A STUDY ON MAXIMUM DISTANCE SEPARABLE MATRICES WITH THEIR APPLICATIONS

A Thesis Submitted

in Fulfilment of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

by

Ayantika Laha

(2018MAZ0008)

DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY ROPAR

April, 2024

To my Mother
&
the loving memory of my Father

Declaration of Originality

I hereby declare that the work which is being presented in the thesis entitled **A STUDY ON MAXIMUM DISTANCE SEPARABLE MATRICES WITH THEIR APPLICATIONS** has been solely authored by me. It presents the result of my own independent investigation/research conducted during the time period from January, 2019 to February, 2024 under the supervision of Dr. Tapas Chatterjee, Associate Professor, Indian institute of Technology, Ropar. To the best of my knowledge, it is an original work, both in terms of research content and narrative, and has not been submitted or accepted elsewhere, in part or in full, for the award of any degree, diploma, fellowship, associateship, or similar title of any university or institution. Further, due credit has been attributed to the relevant state-of-the-art and collaborations (if any) with appropriate citations and acknowledgments, in line with established ethical norms and practices. I also declare that any idea/data/fact/source stated in my thesis has not been fabricated/ falsified/ misrepresented. All the principles of academic honesty and integrity have been followed. I fully understand that if the thesis is found to be unoriginal, fabricated, or plagiarized, the Institute reserves the right to withdraw the thesis from its archive and revoke the associated Degree conferred. Additionally, the Institute also reserves the right to appraise all concerned sections of society of the matter for their information and necessary action (if any). If accepted, I hereby consent for my thesis to be available online in the Institute's Open Access repository, inter-library loan, and the title & abstract to be made available to outside organizations.

Signature

Name: Ayantika Laha
Entry Number: 2018MAZ0008
Program: PhD
Department: Mathematics
Indian Institute of Technology Ropar
Rupnagar, Punjab 140001

Date: April 26, 2024

Acknowledgement

The present thesis is an outcome of consistent guidance and enlightening discussions with my supervisor, Dr. Tapas Chatterjee during my doctoral journey at IIT Ropar. It is undeniable that without his encouragement and enriching conversations, this work would not have attained its current state of completion. I extend my gratitude to him not only for his contributions to the mathematical aspects but also for imparting valuable lessons that have fostered my personal growth, making me a more contemplative, assured, and patient individual.

I extend my heartfelt appreciation to Prof. Somitra Kumar Sanadhya for his invaluable guidance and support during my Ph.D. journey. I am also grateful for his financial assistance, which enabled me to travel and attend conferences, enriching my academic experience. I am deeply grateful to my esteemed teachers and tutors who have played pivotal roles at every stage of my academic life, from my formative years in school to the present moment. A special acknowledgment goes to Dr. Avishek Adhikary for introducing me to the realm of cryptography and offering guidance during my post-graduation. I want to thank my doctoral committee members Dr. Madeti Prabhakar, Dr. Arti Pandey, and Dr. Venkata M. Gunturi, for providing me some useful suggestions and tips during presentations. I also acknowledge the supportive environment provided by the faculty members of the Department of Mathematics at IIT Ropar, spanning diverse research areas. My sincere gratitude to Prof. Santanu Sarkar from IIT Madras and Prof. Luciane Quoos Conte from Universidade Federal do Rio de Janeiro, Brazil for the careful reading of my thesis and recommended for the award of the PhD degree.

I am very grateful for various lab, library, mess, sports, hostel etc. facilities provided by IIT Ropar to make my stay an enjoyable and fruitful experience. The beautiful campus of IIT Ropar holds a special place in my heart, and I will always cherish the memories created here. A special thanks to Jaspreet ma'am and Neeraj ji for their technical and administrative assistance. Additionally, I extend sincere thanks to IIT Ropar for the financial support and NBHM, DAE for partial financial support, and also the FIST program of the Department of Science and Technology, Government of India, Reference No. SR/FST/MS-I/2018/22(C), for facilitating the successful conduct of my research within the institution.

