 1.3.
The characteristic of a finite field $\mathbb{F}_q$ *is always a prime number.*

Theorem 1.3.
Let $\mathbb{F}_q$ *be a finite field with characteristic* p. *In this case, the field* $\mathbb{F}_q$ *consists of* p^n *elements, where* n *represents the degree of the extension field* $[\mathbb{F}_q : \mathbb{Z}_p]$.

Theorem 1.4.
For any prime p *and any positive integer* n, *there exists a finite field, unique up to isomorphism, with* $q = p^n$ *elements. Since constructing finite fields requires irreducible polynomials.*

Proposition 1.3.
Suppose that $h(X)$ *is an irreducible polynomial over* $\mathbb{F}_p$ *of degree* n. *Then* $\mathbb{F}_p[X]/\langle h(X)\rangle$ *is a field of order* p^n.

Example 1.20.

1. *The polynomial* $3X^2 + 2 \in \mathbb{F}_3[X]$ *is irreducible over* $\mathbb{F}_3$, *so* $\mathbb{F}_3[X]/\langle 3X^2 + 2\rangle$ *is the finite field of order 9.*
2. *The polynomial* $X^2 + X + 1 \in \mathbb{F}_5[X]$ *is irreducible over* $\mathbb{F}_5$, *so* $\mathbb{F}_5[X]/\langle X^2 + X + 1\rangle$ *is the finite field of order 25.*
3. *The polynomial* $X^4 + X + 1 \in \mathbb{F}_2[X]$ *is irreducible over* $\mathbb{F}_2$, *so* $\mathbb{F}_2[X]/\langle X^4 + X + 1\rangle$ *is the finite field of order 16.*

1.2.1 Some features of finite fields

Definition 1.17 (Order)**.**
The smallest positive integer k, *denoted as* $ord(\alpha)$, *represents the order of a nonzero element* $\alpha \in \mathbb{F}_q$. *It signifies the number of times* α *needs to be multiplied by itself to yield the result of 1.*

Example 1.21.
In order to create the field $\mathbb{F}_4$, *it is necessary to take into account the irreducible polynomial* $X^2 + X + 1$ *over* $\mathbb{F}_2$. *By setting* $\omega^2 + \omega + 1 = 0$, *the field* $\mathbb{F}_4$ *can be defined as the collection of elements* $\{a + b\omega \mid a, b \in \mathbb{F}_2\} = \{0, 1, \omega, 1 + \omega = \omega^2\}$, *this means that* $ord(\omega) = 4$.

Theorem 1.5.

(i) Any finite field of order p^n *is the splitting field of* $X^{p^n} - X$ *and also of* $X^{p^n-1} - X \in \mathbb{F}_p$;

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

Lemma 1.1.
Assume that $\mathbf{F}$ *is a field and* p *is a prime number. The statements below are all equal*

(i) $m \mid n$;

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

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

Proposition 1.4.
For p *a prime number and* $n, m \succ 0$, *we have* $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ *if and only if* $m \mid n$.

Example 1.22.

(i) Let $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha+1\}$, *where* α *is a root of the irreducible polynomial* $X^2 + X + 1 \in \mathbb{F}_2$.

(ii) Let $\mathbb{F}_{2^4} = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^3, \alpha^3+1, \alpha^3+\alpha, \alpha^3+\alpha+1\}$, *where* α *is a root of the irreducible polynomial* $X^4 + X + 1 \in \mathbb{F}_2$. *Hence, we have* $\mathbb{F}_{2^2} \subset \mathbb{F}_{2^4}$ *since the elements of* $\mathbb{F}_{2^2}$ *are a subset of the elements of* $\mathbb{F}_{2^4}$. *This inclusion holds because* $2 \mid 4$.

Lemma 1.2.
Let $\mathbf{F}$ *be a field of characteristic* $p \succ 0$, *then for all* a, $b \in \mathbb{F}_q$, *we have*

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

Example 1.23.
In a finite field of characteristic 2, *we have*

1. $(a+b)^2 = a^2 + b^2$.
2. $(a+b)^{2^4} = a^{2^4} + b^{2^4}$.
3. $(a+b)^{2^5} = a^{2^5} + b^{2^5}$.

1.3 Linear codes

Definition 1.18 (Linear codes)**.**
An $[n, k, d]$ *linear code* $\mathbf{C}$ *over* $\mathbb{F}_q$ *is a subspace of* $\mathbb{F}_q^n$, *with length* n, *dimension* k *and minimum distance* $d = d_{min}$.

Example 1.24.

1. *Let* $\mathbf{C} = \{0000, 1100, 2200, 0001, 0002, 1101, 1102, 2201, 2202\}$ *be a linear code of length 4 over* $\mathbb{F}_3$.

2. *Let* $\mathbf{C} = \{000, 001, 010, 011\}$ *be a linear code of length 3 over* $\mathbb{F}_2$.

Definition 1.19 (Hamming distance)**.**
Let $\boldsymbol{c} = (c_1, c_2, \cdots, c_n)$ *and* $\tilde{\boldsymbol{c}} = (\tilde{c}_1, \tilde{c}_2, \cdots, \tilde{c}_n)$, *where* $\boldsymbol{c}$ *and* $\tilde{\boldsymbol{c}} \in \mathbb{F}_q^n$. *The Hamming distance between* $\boldsymbol{c}$ *and* $\tilde{\boldsymbol{c}}$ *is the number of position, where* $\boldsymbol{c}$ *and* $\tilde{\boldsymbol{c}}$ *are different, and defined by* $d_H(\boldsymbol{c}, \tilde{\boldsymbol{c}})$.

$$d_H(\boldsymbol{c}, \tilde{\boldsymbol{c}}) = \mid \{i : 1 \leq i \leq n, \boldsymbol{c}_i \neq \tilde{\boldsymbol{c}}_i\} \mid .$$

Example 1.25.
Let $\mathbf{C}_H = \{000, 001, 002, 010, 020, 011, 012, 021, 022\}$ *be a linear code of lenght* 3 *over* $\mathbb{F}_3$. *Take* $\boldsymbol{c} = (002)$ *and* $\tilde{\boldsymbol{c}} = (012)$. *Then* $d_H(\boldsymbol{c}, \tilde{\boldsymbol{c}}) = 2$.

Example 1.26.
Let $\mathbf{C} = \{0000, 0010, 1101, 0111, 1000, 1010, 0101, 1111\}$ *be a linear code of length* 4 *over* $\mathbb{F}_2$. *Take* $\boldsymbol{c} = (1000)$, *and* $\tilde{\boldsymbol{c}} = (1010)$. *Then* $d_H(\boldsymbol{c}, \tilde{\boldsymbol{c}}) = 1$.

Definition 1.20 (Minimum distance)**.**
The minimum distance d_{min} *or* d, *of a linear code* $\mathbf{C}$ *is given as*

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

Example 1.27.

1. *Let* $\mathbf{C}_1 = \{0000, 0111, 0001, 0110, 1100, 1011, 1101\}$ *be a linear code of length* 4 *over* $\mathbb{F}_2$. *Hence,* $d_{min} = 1$.

2. *Let* $\mathbf{C}_2 = \{100, 121, 101, 120, 020, 001, 021\}$ *be a linear code of length* 3 *over* $\mathbb{F}_3$. *Hence,* $d_{min} = 1$.

