Double Circulant Self-Dual Codes from Legendre Sequences

by

Najme Sahami
B.Sc., Kourdestan University, 2003
M.Sc., University of Yazd, 2007
Ph.D., University of Kashan, 2020

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

MASTER OF APPLIED SCIENCE

in the Department of Electrical and Computer Engineering

Double Circulant Self-Dual Codes from Legendre Sequences

by

Najme Sahami
B.Sc., Kourdestan University, 2003
M.Sc., University of Yazd, 2007
Ph.D., University of Kashan, 2020

Supervisory Committee

Dr. T. Aaron Gulliver, Supervisor
(Department of Electrical and Computer Engineering)

Dr. Majid Mazrooei, Departmental Member
(Department of Electrical and Computer Engineering)

ABSTRACT

A Legendre sequence $\mathbf{s}$ of length p, p an odd prime, is used to create a circulant matrix $\mathbf{S}$. An alternative Legendre sequence $\tilde{\mathbf{s}}$ is employed to form another circulant matrix $\tilde{\mathbf{S}}$. By concatenating these two matrices, we obtain the matrix $\mathbf{D}'$ which is used to form a bordered double circulant code with length $2p+2$ and dimension $k = p+1$ over $\mathbb{F}_q$, q a prime, and $\gcd(p,q) = 1$. We demonstrate that for $p = 2qm-1$ the code generated by $\mathbf{D} \triangleq \left[\begin{array}{c|c|c} 11 & \mathbf{1}^T & \mathbf{1}^T \\ \hline \mathbf{10} & \mathbf{S} & \tilde{\mathbf{S}} \end{array}\right]$ over $\mathbb{F}_q$ is self-dual.

The idempotent elements of the ideals generated by $s(x)$ and $\tilde{s}(x)$, the leading polynomials of the $p \times p$ matrices $\mathbf{S}$ and $\tilde{\mathbf{S}}$, respectively, for $p = 4kq-1$ are investigated and used to find the rank of these matrices over $\mathbb{F}_q$. We define a specific row-column permutation of $\left[\mathbf{S}|\tilde{\mathbf{S}}\right]$ which leads to a non-singular matrix, revealing that these codes can be defined as a direct sum of codes.

Contents

List of Tables

Notation

$wt(c)$	Weight of a codeword c
$C^{\perp}$	Dual code of code C
(x, y)	Inner product of two vectors x and y
$\oplus$	Direct sum
$\mathbb{F}_q$	Field with order q
$\mathbb{F}_q^n$	Vector space over $\mathbb{F}_q$
$\mathbb{F}_q[x]$	Ring of polynomials in x over $\mathbb{F}_q$
$\langle a \rangle$	Principal ideal generated by a
$\equiv$	Congruence
mod p	Modulo p
$x \mid y$	x divides y without remainder
$\bigcap$	Intersection
dim	Dimension

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor, Dr. T. Aaron Gulliver, for his exceptional guidance and support throughout my research. His request to generalize the construction of binary double-circulant codes from Legendre sequences, which he and Dr. Matthew Parker previously developed in their personal communication, to the non-binary case, was a challenging and rewarding task that significantly shaped this project. Although I did not directly communicate with Dr. Parker, his earlier work with Dr. Gulliver provided a crucial foundation for my research.

I am deeply grateful to Dr. Majid Mazrooei, a member of my supervisory committee, for his thorough review of my thesis draft and his valuable feedback which greatly improved the work.

I also want to thank Janice Closson, Ashleigh Carlsen, and Dan Mai who always helped me.

I would like to also thank my mom, dad, and siblings.

To my mom and dad!

Chapter 1

Introduction

Coding theory studies techniques to correct errors in data transmission and storage based on concepts such as finite fields, polynomials, group theory, and linear algebra. These mathematical structures form the foundation for designing efficient codes to detect and correct errors due to noise, interference, or physical damage. Coding theory is essential for guaranteeing the reliability of data as it is transferred across networks and stored in media.

In 1947, at Bell Labs, Richard Hamming made a key contribution to coding theory. Hamming worked with calculating machines and the loss of results due to errors sparked his interest in error detection and correction. His insight led to the concept of Hamming distance [14] and this paved the way for Hamming codes, the first family of error-correcting codes. The primary challenge in coding theory is to generate good codes with a small number of parity check symbols and large minimum distance for a given dimension. In addition, given a minimum distance, the goal is to find a code with a large dimension. However, these goals often conflict with each other, requiring the optimization of one parameter while keeping the other two fixed.

The best-known error-correcting codes, such as those of Hamming, Golay, Bose-Chaudhuri-Hocquenghem [19], and Reed-Solomon [29], have algebraic structures that allow for efficient encoding and decoding. Moreover, cyclic codes typically possess good error-correction abilities while being simple to use.

Linear Code

A linear $[n, k]$ code C over $\mathbb{F}_q$ is a k-dimensional vector subspace of $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the finite field of size q, q a prime power. The parameter n is called the length of C. The elements of a code C are called codewords and have the form $c = (c_1, c_2, \ldots, c_n)$,

where c_i is an element of $\mathbb{F}_q$, $i = 1, 2, \ldots n$. The weight of a codeword is the number of non-zero coordinates. Denote the weight of a codeword c by $\mathrm{wt}(c)$. The minimum weight of C is the smallest weight among all non-zero codewords of C. An $[n, k, d]_q$ code is an $[n, k]$ code over $\mathbb{F}_q$ with minimum weight d. Two linear codes are equivalent if one can be obtained from the other by a permutation of coordinates and/or a permutation of the symbols in a given position.

Optimal Linear Code

An optimal linear code has the largest possible minimum distance d for given values of n and k. This is important because the minimum distance d determines the ability of a code to detect and correct errors. Specifically, a code with minimum distance d detects up to $d-1$ errors and corrects up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

Dual Code

The dual code $C^\perp$ of C is defined as

$$C^\perp = \{x \in \mathbb{F}_q^n \mid (x, y) = 0 \quad \forall y \in C\}, \tag{1.1}$$

where (x, y) denotes the inner product of two vectors. It is clear that $C^\perp$ is a linear subspace of dimension $n-k$ over $\mathbb{F}_q$, so $C^\perp$ is an $[n, n-k, d^\perp]$ code, where $d^\perp$ denotes the minimum distance of $C^\perp$. A code C is called self-dual if $C = C^\perp$. In this case $k = n - k$, so $n = 2k$ and thus n must be even and $k = n/2$. An $[n, k]$ code C can be defined by a generator matrix G or a parity-check matrix H [20].

Generator Matrix

G is a $k \times n$ matrix such that the codewords $c \in C$ are generated as

$$c = mG,$$

where m is a row vector of length k.

Parity-Check Matrix

H is an $(n-k) \times n$ matrix such that a vector c is a codeword if and only if

$$Hc^T = \mathbf{0}.$$

Direct Sum

Let C_i be an $[n_i, k_i, d_i]$ code, $i \in \{1, 2\}$ over $\mathbb{F}_q$. Their direct sum is the $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]$ code

$$C_1 \oplus C_2 = \{(c_1, c_2) \,|\, c_1 \in C_1, c_2 \in C_2\}.$$

Let G_i and H_i be the generator matrix and the parity check matrix for C_i, respectively, then

$$G_1 \oplus G_2 = \left[\begin{array}{c|c} G_1 & \mathbf{0} \\ \hline \mathbf{0} & G_2 \end{array}\right],$$

and

$$H_1 \oplus H_2 = \left[\begin{array}{c|c} H_1 & \mathbf{0} \\ \hline \mathbf{0} & H_2 \end{array}\right],$$

are a generator matrix and parity check matrix for $C_1 \oplus C_2$ [20, Section 1.5.4].

Linear Complementary Dual (LCD) Codes

A pair of linear codes C and $C^\perp$ over $\mathbb{F}_q$ is called linear complementary dual (LCD) if their direct sum $C \oplus C^\perp$ spans the entire space $\mathbb{F}_q^n$. In other words, the two codes have complementary dimensions and their intersection is trivial, i.e., $C \cap C^\perp = \{\mathbf{0}\}$ [4].

Cyclic Code

A cyclic code is a linear code in which every cyclic shift of a codeword results in another codeword

$$(c_0, c_1, \ldots, c_{n-1}) \in C \rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in C.$$

Algebra of Polynomials Over $\mathbb{F}_q$ Modulo $x^n - 1$

Let $R = \mathbb{F}_q[x]$ be the ring of all polynomials in x over $\mathbb{F}_q$ and let f be the ideal in R generated by $x^n - 1$. The polynomials of degree less than n form a complete set of representatives for the residue classes of the ring R modulo f. The quotient ring R modulo f, when considered as an additive group, is isomorphic to $R_{(n)} = \mathbb{F}_q[x]/\langle x^n - 1\rangle$. This isomorphism is given by

$$a_0 x^0 + a_1 x^1 + \cdots + a_{n-1} x^{n-1} \longleftrightarrow (a_0, a_1, \ldots, a_{n-1}).$$

Thus, we identify codewords of length n with polynomials of degree less than n. The

polynomial $xa(x)$ modulo $(x^n - 1)$ corresponds to the vector $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$. This means that multiplication by x in the ring R modulo f results in a cyclic shift. Consequently, a linear code C is cyclic if and only if C is an ideal in R modulo f. Every ideal in $R_{(n)} = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ is a principal ideal, meaning it is generated by a polynomial $g(x)$ of degree less than n that divides $x^n - 1$. This polynomial $g(x)$ is referred to as the generator polynomial of the cyclic code C. For cyclic codes of length n over $\mathbb{F}_q$, the condition $\gcd(n, q) = 1$ is imposed to ensure that $x^n - 1$ does not have repeated roots [1].

Theorem 1.0.1. *[24, §3, Theorem 1] Let C be a non-zero ideal in R_n, i.e., a cyclic code of length n.*

1. *There is a unique monic polynomial $g(x)$ of minimal degree in C.*
2. *$C = \langle g(x)\rangle$, i.e., $g(x)$, is a generator polynomial of C.*
3. *$g(x)$ divides $x^n - 1$.*
4. *Any $c(x) \in C$ can be written uniquely as $c(x) = f(x)g(x)$ in $\mathbb{F}_q[x]$, where $f(x) \in \mathbb{F}_q[x]$ has degree $< n - r$, $r = \deg g(x)$. The dimension of C is $n - r$. Thus, the message $f(x)$ becomes the codeword $f(x)g(x)$.*

In this chapter, we provide the definitions and key properties of circulant matrices, group algebra, and quadratic residues modulo a prime p. We then introduce double circulant codes which are generated by circulant matrices formed using quadratic residue sets.

1.1 Group Algebra

Group algebras can be defined more generally for any group and over any field. However, in the context of coding theory, we will focus on finite groups and finite fields.

Definition 1.1.1. Let G be a finite group written multiplicatively and $\mathbf{K}$ a finite field. The group algebra of G over $\mathbf{K}$ consists of formal linear combinations

$$\alpha = \sum_{g \in G} \alpha_g g, \text{ where } \alpha_g \in \mathbf{K}.$$

Given

$$\alpha = \sum_{g \in G} \alpha_g g \quad \text{and} \quad \beta = \sum_{g \in G} \beta_g g,$$

we have

$$\alpha = \beta \Leftrightarrow \alpha_g = \beta_g, \text{ for all } g \in G.$$

The support of an element $\alpha \in \mathbf{K}G$ is

$$\text{supp}(\alpha) = \{g \in G \mid \alpha_g \neq 0\}.$$

The representation $\mathbf{K}G$ depends on the field $\mathbf{K}$, in particular, the characteristic of $\mathbf{K}$.

