Codes with Singleton Defects of One and Two

by

Zhipeng Zhang

Bachelor of Science in Computer Science and Mathematics, University of Alberta, 2021

A Thesis Submitted in Partial Fulfilment of
the Requirements for the Degree of

Master of Science

In the Graduate Academic Unit of Mathematics

Supervisor(s): Tim Alderson, PhD, Mathematics and Statistics

Examining Board: Andrea Burgess, PhD, Mathematics and Statistics, Chair
Idris Gadoura, PhD, Engineering

This thesis is accepted by the
Dean of Graduate Studies

THE UNIVERSITY OF NEW BRUNSWICK

April 2024

Abstract

This thesis covers codes with Singleton defects of one and two. The discussion on codes with a Singleton defect of one begins by introducing almost MDS and near MDS codes, then proceeds to explore the maximum lengths of MDS and near MDS codes. This part of the discussion concludes by proving some results using projective geometry. Following this, the thesis shifts its focus to studying almost almost MDS and near near MDS codes, which are codes with a Singleton defect of two. This analysis begins with definitions of almost almost MDS and near near MDS codes, followed by an exploration of the differences between these codes within the context of projective geometry, and ends with an upper bound on the length of long almost almost MDS codes.

Dedication

To my orange male cat, named Burk.

Figure 1: An image of Burk

Acknowledgements

Firstly, I would like to thank my thesis supervisor, Dr. Tim Alderson, for the considerable time and effort he has put into this thesis. I also learned a tremendous amount of mathematical knowledge from him. Furthermore, I would not have been able to learn how to write a thesis and how to conduct research without his guidance.

Secondly, I would like to thank Dr. James McClure, the English professor from the UNB Saint John campus Writing Centre, for helping me improve my English and writing skills. Together, we enhanced the quality of this thesis.

Table of Contents

List of Tables

List of Figures

List of Symbols, Nomenclature or Abbreviations

Unless specified otherwise, the symbols in this list are defined as follows:

p	A prime number.
q	A prime power.
$\mathbb{F}_q$	A finite field with q elements.
$\mathbb{F}_q^n$	A vector space over $\mathbb{F}_q$, each element of which has length n.
C	A code.
$d(u, v)$	The Hamming distance between the two n-tuples u and v.
$d(C)$	The minimum distance of C.
$[n, k, d]_q$	A linear code over $\mathbb{F}_q$ of length n, dimension k, and minimum distance d.
G	A generator matrix.
H	A check matrix.
$C^\perp$	A dual code of C.
$wt(u)$	The weight of a codeword u.
$\mathrm{supp}(C)$	The support of C.
$d_r(C)$	The r-th generalized Hamming weight of C.
$\mathrm{PG}(k, q)$	A k dimensional projective space over $\mathbb{F}_q$.

Chapter 1

Preliminaries

1.1 Introduction

The field of information theory was initially established by Harry Nyquist and Ralph Hartley in the 1920s and Claude Shannon in the 1940s. Coding theory is one direct application of information theory. Coding theory has a lot of subareas, for example, data compression, error correction, cryptography, and more. In this thesis, we will specifically focus on error-correcting codes.

Imagine someone sent a message to us, which we do not know the content of, through a noisy channel; in such a scenario, we may receive a corrupted message. If the message is not encoded using error-correcting codes, then there would be no way to detect and correct the errors. Therefore, error-correcting codes are essential, which is why we are researching this area.

In this chapter, we will introduce some mathematical concepts central to this thesis. The results presented here follow from the basic theory. For details, the interested reader is referred to [7, 9, 14, 15, 18, 19, 25].

1.2 Finite Fields

We start this section with Definition 1.2.1, which is fundamental for understanding the content that follows.

Definition 1.2.1. *A binary operation $\star$ on a set G is a function $\star$: $G \times G \to G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$.*

Example 1.2.2. *On the set of real numbers, $+$ is a binary operation because the sum of two real numbers is a real number.*

With Definition 1.2.1 established, we can introduce the next definition:

Definition 1.2.3. *A **group** is an ordered pair $(G, \star)$ where G is a set, and $\star$ is a binary operation on G satisfying the following axioms:*

i. $(a \star b) \star c = a \star (b \star c)$, *for all* $a, b, c \in G$,

*ii. there exists an element e in G, called an **identity** of G, such that for all $a \in G$ we have $a \star e = e \star a = a$,*

iii. for each $a \in G$, there is an element a^{-1} of G, called an inverse of a, such that $a \star a^{-1} = a^{-1} \star a = e$.

Example 1.2.4. *The ordered pair $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is the set of integers, is a group. This can be easily verified as the associative law is true for integers, $a+0 = 0+a = a$ for all $a \in \mathbb{Z}$, and $a + (-a) = (-a) + a = 0$ for every $a, -a \in \mathbb{Z}$.*

Additionally, there is a special type of group, and it is defined below:

Definition 1.2.5. *The group $(G, \star)$ is called **abelian** (or **commutative**) if $a \star b = b \star a$, for all $a, b \in G$.*

Example 1.2.6. *The group $(\mathbb{Z}, +)$ is also abelian as $a + b = b + a$ for all $a, b \in \mathbb{Z}$.*

We now use Definition 1.2.5 to establish the next definition:

Definition 1.2.7. *A **commutative ring** R is a set with two binary operations, addition and multiplication, such that it is a commutative group with respect to addition with identity element* 0*, and multiplication is commutative ($ab = ba$), associative ($(ab)c = a(bc)$), distributive ($a(b + c) = ab + ac$) and has an identity element* 1*.*

Example 1.2.8. *$\mathbb{Z}$ is a commutative ring, often referred to as the ring of integers.*

A commutative ring is a special set, that is closed under addition and multiplication. Furthermore, if we sum an element with 0, then the result is the element itself; while every element multiplied by 1 is itself. Also, the multiplication of elements has to be commutative, associative, and distributive. Moreover, there is an important type of commutative ring.

Definition 1.2.9. *A **field** is a commutative ring in which every non-zero element has a multiplicative inverse. In other words, for all $a \neq 0$, there is an element b such that $ab = 1$. In particular, this implies that if $ab = 0$, then either $a = 0$ or $b = 0$.*

Example 1.2.10. *The rational numbers, $\mathbb{Q}$; the real numbers, $\mathbb{R}$; and the complex numbers, $\mathbb{C}$, are all fields.*

In the above example, the sum $1 + \cdots + 1$ is never zero. Now, let $\mathbb{F}$ be a field with multiplicative identity 1. Suppose there is an n for which summing n ones gives zero, and let n be minimal with this property. If p is a proper divisor of n then

$$\underbrace{1 + \cdots + 1}_{n} = \underbrace{(1 + \cdots + 1)}_{p}\underbrace{(1 + \cdots + 1)}_{\frac{n}{p}} \tag{1.1}$$

which contradicts the minimality of n, since the left-hand is zero implies one of the terms in the product on the right-hand side is zero. It follows that n is a prime p.

The number p is called the **characteristic** of the field. If no such n exists, then the characteristic is zero.

The ring $\mathbb{Z}/p\mathbb{Z}$, the integers modulo p, is a field of characteristic p and is denoted $\mathbb{F}_p$.

Example 1.2.11. *$\mathbb{F}_2$ is the binary field with elements 0 and 1; $\mathbb{F}_3$ is the ternary field with elements 0, 1, and 2.*

The ring $\mathbb{Z}/n\mathbb{Z}$ is not a field when n is not a prime, since it has non-zero elements which have no multiplicative inverse. In order to proceed further, we need to introduce following definitions:

Definition 1.2.12. *A **two-sided ideal** I of a ring is a subset that is closed under addition and by multiplication by any element of the ring.*

With that established, we can now talk about the next definition:

Definition 1.2.13. *The quotient of a ring R by a two-sided ideal I is denoted by R/I. The result is called a **quotient** or **factor ring**.*

In addition,

Definition 1.2.14. *Let G be a group and H a subgroup of G. Define a **left coset** of H with representative $g \in G$ to be the set*

$$gH = \{gh : h \in H\}.$$

***Right cosets** can be defined similarly by*

$$Hg = \{hg : h \in H\}.$$

*If left and right cosets coincide or if it is clear from the context to which type of coset that we are referring, we will use the word **coset** without specifying left or right.*

With the above definitions in mind, we can now continue. In the following theorem, (f) denotes the set of elements of the ring of polynomials $\mathbb{F}_p[X]$ which are multiples of the polynomial f. The elements of the quotient ring $\mathbb{F}_p[X]/(f)$ are cosets of the form $g + (f)$, where addition is defined as

$$g + (f) + h + (f) = g + h + (f) \tag{1.2}$$

and multiplication is defined as

$$(g + (f))(h + (f)) = gh + (f). \tag{1.3}$$

One can think of the quotient ring as the polynomials modulo f. Additionally, there is a special type of polynomial, which we will define as follows:

Definition 1.2.15. *A polynomial $f(X)$ in $\mathbb{F}_p[X]$ is said to be **reducible** if it can be expressed as $f(X) = a(X)b(X)$, where $a(X)$ and $b(X)$ are polynomials in $\mathbb{F}_p[X]$ with degrees less than the degree of $f(X)$. If $f(X)$ cannot be expressed in this way, then it is called **irreducible**.*

Following the definition of reducible and irreducible polynomials, we can now introduce the next theorem:

Theorem 1.2.16. *If f is an irreducible polynomial in the ring $\mathbb{F}_p[X]$, then $\mathbb{F}_p[X]/(f)$ is a field of characteristic p.*

Before getting into the next section, we need one more theorem. In order to introduce that theorem, we need the following definition:

Definition 1.2.17. *A linear map T is called an **isomorphism** if the following two conditions are satisfied:*

i. T is one to one. That is, if $T(x) = T(y)$, then $x = y$.

ii. T is onto. That is, if $w \in W$, then there exists $v \in V$ such that $T(v) = w$.

Two such subspaces which have an isomorphism are said to be ***isomorphic****.*

We can now talk about the theorem.

Theorem 1.2.18. *A finite field with q elements is isomorphic to $\mathbb{F}_q$.*

1.3 Vector Spaces

We start this section with Definition 1.3.1 because it is essential to the main topic of this thesis.

Definition 1.3.1. *Let $\mathbb{F}$ be a field whose elements are referred to as* ***scalars****. A* ***vector space*** *over $\mathbb{F}$ is a nonempty set V, whose elements are referred to as* ***vectors****, together with two operations. The first operation, called* ***addition*** *and denoted by $+$, assigns to each pair (u, v) of vectors in V a vector $u + v$ in V. The second operation, called* ***scalar multiplication*** *and denoted by juxtaposition, assigns to each pair $(r, u) \in \mathbb{F} \times V$ a vector ru in V. Furthermore, the following properties must be satisfied:*

i. ***(Associativity of addition)*** *For all vectors $u, v, w \in V$*

$$u + (v + w) = (u + v) + w \tag{1.4}$$

ii. ***(Commutativity of addition)*** *For all vectors $u, v \in V$*

$$u + v = v + u \tag{1.5}$$

iii. ***(Existence of a zero)*** *There is a vector $0 \in V$ with the property that*

$$0 + u = u + 0 = u \tag{1.6}$$

for all vectors $u \in V$.

iv. ***(Existence of additive inverses)*** *For each vector $u \in V$, there is a vector in V, denoted by $-u$, with the property that*

$$u + (-u) = (-u) + u = 0 \tag{1.7}$$

v. ***(Properties of scalar multiplication)*** *For all scalars $a, b \in \mathbb{F}$ and for all vectors $u, v \in V$*

$$\begin{aligned} a(u+v) &= au + av \\ (a+b)u &= au + bu \\ (ab)u &= a(bu) \\ 1u &= u \end{aligned} \tag{1.8}$$

By $\mathbb{F}_q^n$ we denote the set of all ordered n-tuples over $\mathbb{F}_q$, that is $\mathbb{F}_q^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{F}_q\}$.

It is easily verified that $\mathbb{F}_q^n$ satisfies all the axioms in Definition 1.3.1. So, $\mathbb{F}_q^n$ is a vector space. In addition, another important concept regarding vector spaces is that of a subspace.

Definition 1.3.2. *A **subspace** of a vector space V is a subset S of V that is a vector space in its own right under the operations obtained by restricting the operations of V to S.*

In other words, a subspace of the vector space V is a vector space under the same addition and scalar multiplication defined by V. With this concept established, we can discuss how to generate a subspace.

Definition 1.3.3. *Let S be a subspace of V. A subset $\{v_1, v_2, \ldots, v_n\}$ of S is called a **generating set** (or **spanning set**) of S if every vector in S can be expressed as a linear combination of $v_1, v_2, \ldots, v_n$.*

We will introduce a special type of generating set, but before that, we need the following definition:

Definition 1.3.4. *A nonempty set of vectors $S = \{v_1, v_2, \ldots, v_n : v_i \in V\}$ is **linearly independent** if, for any $r_1, r_2, \ldots, r_n$ in $\mathbb{F}_q$, we have*

$$r_1v_1 + r_2v_2 + \ldots + r_nv_n = 0 \Rightarrow r_1 = r_2 = \ldots = r_n = 0. \tag{1.9}$$

*If a set of vectors is not linearly independent, then it is said to be **linearly dependent**.*

We can now talk about the special type of generating set.

Definition 1.3.5. *Let S be a subspace of V. A generating set of S which is also linearly independent is called a **basis** of S. The number of vectors in a basis of S is called the **dimension** of S.*

Definition 1.3.6. *If $S = \{v_1, v_2, \ldots, v_n\}$ is a set of vectors in $\mathbb{F}_q^n$, then by $\langle v_1, v_2, \ldots, v_n\rangle$ or $\langle S\rangle$, we denote the span of S, where*

$$\langle S\rangle = \left\{ \sum_{i=1}^{n} a_i v_i : a_i \in \mathbb{F}_q \right\}. \tag{1.10}$$

If $\{v_1, v_2, \ldots, v_n\}$ is a basis of S, then $S = \langle v_1, v_2, \ldots, v_n\rangle$.

Example 1.3.7 (Basis)**.** *Let v_1 and v_2 be two vectors over $\mathbb{F}_2$. If $v_1 = (1\ 0)$ and $v_2 = (0\ 1)$, then the following set of vectors, $S = \{v_1, v_2\}$, is a basis of a two dimensional vector space because $r_1v_1 + r_2v_2 = 0 \Rightarrow r_1 = r_2 = 0$. In other words, S is linearly independent.*

Example 1.3.8 (Not a basis)**.** *Consider three vectors u_1, u_2, and u_3 over $\mathbb{F}_2$. If $u_1 = (1\ 0\ 0)$, $u_2 = (0\ 1\ 0)$, and $u_3 = (1\ 1\ 0)$, then $T = \{u_1, u_2, u_3\}$ is not a basis of a three dimensional vector space since $r_1u_1+r_2u_2+r_3u_3 = 0$ when $r_1 = r_2 = 1, r_3 = -1$. That is to say, T is linearly dependent.*

In addition, we will also discuss another important concept from linear algebra.