Definition 1.21 (Sphere and Ball)**.**

1. *Let* $\mathbf{r} \in \mathbb{N}, \mathbf{a} \in \mathbb{F}_q^n$. *The ball of center* $\mathbf{a}$ *and radius* $\mathbf{r}$ *as the set*

$$B(\mathbf{a}, \mathbf{r}) = B_{\mathbf{r}}(\mathbf{a}) = \{x \in \mathbb{F}_q^n : d_H(x, \mathbf{a}) \preceq \mathbf{r}\}.$$

2. *Let* $\mathbf{r} \in \mathbb{N}, \mathbf{a} \in \mathbb{F}_q^n$. *The spher of center* $\mathbf{a}$ *and radius* $\mathbf{r}$ *as the set*

$$S(\mathbf{a}, \mathbf{r}) = S_{\mathbf{r}}(\mathbf{a}) = \{x \in \mathbb{F}_q^n : d_H(x, \mathbf{a}) = \mathbf{r}\}.$$

Example 1.28.
Let $\mathbb{F}_q = \mathbb{F}_2$, $\mathbf{r} = 1, \mathbf{a} = 00000$ *and* $n = 5$,

$$S(00000, 1) = \{10000, 01000, 00100, 00010, 00001\}.$$

$$B(00000, 1) = \{00000, 10000, 01000, 00010, 00001, 00100\}.$$

Example 1.29.
Let $\mathbb{F}_q = \mathbb{F}_2$, $\mathbf{r} = 1, \mathbf{a} = 00000$ *and* $n = 3$,

$$S(00000, 1) = \{100, 010, 001\}.$$

$$B(00000, 1) = \{000, 100, 010, 001\}.$$

Proposition 1.5.
Let $\mathbb{F}_q$ *be the finite field of order* q. *Then*

(i) $\mid S(\mathbf{a}, \mathbf{r}) \mid = \sum_{i=0}^{\mathbf{r}} \mathbf{C}_n^i (q-1)^i$ *and* $\mathbf{C}_n^i = \frac{n!}{i!(n-i)!}$;

(ii) $\mid B(\mathbf{a},\mathbf{r}) \mid = \begin{pmatrix} n \\ \mathbf{r} \end{pmatrix} (q-1)^{\mathbf{r}}$.

Theorem 1.6 (Spher packing Bound)**.**
If $\mathbf{C}$ *is an* $[n,k,d]$ *linear code of* $\mathbb{F}_q^n$*, then*

$$M \cdot \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \mathbf{C}_n^i (q-1)^i \leqslant q^n,$$

where $M = q^k$.

Remark 1.4.
If the equality $M \cdot \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \mathbf{C}_n^i (q-1)^i = q^n$*, then the* $[n,k,d]$ *linear code* $\mathbf{C}$ *is called a perfect code.*

Proposition 1.6.
Let $\mathbf{C}$ *be an* $[n,k,d]$ *linear code over* $\mathbb{F}_q$*. Then*

1. *The code* $\mathbf{C}$ *can detect up to* $d-1$ *errors.*

2. *The code* $\mathbf{C}$ *can correct up to* $\lfloor \frac{d-1}{2} \rfloor$ *errors.*

Example 1.30.
Let $\mathbf{C} = \{00000, 00101, 01011, 10011, 10110, 11000, 11101\}$ *be a linear code of length 5 over* $\mathbb{F}_2$*. Then* $\mathbf{C}$ *can detect* $d-1 = 2-1 = 1$ *error, and it can not correct any error.*

Definition 1.22 (Generator Matrix)**.**
A matrix G *is called a generator matrix for a linear code* $\mathbf{C}$ *if its rows constitute a basis for* $\mathbf{C}$*. Numerous generator matrices can be found for linear codes in general.*

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

Example 1.31.

1. *Let* $\mathbf{C}_1 = \{0000, 1110, 0111, 1001\}$ *be a linear* $[4,2]$ *code with generator matrix*

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

2. *Let* $\mathbf{C}_2 = \{00000, 11100, 22200, 22111, 00211, 11011, 11222, 22022\}$ *be a linear* $[5,3]$ *code with generator matrix*

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 2 & 2 & 1 & 1 & 1 \end{pmatrix}.$$

Example 1.32.
Let G *be a generator matrix of a linear code* $\mathbf{C}$ *over* $\mathbb{F}_2$ *with parameters* $[6,3]$*, giving*

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

Then, we have

$$\begin{aligned}\mathbf{C} &= \{x_1(100110), x_2(010011), x_3(001101) : x_1, x_2, x_3 \in \mathbb{F}_2\} \\ &= \{000000, 001101, 010011, 011110, 100110, 101011, 110101, 111000\}.\end{aligned}$$

So, $\mathbf{C}$ is a $[6, 3, 3]$ linear code over $\mathbb{F}_2$.

Definition 1.23 (Vandermonde matrix)**.**
A Vandermonde matrix is an $n \times m$ matrix of the form

$$V_{mn}(a_n) = [a_i^{j-1}]_{ij}^{m,n} = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{k-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}.$$

Definition 1.24.
A non-singular matrix is a square matrix with a non-zero determinant. Because it has a determinant value, the non-singular matrix is invertible, and its inverse may be obtained.

Example 1.33.
Consider the matrix A over $\mathbb{F}_{11}$

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix},$$

we calculate the determinate parameters of A, $detA = (3 \times 2 - 1 \times 4) = 4 \neq 0$.

Definition 1.25 (Inner product)**.**
The inner product of two vectors $\mathbf{c} = (\mathbf{c_1}, ..., \mathbf{c_n})$ and $\tilde{\mathbf{c}} = (\tilde{\mathbf{c}}_1, ..., \tilde{\mathbf{c}}_n)$ over $\mathbb{F}_q$ is

$$\langle \mathbf{c}, \tilde{\mathbf{c}} \rangle = \sum_{i=1}^{n} \mathbf{c}_i \tilde{\mathbf{c}}_i.$$

If $\langle \tilde{\mathbf{c}}, \mathbf{c} \rangle = 0$, then the vectors are said to be orthogonal.

Example 1.34.

1. *Let $\mathbf{c} = (111110), \tilde{\mathbf{c}} = (011121) \in \mathbb{F}_3^6$. Then $\langle (111110), (011121) \rangle = 2$.*
2. *Let $\mathbf{c} = (1011), \tilde{\mathbf{c}} = (0111) \in \mathbb{F}_2^4$. Then $\langle (1011), (0111) \rangle = 0$.*

Definition 1.26 (The dual code)**.**
Let $\mathbf{C}$ be a linear code of $\mathbb{F}_q^n$. The dual (or orthogonal) code $\mathbf{C}^\perp$ of $\mathbf{C}$ is defined by

$$\mathbf{C}^\perp = \{\tilde{\mathbf{c}} \in \mathbb{F}_q^n :< \mathbf{c}, \tilde{\mathbf{c}} >= 0 : \forall \mathbf{c} \in \mathbf{C}\}.$$

Example 1.35.
Consider the linear code $\mathbf{C} = \{000, 011, 110, 101\}$. Then the dual code of $\mathbf{C}$ is

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

Remark 1.5.
Let $\mathbf{C}$ *be an* $[n, k, d]$ *linear code, then the dual* $\mathbf{C}^{\perp}$ *is a linear code of length* n *and dimension* $n - k$*, and* $(\mathbf{C}^{\perp})^{\perp} = \mathbf{C}$ *.*