Theorem 1.1.2. *[1, Theorem 3.3.1]. Let $\mathscr{I}$ be an ideal of $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ and $\gcd(q, n) = 1$. There exists a unique polynomial $e(x) \in \mathscr{I}$, known as the idempotent, with the following properties*

(i) $e^2(x) = e(x)$, i.e., $e(x)$ is idempotent.

(ii) $e(x)$ generates the ideal $\mathscr{I}$.

(iii) For every polynomial $a(x) \in \mathscr{I}$, $a(x)e(x) = a(x)$. In other words, $e(x)$ acts as a unit for $\mathscr{I}$.

The following theorem extends this concept to the intersection and sum of ideals, and demonstrates how idempotents behave under these operations.

Theorem 1.1.3. *[23, Lemma 2.11]. Let $\mathscr{I}_1$ and $\mathscr{I}_2$ be ideals in R_n with $\gcd(n, q) = 1$ and idempotents $e_1(x)$ and $e_2(x)$. Then*

(i) $\mathscr{I}_1 \cap \mathscr{I}_2$ has idempotent $e_1(x)e_2(x)$,

(ii). $\mathscr{I}_1 + \mathscr{I}_2$, has idempotent $e_1(x) + e_2(x) - e_1(x)e_2(x)$.

In the context of coding theory, circulant matrices play an important role, especially when considering their relationship with group algebras. Notably, circulant matrices formed from elements of a finite group G over a field $\mathbb{F}_q$ are closely related to the elements of the group algebra $\mathbb{F}_q G$. This connection highlights the properties and structure of circulant matrices used in coding theory. A circulant matrix is defined as follows.

Definition 1.1.4. A circulant matrix is a square matrix of size n with elements a_i from the ring R, where each row is a right shift of the previous one. We denote this matrix as $A = \text{circ}(a_0, a_1, \ldots, a_{n-1})$, and has the form

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \ldots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{bmatrix}. \tag{1.2}$$

Rows and columns are numbered from 0 to $n-1$. An element $a_k = a_{j-i}$ (row i, column j) is determined solely by $(j-i)$ [21].

Circulant matrices are fully described by the polynomial derived from their leading row

$$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \pmod{x^n - 1}, \tag{1.3}$$

which is denoted by the leading polynomial of the circulant matrix. It is well known that the algebra of $n \times n$ circulant matrices over $\mathbb{F}_q$ is isomorphic to the algebra of polynomials in the ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.

Remark 1.1.5. [33]. Let the set of all $n \times n$ circulant matrices over $\mathbb{F}_q$ be denoted by $C_n\mathbb{F}_q$. Let $G = \langle x \rangle$ be the cyclic group of order n. Then the mapping

$$\phi : \mathbb{F}_q G \to C_n(\mathbb{F}_q)$$

defined by

$$\phi\left(\sum_{i=0}^{n-1} a_i x^i\right) = \text{circ}(a_0, a_1, \ldots, a_{n-1}),$$

is an isomorphism from $\mathbb{F}_q G$ to $C_n(\mathbb{F}_q)$.

From this, we can conclude that the isomorphism between the algebra of polynomial $a(x)$ modulo $x^n - 1$ and circulants over $\mathbb{F}_q$ is thorough. In other words, when we multiply two polynomials $a(x)$ and $b(x)$ modulo $x^n - 1$, the result is identical to the leading polynomial of the circulant product AB, where A and B are the circulant matrices associated with $a(x)$ and $b(x)$, respectively [21]. Using this relationship, a polynomial $a(x)$ is regarded as invertible if there exists a polynomial $a(x)^{-1}$ such that

$a(x)a(x)^{-1} = 1$ modulo $(x^n - 1)$. A^T is a circulant matrix corresponding to the polynomial $a^T(x) = a_0 + a_{n-1}x + \cdots + a_1x^{n-1}$. The transpose polynomial $a(x)^T$, which corresponds to the first column of the matrix A, can be defined as

$$a(x)^T = \sum_{i=0}^{n-1} a_i x^{n-i} \qquad \text{mod } (x^n - 1).$$

Matrix A is called orthogonal if $AA^T = I$. Thus, the polynomial $a(x)$ is said to be an orthogonal polynomial if

$$a(x)a(x)^T = 1 \qquad \text{mod } (x^n - 1).$$

This implies that $a(x)$ is invertible in $\mathbb{F}_q/\langle x^p - 1\rangle$ [21].

Theorem 1.1.6. *[28, Theorem 8.1]. In the algebra of the polynomials modulo $x^n - 1$, a subspace is a cyclic subspace if only and if it is an ideal.*

Theorem 1.1.7. *[30, Theorem 1.14]. Let U and W be subspaces of a vector space V. Then*

$$dim\ (U + W) = dim\ U + dim\ W - dim\ (U \cap W). \tag{1.4}$$

Corollary 1.1.8. *The rank of an $n \times n$ circulant A over the $\mathbb{F}_q$ is the dimension of the principal ideal generated by the leading polynomial $a(x)$ in $\mathbb{F}_q[x]/\langle x^p - 1\rangle$.*

Proof. According to Remark 1.1.5 and Theorem 1.1.6, the dimension of the ideal generated by $a(x) = \sum_{i=0}^{n-1} a_i x^i$ as a cyclic subspace is the same as the dimension of the subspace spanned by the $n \times n$ circulant matrix formed by $a(x)$. The vector subspace generated by a circulant matrix is the set of all vectors obtained by multiplying the circulant matrix by any vector in $\mathbb{F}_q^n$. Since the rank of the matrix equals the number of linearly independent rows (or columns), it determines the dimension of the vector subspace generated by the matrix. Therefore, the dimension of the vector space generated by a circulant matrix is equal to the rank of the matrix. □

1.2 Double Circulant Codes

We now define double circulant codes which are a specific class of linear error-correcting codes derived from double circulant matrices. These codes have applications in various fields such as telecommunications, data storage, and cryptography.

Definition 1.2.1. Let $\mathbf{D}'$ and $\mathbf{D}$ be matrices of the form

$$\mathbf{D} = \begin{bmatrix} \mathbf{P} & \tilde{\mathbf{P}} \end{bmatrix}, \tag{1.5}$$

and

$$\mathbf{D} = \left[\begin{array}{cc|c} 11 & \mathbf{1}^T & \mathbf{1}^T \\ \mathbf{10} & \mathbf{P} & \tilde{\mathbf{P}} \end{array}\right], \tag{1.6}$$

respectively, where $\mathbf{P}$ and $\tilde{\mathbf{P}}$ are $n \times n$ circulant matrices, $\mathbf{1}$ is the $n \times 1$ all-ones vector and $\mathbf{0}$ is the $n \times 1$ all-zeroes vector. The codes generated by $\mathbf{D}'$ and $\mathbf{D}$ are called double circulant and bordered double circulant codes, respectively.

There are several good reasons to examine and investigate double circulant codes.

1. Numerous good codes such as quadratic residue codes, symmetry codes, and extended cyclic codes over $\mathbb{F}_4$ and their binary images are double circulant [1].
2. The encoding of double circulant codes is simple.
3. Many known self-dual codes are double-circulant [3, 8, 9, 10, 15].

1.3 Partition of Quadratic Residue Circulants

Let p be a prime and a be an integer in the set $\{1, 2, \ldots, p-1\}$. If the powers of a generate all residue classes coprime to p, then a is a primitive root modulo p. The quadratic residues modulo p are the even powers of a mod p and the quadratic non-residues modulo p are the odd powers of a modulo p [2, 17]. We denote $\mathscr{A} = \{a^{2i}\}$ as the set of quadratic residues modulo p and $\mathscr{B} = \{a^{2i+1}\}$ as the set of quadratic non-residues modulo p. There are $\frac{p-1}{2}$ residues and $\frac{p-1}{2}$ non-residues modulo p, i.e., there are $(2t-1)$ quadratic residues modulo $(p = 4t-1)$ and $2t$ quadratic non-residues modulo $p = 4t+1$ [21].

Example 1.3.1. Let $p = 7$ so $a = 3$ is primitive root modulo p. The sequence of powers of $a = 3$ forms the residue set modulo 7 in a consecutive manner as follows

$\mathbb{Z}_7^*$	3^1	3^2	3^3	3^4	3^5	3^6
$\mathscr{A}$		2		4		1
$\mathscr{B}$	3		6		5	

The set of residues, denoted by $\mathscr{A} = \{1, 2, 4\}$, is in the first row of the table (even powers of 3) and the set of non-residues, denoted by $\mathscr{B} = \{3, 5, 6\}$, is in the second row (odd powers of 3), with both sets containing three elements.

Let $p = 4t - 1$ be a prime. The polynomials for the sets $\mathscr{A}$ and $\mathscr{B}$ are defined as

$$l(x) = \sum_{l \in \mathscr{A}} x^l \quad \text{and} \quad n(x) = \sum_{n \in \mathscr{B}} x^n. \tag{1.7}$$

Given that the residues and non-residues cover all residues modulo p, we can rewrite the sum of their polynomials as

$$l(x) + n(x) = \sum_{i=1}^{p-1} x^i. \tag{1.8}$$

This is because every residue and non-residue modulo p appears exactly once in the sum. Hence, the sum of the polynomials representing residues and non-residues modulo p is $x + x^2 + \ldots + x^{p-1}$. If $j(x) = 1 + x + x^2 + \ldots + x^{p-1}$, then we have

$$j(x) = 1 + l(x) + n(x). \tag{1.9}$$

Let $l(x) = \sum_{l \in \mathscr{A}} x^l$ be the leading polynomial of the circulant matrix $\mathbf{Q}$ with size $(p-1) \times (p-1)$ and let $n(x) = \sum_{n \in \mathscr{B}} x^n$ be the leading polynomial of the circulant matrix $\mathbf{N}$ with size $(p-1) \times (p-1)$ [21]. In Example 1.3.1, the polynomials

$$l(x) = x + x^2 + x^4 \quad \textit{and} \quad n(x) = x^3 + x^5 + x^6,$$

are the leading polynomials of the circulant matrices

$$\mathbf{Q} = \begin{bmatrix} 110100 \\ 011010 \\ 001101 \\ 100110 \\ 010011 \\ 101001 \end{bmatrix} \quad \text{and} \quad \mathbf{N} = \begin{bmatrix} 001011 \\ 100101 \\ 110010 \\ 011001 \\ 101100 \\ 010110 \end{bmatrix}, \tag{1.10}$$

respectively. For prime of the form $p = 4t + 1$, we add $1 = x^0$ to keep the weight of $1 + \sum_{l \in \mathscr{A}} x^l$ odd [21].

Theorem 1.3.2. *[16, Theorem 85]. Multiplying two quadratic residues or two non-residues produces a residue, whereas the product of a quadratic residue and a non-residue results in a non-residue.*

As a consequence

$$l_i\mathscr{A} = n_i\mathscr{B} = \mathscr{A}, \quad \text{and} \quad n_i\mathscr{A} = l_i\mathscr{B} = \mathscr{B}. \tag{1.11}$$

where l_i is an element of $\mathscr{A}$ and n_i is an element of $\mathscr{B}$ [21].

The properties of double circulant codes rely heavily on the form of p. To investigate these codes further, we require the following elementary results from number theory.