Definition 1.3.9. *Let A be an $m \times n$ matrix over any field $\mathbb{F}$. the rows of A span a subspace of $\mathbb{F}^n$ known as the **row space** of A and the columns of A span a subspace of $\mathbb{F}^m$ known as the **column space** of A. The dimensions of these spaces are called the **row rank** and **column rank**, respectively.*

Note that, the row space of A is $\{xA : x \in \mathbb{F}^m\}$, and the column space of A is $\{Ax : x \in \mathbb{F}^n\}$.

There is an interesting fact about the row rank and column rank (see e.g. [18]),

Proposition 1.3.10. *The row rank of a matrix is always equal to its column rank.*

We shall also require the notion of full rank.

Definition 1.3.11. *An $m \times n$ matrix has a **full row rank** if its row rank is m, and it has a **full column rank** if its column rank is n. If a matrix has full row rank or full column rank, then we say the matrix has full rank.*

Having established this definition, we will now introduce a fundamental form of matrices.

Definition 1.3.12. *A matrix is said to be in **row echelon form** if it satisfies all of the following conditions:*

i. If the first nonzero entry in each nonzero row is 1*.*

ii. If row k does not consist entirely of zeros, then the number of leading zero entries in row $k+1$ is greater than the number of leading zero entries in row k.

iii. If there are rows whose entries are all zero, then they are below the rows having nonzero entries.

There is a special case of the row echelon form.

Definition 1.3.13. *A matrix is said to be in* ***reduced row echelon form*** *if both of the following hold:*

i. The matrix is in row echelon form.

ii. The first nonzero entry in each row is the only nonzero entry in its column.

Example 1.3.14. *Let M be a matrix over $\mathbb{F}_{17}$. If*

$$M = \begin{bmatrix} 1 & 5 & 1 \\ 2 & 11 & 5 \end{bmatrix}, \tag{1.11}$$

then the row echelon form of M is

$$\begin{bmatrix} 1 & 5 & 1 \\ 0 & 1 & 3 \end{bmatrix}, \tag{1.12}$$

and the reduced row echelon form of M is

$$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 3 \end{bmatrix}. \tag{1.13}$$

We now provide the following definition as we are going to use it later.

Definition 1.3.15. *Let V be a vector space, and let W be a subspace of V. The* ***orthogonal complement*** *of W is defined as*

$$W^{\perp} = \{\ v \in V : v \cdot w = 0 \text{ for all } w \in W\}. \tag{1.14}$$

In particular, the dimension of W plus the dimension of $W^{\perp}$ equals the dimension of V.

We end this section with the next theorem.

Theorem 1.3.16. *Let W be any non-zero subspace of a vector space V. Then every basis of W can be extended to a basis of V.*

1.4 Codes

We start this section with the definition of codes.

Definition 1.4.1. *Let A be a finite set of q elements called the **alphabet**. A **block code** (or simply a **code**) C is a subset of A^n. C is called a q-**ary** code of **length** n. The elements of a code C are called **codewords**.*

We will now introduce a method used to measure the distance between two n-tuples.

Definition 1.4.2. *The **(Hamming) distance** between two n-tuples u and v, denoted $d(u, v)$, is the number of coordinate positions in which they differ.*

In the rest of the thesis, Hamming distance is referred to as distance.

Example 1.4.3. *If $u = (1\ 0\ 1)$, $v = (0\ 1\ 1)$, and $w = (2\ 1\ 1)$, then $d(u, v) = 2$ as the two 3-tuples u and v are different at two coordinate positions; $d(u, w) = 2$ because u and w have different elements at two coordinate positions; $d(v, w) = 1$ since v and w differ at their first coordinate position.*

Now, let x and y be two n-tuples. Based on Definition 1.4.2, $d(x, y) = d(y, x) \geqslant 0$ for all x, y. In addition, $d(x, y) = 0$ if and only if $x = y$.

Lemma 1.4.4. *$d(x, y) \leqslant d(x, z) + d(z, y)$ for all $x, y, z \in \mathbb{F}_q^n$.*

The lemma mentioned above is commonly referred to as the triangle inequality.

Definition 1.4.5. *A metric space is a pair (X, d) where X is a set and d is a real valued mapping on $X \times X$, such that the following axioms hold:*

i. $d(x, y) \geqslant 0$ *for all* $x, y \in X$;

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

iii. $d(x, y) = d(y, x)$ *for all* $x, y \in X$;

iv. $d(x, y) \leqslant d(x, z) + d(z, y)$ *for all* $x, y, z \in X$.

The d is called a metric on X. According to Definition 1.4.5, Hamming distance is a metric on A^n.

Definition 1.4.6. *The **minimum distance** of a code C is the minimum distance between any two distinct codewords of C, denoted $d(C)$. That is*

$$d(C) = \min\{d(x, y) : x, y \in C, \text{ and } x \neq y\}. \tag{1.15}$$

Example 1.4.7. *Let $c_1 = (1\ 0\ 1)$, $c_2 = (0\ 2\ 0)$, and $c_3 = (0\ 0\ 0)$, and let C be a ternary code, where*

$$C = \{c_1, c_2, c_3\}. \tag{1.16}$$

We have $d(c_1, c_2) = 3$, $d(c_1, c_3) = 2$, and $d(c_2, c_3) = 1$. Hence, $d(C) = d(c_2, c_3) = 1$.

For fixed parameters n and q, the minimum distance of a code is key to both the detection and correction of errors. As mentioned by Hill in [19],

"*Suppose a codeword x, unknown to us, has been transmitted and that we received the vector y which may have been distorted by noise. It seems reasonable to decode y as that codeword x', hopefully x, such that $d(x', y)$ is as small as possible.*"

The above decoding method is known as nearest neighbour decoding. Through this method, the received vector will firstly be compared with every codeword; if the vector is not equal to any of the codewords, then at least one error occurred. This is known as error detection. If errors are detected, then the received vector y will be decoded to a codeword x', where $d(x', y)$ is as small as possible. The second procedure is called error correction.

Example 1.4.8. *Let us consider a code C as introduced in Example 1.4.7:*

$$C = \{c_1, c_2, c_3\}, \tag{1.17}$$

where $c_1 = (1\ 0\ 1)$, $c_2 = (0\ 2\ 0)$, and $c_3 = (0\ 0\ 0)$. Assume a codeword of C, unknown to us, was sent and that we received the vector $v = (1\ 1\ 1)$. Since v is not a codeword of C, we know that at least one error has occurred. Since $d(v, c_1) = 1$, $d(v, c_2) = 2$, $d(v, c_3) = 3$, the vector v will be decoded as $c_1 = (1\ 0\ 1)$.

Theorem 1.4.9. *If a code C has minimum distance d, then C can be used to detect up to $d - 1$ errors, and to correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors in any codeword.*

Proof. Since the code C has minimum distance d, according to Definition 1.4.6, for every pair of codewords x and y, x and y must differ in at least d bits. Assume x is sent and x' is received, where x' has e errors and $1 \leqslant e \leqslant d - 1$. Therefore, x' cannot be a codeword. Hence, C can detect up to $d - 1$ errors. Moreover, suppose a codeword v was sent, and the vector v' is received. Let v' have at most e' errors. Assume, by way of contradiction, if $e' \leqslant \left\lfloor \frac{d-1}{2} \right\rfloor$ and v' is decoded as another codeword u, then $d(v', u) \leqslant e'$. As a result, $d(v, u) \leqslant d(v, v') + d(v', u) \leqslant 2 \cdot e' \leqslant d - 1$, which contradicts that the minimum distance is d. Thus, C can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors in any codeword. □

Minimum distance is one of the most important properties of a code. It determines how many errors a code can detect or correct under the nearest neighbour decoding.

1.5 Linear codes

We start this section with the definition of linear codes.

Definition 1.5.1. *If the alphabet $A = \mathbb{F}_q$ and the code C is a vector subspace of $\mathbb{F}_q^n$, then we say that C is a* ***linear code over*** $\mathbb{F}_q$ *or simply a* ***linear code****.*

Example 1.5.2. *Let C be the following elements of $\mathbb{F}_2^3$:*

$$C = \{(0\ 0\ 0), (0\ 1\ 1), (1\ 0\ 1), (1\ 1\ 0)\}. \tag{1.18}$$

$C = \langle (0\ 1\ 1), (1\ 0\ 1) \rangle$ and is a linear code with a dimension of two.

If C is a k-dimensional subspace of $\mathbb{F}_q^n$ then it follows that $|C| = q^k$, where $|C|$ is the number of codewords in C.

We will only discuss linear codes in the rest of this thesis. In addition, the notation we use to denote linear codes is defined in Definition 1.5.3.

Definition 1.5.3. *A k-dimensional linear code of length n and minimum distance d over $\mathbb{F}_q$ is an $[\mathbf{n}, \mathbf{k}, \mathbf{d}]_\mathbf{q}$ code.*

We can now talk about matrices which generate linear codes.

Definition 1.5.4. *A $k \times n$ matrix G whose rows are a basis for an $[n, k, d]_q$ code C is called a* ***generator matrix*** *for C. In particular, $C = \{xG : x \in \mathbb{F}_q^k\}$.*

A generator matrix G of a linear $[n, k, d]_q$ code C has k rows and n columns. Additionally, C is the row space of G. Moreover, linear codes are determined by their generator matrices.

Example 1.5.5. *The following matrix is a generator matrix of the code C from Example 1.5.2:*

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}. \tag{1.19}$$

We can easily see that $d(C) = \min\{d(u,v) : u, v \in C \text{ and } u \neq v\} = 2$. *Since* G *has two rows, three columns, and* $d(C) = 2$, $C = \{xG : x \in \mathbb{F}_2^2\}$ *is a* $[3,2,2]_2$ *code.*

Another significant matrix needs to be defined before we use it in the thesis.

Definition 1.5.6. *A* ***check matrix*** *for an* $[n,k,d]_q$ *linear code* C *is an* $(n-k) \times n$ *matrix* H *with entries from* $\mathbb{F}_q$, *with the property that*

$$C = \{u \in \mathbb{F}_q^n \mid uH^t = 0\}, \tag{1.20}$$

where H^t *denotes the transpose of the matrix* H.

Additionally, the following lemma provides a straightforward method for constructing a check matrix for a linear code with a given generator matrix, or vice versa.

Lemma 1.5.7. *If* $G = [I_k \ A]$ *is a generator matrix for an* $[n,k,d]_q$ *code* C, *then a check matrix for* C *is given by* $H = \left[-A^T \ I_{n-k}\right]$.

Example 1.5.8. *Let* G *be a generator matrix of a binary code* C, *where*

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}. \tag{1.21}$$

A check matrix of C *is*

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}. \tag{1.22}$$

If $x = (1\ 0\ 1\ 1)$ is the message, then $w = xG = (1\ 0\ 1\ 1\ 0\ 0\ 0)$ is the codeword. One can verify that $wH^t = 0$.

A check matrix is also a generator matrix of another kind of code, which will be defined as follows:

Definition 1.5.9. *The **dual code** of a linear code C is*

$$C^{\perp} = \{v \in \mathbb{F}_q^n \mid u \cdot v = u_1v_1 + \ldots + u_nv_n = 0, \text{ for all } u \in C\}. \tag{1.23}$$

Every linear code C has a zero codeword. Hence, there is a simpler way to find the minimum distance of C. In order to talk about that in Section 1.6, we need the following:

Definition 1.5.10. *The **weight** of a vector u, denoted $wt(u)$, is the number of non-zero coordinates of u.*

Note that $wt(u)$ is the Hamming distance of u from the zero vector.

Example 1.5.11. *If $v_1 = (1\ 0\ 1\ 0\ 1)$, then $wt(v_1) = 3$; if $v_2 = (1\ 2\ 1\ 0\ 2)$, then $wt(v_2) = 4$.*

1.6 Properties of linear codes

We now present some elementary properties of linear codes which shall be useful in this thesis. For details, the interested reader is referred to [7] and [19].

Lemma 1.6.1. *The minimum distance d of a linear code C is equal to the minimum weight w among all non-zero codewords of C.*

The minimum distance of a linear code C can be determined by any check matrix of C.

Lemma 1.6.2. *Let C be a linear $[n, k, d]_q$ code with check matrix H. Then the minimum distance of C is d if and only if any $d-1$ columns of H are linearly independent but some d columns are linearly dependent.*

Example 1.6.3. *Let H be the check matrix of C from Example 1.5.8, where*

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}. \tag{1.24}$$

Every pair of columns of H is linearly independent, and there exists at least one linearly dependent set of three columns, say columns 3, 5, and 6. In other words, $d(C) = 3$. From G, where

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \tag{1.25}$$

one can verify that C is indeed a $[7, 4, 3]_2$ code.

The next lemma is obtained from Definition 1.5.6 and Definition 1.5.9.

Lemma 1.6.4. *A check matrix H for an $[n, k, d]_q$ code C is a generator matrix of $C^{\perp}$.*

Example 1.6.5. *We use the generator matrix G from Example 1.5.5, where*

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}. \tag{1.26}$$

According to G, a check matrix of C is

$$H = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}. \tag{1.27}$$

It is clear that H generates two codewords: (1 1 1) *and* (0 0 0)*, which are precisely all codewords of $C^{\perp}$.*

A simple dimension argument shows that the dual of a dual code of C is the code C itself.

Lemma 1.6.6. *For any $[n, k, d]_q$ code C, $(C^{\perp})^{\perp} = C$.*

The notion of code equivalence is central to this thesis. Therefore, we need to introduce the following important definition:

Definition 1.6.7 (Code Equivalence)**.** *Two $k \times n$ matrices generate equivalent linear $[n, k, d]_q$ codes if one matrix can be obtained from the other by a sequence of operations of the following types:*

(R1) *Permutation of the rows.*

(R2) *Multiplication of a row by a non-zero scalar.*

(R3) *Addition of a scalar multiple of one row to another.*

(C1) *Permutation of the columns.*

(C2) *Multiplication of any column by a non-zero scalar.*

Suppose G is a generator matrix of an $[n, k, d]_q$ code C. If we get another generator matrix G' by performing any operations from (R1) to (R3), then G and G' generate the same codewords. Moreover, if we obtain G' by performing any operations from (R1) to (R3) combined with any operations from (C1) to (C2), then G and G' are equivalent, which means the codes they generate have the same fundamental parameters n, k and d.