Remark 1.6.
A code $\mathbf{C}$ *is self-orthogonal provided* $\mathbf{C} \subseteq \mathbf{C}^{\perp}$ *and self-dual provided* $\mathbf{C} = \mathbf{C}^{\perp}$*.*

Definition 1.27 (parity-cheek matrix)**.**
A parity-check matrix H *for a linear code* $\mathbf{C}$ *is a generator matrix for the dual code* $\mathbf{C}^{\perp}$*.*

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

Theorem 1.7.
If $G = [I_k \mid A]$*, then a generator matrix for* $\mathbf{C}^{\perp}$ *is* $H = [-A^T \mid I_{n-k}]$*, where* I *is the identity matrix.*

Example 1.36.
Let H *be a parity-cheek matrix of a linear code* $\mathbf{C}$ *over* $\mathbb{F}_2$ *with parameter* $[5, 2]$

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

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

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

Then $\mathbf{c} = (c_1, c_2, c_1 + c_2, c_1, c_2)$*. The code* $\mathbf{C}$ *have* $q^k = 2^2$ *codewords , then*

$$\mathbf{C} = \{00000, 01101, 10110, 11011\}.$$

Example 1.37.
Let $\mathbf{C} = \{000000, 100110, 010011, 110101\}$ *be the* $[6, 2]$ *linear code given by the generator matrix* $G = [I_k|A]$ *with corresponding parity cheek matrix* $H = \left[-A^T|I_{n-k}\right]$

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

Theorem 1.8 (Singleton Bound)**.**
The minimum distance of an $[n, k, d]_q$ *linear code satisfies*

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

Definition 1.28 (Maximum Distance Separable)**.**
A code $\mathbf{C}$ *that achieves the Singleton bound is referred to as an* MDS *code, which stands for maximum distance separable.*

Theorem 1.9.
The dual of an MDS code is an MDS code.

Example 1.38.
Consider the $[3, 2, 2]$ binary linear code whose generator matrix G is :

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

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

Chapter 2

Some linear codes

The Hamming and Reed-Solomon codes are a family of linear error correction codes. In this chapter, we briey recall some basic notations and results on Reed-Solomon codes and Hamming codes [1], [4],[6], [9], [10], [11].

2.1 Introduction to error correction codes

The first error correcting codes were discovered by Richard Hamming in 1947 at Bell Labs. These codes were designed to detect and correct errors in bit strings, which was a significant problem at the time as machines could take days to perform modest calculations and would halt upon detecting erroneous data. Hamming's contributions to coding theory, including Hamming codes, Hamming matrix, Hamming window, Hamming numbers, Hamming bound, and Hamming distance, had irrevocable implications on the fields of computer science and telecommunications.

In summary, error detection and correction have been developed and refined over time to ensure reliable delivery of digital data in computer science and telecommunication. Modern techniques include parity bits, checksums, and cyclic redundancy checks, as well as error correction codes such as Hamming codes and Reed-Solomon codes, which can detect and correct errors in transmitted data. These techniques are essential for ensuring the accuracy and reliability of digital communication and storage systems.

The benefits of error correction in our lives are profound and essential for personal growth and success, error correction serves as a crucial mechanism for improvement, learning, and progress. By actively engaging in error correction, individuals can experience the following benefits: Continuous Improvement, Problem-Solving Skills,.., Personal Development.

2.1.1 History of Hamming codes

In the late 1940's Richard Hamming recognized that the further evolution of computers required greater reliability, in particular the ability to not only detect errors, but correct them. His search for error-correcting codes led to the Hamming codes, perfect 1-error correcting codes, and the extended Hamming codes, 1-error correcting and 2-error detecting codes. Here are some common applications of using Hamming code:

- Computer Memory.
- Modems.
- Satellites.
- Embedded Processor.
- Open connectors.

2.1.2 Hamming codes

Definition 2.1. *(Binary Hamming codes)*
For any positve integer r, define the matrix $H_r \in \mathbb{F}_2^{r\times(2^r-1)}$ *to be the* $r\times(2^r-1)$ *matrix whose i th column* H_r^i *is the binary representation of i, for* $1 \leqslant i \leqslant 2^r-1$.
The $[2^r-1, 2^r-r-1]_2$ *Hamming code denoted by* $\mathbf{C}_H$ *is the code with parity check matrix* H_r. *In other words, the general* $[2^r-1, 2^r-r-1]_2$ *Hamming code is*

$$\mathbf{C}_H = \left\{\mathbf{c} \in \mathbb{F}_2^{2^r-1} \mid H_r \cdot \mathbf{c}^T = 0\right\}.$$

Example 2.1.
Let r=3, there is a Hamming code of length $n = 2^r-1 = 2^3-1 = 7$, *and* $k = 2^r-1-r = 2^3-1-3 = 4$, *with* $\mathbf{C}_H = \{\boldsymbol{c} \in \mathbb{F}_2^7 : H_r \cdot \mathbf{c}^T = 0\} = \{m \in \mathbb{F}_2^4 : m \cdot G_3\}$. *The check metrix and the generator matrix for the* $[7,4]$ *Hamming code are:*

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \simeq \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\Rightarrow G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

This yields, $\mathbf{C}_H = \{m \in \mathbb{F}_2^4 : mG_3\} = \{0000000, 0001111, 0100101, 1000011, 0010110, 1110000, 1101000, 0111100, 0011001, 0101010, 0110011, 1010101, 1001100, 1100110, 0001111, 1111111\}$.

Example 2.2.
Consider the [15,11] Hamming code with generator matrix G_r, *and check matrix* H_r *as follows:*

$$H_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

$$G_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Remark 2.1.
We also denote the Hamming code by Ham(r,2).

Definition 2.2. *(Hamming minimum distance)*
The minimum distance of a code $\mathbf{C}_H$ denoted by d_{min}, it is the smallest Hamming distance between any two codewords in $\mathbf{C}_H$.

Theorem 2.1.
Hamming codes have a minimum distance 3.

Proof.
This directly follows from the definition of the Hamming code $\mathbf{C}_H$. Since n is the greatest number of columns of its parity check matrices consistent with the condition that no two columns are dependent, the size of the smallest set of dependent columns is 3. Therefore, d_{min} of a linear code $\mathbf{C}_H$ is the size of the smallest linearly dependent set of columns of it's parity check matrix H_r. □

Corollary 2.1.
The Hamming code can correct single-bit error and detect the presence of two-bit errors in data blocks.

Proof.
Since the minimal distance of Hamming code is 3, then the Hamming code can correct $\lfloor \frac{d_{min}-1}{2} \rfloor = \lfloor \frac{3-1}{2} \rfloor = 1$, and can detect $d_{min} - 1 = 3 - 1 = 2$. □

Theorem 2.2.
The Hamming code are perfect single-error correcting codes.

Proof.
Recall that a perfect codes that satisfies the sphere-packing bound, that any Hamming code has d_{min}= 3, and hence is 1-error-correcting. The union of all spheres of radius 1 centered at the codewords contain we note that:

$$\begin{aligned} q^k \left(\begin{pmatrix} n \\ 0 \end{pmatrix} + (q-1) \begin{pmatrix} n1 \end{pmatrix} \right) &= q^k \left(1 + (q-1) \times \frac{q^r - 1}{q-1} \right) \\ &= q^k \times q^r \\ &= q^{k+r} \\ &= q^n. \end{aligned}$$

□

Proposition 2.1.
(i) There is equivalency among all binary Hamming codes of a certain length;
(ii) $k = 2^r - 1 - r$ *is the dimension of Ham(r, 2).*

Proof.