I am deeply grateful for the unwavering support of my friends at IIT Ropar, particularly my fellow PhD candidates in the Mathematics Department, who have been invaluable companions throughout my doctoral journey. Special thanks to Suraj da, Sonika di, Subhajit da, Vikash, Himanshu, Swati, Neelam, Palak and my six bathcmates, Sonam, Niharika, Aditi, Monika, Ankita, Kusum for their valuable time and discussions. I feel genuinely grateful for the constant presence of Abhik and Suman by my side throughout these years. A special note of thanks to Anurima and Rimpa for being constants in my life since our school days.

Finally, I wish to extend my deepest gratitude and love to my parents for believing in me and my dreams, and consistently encouraging me to pursue them. Their unwavering

support in every step of my life and providing me with such a beautiful, comfortable life fills me with profound appreciation and admiration. Their love and guidance have shaped me into the person I am today, and for that, I am truly blessed. I am also thankful for the joy and companionship that my brother Ayantanu brings to my life. He is not only my steadfast companion in travel and enjoying food but also in sharing our love for watching movies and sports. His presence enriches my life in countless ways, and I am deeply grateful to have him by my side. I also thank my grandfathers and grandmothers for their boundless love and unwavering support. Above all, I express profound gratitude to the divine power I believe in, which has become my constant protector and guiding force. I am thankful for the strength granted to navigate life's challenges and for the blessings of wisdom and love that gracefully enrich my journey, infusing it with resilience and beauty.

Ayantika Laha
IIT Ropar

Certificate

This is to certify that the thesis entitled **A STUDY ON MAXIMUM DISTANCE SEPARABLE MATRICES WITH THEIR APPLICATIONS**, submitted by **Ayantika Laha (2018MAZ0008)** for the award of the degree of **Doctor of Philosophy** of Indian Institute of Technology Ropar, is a record of bonafide research work carried out under my guidance and supervision. To the best of my knowledge and belief, the work presented in this thesis is original and has not been submitted, either in part or full, for the award of any other degree, diploma, fellowship, associateship or similar title of any university or institution.

In my opinion, the thesis has reached the standard fulfilling the requirements of the regulations relating to the Degree.

Signature of the Supervisor
Dr. Tapas Chatterjee
Mathematics
Indian Institute of Technology Ropar
Rupnagar, Punjab 140001

April 26, 2024

Abstract

In our digitally connected world we share a lot of personal information and classified data through insecure channels which require robust protection against third-party threats. Thus, establishing secure communication channels becomes imperative and block ciphers emerge as key guardians of confidentiality, integrity, and authenticity in this digital landscape. The use of Maximum Distance Separable (MDS) matrices in block cipher design plays a crucial role in defending against various attacks, and this thesis delves into the intricate world of MDS matrices. MDS matrices trace their origins to the generator matrix of maximum distance separable codes in coding theory — a code that achieves the Singleton bound. Stemming from the most fascinating code of coding theory and finding applications in symmetric key cryptography schemes, MDS matrices have garnered substantial attention due to their various direct constructions, recursive constructions, and lightweight constructions. Each method of constructing MDS matrices unfolds its significance, creating a vibrant landscape for independent research.

The initial part of this thesis specifically emphasizes the direct construction of MDS matrices and introduces easily implementable strategies for their inverse matrices. This research endeavor began in 1977 with the proposition by Macwillams and Solane that utilizes Cauchy matrices over finite fields for the direct construction of MDS matrices. Following this result, we introduce a new construction for MDS matrices which are not involutory, but semi-involutory in nature. These findings open up a new avenue in the construction of easily invertible MDS matrices, considering the generalization of both involutory and orthogonal properties. We have demonstrated that several Cauchy based constructions proposed by Youssef, Mister and Tavares, Gupta and Ray, while not inherently involutory or orthogonal, can have their inverse matrices easily implemented by utilizing the original matrix and multiplying it with specific diagonal matrices. In this thesis, we study another significant category of matrices – circulant matrices. Our initial focus involves examining the characteristics of the associated diagonal matrices of a circulant semi-involutory (semi-orthogonal) matrix over finite fields. Next, our attention turns to the diverse generalizations of circulant matrices. Specifically, we explore two prominent types: g-circulant matrices, introduced by Friedman in 1961, and cyclic matrices, which were introduced by Liu and Sim in 2016. We establish a profound connection between these two matrices and leveraging this connection, we provide a positive resolution to the conjecture posited by Liu and Sim. Infact, we prove the non-existence of involutory g-circulant MDS matrices of order $2^d \times 2^d$ over the finite field $\mathbb{F}_{2^m}$. A thorough exploration into g-circulant MDS matrices is conducted, considering properties such as involutory, orthogonal, semi-involutory, and semi-orthogonal.