Theorem 1.3.3. *[16, Theorem 82]. Let p be a prime of the form $p = 4t - 1$, then $-1 \equiv (p-1) \mod p$ is a quadratic non-residue. -1 is a quadratic residue of primes of the form $p = 4t + 1$, .*

Therefore, for $p = 4t - 1$, if $x^i \in l(x)$ then we have

$$x^{-i} = a^{p-i} \in n(x) \quad \text{and} \quad l(x)^T = n(x). \tag{1.12}$$

For primes of the form $p = 4t + 1$

$$l(x)^T = l(x) \quad \text{and} \quad n(x) = n(x)^T. \tag{1.13}$$

For example, for $p = 7$ we have $l(x)^T = x^{-1} + x^{-2} + x^{-4} = x^6 + x^5 + x^3 = n(x) \mod x^7 - 1$. The following lemma refers to Theorems 89, 96 and Theorem 97 in [16].

Lemma 1.3.4. *[16]. Let p be a prime.*

i) If $p = 8k \pm 1$, then 2 is quadratic residue $\mod p$.

ii) If $p = 8k \pm 3$, then 2 is a quadratic non-residue $\mod p$.

iii) if $p = 6k + 1$, then -3 is a quadratic residue $\mod p$ *and if $p = 6k + 5$, then -3 is a quadratic non-residue* $\mod p$.

iv) If $p = 10k \pm 1$, then 5 is a quadratic residue $\mod p$ *and if $p = 10k \pm 3$, then 5 is a quadratic non-residue* $\mod p$.

Theorem 1.3.5. *[1, Theorem 4.5.1]. Let p be a prime. Then 3 is a quadratic residue* mod p *if and only if $p = 12k \pm 1$.*

Theorem 1.3.6. *[26, Theorem 1.2]. Let p be an odd prime and set*

$$d_p \;=\; \left\{ \begin{array}{ll} \frac{p-1}{4} & \textit{if} \quad p \equiv 1 \mod 4 \\ \frac{p+1}{4} & \textit{if} \quad p \equiv 3 \mod 4 \end{array} \right\}. \tag{1.14}$$

Then every quadratic residue [non-residue] can be written as a sum of two quadratic residues [non-residues] in exactly $d_p - 1$ ways. Every quadratic residue [non-residue] can be written as a sum of two quadratic non-residues [residues] in exactly d_p ways. Moreover, every non-zero residue can be written as a sum of a quadratic residue and a non-residue in exactly $p - 1 - 2d_p$ ways.

If p is a prime of the form $p = 4k-1$, then $\frac{1}{4}(p-3) = k-1 \in \mathbb{Z}$ and $\frac{1}{4}(p+1) = k \in \mathbb{Z}$. Furthermore, if $p = 4k + 1$, then $\frac{1}{4}(p-5) = k - 1 \in \mathbb{Z}$ and $\frac{1}{4}(p-1) = k \in \mathbb{Z}$.

Theorem 1.3.7. *[1, Theorem 4.5.3]. Let p be a prime, $\mathscr{A}$ the set of residues modulo p, and $\mathscr{B}$ the set of non-residues modulo p. Then in the polynomial ring $\mathbb{Z}[x]/\langle x^p - 1\rangle$, the following relations hold.*

(i) If p is of the form $p = 4k - 1$, then

$$(\sum_{l\in\mathscr{A}} x^l)^2 = \frac{1}{4}(p-3)\sum_{l\in\mathscr{A}} x^l + \frac{1}{4}(p+1)\sum_{n\in\mathscr{B}} x^n, \tag{1.15}$$

$$(\sum_{n\in\mathscr{B}} x^n)^2 = \frac{1}{4}(p+1)\sum_{l\in\mathscr{A}} x^l + \frac{1}{4}(p-3)\sum_{n\in\mathscr{B}} x^n, \tag{1.16}$$

$$(\sum_{l\in\mathscr{A}} x^l)(\sum_{n\in\mathscr{B}} x^n) = \frac{1}{4}(p-3)j(x) + \frac{1}{4}(p+1), \tag{1.17}$$

where $j(x) = 1 + x + x^2 + \ldots + x^{p-1}$ and $x^p - 1 = (x-1)j(x)$.

(ii) If p is of the form $p = 4k + 1$, then

$$(\sum_{l\in\mathscr{A}} x^l)^2 = \frac{1}{4}(p-5)\sum_{l\in\mathscr{A}} x^l + \frac{1}{4}(p-1)\sum_{n\in\mathscr{B}} x^n + \frac{1}{4}(p-1), \tag{1.18}$$

$$(\sum_{n\in\mathscr{B}} x^n)^2 = \frac{1}{4}(p-1)\sum_{l\in\mathscr{A}} x^l + \frac{1}{4}(p-5)\sum_{n\in\mathscr{B}} x^n + \frac{1}{4}(p-1), \tag{1.19}$$

$$(\sum_{l\in\mathscr{A}} x^l)(\sum_{n\in\mathscr{B}} x^n) = \frac{1}{4}(p-1)j(x) + \frac{1}{4}(p-1), \tag{1.20}$$

where $j(x) = 1 + x + x^2 + \ldots + x^{p-1}$ *and* $x^p - 1 = (x-1)j(x)$.

In this thesis, p is an odd prime. In Chapter 2, we begin with defining the Legendre sequence of length p [31]. We review the structure and properties of this sequence that was investigated in [11]. This work employed the Legendre sequences to construct $p \times p$ circulant matrices $\mathbf{S}$ and $\tilde{\mathbf{S}}$, and bordered double circulant matrices $\mathbf{D}$ of size $n = 2p + 2$. In Chapter 3, we demonstrate that when $p = 2qm - 1$, q prime, the code generated by $\mathbf{D}$ over $\mathbb{F}_q$ is self-dual with dimension $k = p + 1$. Furthermore, we present an LCD code which is the decomposition of the associated double circulant codes of length $2p$ where $p = 4kq - 1$ is a prime over $\mathbb{F}_q$.

Chapter 2

Double Circulant Codes

In this chapter, the structure and properties of Legendre sequences are reviewed and then the results in [11] are studied and extended to obtain non-binary double circulant codes.

2.1 The Structure of Legendre Sequences

Let p be an odd prime and a be a primitive root modulo p. We begin with the definition of Legendre sequence of length p using the sets of quadratic residues and non-residues modulo p, $\mathscr{A} = \{a^{2i}\}$ and $\mathscr{B} = \{a^{2i+1}\}$, respectively.

Definition 2.1.1. [11]. Let p be an odd prime. The binary Legendre sequence $\mathbf{s}$ of length p is defined as follows

$$\mathbf{s} = (s_0, s_1, \ldots, s_{p-1}) \quad \text{with} \quad s_0 = 0, \quad \text{and} \quad s_t = \begin{cases} 1 & \text{if } t \in \mathscr{A}, \\ 0 & \text{if } t \in \mathscr{B}. \end{cases} \tag{2.1}$$

Definition 2.1.2. [11]. The alternative Legendre sequence $\tilde{\mathbf{s}}$, has $\tilde{s}_0 = 1$ and $\tilde{s}_t = s_t$ if $t \neq 0$.

Definition 2.1.3. [11]. Consider a sequence $\mathbf{u} = (u_0, u_1, \ldots, u_{p-1})$, where p is an odd prime. the jth component of the cyclic autocorrelation $\mathbf{u}$ is defined as

$$u_j = \sum_{t=0}^{p-1} (-1)^{|s_t - s_{(t+j)}|}, \tag{2.2}$$

where the index t is taken modulo p.

The cyclic autocorrelation of $\mathbf{s}$ is a measure that quantifies the similarity between the sequence and its cyclic shifts. Similarly, we define $\tilde{\mathbf{u}}$ as the cyclic autocorrelation vector for the binary sequence $\tilde{\mathbf{s}}$. The following lemma gives the autocorrelation vectors $\mathbf{u}$ and $\tilde{\mathbf{u}}$ for p prime.

Lemma 2.1.4. *[11, Lemma 1] Let p is an odd prime, the cyclic autocorrelation vectors $\boldsymbol{u}$ and $\tilde{\boldsymbol{u}}$ possess the following values*

$$\begin{aligned} u_0 = \tilde{u}_0 &= p, \\ u_j, \tilde{u}_j &= -1, \qquad j \neq 0, \quad p = 4k+3, \\ u_j, \tilde{u}_j &\in \{1, -3\}, \quad j \neq 0, \quad p = 4k+1, \\ u_j + \tilde{u}_j &= -2, \qquad j \neq 0. \end{aligned}$$

The property, $u_j + \tilde{u}_j = -2$ for $j \neq 0$, plays a particular role in the construction of double circulant codes of length $2p$. Such codes are constructed by concatenating the sequence $\mathbf{s}$ and its shifted version, providing a balanced structure.

Example 2.1.5. Let $p = 5$. The sequence of powers of $a = 2$ forms the following sets modulo 5

$\mathbb{Z}_5^*$	2^1	2^2	2^3	2^4
$\mathscr{A}$		4		1
$\mathscr{B}$	2		3	

The Legendre sequence of length 5 is $\mathbf{s} = 01001$, where $s_t = 1$ for $t \in \mathscr{A} = \{1, 4\}$ and $s_t = 0$ for $t \in \mathscr{B} = \{2, 3\}$. The alternative Legendre sequence is $\tilde{\mathbf{s}} = 11001$. It follows that $\mathbf{u} = 5, -3, 1, 1, -3$ and $\tilde{\mathbf{u}} = 5, 1, -3, -3, 1$, so $\mathbf{u} + \tilde{\mathbf{u}} = 10, -2, -2, -2, -2$. This means that by adding two extra columns to the combined circulant matrices generated by $\mathbf{s}$ and $\tilde{\mathbf{s}}$, we can create a matrix with orthogonal rows.

2.2 Doubly-Extended Code Construction

In this section, the form $\mathbf{r} = \mathbf{s}|\tilde{\mathbf{s}}$ and some properties of this structure are introduced [11]. They are used to obtain new results for $\mathbf{r}$ for primes of the form $p = 2qm - 1$, q prime.