Example 1.6.8. *Let G be a generator matrix over $\mathbb{F}_3$, as presented below*

$$G = \begin{bmatrix} 1 & 1 & 2 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}. \tag{1.28}$$

If we apply any combination of operations from (R1), (R2) and (R3) to G, such as exchange row one with row two, multiply row one by two, and finally add row one to row two, then we get G', which is shown below:

$$G' = \begin{bmatrix} 0 & 0 & 2 & 2 \\ 1 & 1 & 1 & 2 \end{bmatrix}. \tag{1.29}$$

Let C' be the code generated by G'. We can see that C and C' are the same code. This can be easily verified as they both have the following codewords:

$$\begin{aligned} C = C' = \{&(0\ 0\ 0\ 0), (0\ 0\ 1\ 1), (0\ 0\ 2\ 2), (1\ 1\ 2\ 0), \\ &(1\ 1\ 0\ 1), (1\ 1\ 1\ 2), (2\ 2\ 1\ 0), (2\ 2\ 2\ 1), (2\ 2\ 0\ 2)\}. \end{aligned} \tag{1.30}$$

However, if we obtained G'' from G by performing any combination of operations from (C1) and (C2), or any operations from (R1) to (R3) combined with any operations from (C1) to (C2), such as exchange column two and column three, and multiply column four by two, then

$$G'' = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{bmatrix}, \tag{1.31}$$

and the code C'' which is generated by G'' is shown below:

$$\begin{aligned} C'' = \{&(0\ 0\ 0\ 0), (0\ 1\ 0\ 2), (0\ 2\ 0\ 1), (1\ 2\ 1\ 0), \\ &(1\ 0\ 1\ 2), (1\ 1\ 1\ 1), (2\ 1\ 2\ 0), (2\ 2\ 2\ 2), (2\ 0\ 2\ 1)\}. \end{aligned} \tag{1.32}$$

Although both C and C'' are $[4, 2, 2]_3$ codes, it is clear that they are different. Moreover, in accordance with Definition 1.6.7, we can reformat G'' into the standard form as shown below:

$$G'' \to \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & 2 \end{bmatrix}. \tag{1.33}$$

Now, based on Lemma 1.5.7, we can easily determine the associated check matrix H'' of C'', which is defined as follows:

$$H'' = \begin{bmatrix} 2 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}. \tag{1.34}$$

Additionally, Definition 1.6.9 needs to be discussed in order to be used in Chapter 3.

Definition 1.6.9. *Let $M = [u_1\ u_2\ \cdots\ u_n]$ be a matrix. The **multiplicity** of a column u_j, denoted $m(u_j)$, is the number of columns of M in $\langle u_j \rangle$, that is $m(u_j) = |\{i : u_i \in \langle u_j \rangle\}|$.*

In other words, $m(u_j)$ is the number of columns that are scalar multiples of u_j. If M is viewed as a generator matrix of a code C, then column multiplicity corresponds (up to equivalence) to repeated coordinates.

1.7 Generalized Hamming weight

We discuss generalized Hamming weight in this section. Therefore, we begin with a term that will be used to define the generalized Hamming weight.

Definition 1.7.1. *The **support**, denoted* $\mathrm{supp}(C)$*, of a block code C over $\mathbb{F}_q$ is the set of coordinate positions where the codewords in C are not all zero.*

The support of a code C is a set of coordinate positions where the codewords of C are not entirely zero.

Example 1.7.2. *Let C be the code shown in Example 1.5.2, where*

$$C = \{(0\ 0\ 0), (0\ 1\ 1), (1\ 0\ 1), (1\ 1\ 0)\}, \tag{1.35}$$

It was observed that $\mathrm{supp}(C) = \{1, 2, 3\}$*, so* $|\mathrm{supp}(C)| = 3$*. Now, consider another code C' over $\mathbb{F}_2$:*

$$C' = \{(0\ 0\ 0), (0\ 1\ 0), (1\ 0\ 0), (1\ 1\ 0)\}. \tag{1.36}$$

Here $\mathrm{supp}(C') = \{1, 2\}$*, and* $|\mathrm{supp}(C')| = 2$*.*

In addition, an $[n, r]$ subcode of the linear $[n, k, d]_q$ code C is an r dimensional subspace of C. In general, we consider only codes with $|\mathrm{supp}(C)| = n$ when C is an $[n, k, d]_q$ code. Otherwise, C would have a coordinate that is identically zero, which essentially adds no meaningful properties to the code. Such codes are said to be **degenerate**. Unless otherwise specified, the codes considered here are assumed to be non-degenerate; we note that a non-degenerate code may have degenerate subcodes.

Definition 1.7.3. *Let C be an $[n, k, d]_q$ code. The r-th* ***generalized Hamming weight*** *$d_r(C)$ is defined to be the cardinality of the minimal support of an $[n, r]$ subcode of C, $1 \leqslant r \leqslant k$.*

Note that $d_1(C)$ is equal to the minimum distance of C. Moreover, $d_r(C)$ increases as r increases.

Lemma 1.7.4 ([32])**.** *For every linear $[n, k, d]_q$ code C*

$$0 < d(C) = d_1(C) < d_2(C) < \ldots < d_k(C) \leqslant n. \tag{1.37}$$

Example 1.7.5. *Let C be a $[4, 2, 2]_2$ code, where*

$$C = \{(0\ 0\ 0\ 0), (1\ 1\ 0\ 0), (0\ 0\ 1\ 1), (1\ 1\ 1\ 1)\}, \tag{1.38}$$

with generator matrix

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}. \tag{1.39}$$

We can see that $d_1(C) = d(C) = 2$*, and* $d_2(C) = |\operatorname{supp}(C)| = 4$.

The following corollary is deduced by Wei using Lemma 1.7.4.

Corollary 1.7.6 ([32])**.** *(Generalized Singleton bound)*

$$d_r(C) \leqslant n - k + r,\ r = 1, 2, \ldots, k. \tag{1.40}$$

Note that, in particular, Corollary 1.7.6 gives $d(C) \leqslant n - k + 1$. This inequality is known as the Singleton Bound, which we shall discuss in detail in Chapter 2.

Example 1.7.7. *From Example 1.7.5, where*

$$C = \{(0\ 0\ 0\ 0), (1\ 1\ 0\ 0), (0\ 0\ 1\ 1), (1\ 1\ 1\ 1)\}, \tag{1.41}$$

we see that $d_1(C) = 2 < 4 - 2 + 1 = 3$*, and* $d_2(C) = 4 = 4 - 2 + 2$.

In [32], Wei also pointed out the next useful lemma.

Lemma 1.7.8. *Let* C *be a linear* $[n, k, d]_q$ *code and* $C^{\perp}$ *be its dual. Then*

$$\{d_r(C) | r = 1, 2, \ldots, k\} \cup \{n + 1 - d_r(C^{\perp}) | r = 1, 2, \ldots, n - k\} = \{1, 2, \ldots, n\}. \tag{1.42}$$

1.8 Finite projective geometries

Since projective geometry plays an important role in this thesis, the connection between codes and projective geometries will be discussed in this section. For details, the interested reader is referred to [6] or [11]. Let us begin with Definition 1.8.1.

Definition 1.8.1. *The* ***projective space*** $\mathrm{PG}(k-1,q)$ *is the geometry whose* i*-dimensional subspaces are the* $(i+1)$*-dimensional subspaces of the* k*-dimensional vector space over* $\mathbb{F}_q$*, for* $i = 0, \ldots, k-2$*.*

Two projective subspaces are said to be **incident** if their intersection is non-empty, that is to say, they have at least one projective point in common; and are otherwise said to be **skew** (or sometimes **parallel**).

Example 1.8.2. *Let* V *be a* 4*-dimensional vector space over* $\mathbb{F}_3$ *and let* $P = (1\ 2\ 2\ 1)$ *be a point in* V*. If* ℓ *is the* 1*-dimensional subspace generated by* P*, then*

$$\ell = \{(0\ 0\ 0\ 0), (1\ 2\ 2\ 1), (2\ 1\ 1\ 2)\}. \tag{1.43}$$

Now, let Π *be the corresponding projective space* $\mathrm{PG}(3,3)$*. The projective point* Q *corresponding to the one dimensional subspace* ℓ *could therefore be equally described by the coordinates of either of the two non-zero representatives of* ℓ*. That is, both* $(1\ 2\ 2\ 1)$*, and* $(2\ 1\ 1\ 2)$ *represent the same projective point.*

In addition, projective spaces have hyperplanes, which are defined as follows:

Definition 1.8.3. *A* ***hyperplane*** *of* $\mathrm{PG}(k,q)$ *is a subspace of co-dimension* 1*, that is, a subspace of dimension one less than that of the whole space.*

To help us distinguish between vector subspaces and projective subspaces, projective subspaces are referred to as flats.

Definition 1.8.4. *An n-**flat** in $\Pi = \mathrm{PG}(k,q)$ is an n-dimensional projective subspace of Π. That is, 0-flats are projective points; 1-flats are projective lines; 2-flats are projective planes; etc.*

We now discuss the number of l-flats in $\mathrm{PG}(k,q)$.

Theorem 1.8.5. *For $l < k+1$, the number of l-flats in $\mathrm{PG}(k,q)$ is*

$$\frac{\left(q^{k+1}-1\right)\left(q^{k+1}-q\right)\cdots\left(q^{k+1}-q^{l}\right)}{\left(q^{l+1}-1\right)\left(q^{l+1}-q\right)\cdots\left(q^{l+1}-q^{l}\right)}. \tag{1.44}$$

In particular, the number of points in $\mathrm{PG}(k,q)$ is $\frac{q^{k+1}-1}{q-1} = q^k + \cdots + 1$, which is also the number of hyperplanes in $\mathrm{PG}(k,q)$. Still more generally, there are

$$\frac{\left(q^{k-m}-1\right)\cdots\left(q^{k-m}-q^{l-m-1}\right)}{\left(q^{l-m}-1\right)\cdots\left(q^{l-m}-q^{l-m-1}\right)} \tag{1.45}$$

l-flats containing a given m-flat, where $l < k+1$ and $m < l$. In particular, the number of points on any projective line is $q+1$.

Note, from eq. (1.45), that the number of points on a hyperplane is equal to the number of hyperplanes incident with a point. This leads us to one of the most interesting properties of $\mathrm{PG}(k,q)$, which is that the principle of duality holds. We describe this next.

1.8.1 Principle of Duality

Consider a $(k+1)$-dimensional vector space V. Let U be a 1-dimensional subspace of V, and let H be the set containing all vectors $h \in V$ such that $h \cdot u = 0$ for all $u \in U$. It can be easily verified that H is a subspace of V. Furthermore, based on Definition 1.3.15, H is k-dimensional.

As demonstrated in Example 1.8.2, V corresponds to a projective space $\Pi = \mathrm{PG}(k,q)$, H corresponds to a hyperplane of Π, and U corresponds to a

projective point in Π.

From the previous mapping, where the 1-dimensional subspace U is mapped to the subspace H of V, it becomes evident that a projective point represented by U in Π can be mapped to a hyperplane represented by H of Π. This leads to the principle of duality:

For any incidence result about points and hyperplanes of Π, there is always a corresponding dual result regarding hyperplanes and points, where the roles of hyperplanes and points are exchanged.

In other words, any result for points and hyperplanes in projective geometry will have a symmetrical dual result where the roles of hyperplanes and points are swapped. For example, in a projective plane, any two lines meet in a point, and dually, any two points are on one line. Moreover, as eq. (1.45) might indicate, the principle of duality can be generalized as follows:

Let S be an m-flat of Π. In the dual, S is mapped to the $(k-1-m)$-flat $S^{\perp} = \{v \in \Pi : u \cdot v = 0 \text{ for all } u \in S\}$. Hence, let X and Y be two flats in Π, so that $X \subset Y$ if and only if $Y^{\perp} \subset X^{\perp}$. Now, we can deduce the generalized principle of duality:

Any incidence result regarding m-flats and $(k-1-m)$-flats in Π will have a symmetrical dual result in which the roles of $(k-1-m)$-flats and m-flats are interchanged.

1.8.2 Arcs

We start this subsection with the following definition, bringing the vector space notion of linear independence into the projective setting:

Definition 1.8.6. *A set of m points of $\mathrm{PG}(k,q)$ are in **general position** if they are not contained in a $(m-2)$-flat.*

For example, if three points in a plane are not on one line, then we say they are in general position. With that established, we now use the principle of duality to rewrite Definition 1.8.6.

Definition 1.8.7. *A set of m hyperplanes of $\mathrm{PG}(k,q)$ are in **general position** if they are not incident with a common $(m-2)$-flat.*

For instance, if three planes in $\mathrm{PG}(3,q)$ are not incident with the same line, then we say they are in general position.

Definition 1.8.8. *An **n-arc** in $\mathrm{PG}(k,q)$ is a set of n points such that every $k+1$ are in general position.*

An n-arc in $\mathrm{PG}(k,q)$ is a set of n points where no $k+1$ points are contained in a $(k-1)$-flat. Based on that understanding, according to the principle of duality, we can get the next definition.

Definition 1.8.9. *A **dual n-arc** in $\mathrm{PG}(k,q)$ is a collection of $n \geqslant k+1$ hyperplanes in general position.*

More generally, we have the following definitions:

Definition 1.8.10. *An $(\mathbf{n},\mathbf{r})$-**arc** κ in $\Pi = \mathrm{PG}(k,q)$, $k \leqslant r$ is an n-set of points such that each hyperplane of Π incident with at most r points in κ and some hyperplane is incident with $r-1$ points of κ.*

In particular, an (n,k)-arc is an n-arc. Moreover, the principle of duality and Definition 1.8.10 yield the next definition.

Definition 1.8.11. *An **dual** $(\mathbf{n},\mathbf{r})$-**arc** in $\mathrm{PG}(k,q)$, $k \leqslant r$ is an n-set of hyperplanes, at most r of which are incident with a common point and there exist $r-1$ hyperplanes incident with a common point.*

1.8.3 Projective Systems

With previous definitions in mind, we now discuss the relation between codes and projective geometries.

Definition 1.8.12. *Let C be an $[n, k, d]_q$ code with a generator matrix G. The columns of G can be considered as an n-multiset P of points $\lambda_1, \lambda_2, \ldots, \lambda_n$ (or dually, hyperplanes) in $\mathrm{PG}(k-1, q)$ at most $n-d$ per hyperplane (respectively, $n-d$ per point), and there exists at least one hyperplane that contains $n-d$ points (or dually, $n-d$ hyperplanes are incident with a point), called a **projective system** associated with C. If $\lambda \in P$, then $m(\lambda) = |\{i : \lambda_i = \lambda\}|$ is the **multiplicity** of λ (in P).*

Note that, Definition 1.6.9 pertains to the multiplicity of columns in a matrix, while Definition 1.8.12 deals with the multiplicity of hyperplanes in a projective system. These two definitions coincide depending on context.

There is indeed a direct correspondence between linear codes and projective systems. Some authors go so far as defining linear codes by way of the corresponding projective system.

Definition 1.8.13 ([23])**.** *A multiset C of n points in $\mathrm{PG}(k-1, q)$ is defined such that:*

i. Each hyperplane of $\mathrm{PG}(k-1, q)$ meets C in at most $n-d$ points, and

ii. there is a hyperplane meeting C in exactly $n-d$ points.

Such a multiset is called an $[n, k, d]_q$ code.