(i) Any parity-check matrix may be derived from another for a given length by permuting the columns. Hence, the binary Hamming codes that correspond to them are comparable.

(ii) The dimension of Ham(r, 2) is $2^r - 1 - r$, since H is a parity-check matrix for Ham(r, 2). □

2.2 How to detect and correct the message with Hamming code

The procedure used to detect and correct the message encompasses the following steps :

(i) Calculate the number of redundant bits using the formula $2^r \geqslant k + r + 1$, where r number of redundant and k is the number of data bits.

(ii) Identify the position of redundant bits by marking the bit position starting from 1, in the form of binary, we define all bit positions that are powers of two as parity bits and the other bit positions as data bits.

(iii) Calculate the values of redundant bits based on the parity of the data bits they cover.

(iv) Transmit the data along with the calculated redundant bits to the receiver.

(v) Check for errors at the receiver and using the parity bits to detect any errors in the data.

(vi) Correct the errors using the parity bit values to correct the error in the received data.

Example 2.3.
Consider the [7,4] Hamming code, where we have 4 data bits (D_1, D_2, D_3, D_4) *and 3 parity bits* (P_1, P_2, P_3)*. Let's say we want to send the 4-bits message 0110. The number of parity bits required is calculated using the formula* $2^r \geqslant k + r + 1$*, this implies that* $2^3 \geqslant 4 + 3 + 1$*, so r=3.*

- *Encode :*
  0110 $\hookrightarrow P_1P_20P_3110$*. Then, we calculate parity bits:*
  $P_1 = D_1 \oplus D_2 \oplus D_4 = 0 \oplus 1 \oplus 0 = 1$;
  $P_2 = D_1 \oplus D_3 \oplus D_4 = 0 \oplus 1 \oplus 0 = 1$;
  $P_3 = D_2 \oplus D_3 \oplus D_4 = 1 \oplus 1 \oplus 0 = 0$.
  So, our codeword is $\mathbf{c} = 1100110$.

- *Transmission with an error:*
  Let's say during transmission, bit 3 gets change.
  So the recieved message becomes: $\mathbf{c}' = 1110110$.

- *Detecting :*
  Say we received $\mathbf{c}'$. *The receiver calculates the parity bits, and get*
  $P'_1 = D'_1 \oplus D'_2 \oplus D'_4 = 0 \oplus 1 \oplus 0 = 0$;
  $P'_2 = D'_1 \oplus D'_3 \oplus D'_4 = 0 \oplus 1 \oplus 0 = 0$;
  $P'_3 = D'_2 \oplus D'_3 \oplus D'_4 = 1 \oplus 1 \oplus 0 = 0$.
  Let's compare the received parity with the calculated parity bit : $P'_1 \neq P_1, P'_2 \neq P_2, P'_3 = P_3$

- *Correcting the errors:*
  The received identifies the error in bit 3 and flips from 1 to 0.
  The corrected message is 1100110.

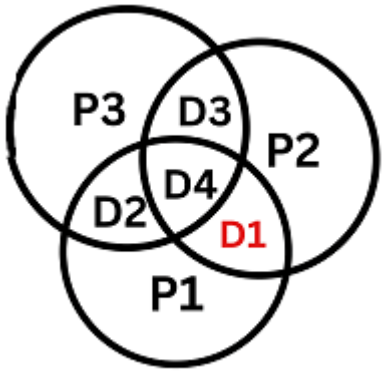

Figure : Summarize Hamming method.

Example 2.4.
Table 1: encoding a 8-bit message and locating error

Encode												
1	2	3	4	5	6	7	8	9	10	11	12	*Position*
P_1	P_2	D_1	P_3	D_2	D_3	D_4	P_4	D_5	D_6	D_7	D_8	*Transmitted bit*
P_1	P_2	0	P_3	0	0	1	P_4	1	1	0	0	*Message*
0	0	0	1	0	0	1	0	1	1	0	0	*Encode*
												Error
0	0	0	1	0	0	1	0	1	1	0	0	*Receive*

Syndrome calculation :
$A = P_1 \oplus D_1 \oplus D_2 \oplus D_4 \oplus D_5 \oplus D_7 = 0$;
$B = P_2 \oplus D_1 \oplus D_3 \oplus D_4 \oplus D_6 \oplus D_7 = 0$;
$C = P_3 \oplus D_2 \oplus D_3 \oplus D_4 \oplus D_8 = 0$;
$E = P_4 \oplus D_5 \oplus D_6 \oplus D_7 \oplus D_8 = 0$.
The above results show to us there is no error detection.

2.3 Reed-Solomon codes

2.3.1 History of Reed-Solomon codes

Reed-Solomon codes were invented in 1960 by Gustave Solomon and Irving Reed. This codes are a new class of error-correcting codes. They are widely used in various technologies like :

- Bar code, QR code.
- High-Speed Modems.
- Storage areas, CD, DVD blu ray.
- Deep Space and Satellite Communications.
- Wireless and Mobile Communication.

Definition 2.3. *(Reed-Solomon codes)*
The Reed-Solomon code is an $[n, k, n-k+1]q$-code. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be any n distinct members of $\mathbb{F}_q$. These are called the evaluation points of the code. For each vector $\mathbf{m} = (m_0, \ldots, m_{k-1}) \in \mathbb{F}_q^k$, define a polynomial

$$f_{\mathbf{m}}(x) = \sum_{i=0}^{k-1} \mathbf{m}_i x^i,$$

which is of degree at most $k-1$. Then, for each $\mathbf{m} \in \mathbb{F}_q^k$ there is a corresponding codeword $\mathbb{RS}$ defined by

$$\mathbb{RS}(\mathbf{m}) = \langle f_{\mathbf{m}}(\alpha_1), f_{\mathbf{m}}(\alpha_2), \ldots, f_{\mathbf{m}}(\alpha_n) \rangle.$$

For any $\mathbf{m}, \mathbf{m}' \in \mathbb{F}_q^k$ and any scalar $\mathbf{a} \in \mathbb{F}_q$

$$\mathbb{RS}(\mathbf{m} + \mathbf{m}') = \mathbb{RS}(\mathbf{m}) + \mathbb{RS}(\mathbf{m}');$$

$$\mathbb{RS}(a\mathbf{m}) = a\mathbb{RS}(\mathbf{m}).$$

Note that, the generator matrix of a $\mathbb{RS}$ code is obtained as follow

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{k-1} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{m}_0 \\ \mathbf{m}_1 \\ \mathbf{m}_2 \\ \cdots \\ \mathbf{m}_{k-1} \end{pmatrix} = \begin{pmatrix} f(\alpha_1) \\ f(\alpha_2) \\ \cdots \\ f(\alpha_n) \end{pmatrix}. \tag{2.1}$$

This system can be shown to have a unique solution for the k information symbols

$$\{\mathbf{m}_0, \mathbf{m}_1, \cdots, \mathbf{m}_{k-2}, \mathbf{m}_{k-1}\},$$

by computing the determinant of the following coefficient matrix.

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{k-1} \end{pmatrix}. \tag{2.2}$$

The determinant of this matrix reduces to that of a Vandermonde matrix, and it can be shown that all Vandermonde matrices are nonsingular.