Lemma 2.2.1. *[11]. Let $\boldsymbol{r} = \boldsymbol{s}|\tilde{\boldsymbol{s}}$, then*

$$wt(\boldsymbol{r}) = p. \tag{2.3}$$

Proof. From the definition of $\mathbf{s}$, there are $(p-1)/2$ non-zero elements, $wt(\mathbf{s}) = (p-1)/2$ and as $\tilde{s}_0 = 1$, $wt(\tilde{\mathbf{s}}) = (p-1)/2+1$. Thus $wt(\mathbf{r}) = wt(\mathbf{s}) + wt(\tilde{\mathbf{s}}) = 2(p-1)/2+1 = p$. □

Lemma 2.2.2. *[11]. let $\rho = (\rho_0, \rho_1, \ldots, \rho_{2p-1})$ be the cyclic autocorrelation of $\boldsymbol{r}$, where*

$$\rho_j = \sum_{t=0}^{2p-1} (-1)^{r_t - r_{t+j}},$$

where the index of r is taken modulo $2p$. Then

$$\rho_j = -2, \quad 0 \leqslant j \leqslant 2p.$$

Theorem 2.2.3. *Let $w = (w_0, w_1, \ldots, w_{p-1})$ be the $\{0,1\}$-cyclic autocorrelation of $\boldsymbol{r}$, where*

$$w_j = \sum_{t=0}^{2p-1} r_t r_{t+j},$$

where the index of r is taken modulo $2p$. Then

$$w_j = qm - 1, \quad p = 2qm - 1, \quad 0 < j < p. \tag{2.4}$$

Proof. We can alternatively define w_j by $w_j = |\{t | r_t = r_{t+j} = 1,\ 0 \leqslant t < 2p\}|$. Define the set $A = \{t | r_t \neq r_{t+j}, 0 \leqslant t < 2p\}$. As r_t and r_{t+j} cover the same set of values as t varies, it follows that

$$wt(\mathbf{r}) = |\{t | r_t = 1\}| = w_j + \frac{|A|}{2}. \tag{2.5}$$

Lemma 2.2.2 implies that $|A| = p+1$ which, together with Lemma 2.2.1 and (2.5), give $w_j = \frac{p-1}{2}$, and the theorem follows. □

Definition 2.2.4. [11]. Let p be an odd prime, and $\mathbf{S}$ and $\tilde{\mathbf{S}}$ be the $p \times p$ circulant matrices with $\mathbf{s}$ and $\tilde{\mathbf{s}}$ as their first rows, respectively. Then the matrix

$$D' = \left[\mathbf{S} | \tilde{\mathbf{S}}\right],$$

generates a length $2p$ double circulant linear code.

A direct corollary of Theorem 2.2.3 is as follows.

Corollary 2.2.5. *[11]. Let $q = 2$ and $\boldsymbol{d}_i$ be the ith row of $\boldsymbol{D}'$, then*

$$wt(\boldsymbol{d}_i + \boldsymbol{d}_j) = p + 1.$$

Therefore, the inner product of any pair of rows of $\boldsymbol{D}'$ is zero.

Remark 2.2.6.

$$D' = \left[\mathbf{S}|\tilde{\mathbf{S}}\right],$$

is a circulant matrix.

Proof. Based on the definition of $\tilde{\mathbf{s}}$, which has the same entries as $\mathbf{s}$ except for $\tilde{s}_0 = 1$, the matrix $\mathbf{D}'$ is a circulant matrix, as follows

$$D' = \left[\mathbf{S}|\tilde{\mathbf{S}}\right]$$

$$= \left[\begin{array}{ccccc|ccccc} 0 & s_1 & s_2 & \dots & s_{p-1} & 1 & s_1 & s_2 & \dots & s_{p-1} \\ s_{p-1} & 0 & s_1 & \dots & s_{p-2} & s_{p-1} & 1 & s_1 & \dots & s_{p-2} \\ s_{p-2} & s_{p-1} & 0 & \dots & s_{p-3} & s_{p-2} & s_{p-1} & 1 & \dots & s_{p-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ s_1 & s_2 & s_3 & \dots & 0 & s_1 & s_2 & s_3 & \dots & 1 \end{array}\right].$$

□

Definition 2.2.7. [11]. Let $\mathbf{1}$ be the $p \times 1$ all-ones vector and $\mathbf{0}$ be the $p \times 1$ all-zeroes vector. Then the matrix

$$\mathbf{D} = \left[\begin{array}{c|c|c} 11 & \mathbf{1}^T & \mathbf{1}^T \\ \hline \mathbf{10} & \mathbf{S} & \tilde{\mathbf{S}} \end{array}\right] \tag{2.6}$$

generates a length $2p + 2$ bordered double circulant linear code.

Example 2.2.8. Let $p = 5$. The Legendre sequence of length 5 is $\mathbf{s} = 01001$, and the corresponding alternative Legendre sequence is $\tilde{\mathbf{s}} = 11001$. Concatenating the

circulant matrices formed from these sequences gives

$$D' = \left[\begin{array}{c|c} 01001 & 11001 \\ 10100 & 11100 \\ 01010 & 01110 \\ 00101 & 00111 \\ 10010 & 10011 \end{array}\right].$$

This is a double circulant generator matrix for a $[10, 5, 5]$ optimal ternary linear code [13]. According to Remark 2.2.6, D' always generates a cyclic code. The above matrix can be bordered by the all-ones and all-zeroes columns, and then the all-ones row resulting in

$$D = \left[\begin{array}{c|c|c} 11 & 11111 & 11111 \\ 10 & 01001 & 11001 \\ 10 & 10100 & 11100 \\ 10 & 01010 & 01110 \\ 10 & 00101 & 00111 \\ 10 & 10010 & 10011 \end{array}\right].$$

D is a generator matrix for the $[12, 6, 6]$ extended ternary Golay code g_{12}, which is an optimal self-dual code [20].

Double circulant binary codes for $p = 8k \pm 3$ were constructed in [11], including a number of self-dual codes. Self-orthogonal codes and other codes with good minimum distance were also constructed. In the following section, we study the extended linear codes derived from Legendre sequences for the case $p = 8k \pm 3$ as introduced in [11].

2.3 Extended Binary Linear Codes from Legendre Sequences

Let p be a prime integer of the form $p = 4t - 1$, and let $\mathbf{s}$ be the Legendre sequence of length p. Define $s(x) = \sum_{l \in \mathscr{A}} x^l$ as the leading polynomial of a circulant matrix $\mathbf{S}$. Additionally, let $\tilde{s}(x)$ be the leading polynomial of the circulant matrix $\tilde{\mathbf{S}} = \mathbf{S} + I_p$. Furthermore, let $n(x) = \sum_{n \in \mathscr{B}} x^n$ be the leading polynomial of a circulant matrix $\mathbf{N}$, and let $\tilde{n}(x)$ be the leading polynomial of the circulant matrix $(\mathbf{N} + I_p)$ where I_p is the $p \times p$ identity matrix. It is often preferred to have a code in systematic or reduced

echelon form

$$\Big[I_p|P\Big]$$

where I_p is a $p\times p$ identity matrix. Transforming the double circulant code constructed previously to this form depends on the invertibility of either $\mathbf{S}$ or $\tilde{\mathbf{S}}$. This, in turn, implies that the leading polynomials $s(x)$ or $\tilde{s}(x)$ must be invertible in $\mathbb{F}_q[x]/\langle x^p-1\rangle$. The invertibility of the polynomials $s(x)$ and $\tilde{s}(x)$ depends on the value of p. In the binary case, for $p=8k\pm 1$, neither $s(x)$ nor $\tilde{s}(x)$ is invertible. For $p=8k+3$, $s(x)$ is always invertible, while for $p=8k-3$, $\tilde{s}(x)$ is always invertible. These conditions are derived from the fact that 2 is a quadratic residue for $p=8k\pm 1$ and a quadratic non-residue for $p=8k\pm 3$ [21, Lemma 12]. A row echelon form for the doubly-extended binary generator matrix $\mathbf{D}$, which includes the identity matrix in either the first $p+2$ or the last $p+2$ columns, was introduced in [11] for $p=8k+3$. In this matrix, neither the columns from 0 to $p+1$ nor the columns from $p+2$ to $2p+2$ can be considered as information sets. The following results are taken from [11] for the polynomials $s(x)$ and $\tilde{s}(x)$ defined in the ring $\mathbb{F}_2[x]/\langle x^p-1\rangle$

$$\begin{aligned}
\tilde{s}(x)^{-1}=\tilde{s}(x)^2=\tilde{n}(x) \qquad & \text{for } p=8k-3,\\
s(x)^{-1}=s(x)^2=n(x) \qquad & \text{for } p=8k+3,\\
\tilde{s}(x)^{-1}s(x)=n(x) \qquad & \text{for } p=8k-3,\\
s(x)^{-1}\tilde{s}(x)=\tilde{n}(x) \qquad & \text{for } p=8k+3.
\end{aligned}$$

Therefore, when 2 is a quadratic non-residue modulo p, a $p\times p$ circulant matrix P can be obtained such that the first row of the circulant matrix is the coefficients of $\tilde{n}(x)$ when $p=8k-3$, and for $p=8k+3$, it is the coefficients of $n(x)$ [11]. In these cases, a double circulant binary code can be constructed with the specified first row of the circulant matrix. When $p=8k+3$, the codes obtained (whether bordered or pure), are equivalent to those described in [12, 18, 21, 27].

Example 2.3.1. [11, Example 2.4.1]. Let $p=5$, so $\tilde{s}=11001$ and $\tilde{s}(x)=x^4+x+1$ is a polynomial in $\mathbb{F}_2[x]/\langle x^p-1\rangle$ such that $\tilde{s}(x)^3=1$ so it is invertible [21]. Then

$\tilde{s}(x)^{-1} = x^3 + x^2 + 1$. Thus

$$\tilde{\mathbf{S}} = \begin{bmatrix} 11001 \\ 11100 \\ 01110 \\ 00111 \\ 10011 \end{bmatrix} \qquad \text{and} \qquad \tilde{\mathbf{S}}^{-1} = \begin{bmatrix} 10110 \\ 01011 \\ 10101 \\ 11010 \\ 01101 \end{bmatrix}.$$

As $\tilde{\mathbf{S}}^{-1}\tilde{\mathbf{S}} = \mathbf{I}$

$$\tilde{\mathbf{S}}^{-1}\mathbf{D} = \mathbf{P}|\mathbf{I},$$

where

$$\mathbf{P} = \begin{bmatrix} 00110 \\ 00011 \\ 10001 \\ 11000 \\ 01100 \end{bmatrix},$$

as $\tilde{s}(x)^{-1}s(x) = (x^3+x^2+1)(x^4+x) \mod x^5+1 = x^3+x^2$. The systematic generator matrix then has the form

$$G = \begin{bmatrix} 100000|011111 \\ 010000|100011 \\ 001000|110001 \\ 000100|111000 \\ 000010|101100 \\ 000001|100110 \end{bmatrix}.$$

This is a bordered double circulant generator matrix for a $[12, 6, 4]$ binary linear code.

In Chapter 3, we will show that the polynomials $s(x)$ and $\tilde{s}(x)$ are not invertible in $\mathbb{F}_q[x]/\langle x^p - 1\rangle$ when $p = 4kq - 1$.

Chapter 3

Double Circulant Self-Dual Codes from Legendre Sequences for $p = 2qm - 1$ over $\mathbb{F}_q$

In this chapter, we present bordered double circulant codes of length $2p+2$ for primes of the form $p = 2qm-1$ over $\mathbb{F}_q$. We show that this construction results in a large class of self-dual codes. Toward the end, we introduce a decomposition of the corresponding double circulant codes of length $2p$. The motivation for this approach comes from [11], which presented the construction of doubly-extended circulant binary codes of length $2p + 2$ and dimension $p + 1$. From Chapter 2, $\mathbf{S}$ and $\tilde{\mathbf{S}}$ are the $p \times p$ circulant matrices with $\mathbf{s}$ and $\tilde{\mathbf{s}}$ as their first rows, respectively. Then

$$\mathbf{D}' = \left[\mathbf{S}|\tilde{\mathbf{S}}\right],$$

is a matrix with size $p \times 2p$ and

$$\mathbf{D} = \left[\begin{array}{c|c|c} 11 & \mathbf{1}^T & \mathbf{1}^T \\ \hline \mathbf{10} & \mathbf{S} & \tilde{\mathbf{S}} \end{array}\right], \tag{3.1}$$

is a matrix with size $(p + 1) \times (2p + 2)$.