Based on Definition 1.8.1, a point P in $\mathrm{PG}(k-1, q)$ corresponds to a one dimensional (vector) subspace $\langle P \rangle$ in a k-dimensional vector space over the same field. In other words, if we multiply P by non-zero scalars in $\mathbb{F}_q$, then the corresponding projective point $\langle P \rangle$ is invariant.

As per Definition 1.6.7 (C2), multiplication of any column of a generator matrix G by a non-zero scalar yields an equivalent code. Therefore, columns of a generator matrix of an $[n, k, d]_q$ code can be considered as points (or dually, hyperplanes) in $\mathrm{PG}(k-1, q)$.

Definition 1.8.14. *A linear $[n, k, d]_q$ code is **projective** if every pair of columns in an associated generator matrix are linearly independent.*

That is to say, no two columns represent the same projective point (or dually, hyperplane). Furthermore, it is important to mention that not all linear codes are projective.

Example 1.8.15. *Let G_1 and G_2 be the generator matrices of C_1 and C_2, respectively. In particular, G_1 is defined over $\mathbb{F}_3$, and its representation is as follows:*

$$G_1 = \begin{bmatrix} 1 & 1 & 2 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \tag{1.46}$$

while G_2 is defined over $\mathbb{F}_7$, and it is provided below:

$$G_2 = \begin{bmatrix} 1 & 3 & 1 & 1 \\ 2 & 6 & 0 & 2 \\ 3 & 2 & 2 & 1 \end{bmatrix}. \tag{1.47}$$

In both G_1 and G_2 the first two columns are linearly dependent. The code C_1 has the first two coordinates of each codeword been identical, whereas C_2 is equivalent to a code with the same property.

Chapter 2

AMDS codes and NMDS codes

In this chapter, we first introduce MDS codes. We then discuss AMDS and NMDS codes, and explain why the research community is interested in them. In addition, we will discuss the maximum length of MDS codes and NMDS codes, as it plays an important role in the error-correcting ability of a code. In the final section, we discuss the conditions under which AMDS codes are projective. Subsequently, we prove an upper bound for the dimension of long NMDS codes.

2.1 MDS, AMDS, and NMDS codes

We begin this section with Theorem 2.1.1, as it is significant for understanding the content that follows.

Theorem 2.1.1 ([7]). ***(Singleton bound)*** *A q-ary code C of length n and minimum distance d satisfies*

$$|C| \leqslant q^{n-d+1}. \tag{2.1}$$

In particular, if C is a linear $[n, k, d]_q$ code, then $d \leqslant n - k + 1$.

Proof. Since the code has minimum distance d, we can delete fixed $d - 1$ bits from every codeword, and the remaining codewords of length $n - d + 1$ are mutually

distinct. Therefore, $|C| \leqslant q^{n-d+1}$. Moreover, $|C| = q^k \leqslant q^{n-d+1}$. Therefore, after rearranging the equation, we get $d \leqslant n - k + 1$. □

An MDS code is defined as a code that meets or achieves the Singleton bound.

Definition 2.1.2 ([7]). *A **Maximum Distance Separable** (MDS) code is a code meeting the Singleton bound. In particular, a linear $[n, k, d]_q$ code is MDS if (and only if) $d = n - k + 1$.*

Example 2.1.3 (One dimensional MDS). *For $n > 0$, let C be the code with generator matrix*

$$G = [I_1 \ A] = \left[\underbrace{1 \ 1 \ \cdots \ 1 \ 1}_{n \ terms}\right], \tag{2.2}$$

and check matrix

$$H = \left[-A^T \ I_{n-1}\right], \tag{2.3}$$

where

$$-A^T = \left.\begin{bmatrix} -1 \\ -1 \\ -1 \\ \vdots \\ -1 \end{bmatrix}\right\} n-1. \tag{2.4}$$

Such codes can be constructed (over any alphabet) of arbitrary length, and are of little interest in application. As such, one dimensional codes are considered trivial. In addition, as indicated by eq. (2.2)*,*

$$C = \left\{(\underbrace{0 \ 0 \ \cdots \ 0 \ 0}_{n}), (\underbrace{1 \ 1 \ \cdots \ 1 \ 1}_{n}), (\underbrace{2 \ 2 \ \cdots \ 2 \ 2}_{n})\right\} \tag{2.5}$$

is the repetition code. Moreover, since $d(C) = n = n - k + 1$, *C is also an* $[n, 1, n]_3$ *MDS code.*

Example 2.1.4 (Two dimensional MDS)**.** *Let C be a code over* $\mathbb{F}_3$ *with generator matrix*

$$G = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix}. \tag{2.6}$$

C is a $[4, 2, 3]_3$ *MDS code. This can be seen by either generating all codewords, or extrapolated from an associated check matrix*

$$H = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}. \tag{2.7}$$

One can check that every pair of columns of H is linearly independent, whereas all sets of three columns are linearly dependent, as the columns are two-dimensional. As per Lemma 1.6.2, C is indeed a $[4, 2, 3]_3$ *MDS code.*

The next theorem discusses the relationship between an MDS code and its dual code.

Theorem 2.1.5 ([7])**.** *The dual of a linear* $[n, k, n - k + 1]_q$ *MDS code is a linear* $[n, n - k, k + 1]_q$ *MDS code.*

Example 2.1.6. *As presented in Example 2.1.4, C is an MDS code. Let* $C^{\perp}$ *denote the dual code of C. Furthermore, G is a check matrix of* $C^{\perp}$, *where*

$$G = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{bmatrix}. \tag{2.8}$$

All sets of three columns are linearly dependent since the columns are two dimensional; yet, each pair of columns within G remains linearly independent. Therefore, as indicated by Lemma 1.6.2, $C^{\perp}$ *is also a* $[4, 2, 3]_3$ *MDS code.*

According to Theorem 1.4.9, if a code has a larger minimum distance, then the code can detect and correct more errors. From Theorem 2.1.1 and Definition 2.1.2, MDS codes have the largest minimum distance among codes with the same length, alphabet, and dimension. In other words, MDS codes have the best possible error-correcting ability. Nevertheless, we will see that the maximum length of all known MDS codes is unfortunately quite "small". Regarding the length and the Singleton bound, Walker states the following in [31]:

"*In practice, we want to work with codes which are long with respect to the alphabet size. Thus we look for codes which are long, efficient, and correct many errors, but which perhaps are not optimal with respect to the Singleton Bound.*"

This implies that with a larger value of n, the code can incorporate more redundancies, thereby enhancing its ability to detect and correct errors. Therefore, AMDS and NMDS codes will be introduced later because their error-correcting ability is almost as good as MDS codes, in addition, they are longer than all known MDS codes. The maximal length of MDS and NMDS codes will be discussed in detail in Section 2.2 and Section 2.3, respectively.

The next definition establishes the concept of the Singleton defect, which is a method for measuring the difference between the minimum distance of a code C and the minimum distance of an MDS code with the same length, alphabet, and dimension as C.

Definition 2.1.7 ([16])**.** *With C an $[n, k, d]_q$ code,* $\mathrm{def}(C) = n + 1 - k - d$ *is called the* ***Singleton defect*** *of C.*

Since this chapter mainly focuses on AMDS and NMDS codes, their formal definitions are provided below.

Definition 2.1.8. *A code C is an* ***almost MDS code*** *or an* ***AMDS code*** *for short, if* $\mathrm{def}(C) = 1$. *If C is AMDS and $C^{\perp}$ is also AMDS, then C is said to be a* ***near MDS code*** *or simply an* ***NMDS code****.*

Example 2.1.9 (Trivial AMDS code)**.** *For $n > 0$, let C be the code with generator matrix*

$$G = [I_1 \ A] = \left[\underbrace{1 \ 1 \ \cdots \ 1}_{n-1 \ terms} \ 0\right], \tag{2.9}$$

and check matrix

$$H = \left[-A^T \ I_{n-1}\right], \tag{2.10}$$

where

$$-A^T = \left.\begin{bmatrix} -1 \\ -1 \\ -1 \\ \vdots \\ 0 \end{bmatrix}\right\} n-1. \tag{2.11}$$

It can be easily verified that C is an $[n, 1, n-1]_q$ AMDS code.

Example 2.1.10 (AMDS Code)**.** *Let C be a code over $\mathbb{F}_3$ with a generator matrix G, where*

$$G = \begin{bmatrix} 1 & 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}. \tag{2.12}$$

By applying Lemma 1.6.2, we can confirm that C is a $[6, 3, 3]_3$ AMDS code, as evidenced by an associated check matrix H, where

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 2 & 2 & 2 & 0 & 0 & 1 \end{bmatrix}. \tag{2.13}$$

Furthermore, $C^{\perp}$ is a $[6, 3, 2]_3$ code because G has pairwise linearly dependent columns. Therefore, C is AMDS and not NMDS.

Example 2.1.11 (Trivial NMDS code)**.** *Recall from Example 2.1.9 that C is an AMDS code with generator matrix*

$$G = [I_1 \ A] = \left[\underbrace{1 \ 1 \ \cdots \ 1}_{n-1 \ terms} \ 0 \right]. \tag{2.14}$$

It can be easily verified from G that $C^{\perp}$ is an $[n, n-1, 1]_q$ AMDS code. Therefore, C is NMDS.

Example 2.1.12 (NMDS code)**.** *Let C be a code over $\mathbb{F}_3$ and let G be a generator matrix of C, where*

$$G = \begin{bmatrix} 1 & 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}. \tag{2.15}$$

We can check that C is a $[6, 3, 3]_3$ AMDS code from an associated check matrix H, where

$$H = \begin{bmatrix} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 2 & 2 & 2 & 0 & 0 & 1 \end{bmatrix}. \tag{2.16}$$

Furthermore, $C^{\perp}$ is also a $[6, 3, 3]_3$ AMDS code. The reader can verify this from G. As a result, C is NMDS.

Since the error-correcting ability of AMDS codes is very close to that of MDS codes, we call them almost MDS codes. Furthermore, the notation for Almost MDS (AMDS) codes naturally extends to codes with a Singleton defect $\mathrm{def}(C) \geqslant 1$.

Definition 2.1.13 ([16])**.** *Let C be an $[n, k, d]_q$ code. We say that C is an* $\mathbf{A^s}$***MDS code****, if $s = \mathrm{def}(C)$.*

In contrast to the property mentioned in Theorem 2.1.5, for $s > 0$, the dual of an A^sMDS code need not necessarily be A^sMDS. Therefore, it is essential to define N^sMDS codes, which are generalizations of NMDS codes.

Definition 2.1.14. *Let C be an A^sMDS code. C is* $\mathbf{N^s}$***MDS****, if its dual code $C^\perp$ is an A^sMDS code.*

For notation convenience, A^1MDS and N^1MDS codes are written as AMDS and NMDS codes. In the next chapter, we focus on A^2MDS and N^2MDS codes.

In [12], an alternate definition of NMDS codes based on the generalized Singleton bound is provided. In the following lemma, we prove Definition 2.1.8 is equivalent to that in [12].

Lemma 2.1.15. *A linear $[n, k, d]_q$ code C is near-MDS if and only if*

$$d_i(C) = n - k + i, \text{ for } i = 2, 3, \ldots, k; \tag{2.17}$$

and

$$d_1(C) = n - k. \tag{2.18}$$

Proof. Let us assume that C is an NMDS code, which means $\mathrm{def}(C) = \mathrm{def}(C^\perp) = 1$. We shall prove that eq. (2.17) and eq. (2.18) hold. Because $\mathrm{def}(C) = 1$, we can see that eq. (2.18) follows directly from Definition 2.1.7. Likewise, $\mathrm{def}(C^\perp) = 1$ implies

$d_1(C^\perp) = n - k^\perp = n - (n-k) = k$. Based on Lemma 1.7.4, eq. (2.18) gives

$$d_2(C) \geqslant n - k + 1. \tag{2.19}$$

Since $d_1(C^\perp) = k$, $n + 1 - d_1(C^\perp) = n - k + 1$, so eq. (2.19) and Lemma 1.7.8 give $d_2(C) \geqslant n-k+2$. As a result, according to Lemma 1.7.4, we have $d_i(C) \geqslant n-k+i$ for $2 \leqslant i \leqslant k$. By invoking Corollary 1.7.6, we conclude that $d_i(C) = n - k + i$ for $2 \leqslant i \leqslant k$, thus confirming the validity of eq. (2.17).

Now, for the other direction, assume eq. (2.17) and eq. (2.18) hold. We shall show C is NMDS. By examining eq. (2.18), it can be concluded that C is an AMDS code. Subsequently, it becomes sufficient to show $C^\perp$ is also AMDS. Let $C^\perp$ be denoted as an $[n, k^\perp, d^\perp]_q$ code. According to Lemma 1.7.8, eq. (2.17) and eq. (2.18) give

$$S = \{n + 1 - d_r(C^\perp) | r = 1, 2, \ldots, n-k\} = \{1, 2, \ldots, n-k-1, n-k+1\}. \tag{2.20}$$

By referencing Lemma 1.7.4, we find that $\max(S) = n+1-d_1(C^\perp)$ whence $d_1(C^\perp) = k = n - (n-k) = n - k^\perp$, so $C^\perp$ is AMDS. □

The next Lemma follows from Definition 1.8.13. It provides necessary and sufficient conditions under which a matrix generates an AMDS code.

Lemma 2.1.16. *Let C be an $[n, k, d]_q$ code, and let G be a generator matrix of C. C is an AMDS code if and only if G satisfies the following conditions:*

i. There is at least one linearly dependent set of k columns of G;

ii. any $k + 1$ columns of G are of full rank.

In [13], Dodunekov and Landjev provide necessary and sufficient conditions that must be met for a matrix to generate an NMDS code. However, those conditions are not proved in [13], so for completeness, we provide a proof here.

Theorem 2.1.17. *Let C be an $[n, k, d]_q$ code, and let G be a generator matrix of C. C is an NMDS code if and only if G satisfies the following conditions:*

i. Any set of $k-1$ columns of G is linearly independent;

ii. there is at least one linearly dependent set of k columns of G;

iii. any $k+1$ columns of G are of full rank.

Proof. Let us begin by assuming that C is an NMDS code, which implies that both C and $C^{\perp}$ are NMDS. Based on Definition 1.5.6 and Lemma 2.1.15, $d(C^{\perp}) = n - (n-k) = k$. Since G is a check matrix of $C^{\perp}$, through Lemma 1.6.2, one can get (i.). Conditions (ii.) and (iii.) follow from Lemma 2.1.16.

For the other direction, assume the three conditions hold. From Lemma 2.1.16, (ii.) and (iii.) imply C is an $[n, k, n-k]_q$ AMDS code. Using Lemma 1.6.2, (i.) and (ii.) imply that $d(C^{\perp}) = k$, so $C^{\perp}$ is an $[n, n-k, k]_q$ AMDS code. Therefore, C is NMDS. □

As discussed in Chapter 1, columns of a generator matrix G of a linear $[n, k, d]_q$ code C may be considered as points in $\Pi = \mathrm{PG}(k-1, q)$ constituting a projective system associated with C.