Corollary 2.2.
$\mathbb{RS}$ *codes exactly meet the singleton bound.*

Example 2.5.
1. Let q=7, and $\alpha = (1, 2, 3, 4, 5, 6)$. *Choose a basis for polynomials in* $\mathbb{F}_7[X]$ *of degree at most 3 :* $1, X, X^2, X^3$. *The* $\mathbb{RS}$ *is the row span of the generator matrix*

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

2. The generator matrix for the extended Reed-Solomon code is the row span of the generator matrix

$$G_\infty = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 4 & 1 & 0 \\ 1 & 3 & 2 & 6 & 0 \\ 1 & 4 & 2 & 1 & 0 \\ 1 & 5 & 4 & 6 & 0 \\ 1 & 6 & 1 & 6 & 1 \end{pmatrix}.$$

Example 2.6.
Let consider the $\mathbb{RS}$ *code over* $\mathbb{F}_{11}$ *with parameters* $[5, 4]$, *and* $\alpha = (5, 8, 10)$. *Then the generator matrix as:*

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

Chapter 3

Some weights and results

The weights of a linear code over finite fields is one of the key contributions to coding theory. In this chapter, we list some weights along with their corresponding results for Lee and Hamming weights, as well as distribution weights.[3], [6], [12],[13], [14], [15].

3.1 Hamming weights

Definition 3.1 (Hamming weights)**.**
Let $\mathbf{c}$ *be a word in* $\mathbb{F}_q^n$*. The weight of* $\mathbf{c}$ *denoted by* $\mathrm{wt}(\mathbf{c})$ *is defined to be the number of nonzero coordinates in* $\mathbf{c}$*, i.e.,*

$$\mathrm{wt}(\mathbf{c}) =\mid \{i : \mathbf{c}_i \neq 0\} \mid = d_H(\mathbf{c}, 0),$$

where $\mathbf{0}$ *is the zero word.*

Example 3.1.

1. *Let* $\mathbf{c_1} = (12002) \in \mathbb{F}_3^5$*. Then* $\mathrm{wt}(\mathbf{c_1}) = 3$*.*
2. *Let* $\mathbf{c_2} = (0001) \in \mathbb{F}_2^4$*, and* $\mathbf{c_3} = (101110) \in \mathbb{F}_2^6$ *. Then* $\mathrm{wt}(\mathbf{c_2}) = 1$*, and* $\mathrm{wt}(\mathbf{c_3}) = 4$*.*

Remark 3.1.
The Hamming weight can be defined for every element $\mathbf{c}$ *of* $\mathbb{F}_q^n$ *in the following manner :*

$$\mathrm{wt}(\mathbf{c}) = d_H(\mathbf{c}, 0) = \begin{cases} 1 & \text{if } \mathbf{c} \neq 0; \\ 0 & \text{if } \mathbf{c} = 0. \end{cases}$$

Lemma 3.1.
If $\mathbf{c}, \tilde{\mathbf{c}} \in \mathbb{F}_q^n$*, then* $d(\mathbf{c}, \tilde{\mathbf{c}}) = \mathrm{wt}(\mathbf{c} - \tilde{\mathbf{c}})$*.*

Proof.
For any elements $\mathbf{c}$ and $\tilde{\mathbf{c}}$ belonging to the finite field $\mathbb{F}_q^n$, the distance between them denoted as $d_H(\mathbf{c}, \tilde{\mathbf{c}})$ will be zero if and only if $\mathbf{c}$ is equal to $\tilde{\mathbf{c}}$. This equivalence holds because $\mathbf{c} - \tilde{\mathbf{c}}$ will be zero if and only if $\mathbf{c}$ is equal to $\tilde{\mathbf{c}}$, or in other words, the weight (number of non-zero elements) of the difference between $\mathbf{c}$ and $\tilde{\mathbf{c}}$, represented as $\mathrm{wt}(\mathbf{c} - \tilde{\mathbf{c}})$ will be zero. □

Example 3.2.

1. *Let* $\mathbf{c} = (121) \in \mathbb{F}_3^3$, *and* $\tilde{\mathbf{c}} = (101) \in \mathbb{F}_3^3$, *then* $d_H(\mathbf{c}, \tilde{\mathbf{c}}) = \mathrm{wt}(\mathbf{c} - \tilde{\mathbf{c}}) = 1$.
2. *Let* $\mathbf{c} = (120) \in \mathbb{F}_3^3$, *and* $\tilde{\mathbf{c}} = (012) \in \mathbb{F}_3^3$, *then* $d_H(\mathbf{c}, \tilde{\mathbf{c}}) = \mathrm{wt}(\mathbf{c} - \tilde{\mathbf{c}}) = 3$.

Definition 3.2.
Let $\mathbf{C}$ *be a linear code over* $\mathbb{F}_q$. *The minimum Hamming weight of* $\mathbf{C}$, *denoted* $\mathrm{wt}_{min}(\mathbf{C})$ *is the smallest of the weights of the nonzero codewords of* $\mathbf{C}$, *i.e.*

$$\mathrm{wt}_{min}(\mathbf{C}) = \min\{\mathrm{wt}(\mathbf{c}) \mid \mathbf{c} \in \mathbf{C}, \mathbf{c} \neq 0\}.$$

Theorem 3.1.
Let $\mathbf{C}$ *be a linear code over* $\mathbb{F}_q$. *Then min* $d_H = \mathrm{wt}_{min}(\mathbf{C})$.

Proof.
By Definition, and Lemma (3.1), we have

$$\begin{aligned} d_{min} &= min\{d_H(\mathbf{c}, \tilde{\mathbf{c}}) \mid \mathbf{c}, \tilde{\mathbf{c}} \in \mathbf{C}, \mathbf{c} \neq \tilde{\mathbf{c}}\} \\ &= min\{\mathrm{wt}(\mathbf{c} - \tilde{\mathbf{c}}) \mid \mathbf{c} \neq \tilde{\mathbf{c}}\}. \end{aligned}$$

Since $\mathbf{C}$ is a linear code. Then

$$\begin{aligned} d_{min} &= min\{\mathrm{wt}(\mathbf{c} - \tilde{\mathbf{c}}) \mid \mathbf{c} \neq \tilde{\mathbf{c}}\} \\ &= min\{\mathrm{wt}(\tilde{\mathbf{c}}) \mid \tilde{\mathbf{c}} \neq 0\} \\ &= \mathrm{wt}_{min}(\mathbf{C}). \end{aligned}$$

□

Example 3.3.
Consider the linear code $\mathbf{C} = \{0000, 1000, 1001, 0001\}$. *We compute* $\mathrm{wt}_{min}(\mathbf{C})$ *for each codeword of* $\mathbf{C}$, $\mathrm{wt}_{min}(1001) = 2$, $\mathrm{wt}_{min}(0001) = 1$, $\mathrm{wt}_{min}(1001) = 2$. *Hence,*

$$d(\mathbf{C}) = \mathrm{wt}_{min}(C) = 1.$$

Remark 3.2.
The minimum weight of dual code $\mathbf{C}^{\perp}$ *denoted by* $d^{\perp}$.