Theorem 3.0.1. *Let p be a prime of the form $p = 2qm - 1$. The code C with generator matrix $\boldsymbol{D}$ is a self-dual code over $\mathbb{F}_q$, q prime.*

Proof. From Theorem 2.2.3, for $\mathbf{D}'$, $w_j = qm - 1, j = 1, 2, \ldots p - 1$. Then the inner product of any pair of rows 2 to $p + 1$ of $\mathbf{D}$ is qm, which means these rows of $\mathbf{D}$

are orthogonal over $\mathbb{F}_q$. From Lemma 2.2.1, the weight of rows 2 to $p+1$ of D is $p+1 = 2qm$, so these rows are self-orthogonal and are orthogonal to the all-ones row. Since $n = 2p+2$, the block length is $4qm$, so the all-ones row is also self-orthogonal. Thus, all rows of $\mathbf{D}$ are orthogonal, so $\mathbf{D}$ generates C and $C^{\perp}$. Therefore, these linear codes are equal. □

Remark 3.0.2. The dimension of the self-dual code generated by $\mathbf{D}$ is $(2p+2)/2 = p+1$. The minimum distance of this code is upper bounded by $p+2$.

Table 3.1 gives the values of p that result in a self-dual code generated by $\mathbf{D}$ over $\mathbb{F}_q$ from Theorem 3.0.1. In the next section, we show that the code generated by $\mathbf{D}'$ for m even is degenerate, i.e. it can be decomposed as the direct sum of two codes.

Table 3.1: Values of p for the Double Circulant Degenerate Codes over $\mathbb{F}_q$

q	p
2	$8k-1$
3	$12k-1$
5	$20k-1$
7	$28k-1$
11	$44k-1$

3.1 The Structure of Double-Circulant Codes for the Case $p = 4qk-1$ over $\mathbb{F}_q$

In this section, we discuss some properties of the ideals generated by $s(x)$ and $n(x)$ and their idempotent elements. Then we obtain the dimensions of these ideals. As mentioned in Corollary 1.1.8, the rank of the $p \times p$ circulant matrix $\mathbf{S}$ over $\mathbb{F}_q$ is the dimension of the ideal generated by $s(x)$ in $\mathbb{F}_q[x]/\langle x^p - 1\rangle$ as a cyclic subspace over $\mathbb{F}_q$. Then we present a direct sum construction of the codes generated by $\mathbf{S}$ and $\tilde{\mathbf{S}}$.

Remark 3.1.1. [1, Remark 2.2.3], Let $b \in \mathscr{B}$. Then the mapping $\sigma_b : x^j \longrightarrow x^{jb}$, for $j = 1, 2, \ldots, p-1$, (exponents mod p), interchanges the ideals with generators $\sum_{l\in\mathscr{A}} x^l$ and $\sum_{n\in\mathscr{B}} x^n$, that is $R_p(\sum_{l\in\mathscr{A}} x^l)\sigma_b = R_p(\sum_{n\in\mathscr{B}} x^n)$. Hence, they are equivalent.

Let $\mathbf{J}$ be the matrix of order p with 1s in all positions, and let $j(x)$ be the leading polynomial of $\mathbf{J}$ over $\mathbb{F}_q$.

Corollary 3.1.2. *Let p be a prime of the form $p = 4kq - 1$. Let $\mathscr{A}$ be the set of quadratic residues modulo p and $\mathscr{B}$ the set of non-residues modulo p. Then the polynomials $s(x)$ and $n(x)$ in the polynomial ring $\mathbb{F}_q[x]/\langle x^p - 1\rangle$ defined by*

$$s(x) = \sum_{l \in \mathscr{A}} x^l \quad \textit{and} \quad n(x) = \sum_{n \in \mathscr{B}} x^n,$$

satisfy

$$s(x) + n(x) = j(x) - 1, \tag{3.2}$$

$$s(x)^2 = -s(x), \tag{3.3}$$

$$n(x)^2 = -n(x), \tag{3.4}$$

$$s(x)n(x) = -j(x). \tag{3.5}$$

Proof. Let $p = 4kq-1$. Then from Theorem 1.3.7, part (i) and (1.15) in $\mathbb{F}_q[x]/\langle x^p-1\rangle$, we have

$$\begin{aligned} s(x)^2 &= \frac{1}{4}((4kq-1)-3)s(x) + \frac{1}{4}((4kq-1)+1)n(x) && (3.6)\\ &= (kq-1)s(x) + (kq)n(x) && (3.7)\\ &= -s(x) \bmod q. && (3.8) \end{aligned}$$

Similarly, using (1.16) in $\mathbb{F}_q[x]/\langle x^p - 1\rangle$

$$\begin{aligned} n(x)^2 &= \frac{1}{4}((4kq-1)-3)n(x) + \frac{1}{4}((4kq-1)+1)s(x) && (3.9)\\ &= (kq-1)n(x) + (kq)s(x) && (3.10)\\ &= -n(x) \bmod q. && (3.11) \end{aligned}$$

Then from (1.17) in $\mathbb{F}_q[x]/\langle x^p - 1\rangle$

$$\begin{aligned} s(x)n(x) &= \frac{1}{4}((4kq-1)-3)j(x) + \frac{1}{4}((4kq-1)+1) && (3.12)\\ &= (kq-1)j(x) + (kq) && (3.13)\\ &= -j(x) \bmod q. && (3.14) \end{aligned}$$

□

Corollary 3.1.2, (3.3) and (3.4) in $\mathbb{F}_q[x]/\langle x^p - 1\rangle$ imply that the idempotent ele-

ments of the ideals generated by $s(x)$ and $n(x)$ are

$$(-s(x))^2 = s(x)^2 = -s(x), \tag{3.15}$$
$$(-n(x))^2 = n(x)^2 = -n(x). \tag{3.16}$$

It is clear that

$$\langle s(x)\rangle = \langle -s(x)\rangle\,, \tag{3.17}$$
$$\langle n(x)\rangle = \langle -n(x)\rangle\,. \tag{3.18}$$

Now, based on Theorem 1.1.3, $-s(x) - n(x) - s(x)n(x)$ is an idempotent element of the ideal $\langle s(x)\rangle + \langle n(x)\rangle$ and

$$\langle s(x)\rangle + \langle n(x)\rangle = \langle -s(x) - n(x) - s(x)n(x)\rangle. \tag{3.19}$$

Applying (3.2) and (3.5), we get

$$\langle s(x)\rangle + \langle n(x)\rangle = \langle -j(x) + 1 + j(x)\rangle = \langle 1\rangle\,, \tag{3.20}$$

which is an ideal of dimension p.
On the other hand, since $s(x)n(x)$ is an idempotent element of the ideal $\langle s(x)\rangle \cap \langle n(x)\rangle$, according to Theorem 1.1.2

$$\langle s(x)\rangle \cap \langle n(x)\rangle = \langle s(x)n(x)\rangle\,. \tag{3.21}$$

Now, we examine the structure of $\mathbf{D}' = \mathbf{S}|\tilde{\mathbf{S}}$. Let $\mathbf{S}_r^f$ be the matrix formed by r consecutive rows of $\mathbf{S}$, starting from row f, where the row after the last row is the first row. We state the following lemmas.

Lemma 3.1.3. *Let p be a prime of the form $p = 4qk - 1$. Then over $\mathbb{F}_q$, q prime*

$$\textit{rank } \boldsymbol{S}^f_{\frac{p+1}{2}} = \textit{rank } \boldsymbol{S} = \frac{p+1}{2}. \tag{3.22}$$

Proof. The proof for $q = 2$ is given in [21, Lemma 12].
If $q > 2$ then according to Corollary 1.1.8, the rank of the $p \times p$ circulant matrix $\mathbf{S}$ over $\mathbb{F}_q$ is the dimension of the ideal generated by $s(x)$ in $\mathbb{F}_q[x]/\langle x^p - 1\rangle$ as a cyclic subspace. Therefore, we show that the dimension of the ideals generated by $s(x)$ and

$n(x)$ over $\mathbb{F}_q$ equals $\frac{p+1}{2}$ for primes of the form $p = 4qk - 1$. From (3.20)

$$\dim \langle s(x)\rangle + \langle n(x)\rangle \;=\; p \quad \text{over } \mathbb{F}_q.$$

From Theorem 1.1.6, we can consider $\langle s(x)\rangle$ and $\langle n(x)\rangle$ as the cyclic subspaces. Using (1.4) from Theorem 1.1.7

$$\dim \langle s(x)\rangle + \langle n(x)\rangle \;=\; \dim \langle s(x)\rangle \;+\; \dim \langle n(x)\rangle - \;\dim \langle s(x)\rangle \cap \langle n(x)\rangle \quad \text{over } \mathbb{F}_q.$$

From (3.21)

$$\dim \langle s(x)\rangle + \dim \langle n(x)\rangle - \dim\langle s(x)\rangle\langle n(x)\rangle = p \quad \text{over } \mathbb{F}_q. \tag{3.23}$$

Using (3.5), we have

$$\begin{aligned}
\dim \langle s(x)\rangle + \dim \langle n(x)\rangle - \;\dim \langle j(x)\rangle \;&=\; p \quad \text{over } \mathbb{F}_q && (3.24)\\
\Longrightarrow \dim \langle s(x)\rangle + \dim \langle n(x)\rangle - \;1 \;&=\; p \quad \text{over } \mathbb{F}_q && (3.25)\\
\Longrightarrow \dim \langle s(x)\rangle + \dim \langle n(x)\rangle \;&=\; p+1 \quad \text{over } \mathbb{F}_q. && (3.26)
\end{aligned}$$

By Remark 3.1.1, both ideals are equivalent, implying that

$$\dim \langle s(x)\rangle = \dim \langle n(x)\rangle = \frac{p+1}{2} \quad \text{over } \mathbb{F}_q. \tag{3.27}$$

Therefore

$$\text{rank } \mathbf{S}^f_{\frac{p+1}{2}} = \text{rank } \mathbf{S} = \frac{p+1}{2}, \quad \text{over } \mathbb{F}_q. \tag{3.28}$$

□

Remark 3.1.4. Let p be a prime of the form $p = 4kq-1$, q prime. The ideal generated by $j(x)+1$ in the algebra of polynomials modulo x^p-1 over $\mathbb{F}_q$, has dimension $p-1$.

Proof. Since $j(1)+1 = p+1 = 4kq-1+1 = 0 \pmod q$, there exists a polynomial $h(x)$ in $\mathbb{F}_q[x]/\langle x^p-1\rangle$ such that $j(x)+1 = (x-1)h(x)$. Let $I = \langle x-1\rangle$ be an ideal in $\mathbb{F}_q[x]/\langle x^p-1\rangle$. Therefore, $j(x) = x^p - 1/(x-1)$ is the factor of x^p-1 in $\mathbb{F}_q[x]/\langle x^p-1\rangle$. Since, $\gcd(p,q) = 1$, for the ideals in $\mathbb{F}_q[x]/\langle x^p-1\rangle$, x^p-1 has no repeated roots, hence $\gcd(x-1, j(x)) = 1$. Since $j(x)^2 = -j(x)$ in $\mathbb{F}_q[x]/\langle x^p-1\rangle$ we have $(x-1)h(x) + j(x)j(x) = 1$. Furthermore, $h(x)$ and $j(x)$ are co-prime. As $(j(x)+1)^2 = j(x)+1$, it is an idempotent element of the ideal generated by $(x-1)$.