Let C be an NMDS code with a generator matrix G. According to Theorem 2.1.17 (i.), any set of $k-1$ columns of G is linearly independent. From Definition 1.8.1, $k-1$ linearly independent columns of G generate a $(k-2)$-flat. Consequently, the $k-1$ columns, when considered as projective points, cannot be contained in a $(k-3)$-flat. Therefore, by Definition 1.8.6, they are in general position.

In line with Theorem 2.1.17 (ii.), there exists a linearly dependent set of k columns of G. As a result, among these k columns, there exists one that lies within the span of the other $k-1$ columns. In other words, when regarded as projective points, the k columns are in a hyperplane of Π.

Based on Theorem 2.1.17 (iii.), any $k+1$ columns of G are of full rank. Since G is a check matrix for $C^{\perp}$, Proposition 1.3.10 shows that any $k+1$ columns of G have a rank of k. Therefore, as per Definition 1.3.9, when considered as projective points, every set of $k+1$ columns of G are not contained in a common hyperplane of Π.

In this setting, we may reinterpret the conditions of Theorem 2.1.17 as follows:

Theorem 2.1.18 ([22]). *The existence of an $[n,k,d]_q$ NMDS code is equivalent to that of a set S of points in $\Pi = \mathrm{PG}(k-1,q)$ with the following properties:*

i. Every $k-1$ points from S are in general position;

ii. there exist k points from S that lie in a hyperplane of Π;

iii. no $k+1$ points from S lie in a common hyperplane of Π.

Let C be an $[n,k,n-k]_q$ NMDS code with check matrix H. By Lemma 1.6.2, every set of $n-k-1$ columns of H is linearly independent, and there is a linearly dependent set of $n-k$ columns of H. In addition, $C^{\perp}$ is an $[n,n-k,k]_q$ code, so each set of $n-k+1$ columns has full rank; otherwise, it would contradict the minimum distance of $C^{\perp}$. Within the context of the check matrix H, it is possible to reinterpret the conditions stated in Theorem 2.1.17 as follows:

Theorem 2.1.19 ([12]). *A linear $[n,k,d]_q$ code C is near-MDS if and only if a check matrix of C, say H, satisfies the conditions*

i. any set of $n-k-1$ columns of H is linearly independent;

ii. there exist some linearly dependent sets of $n-k$ columns;

iii. any $n-k+1$ columns of H are of full rank.

2.2 MDS main conjecture

This section covers the MDS main conjecture, which posits an upper bound on the maximal length of MDS codes. Over half a century ago, B. Segre [26] proved some groundbreaking results regarding arcs in projective space and posed a question which has now evolved to the main conjecture on MDS codes:

Conjecture 2.2.1 ([5]). *If $k \leqslant q$, then the maximum size $m(k-1,q)$ of an arc in* $\mathrm{PG}(k-1,q)$ *is*

$$m(k-1,q) = \begin{cases} q+2 & \text{if } q \text{ is even and } k \in \{3, q-1\} \\ q+1 & \text{otherwise} \end{cases}. \tag{2.21}$$

Furthermore, in accordance with Definition 1.8.10 and Definition 1.8.12, we can deduce the following lemma:

Lemma 2.2.2. *A projective $[n,k,d]_q$ code and $(n, n-d)$-arcs in* $\mathrm{PG}(k-1,q)$ *are equivalent objects.*

According to Lemma 2.2.2, we can re-state the conjecture as follows:

Conjecture 2.2.3. *Let C be an $[n,k,d]_q$ MDS code with $2 \leqslant k \leqslant q$. If q is even and $k \in \{3, q-1\}$, then $n \leqslant q+2$. Otherwise, $n \leqslant q+1$.*

The statement above is known as the MDS main conjecture. It is important to note that the main conjecture does not pertain to 1-dimensional MDS repetition codes. To avoid trivial cases, $k \geqslant 2$. Moreover, it is well known that the main conjecture holds for 2-dimensional MDS codes (see e.g. [1]).

This conjecture has a long and rich history (see [17], [20], [21], [27], [30], etc.). In 1960, Silverman provided a general upper bound on MDS codes.

Lemma 2.2.4 ([28]). *An $[n,k,d]_q$ MDS code satisfies $n \leqslant q+k-1$ where $k \geqslant 2$.*

After that, in 1988, Bruen et al. proved Corollary 2.2.5.

Corollary 2.2.5 ([10]). *In* $\mathrm{PG}(k,q)$, $q = 2^s$ *where* s *is a positive integer, let* K *be an* n*-arc. Then*

i. $n \leqslant q+1$ *if* $k = 3$.

ii. $n \leqslant q+1$ *if* $k \geqslant 4$ *and* $q \geqslant (k-2)^3$.

iii. For $k \geqslant 5$, *if* $n > q+1$, *then* $n < q + k - \sqrt[3]{q}$.

Following that, in 1990, Blokhuis et al. presented a theorem. To discuss the theorem, the following definition is required:

Definition 2.2.6. *An* n*-arc of* $\Pi = \mathrm{PG}(k,q)$ *is* ***complete*** *if it cannot be extended to an* $(n+1)$*-arc of* Π.

Let us now delve into the aforementioned theorem:

Theorem 2.2.7 ([9]). *Any* $(q+1)$*-arc of* $\mathrm{PG}(3,q)$, q *even and* $q \geqslant 4$ *is complete.*

This theorem confirms that the main conjecture applies to $[n,4,d]_q$ MDS codes where q is even and $q \geqslant 4$.

In 2012, Ball proved the next theorem, which is a major breakthrough towards proving the main conjecture.

Theorem 2.2.8 ([4]). *Let* $q = p^h$, *where* p *is prime. If* $2 < q - p + 1 < k < q - 2$ *then a linear MDS code of dimension* k *over* $\mathbb{F}_q$ *has length at most* $q+1$.

Afterward, Ball and De Beule published [8]. Combining the results from [4] and [8], we obtain the following theorem.

Theorem 2.2.9 ([7]). *Let* $q = p^h$, *where* p *is prime. If* $k \leqslant p$, *then a* k*-dimensional linear MDS code of length* n *satisfies* $n \leqslant q+1$.

In [3], Alderson et al. explained that the columns of a generator matrix G of an MDS code, can be regarded as points belonging to an n-arc in $\mathrm{PG}(k-1,q)$. Therefore, Theorem 2.2.9 can be rewritten as the following:

Theorem 2.2.10. *Let $q = p^h$, where p is prime. If $k \leqslant p$, then an (n,k)-arc in $\mathrm{PG}(k-1,q)$ satisfies $n \leqslant q+1$.*

Specifically, the MDS main conjecture holds over prime fields with conditions applied.

2.3 Maximal length of NMDS codes

MDS codes have the best error-correcting ability among linear codes with fixed length, alphabet and dimension. However, MDS codes are conjectured to be short. Moreover, the number of codewords which are generated by an MDS code can be increased by raising the size of the field $\mathbb{F}_q$ of the MDS code. However, this method requires calculations over a larger field, which can become computationally expensive.

Codes with a larger maximal length need to be explored. With an increasing number of redundancies, a longer non-MDS code may correct more errors than a short MDS code can. Since we still wish to balance efficiency with error-correcting, we first turn to NMDS codes. Hence, some limits on the maximal length of NMDS codes will be discussed in this section using the following notation: Let $m'(k,q)$ be the maximal length of an NMDS code of dimension k over $\mathbb{F}_q$. From Lemma 2.1.16 and Theorem 2.1.17, a two dimensional AMDS code is necessarily NMDS. Moreover, the columns of a corresponding generator matrix is a projective system of points from $\mathrm{PG}(1,q)$, at least one of which has multiplicity 2, and none of which have multiplicity greater than 2. In the maximal case, each point has multiplicity 2, and C is an $[2q+2,2,2q]_q$ NMDS code. Consequently, we have the following:

Lemma 2.3.1. *Any $[n,2,n-2]_q$ AMDS code is NMDS, and $m'(2,q) = 2q+2$.*

Remark 2.3.2. *The second part is shown in [13] with a different proof.*

Dodunekov and Landjev studied the maximal length of NMDS codes over $\mathbb{F}_q$, where $2 \leqslant q \leqslant 5$, in [13]. Similarly, in [24], Marcugini et al. researched the maximal length of NMDS codes over $\mathbb{F}_q$, where $8 \leqslant q \leqslant 11$. Some known results are shown in the following table:

Table 2.1: Bounds on $m'(k, q)$

	q								
$\bar{k}$	2	3	4	5	7	8	9	11	13
2	6	8	10	12	16	18	20	24	28
3	7	9	9	11	15	15	17	21	23
4	8	10	10	12	14	16	16	$20-21$	$21-24$
5		11	11	11	13	15	16	$8-22$	$21-25$
6		12	12	12	$13-14$	$14-15$	$16-17$	$18-23$	$21-26$
7			9	11	$14-15$	$15-16$	$17-18$	$18-24$	$21-27$
8			10	12	$13-16$	$16-17$	$18-19$	$18-25$	$21-28$
9				11	13	$14-18$	$19-20$	$19-26$	$21-29$
10				12	14	15	$20-21$	$20-27$	$21-30$
11					14	15	$16-22$	$18-28$	$21-31$
12					15	16	16	$18-29$	$21-32$
13					15	15	16	$18-30$	$21-33$
14					16	16	17	$18-31$	$21-34$
15						17	17	$18-32$	$21-35$
16						18	18	$20-33$	$21-36$

In the previous section, we saw that the length of MDS codes are generally at most $q+1$. The next section shows there is promise in obtaining strong error-correcting

codes close to MDS with n larger than $q+1$.

2.4 Main result of this chapter

In [12], Dodunekov and Landjev show that not every AMDS code is NMDS. We aim to prove a condition concerning the length of AMDS codes; specifically, if the length of an AMDS code exceeds this condition, the code must be projective.

As discussed in Section 2.2, the main conjecture has been proved for most cases of linear MDS codes. Therefore, we are going to use the main conjecture to enhance the previously mentioned condition.

In the last part of this section, we provide some results on the length of projective NMDS codes.

2.4.1 Projective AMDS Codes

The next lemma, which is proved by Alderson and Bruen in [2], plays an important role in the proof of Corollary 2.4.6, because the multiplicity of hyperplanes is essential to the proof.

Lemma 2.4.1 ([2])**.** *Let C be a linear $[n,k,n-k]_q$ AMDS code $k \geqslant 3$ with an associated projective system of hyperplanes κ. Then no member of κ has multiplicity $m > 2$, and at most one member has multiplicity 2.*

From Theorem 2.1.18 and Lemma 2.4.1, we get the next corollary.

Corollary 2.4.2. *Let C be a linear $[n,k,n-k]_q$ code $k \geqslant 3$. Let κ be the associated projective system of hyperplanes. If C is NMDS, then C is projective.*

In addition, we will show some results using projective systems.

Theorem 2.4.3. *Let C be an $[n, k, n-k]_q$ code, and $k \geqslant 3$. If $n > k+q$, then C is projective.*

Proof. Let C be an $[n, k, n-k]_q$ AMDS code, non-NMDS, with an associated projective system κ of hyperplanes $\lambda_1, \lambda_2, \ldots, \lambda_n$ in $\Pi = \mathrm{PG}(k-1, q)$. By Lemma 2.4.1, there is at most one member of κ that has multiplicity 2. If every member of κ has multiplicity 1, then the code is projective. Now, let $\lambda_n = \lambda_{n-1} = \lambda$.

Let $\Psi = \{\lambda_1, \lambda_2, \ldots, \lambda_{n-2}\}$. According to Lemma 2.1.16 (ii.), any set of $k+1$ columns from G, when regarded as projective points, are in general position. Based on the principle of duality, every $k+1$ members of κ are in general position. Hence, every $k-1$ members of Ψ are in general position.

In line with Definition 1.8.9, the set $S = \{m_i : m_i = \lambda_i \cap \lambda\}$ forms a dual $(n-2)$-arc in λ ($\cong \mathrm{PG}(k-2, q)$). As observed from Section 2.2, an $[n-2, k-1, n-k]_q$ MDS code and a dual $(n-2)$-arc in $\mathrm{PG}(k-2, q)$ are equivalent. In light of Lemma 2.2.4, $n-2 \leqslant q + (k-1) - 1 = q + k - 2$. As a result, $n \leqslant q + k$. □

The next lemma is key to the proof of Theorem 2.4.5.

Lemma 2.4.4. *Let C be an $[n, k, n-k]_q$ AMDS code, and $k \geqslant 3$. If*

$$n > m(k-2, q) + 2, \tag{2.22}$$

then C is projective.

Proof. Assume by way of contradiction, C is an $[n, k, d]_q$ AMDS code, which is not NMDS, with $n > m(k-2, q)+2$. Mimicking the proof of Theorem 2.4.3, we obtain an $[n-2, k-1, n-k]_q$ MDS code. Since $n-2 > m(k-2, q)$, we have a contradiction. □

Combining Conjecture 2.2.1 with Lemma 2.4.4 yields Theorem 2.4.5. Furthermore, since we are going to assume the main conjecture holds in $\mathrm{PG}(k-2,q)$, to avoid trivial cases, $k-2 \geqslant 1$, that is $k \geqslant 3$.

Theorem 2.4.5. *Let C be an $[n,k,n-k]_q$ AMDS code with $k \geqslant 3$, and assume the MDS main conjecture holds in $\mathrm{PG}(k-2,q)$. If*

$$n > \begin{cases} q+4 & \text{if } q \text{ is even and } k \in \{4,q\} \\ q+3 & \text{otherwise} \end{cases}, \tag{2.23}$$

then C is projective.

Proof. As Lemma 2.4.4 shows, if $n > m(k-2,q)+2$, then every AMDS code is projective. In line with Conjecture 2.2.1,

$$m(k-2,q) = \begin{cases} q+2 & \text{if } q \text{ is even and } k \in \{4,q\} \\ q+1 & \text{otherwise} \end{cases}. \tag{2.24}$$

Thus, if

$$n > m(k-2,q)+2 = \begin{cases} q+4 & \text{if } q \text{ is even and } k \in \{4,q\} \\ q+3 & \text{otherwise} \end{cases}, \tag{2.25}$$

then every AMDS code is projective. □

By considering Theorem 2.2.9, we can derive Corollary 2.4.6.

Corollary 2.4.6. *Let $q = p^h$, where p is prime, and $3 \leqslant k \leqslant p$. If $n > q+3$, then every $[n,k,n-k]_q$ code is projective.*

The corollary above offers a theoretical insight, demonstrating that long AMDS codes exhibit projective properties. Therefore, we can arrange codes in categories according to shared characteristics so that researchers can understand them better, and develop better coding methods, in other words, long and efficient codes with good error-correcting abilities.