Example 3.4.
Let $\mathbf{C} = \{000, 110, 011, 101\}$ *be a linear code, with the generator matrix and parity check matrix*

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

Note that, $\mathrm{wt}_{min}(101) = 2$, $\mathrm{wt}_{min}(011) = 2$, $\mathrm{wt}_{min}(110) = 2$. *Then, the minimum weight of* $\mathbf{C}$ *is 2 and the minimum weight of* $\mathbf{C}^{\perp}$ *is 3.*

Lemma 3.2.
If $\mathbf{c}, \tilde{\mathbf{c}} \in \mathbb{F}_2^n$, *then*

$$\mathrm{wt}(\mathbf{c} + \tilde{\mathbf{c}}) = \mathrm{wt}(\mathbf{c}) + \mathrm{wt}(\tilde{\mathbf{c}}) - 2\mathrm{wt}(\mathbf{c} \cap \tilde{\mathbf{c}}),$$

where $\mathbf{c} \cap \tilde{\mathbf{c}}$ *is the vector* $(\mathbf{c}_1\tilde{\mathbf{c}}_1, \ldots, \mathbf{c}_n\tilde{\mathbf{c}}_n)$.

Proof.
The quantity $\text{wt}(\mathbf{c}) - \text{wt}(\mathbf{c} \cap \tilde{\mathbf{c}})$ represents the count of positions i where $\mathbf{c}_i = 1$ but $\tilde{\mathbf{c}} = 0$. Similarly, $\text{wt}(\mathbf{c}) - \text{wt}(\mathbf{c} \cap \tilde{\mathbf{c}})$ denotes the number of positions i where $\tilde{\mathbf{c}}_i = 1$ but $\mathbf{c}_i = 0$. Then

$$\text{wt}(\mathbf{c}) - \text{wt}(\mathbf{c} \cap \tilde{\mathbf{c}}) + \text{wt}(\tilde{\mathbf{c}}) - \text{wt}(\mathbf{c} \cap \tilde{\mathbf{c}}) = \text{wt}(\mathbf{c}) + \text{wt}(\tilde{\mathbf{c}}) - 2\text{wt}(\mathbf{c} \cap \tilde{\mathbf{c}}),$$

the dissimilarity between $\mathbf{c}$ and $\tilde{\mathbf{c}}$ is quantified by the number of locations where they exhibit differences. Therefore, $d(\mathbf{c}, \tilde{\mathbf{c}}) = \text{wt}(\mathbf{c}) + \text{wt}(\tilde{\mathbf{c}}) - 2\text{wt}(\mathbf{c} \cap \tilde{\mathbf{c}})$. Then $d(\mathbf{c}, \tilde{\mathbf{c}}) = \text{wt}(\mathbf{c} - \tilde{\mathbf{c}}) = \text{wt}(\mathbf{c} + \tilde{\mathbf{c}})$, since $-\tilde{\mathbf{c}} = \tilde{\mathbf{c}} \in \mathbb{F}_2^n$. So, $\text{wt}(\mathbf{c} + \tilde{\mathbf{c}}) = \text{wt}(\mathbf{c}) + \text{wt}(\tilde{\mathbf{c}}) - 2\text{wt}(\mathbf{c} \cap \tilde{\mathbf{c}})$. □

Example 3.5.
Let $\mathbf{c} = (0110)$, $\tilde{\mathbf{c}} = (1110) \in \mathbb{F}_2^4$, *then*

$$\begin{aligned} \text{wt}(\mathbf{c} + \tilde{\mathbf{c}}) &= \text{wt}(\mathbf{c}) + \text{wt}(\tilde{\mathbf{c}}) - 2\text{wt}(\mathbf{c} \cap \tilde{\mathbf{c}}) \\ &= 2 + 3 - 4 \\ &= 1. \end{aligned}$$

Note that, $\text{wt}(\mathbf{c}) = 2$, $\text{wt}(\tilde{\mathbf{c}}) = 3$, *and* $\text{wt}(\mathbf{c} \cap \tilde{\mathbf{c}}) = 2$.

Lemma 3.3.
Let $\mathbf{c}, \tilde{\mathbf{c}} \in \mathbb{F}_2$. *If the weights of both* $\mathbf{c}$ *and* $\tilde{\mathbf{c}}$ *are odd, then the weight of* $\mathbf{c} + \tilde{\mathbf{c}}$ *is even.*

Proof.
Let $\mathbf{c}$ and $\tilde{\mathbf{c}}$ be odd-weight binary strings, with $\text{wt}(\mathbf{c}) = 2i+1$ and $\text{wt}(\tilde{\mathbf{c}}) = 2j+1$, where i and j are integers. Let k be the number of positions where both $\mathbf{c}$ and $\tilde{\mathbf{c}}$ have 1's, or $\text{wt}(\mathbf{c} \cap \tilde{\mathbf{c}})$. Then,

$$\begin{aligned} \text{wt}(\mathbf{c} + \tilde{\mathbf{c}}) &= \text{wt}(\mathbf{c}) + \text{wt}(\tilde{\mathbf{c}}) - 2k \\ &= (2i + 1) + (2j + 1) - 2k \\ &= 2i + 2j - 2k + 2 \\ &= 2(i + j - k + 1). \end{aligned}$$

□

Example 3.6.
Let $\mathbf{c} = (1011)$, $\tilde{\mathbf{c}} = (0111) \in \mathbb{F}_2^4$, *then*

$$\begin{aligned} \text{wt}(\mathbf{c} + \tilde{\mathbf{c}}) &= \text{wt}(\mathbf{c}) + \text{wt}(\tilde{\mathbf{c}}) - 2k \\ &= 3 + 3 - 4 \\ &= 2. \end{aligned}$$

Note that, $\text{wt}(\mathbf{c}) = 3$, $\text{wt}(\tilde{\mathbf{c}}) = 3$, *and* $k = 2$.

Lemma 3.4.
Let $\mathbf{c}$ *and* $\tilde{\mathbf{c}}$ *be two elements in the set* $\mathbb{F}_2$. *If one of them has an odd weight and the other has an even weight, then the sum of* $\mathbf{c}$ *and* $\tilde{\mathbf{c}}$ *will have an odd weight.*

Proof.
Assume that $\mathbf{c}$ has an odd weight and $\tilde{\mathbf{c}}$ has an even weight. Consequently, $\mathrm{wt}(\mathbf{c}) = 2i + 1$ and $\mathrm{wt}(\tilde{\mathbf{c}}) = 2j$ for certain integers $i, j \in \mathbb{Z}$. Let k represent the count of positions where both $\mathbf{c}$ and $\tilde{\mathbf{c}}$ contain 1's, or $\mathrm{wt}(\mathbf{c} \cap \tilde{\mathbf{c}})$. Then

$$\begin{aligned} \mathrm{wt}(\mathbf{c} + \tilde{\mathbf{c}}) &= \mathrm{wt}(\mathbf{c}) + \mathrm{wt}(\tilde{\mathbf{c}}) - 2k \\ &= (2i + 1) + (2j) - 2k \\ &= 2i + 2j - 2k + 1 \\ &= 2(i + j - k) + 1. \end{aligned}$$

Thus, $\mathrm{wt}(\mathbf{c} + \tilde{\mathbf{c}})$ has odd weight. □

Example 3.7.
Let $\mathbf{c} = (1201)$, $\tilde{\mathbf{c}} = (0110) \in \mathbb{F}_3^4$, *then*

$$\begin{aligned} \mathrm{wt}(\mathbf{c} + \tilde{\mathbf{c}}) &= \mathrm{wt}(\mathbf{c}) + \mathrm{wt}(\tilde{\mathbf{c}}) - 2k \\ &= 3 + 2 - 0 \\ &= 5. \end{aligned}$$

Note that, $\mathrm{wt}(\mathbf{c}) = 3$, $\mathrm{wt}(\tilde{\mathbf{c}}) = 3$, *and* $k = 0$.