Since

$$\gcd((j(x)+1), x^n-1) = \gcd((x-1)h(x), (x-1)j(x)) = (x-1),$$

$(x-1)$ is an element of the ideal generated by $1+j(x)$, so $\langle 1+j(x)\rangle = \langle x-1\rangle$. According to Theorem 1.0.1, the dimension of $\langle x-1\rangle$ is $p-1$. □

Lemma 3.1.5. *Let p be a prime of the form $p = 4qk-1$. Then over $\mathbb{F}_q$, q prime*

$$\textit{rank } \tilde{\mathbf{S}}^f_{\frac{p-1}{2}} = \textit{rank } \tilde{\mathbf{S}} = \frac{p-1}{2}. \tag{3.29}$$

Proof. We show that in case of $p = 4qk-1$ the ideals generated by $\tilde{s}(x) = s(x)+1$ and $\tilde{n}(x) = n(x)+1$ are idempotent over $\mathbb{F}_q$. From (3.3) in Corollary 3.1.2 we have

$$\begin{aligned}(s(x)+1)^2 &= s(x)^2 + 2s(x) + 1\\ &= -s(x) + 2s(x) + 1\\ &= s(x) + 1,\end{aligned}$$

and based on (3.4) in Corollary 3.1.2, we have that

$$\begin{aligned}(n(x)+1)^2 &= n(x)^2 + 2n(x) + 1\\ &= -n(x) + 2n(x) + 1\\ &= n(x) + 1.\end{aligned}$$

On the other hand

$$(s(x)+1)(n(x)+1) = s(x)n(x) + s(x) + n(x) + 1,$$

from (3.5) in $\mathbb{F}_q[x]/\langle x^p-1\rangle$, we have

$$\begin{aligned}(s(x)+1)(n(x)+1) &= -j(x) + j(x)\\ &= 0.\end{aligned}$$

Therefore, based on Theorem 1.1.3

$$\langle s(x)+1\rangle \cap \langle n(x)+1\rangle = \langle (s(x)+1)(n(x)+1)\rangle = 0. \tag{3.30}$$

From Theorem 1.1.3, the polynomial $(s(x)+1+n(x)+1)$ is an idempotent element of the ideal $\langle s(x)+1\rangle \ + \ \langle n(x)+1\rangle$ such that

$$\langle s(x)+1\rangle \ + \ \langle n(x)+1\rangle \ = \ \langle s(x)+1+n(x)+1\rangle. \tag{3.31}$$

By (3.2), we get

$$\langle s(x)+1\rangle \ + \ \langle n(x)+1\rangle \ = \ \langle j(x)+1\rangle. \tag{3.32}$$

By Remark 3.1.4, $\langle j(x)+1\rangle$ is an ideal with dimension $p-1$ over $\mathbb{F}_q$, so

$$\dim \langle s(x)+1\rangle \ + \ \langle n(x)+1\rangle \ = \ p-1 \quad \text{over } \mathbb{F}_q. \tag{3.33}$$

From (3.21) over $\mathbb{F}_q$

$$\dim \langle s(x)+1\rangle \ + \ \dim\langle n(x)+1\rangle - \ \dim \langle s(x)+1\rangle \cap \langle n(x)+1\rangle \ = \ p-1,$$

and from (3.30)

$$\dim \langle s(x)+1\rangle \ + \ \dim\langle n(x)+1\rangle - \ 0 \ = \ p-1, \quad \text{over } \mathbb{F}_q.$$

According to Remark 3.1.1, the ideals $\langle s(x)+1\rangle$ and $\langle n(x)+1\rangle$ are equivalent, so

$$\dim \langle s(x)+1\rangle = \dim\langle n(x)+1\rangle \ = \ \frac{p-1}{2}, \quad \text{over } \mathbb{F}_q. \tag{3.34}$$

This results in

$$\text{rank } \tilde{\mathbf{S}}^f_{\frac{p-1}{2}} = \text{rank } \tilde{\mathbf{S}} = \frac{p-1}{2}, \quad \text{over } \mathbb{F}_q. \tag{3.35}$$

□

As a consequence of Lemmas 3.1.3 and 3.1.5, for $p = 4qk-1$, the matrices $\mathbf{S}$ and $\tilde{\mathbf{S}}$ do not have maximum rank in $\mathbb{F}_q$ and so are not invertible over $\mathbb{F}_q$. Therefore, we cannot convert $\mathbf{D}'$ to systematic form where the first p columns are the identity matrix. However, other sets of p columns of $\mathbf{D}'$ do form an information set.

Definition 3.1.6. A row-column permutation of D' gives

$$\mathbf{PD}' = \mathbf{A}|\mathbf{B} = \left[\begin{array}{c|c} \mathbf{S}^0_{\frac{p+1}{2}} & \tilde{\mathbf{S}}^{\frac{p-1}{2}}_{\frac{p+1}{2}} \\ \tilde{\mathbf{S}}^{\frac{p+1}{2}}_{\frac{p-1}{2}} & \mathbf{S}^0_{\frac{p-1}{2}} \end{array}\right], \tag{3.36}$$

where $\mathbf{A}$ and $\mathbf{B}$ are $p \times p$ matrices.

In the following lemma we prove that matrix $\mathbf{A}$ is a non-singular matrix.

Lemma 3.1.7. *The matrix $\boldsymbol{A}$ is non-singular over $\mathbb{F}_q$, and*

$$\boldsymbol{A}^{-1} = \begin{bmatrix} -\boldsymbol{I}_{\frac{p+1}{2}} & \boldsymbol{E} \\ -\boldsymbol{F} & \boldsymbol{I}_{\frac{p-1}{2}} \end{bmatrix},$$

where $\boldsymbol{E}$ and $\boldsymbol{F}$ are $\frac{p+1}{2} \times \frac{p-1}{2}$ and $\frac{p-1}{2} \times \frac{p+1}{2}$ matrices, respectively.

Proof. The non-singularity of $\mathbf{A}$ follows as we can explicitly construct its inverse, $\mathbf{A}^{-1}$. From Lemma 3.1.5 we know that a matrix $\mathbf{E}$ exists such that

$$\tilde{\mathbf{S}}^0_{\frac{p+1}{2}} = \mathbf{E}\tilde{\mathbf{S}}^{\frac{p+1}{2}}_{\frac{p-1}{2}},$$

as from Lemma 3.1.5 a row of $\tilde{\mathbf{S}}^0_{\frac{p+1}{2}}$ can be written as a linear combination of the rows of $\tilde{\mathbf{S}}^{\frac{p+1}{2}}_{\frac{p-1}{2}}$. Thus

$$\begin{aligned} \left(-\mathbf{I}_{\frac{p+1}{2}}\ \mathbf{E}\right)\left(\mathbf{S}^0_{\frac{p+1}{2}}\ \tilde{\mathbf{S}}^{\frac{p+1}{2}}_{\frac{p-1}{2}}\right)^T &= -\mathbf{S}^0_{\frac{p+1}{2}} + \mathbf{E}\tilde{\mathbf{S}}^{\frac{p+1}{2}}_{\frac{p-1}{2}} \\ &= -\mathbf{S}^0_{\frac{p+1}{2}} + \tilde{\mathbf{S}}^0_{\frac{p+1}{2}} \\ &= -\mathbf{S}^0_{\frac{p+1}{2}} + \left(\mathbf{S}^0_{\frac{p+1}{2}} + \mathbf{I}_{\frac{p+1}{2}}\right) \\ &= \left(\mathbf{I}_{\frac{p+1}{2}}\ \mathbf{0}\right). \end{aligned}$$

Similar arguments that a matrix $\mathbf{F}$ exists follow from Lemma 3.1.3 such that $\mathbf{S}^{\frac{p+1}{2}}_{\frac{p-1}{2}} = \mathbf{F}\mathbf{S}^0_{\frac{p+1}{2}}$. Thus

$$\begin{aligned} \left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)\left(\mathbf{S}^0_{\frac{p+1}{2}}\tilde{\mathbf{S}}^{\frac{p+1}{2}}_{\frac{p-1}{2}}\right)^T &= -\mathbf{F}\mathbf{S}^0_{\frac{p+1}{2}} + \tilde{\mathbf{S}}^{\frac{p+1}{2}}_{\frac{p-1}{2}} \\ &= -\mathbf{S}^{\frac{p+1}{2}}_{\frac{p-1}{2}} + \tilde{\mathbf{S}}^{\frac{p+1}{2}}_{\frac{p-1}{2}} \\ &= -\mathbf{S}^{\frac{p+1}{2}}_{\frac{p-1}{2}} + \left(\mathbf{S}^{\frac{p+1}{2}}_{\frac{p-1}{2}} + \mathbf{I}_{\frac{p-1}{2}}\right) \\ &= \left(\mathbf{0}\ \mathbf{I}_{\frac{p-1}{2}}\right). \end{aligned}$$

The lemma follows by concatenating the rows of $\left(-\mathbf{I}_{\frac{p+1}{2}}\ \mathbf{E}\right)$, with the rows $\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)$,

and observing that $\mathbf{A}^{-1}$ is unique. □

Corollary 3.1.8. *The vector spaces spanned by $\boldsymbol{S}$ and by $\tilde{\boldsymbol{S}}$ are disjoint and of sizes $q^{\frac{p+1}{2}}$ and $q^{\frac{p-1}{2}}$, respectively.*

Proof. From Lemmas 3.1.3 and 3.1.5, and Definition 3.1.6, it is evident that the first $\frac{p+1}{2}$ rows and the last $\frac{p-1}{2}$ rows of $\mathbf{A}$ each independently achieve maximum rank. Given that we previously established an explicit form for $\mathbf{A}^{-1}$ in Lemma 3.1.7, it follows that the vector spaces spanned by the first $\frac{p+1}{2}$ rows and the last $\frac{p-1}{2}$ rows of $\mathbf{A}$ are disjoint. In other words, the vector spaces spanned by $\mathbf{S}_{\frac{p+1}{2}}$ and $\tilde{\mathbf{S}}_{\frac{p-1}{2}}$ respectively, must be disjoint. Moreover, from Lemmas 3.1.3 and 3.1.5, we deduce that these vector spaces are generated by $\mathbf{S}$ and $\tilde{\mathbf{S}}$, respectively. □

Lemma 3.1.9.

$$\boldsymbol{A}^{-1}(\boldsymbol{A}|\boldsymbol{B}) = \left[\begin{array}{cc|cc} \boldsymbol{I}_{\frac{p+1}{2}} & \boldsymbol{0} & \boldsymbol{E} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{I}_{\frac{p-1}{2}} & \boldsymbol{0} & -\boldsymbol{F} \end{array}\right].$$