Recall that every line in $\mathrm{PG}(k-1,q)$ is incident with $q+1$ points. Therefore, by duality, every $(k-3)$-flat is incident with exactly $q+1$ hyperplanes of $\mathrm{PG}(k-1,q)$.

The following result also appears in [12]. We provide a new and shorter proof.

Theorem 2.4.7. *If $n > k+q$, then every $[n,k,n-k]_q$ code is near-MDS.*

Proof. Let C be an $[n,k,n-k]_q$ AMDS code with a projective system P of points in $\Pi = \mathrm{PG}(k-1,q)$. Assume by way of contradiction, C is AMDS, non-NMDS, and $n > k+q$. According to Lemma 2.1.16 and Theorem 2.1.17, there exists at least one AMDS code with a generator matrix including sets of $k-1$ columns that are linearly dependent. That is to say, there exist $k-1$ points from P that are contained in a $(k-3)$-flat, denoted as Ω, in Π. The number of hyperplanes of Π that contain Ω is $q+1$, and any two such hyperplanes intersect precisely within Π. Moreover, any hyperplane of Π contains at most k points of P. Consequently, we derive that $n \leqslant (k-1) + (q+1)\cdot 1 = k+q$, leading to a contradiction. □

2.4.2 An upper bound on the dimension of NMDS codes

In [29], Tsfasman et al. introduced the following theorem:

Theorem 2.4.8. *Let C be a linear code with an associated projective system P. The r-th generalized Hamming weight of $C^{\perp}$ is*

$$d_r^{\perp} = \min\{|Q| : Q \subset P,\ |Q| - \dim\ \mathrm{lin}\langle Q\rangle = r\}, \tag{2.26}$$

where $\langle Q\rangle$ is the linear span of Q, and $\dim\ \mathrm{lin}\langle Q\rangle$ *is its linear dimension (which is greater by* 1 *than the projective dimension of $\langle Q\rangle$).*

To avoid trivial cases, we assume $d \geqslant 1$ for all $[n,k,d]_q$ NMDS codes discussed in this section. Recall from Example 2.1.11 that one dimensional NMDS codes can be constructed of arbitrary length.

Now, consider a two dimensional $[n, 2, n-2]_q$ NMDS code, namely C, with an associated projective system P in $\Pi = \mathrm{PG}(1, q)$. In this case, Π is a projective line, and P is a collection of projective points on Π. According to Theorem 2.1.18 (iii.), every point of P has multiplicity at most 2. Therefore, $n \leqslant 2(q+1) = 2q+2$.

Example 2.4.9. *Let G be a generator matrix of a code C, where*

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}. \tag{2.27}$$

Let H be an associated check matrix of C, where

$$H = \begin{bmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{bmatrix}. \tag{2.28}$$

As a result, C is a $[4, 2, 2]_3$ NMDS code.

More generally, let C be an $[n, k, n-k]_q$ NMDS code, where $k \geqslant 3$, with an associated projective system P of points $\lambda_1, \lambda_2, \ldots, \lambda_n$ in $\Pi = \mathrm{PG}(k-1, q)$. Since C is NMDS, $C^\perp$ is an $[n, n-k, k]_q$ NMDS code. According to Theorem 2.4.8, $k = d_1^\perp = \min\{|Q| : Q \subset P, |Q| - \dim \mathrm{lin}\langle Q\rangle = 1\}$. Hence, there exist k elements of P spanning a hyperplane in Π, and by the minimality of Q, any collection of $k-1$ or fewer are in general position. In particular, any set of $k-2$ points in P spans a $(k-3)$-flat. Let Ω be such a flat. Through Ω, there are precisely $q+1$ hyperplanes, the union of which is Π. Furthermore, based on the dimension argument, the $q+1$ hyperplanes are each pairwise incident in exactly Ω. Since C is AMDS, each hyperplane through Ω contains at most 2 additional points of P. Therefore, we have $|P| = n \leqslant k - 2 + (q+1) \cdot 2 = 2q + k$.

Lemma 2.4.10. *If C is an $[n, k, d]_q$ NMDS code, where $k \geqslant 2$, then $m'(k, q) \leqslant 2q+k$.*

Remark 2.4.11. *The same bound appears in [13] with a different proof.*

For any q and k, we may always construct a $[k+1, k, 1]_q$ NMDS code, as the following example illustrates.

Example 2.4.12. *Let G be a generator matrix of C, where*

$$G = \underbrace{\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & 0 & 1 \\ & & & \vdots & & \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}}_{k \times k}. \tag{2.29}$$

Clearly, G generates a $[k+1, k, 1]_q$ NMDS code.

The previous example shows that $[k+1, k, 1]_q$ NMDS codes always exist. However, if $n > k+1$, then we do obtain constraints. As discussed in this section, for $k \geqslant 2$, an NMDS code satisfies $n \leqslant 2q + k$. Since $C^\perp$ is also NMDS, we have $n \leqslant 2q + k^\perp = 2q + (n-k)$.

Lemma 2.4.13. *Let C be an $[n, k, n-k]_q$ code with $n > k+1$. If C is NMDS, then $k \leqslant 2q$.*

Chapter 3

AAMDS codes and NNMDS codes

Although AMDS and NMDS codes are longer than MDS codes, they are still not generally considered long. In this chapter, another type of code with a larger maximum length will be explored, beginning with the definition of this code type. We then generalize some results from Chapter 2. In the last part of this chapter, we will present our main results.

3.1 Codes of Singleton defect two

The binary field, $\mathbb{F}_2$, is foundational in computer systems, which are inherently binary due to the efficiency of storing information in a binary format. For example, user inputs, like messages, cause fluctuations in the computer's electrical voltage. These fluctuations are then converted into digital data: an increase in voltage is represented by a '1', and a decrease by a '0'. Consequently, before implementing error-correcting codes, messages must first be translated into this binary format. As a result, in practical applications, error-correcting codes typically operate over the binary field $\mathbb{F}_2$.

As discussed in Chapter 2, the maximum length of binary NMDS codes is bounded

by $2q + k = 2 \cdot 2 + k = 4 + k$. In general, the k bits will be used to record messages, leaving only 4 bits for redundancies. Consequently, while NMDS codes are longer than MDS codes, they are still relatively short compared to NNMDS codes. Since NNMDS codes are a type of AAMDS codes, we will first introduce AAMDS codes.

Definition 3.1.1. *A code C is called an* ***almost almost MDS code*** *or simply an* ***AAMDS code****, if* $\mathrm{def}(C) = 2$.

In other words, AAMDS codes are codes with a Singleton defect of two.

Example 3.1.2. *Let C be a $[7, 4, 2]_3$ code with a generator matrix G, where*

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}. \tag{3.1}$$

We can observe that $def(C) = (7 - 4 + 1) - 2 = 2$, meaning C is AAMDS. This result can be confirmed using the associated check matrix of C, namely H, where

$$H = \begin{bmatrix} 1 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.2}$$

It is evident that every column of H is linearly independent, and there are pairwise linearly dependent columns, such as columns one and five.

Furthermore, similar to how AMDS codes and NMDS codes are defined, NNMDS codes will also be defined as follows:

Definition 3.1.3. *If C is AAMDS and $C^{\perp}$ is also AAMDS, then C is a* ***near near MDS code*** *or simply an* ***NNMDS code****.*

Example 3.1.4. *Let C be a $[7,4,2]_3$ code with a generator matrix G, where*

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 \end{bmatrix}. \tag{3.3}$$

In addition, let H be an associated check matrix of C, where

$$H = \begin{bmatrix} 2 & 1 & 0 & 0 & 1 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}. \tag{3.4}$$

Applying Lemma 1.6.2 yields the conclusion that C is NNMDS.

Note that AAMDS codes can be represented as A^2MDS codes, and NNMDS codes can be denoted as N^2MDS codes.

To avoid trivial cases, all $[n,k,d]_q$ codes discussed in this chapter have $d > 0$. Inspired by Lemma 2.1.15, we have the following:

Lemma 3.1.5. *A linear $[n,k,d]_q$ code C, where $k \geqslant 3$, is N^2MDS if and only if*

$$d_i(C) = n - k + i, \text{ for } i = 3, 4, \ldots, k; \tag{3.5}$$

and

$$d_2(C) = n - k \text{ or } n - k + 1; \tag{3.6}$$

and

$$d_1(C) = n - k - 1. \tag{3.7}$$

Proof. Let us first assume that C is N^2MDS, so $\mathrm{def}(C) = \mathrm{def}(C^\perp) = 2$. We can now prove that eq. (3.5), eq. (3.6), and eq. (3.7) hold. In accordance with Definition 2.1.7,

eq. (3.7) is true because $\text{def}(C) = 2$. Therefore, referring to Lemma 1.7.4 and Corollary 1.7.6, we can deduce the following:

$$n - k \leqslant d_2(C) \leqslant n - k + 2. \tag{3.8}$$

Since $\text{def}(C^\perp) = 2$, $d_1(C^\perp) = n - k^\perp - 1 = k - 1$. Based on Lemma 1.7.8, $d_2(C) \neq n-k+2$. Consequently, $d_2(C) = n-k$ and $d_2(C^\perp) = n-k+1$, or $d_2(C) = n-k+1$ and $d_2(C^\perp) = n - k$, respectively. As a result, eq. (3.6) holds. This implies that $n-k+3 \leqslant d_3(C) \leqslant n-k+3$. Hence, $d_3(C) = n-k+3$. Thus, as per Lemma 1.7.4 and Corollary 1.7.6, $d_i(C) = n - k + i$, for $3 \leqslant i \leqslant k$. In other words, eq. (3.5) is valid.

Next, let us assume that eq. (3.5), eq. (3.6), and eq. (3.7) hold. We then show that C is N^2MDS. Based on eq. (3.7), we can conclude that C is A^2MDS. Now, it is sufficient to show that $C^\perp$ is also A^2MDS. Let $C^\perp$ be denoted as an $[n, k^\perp, d^\perp]_q$ code. In light of Lemma 1.7.8, eq. (3.5) and eq. (3.6) yield

$$\begin{aligned} S &= \{n + 1 - d_r(C^\perp) | r = 1, 2, \ldots, n - k\} \\ &= \{1, 2, \ldots, n - k - 3, n - k - 2, n - k + 1 \text{ or } n - k, n - k + 2\}. \end{aligned} \tag{3.9}$$

From Lemma 1.7.4, we find that $\max(S) = n+1-d_1(C^\perp)$ whence $d_1(C^\perp) = k-1 = n - (n - k) - 1$. As a result, we conclude that $C^\perp$ is A^2MDS. □

As we will see in the next section, the lemma mentioned above may not be applicable to two dimensional N^2MDS codes.

3.1.1 One Dimensional AAMDS and Two Dimensional NNMDS codes

We start the discussion with a trivial case where the code is one dimensional.

Example 3.1.6 (One dimensional A^2MDS code)**.** *Let C be an $[n, 1, n-2]_q$ A^2MDS code with a generator matrix G. Recall from Example 2.1.3 that an associated generator matrix G' of a one dimensional MDS code is as follows:*

$$G' = \left[\underbrace{1\ 1\ \cdots\ 1\ 1}_{n\ terms}\right]. \tag{3.10}$$

If we replace any two non-zero terms in G' with 0s, we obtain G as:

$$G = [I_1\ A] = \left[\underbrace{1\ 1\ \cdots\ 1}_{n-2\ terms}\ 0\ 0\right]. \tag{3.11}$$

By comparing G with G', we can see that $\mathrm{def}(C) = 2$ meaning G is a generator matrix of a repetition $[n, 1, n-2]_q$ A^2MDS code. We can confirm that C is not N^2MDS by examining the associated check matrix H of C:

$$H = \left[-A^T\ I_{n-1}\right], \tag{3.12}$$

where

$$-A^T = \left.\begin{bmatrix} -1 \\ -1 \\ -1 \\ \vdots \\ -1 \\ 0 \\ 0 \end{bmatrix}\right\} n-1. \tag{3.13}$$

We can observe that $C^{\perp}$ is an $[n, n-1, 1]_q$ AMDS code. Hence, C is A^2MDS, non-N^2MDS.

Note that, one dimensional N^2MDS codes will not be discussed here. This is because, if C is an $[n, 1, n-2]_q$ N^2MDS code, then $C^{\perp}$ is an $[n, n-1, 0]_q$ N^2MDS code. As previously mentioned, all codes covered in this chapter have $d > 0$. Now, let us proceed to two dimensional A^2MDS codes.

Example 3.1.7 (Two dimensional A^2MDS code)**.** *Let C be a $[5, 2, 2]_3$ code with a generator matrix G, where*

$$G = \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}. \tag{3.14}$$

We can verify that the code is A^2MDS from an associated check matrix H of C, where

$$H = \begin{bmatrix} 1 & 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.15}$$

We can observe that every column of H is linearly independent, and there exist pairwise linearly dependent columns, such as columns two and three. In addition, every column in G is non-zero, so $C^{\perp}$ is not a $[5, 3, 1]_3$ A^2MDS code. It is evident that C is a $[5, 2, 2]_3$ A^2MDS, non-N^2MDS code.

With Example 3.1.7 established, we can now proceed to two dimensional N^2MDS codes.

Example 3.1.8 (Two dimensional N^2MDS code)**.** *Let G be a generator matrix of a $[6, 2, 3]_3$ N^2MDS code C, where*

$$G = \begin{bmatrix} 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \end{bmatrix}. \tag{3.16}$$

In addition, let H be an associated check matrix of C, where

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.17}$$

Based on Lemma 1.6.2, we can deduce that C is N^2MDS.

When we apply Lemma 3.1.5 to the example above, we obtain $d_2(C) = 5 = 6-2+1$. As per the proof of Lemma 3.1.5, we expect $d_2(C^\perp) = 6 - 2 = 4$. However, in the above example, we find that $d_2(C^\perp) = 3 \neq 4$. This indicates that Lemma 3.1.5 does not pertain to two dimensional N^2MDS codes.

3.1.2 Generator Matrices and Check Matrices of NNMDS codes

Since not all A^2MDS codes are N^2MDS, it is essential to discuss a set of necessary and sufficient conditions under which a matrix generates an N^2MDS code.

Theorem 3.1.9. *Let C be an $[n, k, d]_q$ code, where $k \geqslant 2$, and let G be a generator matrix of C. C is an N^2MDS code if and only if G satisfies the following conditions:*

i. Any set of $k-2$ columns of G is linearly independent;

ii. there is at least one linearly dependent set of $k-1$ columns of G;

iii. there exist $k+1$ columns of G that are not of full rank;

iv. any $k+2$ columns in G are of full rank.