Theorem 3.2.
Let $\mathbf{C}$ *be an* $[n, k]$*-code with parity-check matrix* H*. Then* $d(\mathbf{C}) = d$ *if and only if some* d *columns of* H *are linearly dependent but every* $d - 1$ *columns are linearly independent.*

Proof.
Let $\mathbf{C}$ be a linear code. If $\mathrm{wt}(\mathbf{C}) = d = d_H$, then there exists a codeword in $\mathbf{C}$ with weight d. By theorem we have $d =$wt($\mathbf{C}$). Now $\mathrm{wt}(\mathbf{C}) \preceq d$ if and only if there are d linearly dependent columns in H, while $\mathrm{wt}(\mathbf{C}) \succeq d$ if and only if all collections of $d - 1$ columns are linearly independent. □

Example 3.8.
Consider the $[7, 4]$ *Hamming code over* $\mathbb{F}_2$ *with parity check matrix*

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

The colomns $\{(001), (010), (011)\}$ *of* H *are linearly dependent, then by Theorem, the minimum distance of the code* $\mathbf{C}$ *is 3.*

3.2 Lee weights

Definition 3.3 (Lee weights)**.**
The Lee weight of a scalar $\mathbf{a} \in \mathbb{F}_q$ *is defined as*

$$\mathrm{wt}_L(a) = min(a, q - a),$$

the Lee weight of a vector $\mathbf{x} \in \mathbb{F}_q^n$ *of length* n *is defined as*

$$\mathrm{wt}_L(\mathbf{x}) = \sum_{i=1}^{n} \mathrm{wt}_L(\mathbf{x}_i).$$

Example 3.9.
Let $\mathbf{x}_1 = (235)$, *and* $\mathbf{x}_2 = (412)$ *over* $\mathbb{F}_{11}$. *Then*

(i) $\mathrm{wt}_L(2) = 2$, $\mathrm{wt}_L(3) = 3$, *and* $\mathrm{wt}_L(5) = 1$. *Hence, we obtain that,* $\mathrm{wt}_L(\mathbf{x_1}) = 1+2+3 = 6$.

(ii) $\mathrm{wt}_L(4) = 2$, $\mathrm{wt}_L(1) = 1$, *and* $\mathrm{wt}_L(2) = 2$. *Hence, we obtain that,* $\mathrm{wt}_L(\mathbf{x_2}) = 1+2+2 = 5$.

Example 3.10.
Consider $\mathbf{x} = (5671)$ *over* $\mathbb{F}_{13}$. *Then*
$\mathrm{wt}_L(5) = 3$, $\mathrm{wt}_L(6) = 2$, $\mathrm{wt}_L(7) = 1$, *and* $\mathrm{wt}_L(1) = 1$. *Hence, we obtain that* $\mathrm{wt}_L(\mathbf{x}) = 1+3+2+1 = 7$.

Definition 3.4.
Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. *The Lee distance between* $\mathbf{x}$ *and* $\mathbf{y}$ *is given by the Lee weight of their differencey*

$$d_L(\mathbf{x}, \mathbf{y}) = \mathrm{wt}_L(\mathbf{x} - \mathbf{y})$$

Example 3.11.
Let $\mathbf{x} = (111) \in \mathbb{F}_2^3$, *and* $\mathbf{y} = (101) \in \mathbb{F}_2^3$, *then* $d_L(\mathbf{x}, \mathbf{y}) = \mathrm{wt}_L(\mathbf{x} - \mathbf{y}) = 1$.

Example 3.12.
Let $\mathbf{x} = (142) \in \mathbb{F}_5^3$, *and* $\mathbf{y} = (123) \in \mathbb{F}_4^3$, *then* $d_L(\mathbf{x}, \mathbf{y}) = \mathrm{wt}_L(\mathbf{x} - \mathbf{y}) = 2$.

3.3 Distribution weights

Definition 3.5 (Distribution weights)**.**
The weight distribution of $\mathbf{C}$ *is given as*

$$\mathrm{w}_{\mathbf{C}}(\mathbf{x}, \mathbf{y}) = \sum_{c \in \mathbf{C}} \mathbf{x}^{n-\mathrm{wt}(c)} \mathbf{y}^{\mathrm{wt}(c)} = \sum_{i=0}^{n} A_i \mathbf{x}^{n-i} \mathbf{y}^i,$$

where A_i *represent the quantity of codewords with a weight of* $i \in \mathbf{C}$.

Example 3.13.
Consider the code $\mathbf{C} = \{000, 110, 011, 101\}$ *has the weight distribution* $A_1 = A_3 = 0, A_0 = 1$, *and* $A_2 = 3$. *So, the weight enumerator of* $\mathbf{C}$ *is*

$$\begin{aligned} \mathrm{w}_{\mathbf{C}}(\mathbf{x}, \mathbf{y}) &= 1\mathbf{x}^3\mathbf{y}^0 + 0\mathbf{x}^2\mathbf{y}^1 + 3\mathbf{x}^1\mathbf{y}^2 + 0\mathbf{x}^0\mathbf{y}^3 \\ &= \mathbf{x}^3 + 3\mathbf{x}\mathbf{y}^2. \end{aligned}$$

Definition 3.6.
The weight enumerator for $\mathbf{C}^\perp$ *is given as*

$$\mathrm{w}_{\mathbf{C}^\perp}(\mathbf{x}, \mathbf{y}) = \sum_{c \in \mathbf{C}^\perp} \mathbf{x}^{n-\mathrm{wt}(c)} \mathbf{y}^{\mathrm{wt}(c)} = \sum_{i=0}^{n} A_i^\perp x^{n-i} y^i,$$

where $A_i^\perp$ *represent the quantity of codewords with a weight of* $i \in \mathbf{C}^\perp$.

Example 3.14.
Let $\mathbf{C}^{\perp} = \{000, 111\}$ *be the dual code of the code* $\mathbf{C} = \{000, 110, 011, 101\}$*, then the weight distribution of* $\mathbf{C}^{\perp}$ $A_1^{\perp} = A_2^{\perp} = 0, A_0^{\perp} = 1$*, and* $A_3^{\perp} = 1$*. So, the weight enumerator of* $\mathbf{C}^{\perp}$ *is*

$$\begin{aligned} \mathrm{w}_{\mathbf{C}^{\perp}}(\mathbf{x}, \mathbf{y}) &= 1\mathbf{x}^3\mathbf{y}^0 + 0\mathbf{x}^2\mathbf{y}^1 + 0\mathbf{x}^1\mathbf{y}^2 + 1\mathbf{x}^0\mathbf{y}^3 \\ &= \mathbf{x}^3 + \mathbf{y}^3. \end{aligned}$$