Proof. In the proof of Lemma 3.1.7 we defined $\mathbf{E}$ such that $\tilde{\mathbf{S}}^{0}_{\frac{p+1}{2}} = \mathbf{E}\tilde{\mathbf{S}}^{\frac{p+1}{2}}_{\frac{p-1}{2}}$. More generally, this means that $\tilde{\mathbf{S}}^{f}_{\frac{p+1}{2}} = \mathbf{E}\tilde{\mathbf{S}}^{f+\frac{p+1}{2}}_{\frac{p-1}{2}}$, where the superscripts are taken modulo p. In particular, we have $\tilde{\mathbf{S}}^{\frac{p-1}{2}}_{\frac{p+1}{2}} = \mathbf{E}\tilde{\mathbf{S}}^{0}_{\frac{p-1}{2}}$. Thus

$$\begin{aligned} \left(-\mathbf{I}_{\frac{p+1}{2}}\ \mathbf{E}\right)\left(\tilde{\mathbf{S}}^{\frac{p-1}{2}}_{\frac{p+1}{2}}\ \mathbf{S}^{0}_{\frac{p-1}{2}}\right)^{T} &= -\tilde{\mathbf{S}}^{\frac{p-1}{2}}_{\frac{p+1}{2}} + \mathbf{E}(\tilde{\mathbf{S}}^{0}_{\frac{p-1}{2}} + \mathbf{I}_{\frac{p-1}{2}}) \\ &= -\tilde{\mathbf{S}}^{\frac{p-1}{2}}_{\frac{p+1}{2}} + \tilde{\mathbf{S}}^{\frac{p-1}{2}}_{\frac{p+1}{2}} + \mathbf{E}\mathbf{I}_{\frac{p-1}{2}} \\ &= (\mathbf{E}\ \mathbf{0}). \end{aligned}$$

Similar arguments for $\mathbf{F}$ show that $\mathbf{S}^{f+\frac{p+1}{2}}_{\frac{p-1}{2}} = \mathbf{F}\mathbf{S}^{f}_{\frac{p+1}{2}}$ where the superscripts are taken modulo p. Specifically, we have $\mathbf{S}^{0}_{\frac{p-1}{2}} = \mathbf{F}\mathbf{S}^{\frac{p+1}{2}}_{\frac{p-1}{2}}$. Thus

$$\begin{aligned} \left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)\left(\tilde{\mathbf{S}}^{\frac{p-1}{2}}_{\frac{p+1}{2}}\ \mathbf{S}^{0}_{\frac{p-1}{2}}\right)^{T} &= -\mathbf{F}\tilde{\mathbf{S}}^{\frac{p-1}{2}}_{\frac{p+1}{2}} + \mathbf{S}^{0}_{\frac{p-1}{2}} \\ &= -\mathbf{F}(\mathbf{S}^{\frac{p-1}{2}}_{\frac{p+1}{2}} + \mathbf{I}_{\frac{p+1}{2}}) + \mathbf{S}^{0}_{\frac{p-1}{2}} \\ &= -\mathbf{S}^{0}_{\frac{p-1}{2}} + \mathbf{S}^{0}_{\frac{p-1}{2}} - \mathbf{F}\mathbf{I}_{\frac{p+1}{2}} \\ &= (\mathbf{0}\ -\mathbf{F}). \end{aligned}$$

The result follows by concatenating the rows of $(\mathbf{E}\ \mathbf{0})$ and $(\mathbf{0}\ -\mathbf{F})$. □

Given $\mathbf{B} = \left(\tilde{\mathbf{S}}_{\frac{p+1}{2}}^{\frac{p-1}{2}} \; \mathbf{S}_{\frac{p-1}{2}}^{0}\right)^T$, Lemma 3.1.5 indicates that there are $\frac{p-1}{2}$ linearly independent rows in $\tilde{\mathbf{S}}_{\frac{p+1}{2}}^{\frac{p-1}{2}}$. Similarly, Lemma 3.1.5 shows that the last $\frac{p-1}{2}$ rows of $\mathbf{B}$ are linearly independent. This implies that the rank of $\mathbf{B}$ over $\mathbb{F}_q$ is $p-1$, so $\mathbf{B}^{-1}$ does not exist.

Lemma 3.1.10. *The vector space spanned by* $\left(-\boldsymbol{I}_{\frac{p+1}{2}} \; \boldsymbol{E}\right)$ *is identical to the vector space spanned by* $\boldsymbol{S}$*. Similarly, the vector space spanned by* $\left(-\boldsymbol{F} \; \boldsymbol{I}_{\frac{p-1}{2}}\right)$ *is identical to the vector space spanned by* $\tilde{\boldsymbol{S}}$*.*

Proof. Let $W = span(\mathbf{S})$ and $W' = span\left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)$. Using $\tilde{\mathbf{S}}_{\frac{p+1}{2}}^{f} = \mathbf{E}\tilde{\mathbf{S}}_{\frac{p-1}{2}}^{f+\frac{p+1}{2}}$, where the superscripts are taken modulo p. We have

$$\left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)\tilde{\mathbf{S}} = \left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)(\mathbf{I}_p + \mathbf{S}), \tag{3.37}$$

$$-\tilde{\mathbf{S}}_{\frac{p+1}{2}}^{0} + \mathbf{E}\tilde{\mathbf{S}}_{\frac{p-1}{2}}^{\frac{p+1}{2}} = \left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)\mathbf{S} + \left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right). \tag{3.38}$$

In particular, $\tilde{\mathbf{S}}_{\frac{p+1}{2}}^{0} = \mathbf{E}\tilde{\mathbf{S}}_{\frac{p-1}{2}}^{\frac{p+1}{2}}$. We also have

$$-\tilde{\mathbf{S}}_{\frac{p+1}{2}}^{0} + \tilde{\mathbf{S}}_{\frac{p+1}{2}}^{0} = \left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)\mathbf{S} + \left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right), \tag{3.39}$$

$$\mathbf{0} = \left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)\mathbf{S} + \left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right), \tag{3.40}$$

$$-\left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)\mathbf{S} = \left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right). \tag{3.41}$$

We know that $\left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)$ has maximum rank, so dim $W = \frac{p+1}{2}$. Let $\mathbf{v} \in W$, there exist $c_1, c_2, \ldots, c_{\frac{p+1}{2}} \in \mathbb{F}_q$ such that $\mathbf{v} = (c_1, c_2, \ldots, c_{\frac{p+1}{2}})\left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)$. From (3.41), we have $\mathbf{v} = (c_1, c_2, \ldots, c_{\frac{p+1}{2}})\left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)(-\mathbf{S})$, so $\mathbf{v} \in W'$. This results in $W \subseteq W'$. Since dim W = dim $W' = \frac{p+1}{2}$, so $W = W'$. Therefore, the vector space spanned by $\mathbf{S}$ is identical to that spanned by $\left(-\mathbf{I}_{\frac{p+1}{2}} \; \mathbf{E}\right)$.

A similar argument as above can be used to verify the claim for $\left(-\mathbf{F} \; \mathbf{I}_{\frac{p-1}{2}}\right)$. Since $\mathbf{S}_{\frac{p-1}{2}}^{f+\frac{p+1}{2}} = \mathbf{F}\mathbf{S}_{\frac{p+1}{2}}^{f}$, where the superscripts are taken modulo p, we have $\mathbf{S}_{\frac{p-1}{2}}^{\frac{p+1}{2}} = \mathbf{F}\mathbf{S}_{\frac{p+1}{2}}^{0}$.

Thus

$$\begin{aligned}
\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)\mathbf{S} &= \left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)\left(\tilde{\mathbf{S}}-\mathbf{I}_p\right), && (3.42)\\
-\mathbf{F}\mathbf{S}^{0}_{\frac{p+1}{2}}+\mathbf{S}^{\frac{p+1}{2}}_{\frac{p-1}{2}} &= \left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)\tilde{\mathbf{S}}-\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right), && (3.43)\\
-\mathbf{S}^{\frac{p+1}{2}}_{\frac{p-1}{2}}+\mathbf{S}^{\frac{p+1}{2}}_{\frac{p-1}{2}} &= \left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)\tilde{\mathbf{S}}-\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right), && (3.44)\\
\mathbf{0} &= \left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)\tilde{\mathbf{S}}-\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right), && (3.45)\\
\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)\tilde{\mathbf{S}} &= \left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right). && (3.46)
\end{aligned}$$

Let $U = span\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)$ and $U' = span(\tilde{\mathbf{S}})$. we know that $\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)$ has maximum rank $\frac{p-1}{2}$, therefore dim $U = \frac{p-1}{2}$. Let $\mathbf{u} \in U$, there exist $d_1, d_2, \ldots, d_{\frac{p-1}{2}} \in \mathbb{F}_q$ such that $\mathbf{u} = (d_1, d_2, \ldots, d_{\frac{p-1}{2}})\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)$ and from (3.46) $\mathbf{u} = (d_1, d_2, \ldots, d_{\frac{p-1}{2}})\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)\tilde{\mathbf{S}}$, so $\mathbf{u} \in U'$. This results in $U \subseteq U'$. Since dim U = dim $U' = \frac{p-1}{2}$, so $U = U'$. Therefore, the vector space spanned by $\tilde{\mathbf{S}}$ is identical to that spanned by $\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)$. □

The linear codes generated by $\mathbf{S}$ and $\tilde{\mathbf{S}}$ are $[p, \frac{p+1}{2}, d_S]$ and $[p, \frac{p-1}{2}, d_{\tilde{S}}]$ codes over $\mathbb{F}_q$, respectively. From Lemmas 3.1.3 and 3.1.5 the ranks of the generator matrices $\mathbf{S}$ and $\tilde{\mathbf{S}}$ over $\mathbb{F}_q$ are $\frac{p+1}{2}$ and $\frac{p-1}{2}$, respectively.

Lemma 3.1.11. *The $[2p, p, d]$ code generated by D' has Hamming distance*

$$d = min\{d_S, d_{\tilde{S}}\}.$$

Proof. From Lemma 3.1.10, the linear codes generated by $\mathbf{S}$ and $\tilde{\mathbf{S}}$ are equivalent to those generated by $\left(-\mathbf{I}_{\frac{p+1}{2}}\ \mathbf{E}\right)$ and $\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)$, respectively. So the code generated by D' is the direct sum of these two codes. □

Corollary 3.1.12. *The $[2p, p, d]$ code generated by D' is an LCD code over $\mathbb{F}_q$.*

Proof. From Corollary 3.1.8, the vector spaces spanned by $\mathbf{S}$ and $\tilde{\mathbf{S}}$ are disjoint, and using (3.3) in Corollary 3.1.2, we get

$$\begin{aligned}
(\mathbf{S})(\tilde{\mathbf{S}}) &= (\mathbf{S})(\mathbf{S}+I)\\
&= \mathbf{S}^2+\mathbf{S} = -\mathbf{S}+\mathbf{S} = 0,
\end{aligned}$$

so the code generated by $\tilde{\mathbf{S}}$ is the dual code of the code generated by $\mathbf{S}$. They also partition $\mathbb{F}_q^p$. □

The following example demonstrates the construction of the binary code for $2p = 14$.

Example 3.1.13. Consider the length $p = 7$ Legendre sequence $\mathbf{s} = 0110100$. The alternative Legendre sequence is $\tilde{\mathbf{s}} = 1110100$. Concatenating the circulant matrices formed from these sequences gives

$$\mathbf{D}' = \left[\begin{array}{c|c} 0110100 & 1110100 \\ 0011010 & 0111010 \\ 0001101 & 0011101 \\ 1000110 & 1001110 \\ 0100011 & 0100111 \\ 1010001 & 1010011 \\ 1101000 & 1101001 \end{array}\right].$$

The matrices corresponding to $p = 7$ with the permutation given previously are

$$\mathbf{E} = \begin{bmatrix} 110 \\ 011 \\ 111 \\ 101 \end{bmatrix} \qquad \text{and} \qquad \mathbf{F} = \begin{bmatrix} 1110 \\ 0111 \\ 1101 \end{bmatrix}.$$

Thus, the linear codes generated by $\mathbf{S}$ and $\tilde{\mathbf{S}}$ are the $[7, 4, 3]$ Hamming code and the $[7, 3, 4]$ simplex code, respectively. Note that $(\mathbf{I}\ \ \mathbf{F})$ does not generate the dual code of $(\mathbf{I}\ \ \mathbf{E})$, but rather a code equivalent to the dual code. In addition, $(\mathbf{I}\ \ \mathbf{F})$ is equivalent to the even weight subcode of $(\mathbf{I}\ \ \mathbf{E})$.