Proof. For the "only if" part, let us assume that C is an $[n, k, n-k-1]_q$ N^2MDS code with a generator matrix G. Assume, without loss of generality, G is in reduced row echelon form. According to Definition 3.1.3, we have that C is an $[n, k, n-k-1]_q$ code and its dual code $C^\perp$ is an $[n, n-k, k-1]_q$ code. Now, invoking the results from Lemma 1.6.4 and Lemma 1.6.6, we can establish that a generator matrix G of C is a check matrix of $C^\perp$. Therefore, as asserted in Lemma 1.6.2, (i.) and (ii.) are true. In addition, (iii.) is satisfied. This is because, if all $k+1$ columns are of full rank, then every codeword contains at most k zeros, implying that the code has $d \geqslant n-k \neq n-k-1$. To prove (iv.), we will offer a proof by contradiction. Assume there exist $k+2$ columns in G that are not of full rank. In that case, there would exist a row with $k+2$ zeros in G. This leads to a contradiction because the N^2MDS code would then have a codeword with a weight of at most $n-k-2$, which is inconsistent with its definition.

For the "if" part, assume G satisfies (i.), (ii.), (iii.), and (iv.). According to Lemma 1.6.4 and Lemma 1.6.6, G is a check matrix of $C^\perp$. Since G satisfies (i.) and (ii.), as stated in Lemma 1.6.2, $C^\perp$ is an $[n, n-k, k-1]_q$ A^2MDS code. Additionally, condition (iii.) implies that $d \leqslant n-k-1$. Moreover, as G also satisfies (iv.), based on Definition 1.3.11, every codeword of C has at most $k+1$ zeros. Therefore, $d \geqslant n-k-1$. Hence, $d = n-k-1$, and C is N^2MDS. □

Furthermore, we can simplify Theorem 3.1.9 when $n > q+k$.

Theorem 3.1.10. *Let C be an $[n, k, d]_q$ code, where $k \geqslant 2$, and $n > q+k$, with a generator matrix G. C is an N^2MDS code if and only if G satisfies the following conditions:*

i. Any set of $k-2$ columns of G is linearly independent;

ii. there is at least one linearly dependent set of $k-1$ columns of G;

iii. any $k+2$ columns in G are of full rank.

Proof. We prove that when $n > q+k$, (i.), (ii.), and (iii.) together imply the existence of $k+1$ columns in G that are not of full rank. Given that C is an $[n, k, n-k-1]_q$ N^2MDS code, it follows that $C^{\perp}$ is an $[n, n-k, k-1]_q$ N^2MDS code. Let P be an associated projective system of points of C. In accordance with Theorem 2.4.8, there exist $k-1$ points of P contained in a $(k-3)$-flat. Let Ω be such a flat. As discussed in Section 2.4.2, there exist $q+1$ hyperplanes incident with Ω. Since $n > q+k$, each hyperplane must include more than one additional point of P. This implies the existence of at least one hyperplane that contains m points of P, where $m > (k-1)+1 = k$. In other words, $m \geqslant k+1$. Now, we can observe the presence of $k+1$ points of P that do not generate $\mathrm{PG}(k-1, q)$, indicating the existence of $k+1$ columns in G that are not of full rank. □

As discussed in Chapter 1, the columns in a generator matrix G of a linear $[n, k, d]_q$ code C can be viewed as points in $\Pi = \mathrm{PG}(k-1, q)$. Consider an $[n, k, n-k-1]_q$ N^2MDS code C with generator matrix G. In keeping with Theorem 3.1.9 (i.), any set of $k-2$ columns of G is linearly independent. As shown in Definition 1.8.1, these $k-2$ columns in G generate a $(k-3)$-flat and, when regarded as projective points, cannot be contained in a $(k-4)$-flat in Π. In light of Definition 1.8.6, these $k-2$ points are in general position.

According to Theorem 3.1.9 (ii.), there exists at least one linearly dependent set of $k-1$ columns of G, meaning that one column in the set can be expressed as a linear combination of the other $k-2$ columns. As previously mentioned, every set of $k-2$ columns of G generates a $(k-3)$-flat. As a consequence, there exists at least one set of $k-1$ points contained in a $(k-3)$-flat.

In light of Theorem 3.1.9 (iii.), there exist $k+1$ columns of G that are of rank at most $k-1$, indicating the presence of $k+1$ points lying in a hyperplane of Π.

Based on Theorem 3.1.9 (iv.), all sets of $k+2$ columns in G are of full rank. According to Proposition 1.3.10, every combination of $k+2$ columns has rank k. As stated in Definition 1.3.9, this implies that these $k+2$ columns generate a k-dimensional vector space. In other words, these $k+2$ points are not contained in a common hyperplane of Π.

This setting provides the following:

Theorem 3.1.11. *The existence of an $[n,k,d]_q$ N^2MDS code, where $k \geqslant 3$, is equivalent to that of a set S of points in $\Pi = \mathrm{PG}(k-1,q)$ with the following properties:*

i. Every set of $k-2$ points from S is in general position;

ii. there exist $k-1$ points from S lying on a $(k-3)$-flat in Π;

iii. there are $k+1$ points from S lying in a hyperplane of Π;

iv. no $k+2$ points from S lie in a common hyperplane of Π.

Furthermore, since generator matrices and check matrices are associated with each other, it behooves us to interpret Theorem 3.1.9 within the context of check matrices.

Theorem 3.1.12. *A linear $[n,k,d]_q$ code C, where $n \geqslant k+2$, is N^2MDS if and only if a check matrix H of C satisfies the following conditions:*

i. All sets of $n-k-2$ columns of H are linearly independent;

ii. there exists at least one linearly dependent set of $n-k-1$ columns;

iii. there exist $n-k+1$ columns of H that are not of full rank;

iv. any $n-k+2$ columns in H are of full rank.

Proof. Assuming C is an N^2MDS code with a check matrix H, it is important to note that H is also a generator matrix of $C^\perp$, meaning $C^\perp$ is an $[n, n-k, k-1]_q$ N^2MDS code. As established in Theorem 3.1.9, we have the above conditions.

Considering the opposite direction, assuming (i.), (ii.), (iii.), and (iv.) hold. Theorem 3.1.9 implies that $C^{\perp}$ is an N^2MDS code. Hence, C is also an N^2MDS code. □

Moreover, Theorem 3.1.10 can also be understood as follows:

Theorem 3.1.13. *Let C be a $[n, k, d]_q$ code, where $n > q + k$, with a check matrix H. C is an N^2MDS code if and only if H satisfies the following conditions:*

i. Any set of $n - k - 2$ columns of H is linearly independent;

ii. there is at least one linearly dependent set of $n - k - 1$ columns of H;

iii. any $n - k + 2$ columns in H are of full rank.

3.2 AAMDS codes in projective space

As observed in Section 3.1, columns in a generator matrix of an A^2MDS code are viewed as a set of points in a projective space. Although we briefly discussed the relation between N^2MDS codes and the points in their associated projective spaces, readers may still question the difference between A^2MDS and N^2MDS codes in projective geometry. Consequently, this section aims to answer this question.

Let C be an $[n, k, n - k - 1]_q$ N^2MDS code with generator matrix G. According to Theorem 3.1.9 (i.), all sets of $k - 2$ columns of G are linearly independent. As a result, when $k \geqslant 4$, C is projective. For $k = 3$, pairwise linearly dependent columns may exist because $k - 2 = 1$.

To demonstrate the case where C is A^2MDS, we must obtain the following lemma, which is directly given by Definition 1.8.13:

Lemma 3.2.1. *Let C be a $[n, k, d]_q$ code, where $k \geqslant 2$, with a generator matrix G. C is A^2MDS if and only if G satisfies the following conditions:*

i. there exist $k+1$ columns of G that are not of full rank;

ii. any $k+2$ columns in G are of full rank.

As previously discussed, a generator matrix of an A^2MDS code may have pairwise linearly dependent columns. It is important to note that there are generator matrices of A^2MDS codes without pairwise linearly dependent columns.

Example 3.2.2. *Let C be a $[6,3,2]_3$ A^2MDS code with the following generator matrix G:*

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}. \tag{3.18}$$

Furthermore, for any $[n,k,n-k-1]_q$ A^2MDS code, it is necessary that $k+2 \leqslant n$. This is because if $k+1 \geqslant n$, then it would result in $n-k-1 \leqslant 0$. Additionally, $[k+2,k,1]_q$ A^2MDS codes always exist.

Example 3.2.3. *Consider the $[k+2,k,1]_q$ code, which can be represented with the following generator matrix G:*

$$G = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 2 & 1 \\ & & & \vdots & & & & \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 1 \\ \underbrace{0 & 0 & 0 & \cdots & 0 & 1}_{k \times k} & 0 & 0 \end{bmatrix}. \tag{3.19}$$

If we pick the first $k-1$ columns of G and combine them with the last two columns, then we have $(k-1)+2 = k+1$ columns that are not of full rank. In addition, any $k+2$ columns in G are of full rank. According to Lemma 3.2.1, C is an A^2MDS code for any value of k.

Moreover, based on this observation, we can derive the following key conclusions:

Lemma 3.2.4. *If C is an $[n, k, n-k-1]_q$ A^2MDS code, where $k \geqslant 2$, with a generator matrix G, then no column in G has a multiplicity of $m > 3$.*

Proof. Let G be a generator matrix of an A^2MDS code C. We now prove Lemma 3.2.4 by contradiction. Assume that G contains a column with multiplicity m, where $m \geqslant 4$. Moreover, assume, without loss of generality, that G is in reduced row echelon form. If $m \geqslant k+2$, then we can choose the m columns to form a set of $k+2$ columns that are not of full rank. Otherwise, from G, we select $k+2-m$ linearly independent columns. We then choose another column from G that is linearly independent from these $k+2-m$ columns and has multiplicity m. This selection results in a set of $k+2$ columns. However, the rank of this set is only $(k+2-m)+1 < k$, contradicting Lemma 3.2.1 (ii.). □

Remark 3.2.5. *Lemma 3.2.4 does not pertain to the case where C is one dimensional as C is a repetition code in this situation.*

Having addressed the above trivial case, we will now focus on more complex scenarios. Therefore, let $k \geqslant 2$. In the generator matrix G where columns may have multiplicity 2 or 3, these situations will be examined separately.

In the case where columns have a multiplicity of $m = 2$, if one column already has multiplicity $m = 2$, then all other columns can either be mutually distinct or, at most, one additional column may also have a multiplicity of $m = 2$.

Lemma 3.2.6. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code where $k \geqslant 2$, with a generator matrix G. If there are two columns in G have a multiplicity of $m = 2$, then all other columns are mutually distinct.*

Proof. Let C be an A^2MDS code with generator matrix G. Assume, by way of contradiction, that there are at least three columns in G each having a multiplicity

of $m \geqslant 2$. Following the approach used in the proof of Lemma 3.2.4, we obtain a set of $k+2$ columns which is not of full rank. Hence, we have a contradiction. □

By employing a proof method similar to the one used previously, we can establish the following lemma:

Lemma 3.2.7. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code where $k \geqslant 2$, with a generator matrix G. If G contains a column with a multiplicity of $m = 3$, then all the remaining columns in G must be mutually distinct.*

Combining the insights from Lemma 3.2.4, Lemma 3.2.6, and Lemma 3.2.7 together, we deduce the next theorem.

Theorem 3.2.8. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code where $k \geqslant 2$, with a generator matrix G. No column in G has a multiplicity of $m > 3$. If there is one column that has a multiplicity of $m = 3$ or two columns have a multiplicity of $m = 2$, then all other columns in G are mutually distinct.*

As previously observed in Chapter 1, columns of a generator matrix G for an $[n, k, n-k-1]_q$ A^2MDS code can be regarded as points or hyperplanes in $\mathrm{PG}(k-1, q)$. As a result, we provide the following interpretation of Theorem 3.2.8:

Theorem 3.2.9. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $k \geqslant 2$, with an associated projective system of hyperplanes κ. No member of κ has multiplicity $m > 3$. If there is a member that has multiplicity $m = 3$ or if there are two members that have multiplicity $m = 2$, then all other members of κ are mutually distinct.*

3.3 Main result of this chapter

This section is divided into two parts: the first part focuses on projective A^2MDS codes, and the second part addresses the maximum length of A^2MDS codes.

3.3.1 Projective AAMDS Codes

Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $k > 3$ and with an associated projective system κ of hyperplanes $\lambda_1, \lambda_2, \ldots, \lambda_n$ in $\Pi = \mathrm{PG}(k-1, q)$. If C is not projective, then there are three cases involving multiplicities.

In the first case, there is a member of κ that has a multiplicity $m = 3$, say $\lambda_n = \lambda_{n-1} = \lambda_{n-2} = \lambda$. According to Theorem 3.1.11 (iv.), at most $k+1$ members of κ are incident with a common point. Since $(k+1)-3 = k-2$, the set $S = \{m_i : m_i = \lambda_i \cap \lambda,\ i = 1, \ldots, n-3\}$ forms a dual $(n-3)$-arc in λ. As a result, $n-3 \leqslant m(k-2, q)$.

In the second case, let $\lambda_n = \lambda_{n-1} = \lambda$. As discussed previously, the set $S = \{m_i : m_i = \lambda_i \cap \lambda,\ i = 1, \ldots, n-2\}$ forms a dual $(n-2, k-1)$-arc in λ because $(k+1)-2 = k-1$. The arc is equivalent to an $[n-2, k-1, n-k-1]_q$ NMDS code. Hence, $n-2 \leqslant m'(k-1, q)$.