Theorem 3.3.
If $\mathbf{C}$ *is an* $[n, k, d]$ *linear code with dual code* $\mathbf{C}^{\perp}$*, then*

$$\mathrm{w}_{\mathbf{C}^{\perp}}(\mathbf{x}, \mathbf{y}) = \frac{1}{\mid \mathbf{C} \mid} \mathrm{w}_{\mathbf{C}}(\mathbf{x} + \mathbf{y}, \mathbf{x} - \mathbf{y}),$$

where $\mid \mathbf{C} \mid = q^k$ *. Equivalently*

$$\sum_{k=0}^{n} A_k^{\perp} \mathbf{x}^{n-k} \mathbf{y}^k = \frac{1}{\mid \mathbf{C} \mid} \sum_{i=0}^{n} A_i (\mathbf{x} + \mathbf{y})^{n-i} (\mathbf{x} - \mathbf{y})^i,$$

or

$$\sum_{c^{\perp} \in \mathbf{C}^{\perp}} \mathbf{x}^{n - \mathrm{wt}(c^{\perp})} \mathbf{y}^{\mathrm{wt}(c^{\perp})} = \frac{1}{\mid \mathbf{C} \mid} \sum_{c \in \mathbf{C}} (\mathbf{x} + \mathbf{y})^{n - \mathrm{wt}(c)} (\mathbf{x} - \mathbf{y})^{\mathrm{wt}(c)}.$$

Example 3.15.
Let $\mathbf{C} = \{000, 110, 011, 101\}$ *of* $\mathbb{F}_2^3$*, we get*

$$\begin{aligned} \frac{1}{\mid \mathbf{C} \mid} \sum_{i=0}^{n} A_i (\mathbf{x} + \mathbf{y})^{n-i} (\mathbf{x} - \mathbf{y})^i &= \frac{1}{4} \sum_{i=0}^{3} A_i (\mathbf{x} + \mathbf{y})^{n-i} (\mathbf{x} - \mathbf{y})^i; \\ &= \frac{1}{4} (1(\mathbf{x} + \mathbf{y})^3 + 3(\mathbf{x} + \mathbf{y})^1 (\mathbf{x} - \mathbf{y})^2); \\ &= \frac{1}{4} (4\mathbf{x}^3 + 4\mathbf{y}^3); \\ &= \mathbf{x}^3 + \mathbf{y}^3. \end{aligned}$$

And by using the result in 3.14*, we get*

$$\begin{aligned} \sum_{k=0}^{n} A_k^{\perp} \mathbf{x}^{n-k} \mathbf{y}^k &= \sum_{k=0}^{3} A_k^{\perp} \mathbf{x}^{n-k} \mathbf{y}^k; \\ &= A_0^{\perp} \mathbf{x}^3 \mathbf{y}^0 + A_1^{\perp} \mathbf{x}^2 \mathbf{y}^1 + A_2^{\perp} \mathbf{x}^3 \mathbf{y}^2 + A_3^{\perp} \mathbf{x}^0 \mathbf{y}^3; \\ &= 1\mathbf{x}^3 1 + 0\mathbf{x}^2 \mathbf{y}^1 + 0\mathbf{x}^3 \mathbf{y}^2 + 10\mathbf{y}^3; \\ &= \mathbf{x}^3 + \mathbf{y}^3. \end{aligned}$$

Then

$$\sum_{k=0}^{n} A_k^{\perp} \mathbf{x}^{n-k} \mathbf{y}^k = \frac{1}{\mid \mathbf{C} \mid} \sum_{i=0}^{n} A_i (\mathbf{x} + \mathbf{y})^{n-i} (\mathbf{x} - \mathbf{y})^i = \mathbf{x}^3 + \mathbf{y}^3.$$

Example 3.16.
Let $\mathbf{C} = \{00, 11\}$ *and* $\mathbf{C}^{\perp} = \{00, 11\}$ *of* $\mathbb{F}_2^2$*, we get*

$$\begin{aligned}
\frac{1}{\mid \mathbf{C} \mid} \sum_{i=0}^{n} A_i(\mathbf{x}+\mathbf{y})^{n-i}(\mathbf{x}-\mathbf{y})^i &= \frac{1}{2} \sum_{i=0}^{2} A_i(\mathbf{x}+\mathbf{y})^{n-i}(\mathbf{x}-\mathbf{y})^i; \\
&= \frac{1}{2}(1(\mathbf{x}+\mathbf{y})^2 + 1(\mathbf{x}-\mathbf{y})^2); \\
&= \frac{1}{2}(2\mathbf{x}^2 + 2\mathbf{y}^2); \\
&= \mathbf{x}^2 + \mathbf{y}^2.
\end{aligned}$$

And in other hand, we get

$$\begin{aligned}
\sum_{k=0}^{n} A_k^{\perp} \mathbf{x}^{n-k}\mathbf{y}^k &= \sum_{k=0}^{2} A_k^{\perp} \mathbf{x}^{n-k}\mathbf{y}^k; \\
&= A_0^{\perp}\mathbf{x}^2\mathbf{y}^0 + A_1^{\perp}\mathbf{x}^1\mathbf{y}^1 + A_2^{\perp}\mathbf{x}^0\mathbf{y}^2; \\
&= 1\mathbf{x}^2 1 + 0\mathbf{x}\mathbf{y} + 11\mathbf{y}^2; \\
&= \mathbf{x}^2 + \mathbf{y}^2.
\end{aligned}$$

Then

$$\sum_{k=0}^{n} A_k^{\perp} \mathbf{x}^{n-k}\mathbf{y}^k = \frac{1}{\mid \mathbf{C} \mid} \sum_{i=0}^{n} A_i(\mathbf{x}+\mathbf{y})^{n-i}(\mathbf{x}-\mathbf{y})^i = \mathbf{x}^2 + \mathbf{y}^2.$$

conclusion

In the conclusion of this memory, we provide a summary of the primary findings from this work, which we first provided as: gave definitions and some results of abstract algebra (Groups, Rings, Ideals, Fields, Finite fields) and coding theory, which constitute the main results produced in this work. Then, we studied some linear codes such that Hamming and Reed-Solomon codes. We also touched on discovering and correcting errors by Hamming code. Finally, we studied some weights and their results over finite fields.

Bibliography

[1] I. S. Reed, G. Solomon, Polynomial codes over certain nite elds, J. Soc. Indust. Appl. Math, 8(2), $300 - 304$, (1960).

[2] D. M. Burton, A first course in rings and ideals, Wesley Publishing Company, (1970).

[3] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland publishing company, (1981).

[4] B. Wicker and K. Vijay Bhargava. "An introduction to Reed-Solomon codes." Reed-Solomon codes and their applications (1994) $1 - 16$.

[5] R.Lidl and G.Pilz, Applied abstract algebra , Springer-Verlag New York, (1998).

[6] S. Axler, F. W. Gehring, and K. A. Ribet. Graduate Texts in Mathematics 86, (1999).

[7] D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, J. R. Wall, Coding theory and cryptography the essentials, Taylor and Francis Group, (2000).

[8] I.N. Landjev, Linear codes over finite fields and finite projective geometries, Bulgarian academy of sciences, Discrete Mathematics, (2000).

[9] W. C. Huffman and V. Pless , Fundamentals of error-correcting codes, Cambridge University press, (2003).

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

[11] N. L. Biggs, Codes an introduction to information communication and cryptography, Springer-Verlag London, (2008).

[12] S. B. Wicker and V. K. Bhargava, An introduction to Reed-Solomon Code, University of Victoria, British Columbia, Canada V8W 2Y2, (2009).

[13] V. Guruswami, E. Blais. Notes 6: Reed–Solomon, BCH, Reed–Muller, and concatenated codes. Introduction to Coding Theory CMU : Spring. (2010).

[14] M. Nevin, Mat3343: applied algebra, ottaawa university, (2022).

[15] F.F. Baftani, Lee weight and generalized Lee weight for codes over $\mathbb{Z}_{2^n}$, Mathematics Inter disciplinary Research, 8 (1) (2023) $27 - 33$.