For $p = 23$, and $q = 2$, $\mathbf{S}$ and $\tilde{\mathbf{S}}$ generate the $[23, 12, 7]$ Golay code and its even weight $[22, 11, 8]$ subcode, respectively. The resulting length $2p$ code has parameters $[46, 23, 7]$. The next example gives ternary codes generated by $\mathbf{S}$ and $\tilde{\mathbf{S}}$ with length $p = 11$ and their direct sum.

Example 3.1.14. Let $q = 3$ and $p = 11$. The consecutive powers of $a = 2$ generate the set of residues mod 11 as follows

$\mathbb{Z}_{11}^*$	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
$\mathscr{A}$		4		5		9		3		1
$\mathscr{B}$	2		8		10		7		6	

The Legendre sequence is $\mathbf{s} = 01011100010$, the alternative Legendre sequence is $\tilde{\mathbf{s}} = 11011100010$. Concatenating the circulant matrices formed from the Legendre and alternative Legendre sequences gives

$$D' = \left[\begin{array}{c|c} 01011100010 & 11011100010 \\ 00101110001 & 01101110001 \\ 10010111000 & 10110111000 \\ 01001011100 & 01011011100 \\ 00100101110 & 00101101110 \\ 00010010111 & 00010110111 \\ 10001001011 & 10001011011 \\ 11000100101 & 11000101101 \\ 11100010010 & 11100010110 \\ 01110001001 & 01110001011 \\ 10111000100 & 10111000101 \end{array}\right]. \tag{3.47}$$

The row-column permutation of D' is

$$\mathbf{PD}' = \left[\begin{array}{c|c} 01011100010 & 00010110111 \\ 00101110001 & 10001011011 \\ 10010111000 & 11000101101 \\ 01001011100 & 11100010110 \\ 00100101110 & 01110001011 \\ 00010010111 & 10111000101 \\ \hline 10001011011 & 01011100010 \\ 11000101101 & 00101110001 \\ 11100010110 & 10010111000 \\ 01110001011 & 01001011100 \\ 10111000101 & 00100101110 \end{array}\right]. \tag{3.48}$$

The matrices corresponding to $p = 11$ with the permutation given previously are

$$\mathbf{E} = \begin{bmatrix} 11210 \\ 01021 \\ 11022 \\ 20222 \\ 21112 \\ 21201 \end{bmatrix} \qquad \text{and} \qquad \mathbf{F} = \begin{bmatrix} 211120 \\ 021112 \\ 021021 \\ 110012 \\ 111202 \end{bmatrix}.$$

Thus the linear codes generated by $\mathbf{S}$ and $\tilde{\mathbf{S}}$ are $[11, 6, 5]$ and $[11, 5, 6]$ optimal codes over $\mathbb{F}_3$. Note that $\left(-\mathbf{F}\ \mathbf{I}_{\frac{p-1}{2}}\right)$ does not generate the dual code of $\left(-\mathbf{I}_{\frac{p+1}{2}}\ \mathbf{E}\right)$, but rather a code equivalent to the dual code. The resulting length $2p$ code has parameters $[22, 11, 5]$ over $\mathbb{F}_3$.

Chapter 4

Conclusion and Future Work

In this chapter, we summarize the key findings of this research and discuss their implications. We conclude by highlighting the contributions made to the theory and construction of double circulant codes from Legendre sequences. We also propose several directions for future work that could extend the results presented in this thesis.

4.1 Conclusion

This thesis investigated the application of Legendre sequences in constructing bordered double-circulant self-dual codes and double-circulant LCD codes that can be decomposed as the direct sum of two codes. The Legendre sequence of length p is characterized by sets $\mathscr{A}$ and $\mathscr{B}$ that represent quadratic residues and non-residues modulo p, respectively, where a is a primitive root modulo p. The binary Legendre sequence, denoted by $\mathbf{s}$, has values 1 and 0 based on membership in $\mathscr{A}$ and $\mathscr{B}$. In [11], an alternative Legendre sequence, $\tilde{\mathbf{s}}$, was defined with $\tilde{s}_0 = 1$ instead of $s_0 = 0$. Then for an odd prime p, the Legendre sequences $\mathbf{s}$ and $\tilde{\mathbf{s}}$ of length p were utilized to create the circulant matrices $\mathbf{S}$ and $\tilde{\mathbf{S}}$.

The second chapter reviewed Legendre sequence properties and structure, drawing on previous work. In particular, the study delves into the results in [11], which explored the construction of doubly-extended codes over $\mathbb{F}_2$.

In the third chapter, we established that bordered double circulant Legendre codes with length $2p + 2$ for $p = 2qm - 1$ form a large class of self-dual codes over $\mathbb{F}_q$. We

demonstrated that the generator matrix

$$\mathbf{D} = \left[\begin{array}{c|c|c} 11 & \mathbf{1}^T & \mathbf{1}^T \\ \hline \mathbf{10} & \mathbf{S} & \tilde{\mathbf{S}} \end{array}\right]$$

yields self-dual codes, supported by proofs of orthogonality and self-orthogonality of the rows.

For primes of the form $p = 4kq-1$, the idempotent elements of the ideals generated by the leading polynomials of $\mathbf{S}$ and $\tilde{\mathbf{S}}$ over $\mathbb{F}_q$ were obtained. The investigation into the structure and rank of these circulant matrices highlighted the non-singular matrices through specific row-column permutations of $\mathbf{D} = \mathbf{S}|\tilde{\mathbf{S}}$. This results in a decomposition into a direct sum of codes generated by $\mathbf{S}$ and $\tilde{\mathbf{S}}$ that yields LCD codes.

4.2 Future Work

This thesis has established a framework for constructing bordered double circulant self-dual codes and double circulant LCD codes over $\mathbb{F}_q$ using Legendre sequences of length $p = 2qm - 1$. However, several directions for future research remain.

- **Generalization to Other Primes:** Expand the results to include a broader range of primes beyond $p = 2qm - 1$, particularly when m is odd. Investigate the non-singularity of $\mathbf{S}$ and $\tilde{\mathbf{S}}$ to generate non-degenerate codes of length $2p$.

- **Exploration of Alternative Sequences:** Investigate the use of other sequence families, such as generalized Legendre sequences, to construct circulant matrices to obtain new code constructions.

- **Optimization of Code Constructions:** Focus on optimizing the construction methods for computational efficiency or improved minimum distance.

Bibliography

[1] G. F. M. Beenker, *On Double Circulant Codes*, *Rep. 80.WSK-04*, Department of Mathematics, Technological University, Eindhoven, Netherlands (1980).

[2] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, UK, 2nd edition (1999).

[3] J. H. Conway and N. J. A. Sloane, *A New Upper Bound On The Minimal Distance of Self-dual Codes*, IEEE Trans. Inform. Theory **36** (1990), 1319–1333.

[4] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya, and P. Solé, *On linear complementary pairs of codes*, IEEE Trans. Inform. Theory **64** (2018), 6583–6589.

[5] S. Ernst and T. J. Robert, *Metric Affine Geometry*. Academic Press, New York, NY, USA (1971).

[6] M. Grassl, *Bounds On The Minimum Distance of Linear Codes*, available at `http://www.codetables.de/`.

[7] M. J. E. Golay, *Notes on Digital Coding*, Proc. IRE **37** (1949), p. 657.

[8] T. A. Gulliver, M. Harada, and J.-L. Kim, *Construction of New Extremal Self-dual Codes*, Discrete Math. **263** (2003), 81–91.

[9] T. A. Gulliver and M. Harada, *Weight Enumerators of Double Circulant Codes And New Extremal Self-dual Codes*, Des. Codes. Cryptogr. **11** (1997), 141–150.

[10] T. A. Gulliver and M. Harada, *Classification of Extremal Double Circulant Self-dual Codes of Lengths* 64 *to* 72, Des. Codes. Cryptogr. **13** (1998), 257–269.

[11] T. A. Gulliver and M. G. Parker, *Extended Binary Linear Codes From Legendre Sequences*, Ars Comb. **100** (2011), 435–447.

[12] T. A. Gulliver and N. Senkevitch, *On A Class of Self-dual Codes Derived From Quadratic Residues*, IEEE Trans. Inform. Theory **45** (1999), 701–702.

[13] T. A. Gulliver and N. Senkevitch, *Optimal Ternary Linear Rate 1/2 Codes*, Des. Codes. Cryptogr. **23** (2001), 1677–171.

[14] R. W. Hamming, *Error Detecting and Error Correcting Codes*, Bell Systems Tech. J. **29** (1950), 147–160.

[15] M. Harada, T. A. Gulliver, and H. Kaneta, *Classification of Extremal Double Circulant Self-dual Codes of Length Up To* 62, Discrete Math. **188** (1998), 127–136.

[16] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, London, UK, 4th edition (1960).

[17] T. Helleseth, *Legendre Sums and Codes Related to QR Codes*, Discr. Appl. Math. **35** (1992), 107–113.

[18] T. Helleseth and J. F. Voloch, *Double Circulant Quadratic Residue Codes*, IEEE Trans. Inform. Theory **50** (2004), 2154–2155.

[19] A. Hocquenghem, *Codes Corecteurs d'Erreurs*, Chiffres **2** (1959), 147–156.

[20] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, UK (2003).

[21] M. Karlin, *New Binary Coding Results by Circulants*, IEEE Trans. Inform. Theory **15** (1969), 81–92.

[22] J. Leon, V. Pless, and N. Sloane, *On Ternary Self-dual Codes of Length 24*, IEEE Trans. Inform. Theory **27** (1981), 176–180.

[23] F. J. Mac Williams, *The Structure and Properties of Binary Cyclic Alphabets*, Bell Sys. Tech. J. **44** (1965) 303–332.

[24] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier/North-Holland, New York, NY, USA (1978).

[25] C.L. Mallows and N. J. A. Sloane, *An Upper Bound for Self-dual Codes*, Inform. Control **22** (1973), 188–200, 2001.

[26] C. Monico and M. Elia, *Note on an Additive Characterization of Quadratic Residues Modulo p*, J. Comb. Inform. Syst. Sci. **31** (2006) 209–215.

[27] E. H. Moore, *Double Circulant Codes and Related Algebraic Structures*, Ph.D. dissertation, Dartmouth College (1976).

[28] W. W. Peterson, *Error Correcting Codes*, John Wiley and Sons, New York, NY, USA (1961).

[29] I. S. Reed and G. Solomon, *Polynomial Codes Over Certain Finite Fields*, J. Soc. Ind. Appl. Math. **8** (1960), 300–304.

[30] S. Roman, *Advanced Linear Algebra*, Springer, New York, NY, USA, 3rd edition (2008).

[31] M. R. Schroeder, *Number Theory in Science and Communication*, Springer-Verlag, Berlin, Germany, 4th edition (2006).

[32] C. E. Shannon, *A Mathematical Theory of Communication*, Bell Systems Tech. J. **27** (1948), 379–423, 623–656.

[33] R. K. Sharma and P. Yadav, *Unit Group of Algebra of Circulant Matrices*, Int. J. Group Theory **2**(4) (2013), 1–6.