In the final case, let $\lambda_n = \lambda_{n-1} = \lambda_i$, and $\lambda_{n-2} = \lambda_{n-3} = \lambda_j$. Furthermore, λ_i is incident with λ_j on a common $(k-3)$-flat, so let Ω be such a flat. Since $(k+1)-4 = k-3$, the set $S = \{m_i : m_i = \lambda_i \cap \Omega\}$ forms a dual $(n-4)$-arc in Ω. Consequently, $n-4 \leqslant m(k-3, q)$. Now, we have the following result:

Lemma 3.3.1. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $k > 3$. If $n > m'(k-1, q) + 2$, then C is projective.*

3.3.2 Maximum Length of AAMDS Codes

Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k+2$, and $k \geqslant 5$, with an associated generator matrix G. This code is also associated with a projective system P of points $\lambda_1, \lambda_2, \ldots, \lambda_n$ in $\Pi = \mathrm{PG}(k-1, q)$. In accordance with Theorem 2.4.8,

$$n - d = \max\{|P \cap H|\colon H \text{ is a hyperplane of } \Pi\} = k+1. \tag{3.20}$$

Firstly, let us assume that $C^{\perp}$ is an A^2MDS code, implying that C is N^2MDS. In this scenario, we find that

$$d_1^{\perp} = \min\{|Q| : Q \subset P, |Q| - \dim \operatorname{lin}\langle Q\rangle = 1\} = k - 1. \tag{3.21}$$

Consequently, there exist $k-1$ elements of P that span a $(k-3)$-flat of Π. Let Ω be such a flat. As observed in Chapter 2, there are precisely $q+1$ hyperplanes through Ω, and the union of those hyperplanes is Π. Since $k+1-(k-1) = 2$, each hyperplane through Ω holds at most 2 additional points from P. This implies that $|P| = n \leqslant (k-1) + 2 \cdot (q+1) = k + 2q + 1$. Based on the previous discussion, we can now present the following lemma:

Lemma 3.3.2. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k+2$, and $k \geqslant 5$. If C is N^2MDS, then $n \leqslant k + 2q + 1$.*

Moreover, since $C^{\perp}$ is an A^2MDS code, we have $n \leqslant k^{\perp} + 2q + 1 = n - k + 2q + 1$, which implies $k \leqslant 2q + 1$. With this insight, we can now conclude the next lemma:

Lemma 3.3.3. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k+2$, and $k \geqslant 5$. If C is N^2MDS, then $k \leqslant 2q + 1$.*

Next, let us consider the scenario where $C^{\perp}$ is an $[n, n-k, k]_q$ AMDS code. In this case,

$$d_1^{\perp} = \min\{|Q| : Q \subset P, |Q| - \dim \operatorname{lin}\langle Q\rangle = 1\} = k, \tag{3.22}$$

so there exist k elements of P spanning a hyperplane of Π. Additionally, we note that any $k-2$ columns of G are linearly independent as $d(C^{\perp}) = k$. Hence, these columns span a $(k-3)$-flat of Π. To derive the following lemma, we can adopt a similar approach to that used in the proof of Lemma 3.3.2. Since $k+1-(k-2) = 3$, it follows that $n \leqslant (k-2) + 3 \cdot (q+1) = k + 3q + 1$, leading to the next lemma:

Lemma 3.3.4. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k+2$, and $k \geqslant 5$. If $C^\perp$ is AMDS, then $n \leqslant k+3q+1$.*

Furthermore, as C is A^2MDS, not AMDS, in line with Theorem 2.4.7, we have the condition $n \leqslant q + k^\perp = q + n - k$. Therefore, $k \leqslant q$, leading to the following lemma:

Lemma 3.3.5. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k+2$, and $k \geqslant 5$. If $C^\perp$ is AMDS, then $k \leqslant q$.*

In addition, we can now deduce the following theorem:

Theorem 3.3.6. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $k \geqslant 5$. If $n > k+2q$, then* $\mathrm{def}(C^\perp) \leqslant 2$.

Proof. We prove Theorem 3.3.6 by contradiction. Let C be an $[n, k, n-k-1]_q$ A^2MDS code with an associated projective system P of points in $\Pi = \mathrm{PG}(k-1, q)$. Assume $n > k+2q$ and $\mathrm{def}(C^\perp) \geqslant 3$. As a result, $d^\perp \leqslant k-2$, implying there exist $k-2$ points of P on a $(k-4)$-flat. Applying the principle of duality, we obtain a projective system P' of hyperplanes in Π, and there exist $k-2$ elements of P' incident with a common plane Ω. According to the dimension argument, each other member of P' meets Ω in at least a line. Furthermore, based on Definition 1.8.12, no point is incident with more than $k+1$ members of P'. Since $(k+1)-(k-2) = 3$, C includes a dual $(n-k+2, 3)$-arc in Ω. The arc is equivalent with an $[n-k+2, 3, n-k-1]_q$ NMDS code. In line with Lemma 2.3.1, $n-k+2 \leqslant 2q+2$, which gives $n \leqslant k+2q$, which is a contradiction. □

Finally, consider the case where $C^\perp$ is an $[n, n-k, k-2]_q$ A^3MDS code. In this scenario, we find that

$$d_1^\perp = \min\{|Q| : Q \subset P,\ |Q| - \dim \mathrm{lin}\langle Q\rangle = 1\} = k-2. \tag{3.23}$$

As a result, there are $k-2$ elements of P that span a $(k-4)$-flat of Π. We can then pick a point λ_i such that $\dim \text{proj}\langle Q \cup \lambda_i \rangle = k-3$, where $\dim \text{proj}\langle Q \cup \lambda_i \rangle$ is the projective dimension of the flat spanned by $(Q \cup \lambda_i)$. Furthermore, the existence of such a λ_i is ensured by the condition $\dim \text{lin} < C >= k$. This construction results in a $(k-3)$-flat of Π. Let Ω be such a flat. Since there are $k-2+1 = k-1$ points of P in Ω, we deduce that $n \leqslant (k-1) + 2 \cdot (q+1) = k + 2q + 1$. For this reason, we obtain the following lemma:

Lemma 3.3.7. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k+2$, and $k \geqslant 5$. If $C^\perp$ is A^3MDS, then $n \leqslant k + 2q + 1$.*

Moreover, as observed previously,

Lemma 3.3.8. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k+2$, and $k \geqslant 5$. If $C^\perp$ is A^3MDS, then $k \leqslant 2q + 1$.*

From the above discussion, we derive a general upper bound on the length of A^2MDS codes.

Theorem 3.3.9. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k+2$, and $k \geqslant 5$. If $C^\perp$ is AMDS, then $n \leqslant k + 3q + 1$. Otherwise, $n \leqslant k + 2q + 1$.*

Proof. Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k+2$, and $k \geqslant 5$. For the proof of $n \leqslant k + 3q + 1$, please refer to Lemma 3.3.4. We can now use mathematical induction to show $n \leqslant k + 2q + 1$.

Base Case: Let $C^\perp$ be an A^2MDS code. Because of that, C is N^2MDS. Please refer to the proof of Lemma 3.3.2 for details.

Inductive Hypothesis: Let $C^\perp$ be an A^iMDS code. Assume $n \leqslant k + 2q + 1$ for all i, where $3 \leqslant i \leqslant (h-1)$.

Inductive Step: Prove $n \leqslant k + 2q + 1$, when $C^{\perp}$ is an $[n, n-k, k-h+1]_q$ A^hMDS code. Since

$$d_1^{\perp} = \min\{|Q| : Q \subset P,\, |Q| - \dim \text{lin}\langle Q\rangle = 1\} = k - h + 1, \tag{3.24}$$

then there exist $k - h + 1$ elements of P spanning a $(k - h - 1)$-flat of Π, and any $k - h$ elements of P are linearly independent. We can then pick a point of P, namely λ, such that $\dim \text{proj}\langle Q \cup \lambda\rangle = k - h$. Furthermore, Let $C^{\perp'}$ be an $[n, n-k, k-h+2]_q$ $A^{(h-1)}$MDS code with projective system P' of points. Moreover, $C^{\perp'}$ has $d_1^{\perp'} = \min\{|Q'| : Q' \subset P', |Q'| - \dim \text{lin}\langle Q'\rangle = 1\} = k - h + 2$, and $\dim \text{proj}\langle Q'\rangle = (k - h + 2) - 2 = k - h$. According to the inductive hypothesis, the theorem holds when $C^{\perp'}$ is an $A^{(h-1)}$MDS code. Consequently, we can find $h - 3$ additional points, namely $\lambda_1, \lambda_2, \ldots, \lambda_{h-3}$, such that $\dim \text{proj}\langle Q \cup \lambda \cup \lambda_1 \cup \lambda_2 \cup \ldots \cup \lambda_{h-3}\rangle = k - 3$, otherwise it contradicts the code is k-dimensional. Hence, $n \leqslant (k - h + 1 + 1 + h - 3) + 2 \cdot (q + 1) = k + 2q + 1$. Thus, the theorem is true. □

In addition, we can derive the following result:

Theorem 3.3.10. *Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k + 2$, and $k \geqslant 5$. If $C^{\perp}$ is AMDS, then $k \leqslant q$. Otherwise, $k \leqslant 2q + 1$.*

Chapter 4

Conclusion and Future Research

4.1 Conclusion

In this thesis, we discussed codes with Singleton defects of one and two. Firstly, we introduced the definitions of AMDS and NMDS codes. Subsequently, we compared the error-correcting abilities of MDS codes with those of NMDS codes. We observed that although MDS codes have the best error-correcting ability among linear codes with fixed length, alphabet and dimension, they are short in length. Therefore, a longer NMDS code may have the ability to detect and correct more errors than a shorter MDS code. Afterward, we established that, provided the main conjecture holds, every $[n, k, n-k]_q$ AMDS code becomes projective when $n > q + 3$. We concluded our discussion on codes with a Singleton defect of one by demonstrating that for every $[n, k, n-k]_q$ NMDS code with $n > k + 1$, we have $k \leqslant 2q$.

After that, we delved into the study of AAMDS and NNMDS codes. We began the discussion by defining AAMDS and NNMDS codes. Subsequently, after associating codes with a Singleton defect of two with projective systems, we deduced the following: If we have an $[n, k, n-k-1]_q$ A^2MDS code, where $k \geqslant 2$, with an associated projective system of hyperplanes κ, then no member of κ will have a

multiplicity $m > 3$. If there is a member that has multiplicity $m = 3$ or if there are two members that have multiplicity $m = 2$, then all other members of κ will be mutually distinct.

We concluded our discussion on codes with a Singleton defect of two by proving the following result: Let C be an $[n, k, n-k-1]_q$ A^2MDS code, where $n > k+2$, and $k \geqslant 5$. If $C^\perp$ is AMDS, then $n \leqslant k + 3q + 1$. Otherwise, $n \leqslant k + 2q + 1$.

4.2 Future Research

i. In Section 2.4.1, we discussed that when the main conjecture holds, every $[n, k, n-k]_q$ AMDS code will be projective if $n > q+3$. Future research could explore the conditions under which a code C, being AMDS and satisfying $n > q + 3$, could also qualify as NMDS.

ii. Future research could utilize the results from Section 2.4.2 to derive a general upper bound on the length of AMDS codes.

iii. In this thesis, we discussed codes with Singleton defects of one and two. Future research could aim to generalize our results to codes with a Singleton defect of n, where $n > 2$.

Bibliography

[1] Tim Alderson, *Bruck nets and 2-dimensional codes*, Bull. Inst. Combin. Appl. **52** (2008), 33–44.

[2] TL Alderson and Aiden A Bruen, *Maximal AMDS codes*, Applicable Algebra in Engineering, Communication and Computing **19** (2008), 87–98.

[3] TL Alderson, Aiden A Bruen, and Robert Silverman, *Maximum distance separable codes and arcs in projective spaces*, Journal of Combinatorial Theory, Series A **114** (2007), no. 6, 1101–1117.

[4] Simeon Ball, *On large subsets of a finite vector space in which every subset of basis size is a basis*, J. Eur. Math. Soc **14** (2012), no. 3, 733–748.

[5] ———, *On sets of vectors of a finite vector space in which every subset of basis size is a basis*, Journal of the European Mathematical Society (EMS Publishing) **14** (2012), no. 3, 1–18.

[6] ———, *Finite geometry and combinatorial applications*, vol. 82, Cambridge University Press, 2015.

[7] ———, *A course in algebraic error-correcting codes*, Springer, 2020.

[8] Simeon Ball and Jan De Beule, *On sets of vectors of a finite vector space in which every subset of basis size is a basis ii*, Designs, Codes and Cryptography **65** (2012), no. 1-2, 5–14.

[9] Aart Blokhuis, Aiden A Bruen, and Joseph A Thas, *Arcs in PG (n, q), MDS-codes and three fundamental problems of B. Segre—some extensions*, Geometriae Dedicata **35** (1990), 1–11.

[10] Aiden A Bruen, Joseph A Thas, and Aart Blokhuis, *On MDS codes, arcs in PG (n, q) with q even, and a solution of three fundamental problems of B. Segre*, Inventiones mathematicae **92** (1988), 441–459.

[11] Peter Jephson Cameron, *Combinatorics: topics, techniques, algorithms*, Cambridge University Press, 1994.

[12] Stefan Dodunekov and Ivan Landgev, *On near-mds codes*, Journal of Geometry **54** (1995), no. 1, 30–43.

[13] Stefan M Dodunekov and Ivan N Landjev, *Near-MDS codes over some small fields*, Discrete Mathematics **213** (2000), no. 1-3, 55–65.

[14] Keldon Wayne Drudge, *Extremal sets in projective and polar spaces*, Faculty of Graduate Studies, University of Western Ontario, 1998.

[15] David Steven Dummit and Richard M Foote, *Abstract algebra*, vol. 3, Wiley Hoboken, 2004.

[16] Andreas Faldum and Wolfgang Willems, *Codes of small defect*, Designs, Codes and Cryptography **10** (1997), 341–350.

[17] Massimo Giulietti, Fernanda Pambianco, Fernando Torres, and Emanuela Ughi, *On large complete arcs: odd case*, Discrete mathematics **255** (2002), no. 1-3, 145–159.

[18] Jim Hefferon, *Linear algebra fourth edition*, 2020, `https://leanpub.com/linalgebra`(visited 2024-04-17).

[19] Raymond Hill, *A first course in coding theory*, Oxford University Press, 1986.

[20] JWP Hirschfeld and G Korchmáros, *On the embedding of an arc into a conic in a finite plane*, Finite Fields and Their Applications **2** (1996), no. 3, 274–292.

[21] ———, *On the number of rational points on an algebraic curve over a finite field*, Bulletin of the Belgian Mathematical Society-Simon Stevin **5** (1998), no. 2/3, 313–340.

[22] Ivan Landjev and Assia Rousseva, *The main conjecture for near-MDS codes*, WCC2015-9th International Workshop on Coding and Cryptography 2015, 2015.

[23] Ivan N Landjev, *Linear codes over finite fields and finite projective geometries*, Discrete Mathematics **213** (2000), no. 1-3, 211–244.

[24] Stefano Marcugini, Alfredo Milani, and Fernanda Pambianco, *NMDS codes of maximal length over F_q,* $8 \leqslant q \leqslant 11$, IEEE Transactions on Information Theory **48** (2002), no. 4, 963–966.

[25] Steven Roman, S Axler, and FW Gehring, *Advanced linear algebra*, vol. 3, Springer, 2005.

[26] Beniamino Segre, *Curve razionali normali e k-archi negli spazi finiti*, Annali di Matematica Pura ed Applicata **39** (1955), 357–379.

[27] ———, *Le geometrie di galois*, Annali di Matematica pura ed applicata **48** (1959), 1–96.

[28] Robert Silverman, *A metrization for power-sets with applications to combinatorial analysis*, Canadian Journal of Mathematics **12** (1960), 158–176.

[29] Michael Tsfasman, Serge Vlăduţ, and Dmitry Nogin, *Algebraic geometric codes: basic notions*, vol. 139, American Mathematical Society, 2022.

[30] José Felipe Voloch, *Complete arcs in galois planes of non-square order*, Advances in finite geometries and designs (1991), 401–406.

[31] Judy L Walker, *Codes and curves*, vol. 7, American Mathematical Soc., 2000.

[32] Victor K Wei, *Generalized hamming weights for linear codes*, IEEE Transactions on information theory **37** (1991), no. 5, 1412–1418.

Vita

Candidate's full name: Zhipeng Zhang

Universities attended (with dates and degrees obtained):
University of New Brunswick Saint John (2024)
Master of Science in Mathematics
University of Alberta (2021)
Bachelor of Science in Computer Science and Mathematics

Publications: N/A

Conference Presentations: N/A