We also present a comprehensive exploration of the general structure of semi-involutory maximum distance separable matrices of order of 3×3 over finite fields of characteristic 2. Our findings align with the research conducted on involutory MDS matrices by Güzel, Sakalli, Akleylek, Rijmen and Çengellenmiş and some other authors. These generalized structures provide valuable insights into the overall count of MDS

matrices across finite fields. Notably, for orders exceeding four, the pursuit of such structures remains an open avenue of investigation.

In the last part of the thesis, we revisit a generalization of conventional encryption schemes known as Format Preserving Encryption (FPE) schemes. Traditional encryption techniques inherently mandate the elimination of the input format to maintain the "semantic security" of the encryption algorithm. However, there arise scenarios where it becomes imperative to not only retain the format but also preserve the length of the plaintext. This capability proves valuable in practical applications, such as encrypting sensitive information like credit card numbers, social security numbers, or database entries, where maintaining the original structure is crucial. Note that, a standard block cipher would require a fixed size input and produce a (possibly longer than the plaintext) fixed size output. This gap between what was available and what was needed in certain practical situations prompted the exploration and design of encryption schemes that preserve both the length and format of the input. The first formal study of such schemes, known as Format Preserving Encryption schemes, was initiated by Bellare *et al.* in 2009. Since then, numerous FPE schemes have been proposed by various authors up to the present day. In the year 2016, Gupta *et al.* defined an algebraic structure named Format Preserving Set (FPS) in the diffusion layer of an FPE scheme. Their work established a significant correlation between the cardinality of these sets and the potential message space of an FPE scheme over a finite field. This result affirms that numerous crucial cardinalities within the message space are unattainable over finite fields. Subsequently, Barua *et al.* extended the search of FPS over finite commutative rings. Building upon this generalization, we present diverse constructions of format preserving sets over finite commutative rings with identity and finite modules over principal ideal domains. Notably, we provide examples of format preserving sets with cardinalities of 26 and 52 over torsion modules and rings. These particular cardinalities hold significance as they align with the sets of English alphabets, both in lowercase and with capitalization. Moreover, by considering a finite Abelian group as a torsion module over a PID, we show that a matrix M with entries from the PID is MDS if and only if M is MDS under the projection map on the same Abelian group.

Keywords: Cauchy matrices; Circulant matrices; Cyclic matrices; g-Circulant matrices; Semi-involutory matrices; Semi-orthogonal matrices; MDS matrices; Format preserving encryption; Format preserving set

List of Publications

- T. Chatterjee and **A. Laha**, *A note on Semi-Orthogonal (G-matrix) and Semi-Involutory MDS Matrices*, **Finite Fields and Their Applications**, **92** (2023), Paper No. 102279, 27.
- T. Chatterjee, **A. Laha** and S. K. Sanadhya, *On the Structure of Format Preserving Sets in the Diffusion Layer of Block Ciphers*, **IEEE Transactions on Information Theory**, **68** (2022), no. 12, pp. 8268–8279.
- T. Chatterjee and **A. Laha**, *A Characterization of Semi-Involutory MDS Matrices* (submitted).
- T. Chatterjee and **A. Laha**, *On Cyclic non-MDS Matrices* (submitted).
- T. Chatterjee and **A. Laha**, *On MDS Property of g-Circulant Matrices* (submitted).
- T. Chatterjee and **A. Laha**, *On MDS Property of Circulant Matrices* (submitted).

List of Notations

Notation	Description
$\mathbb{Z}$	Ring of integer
$\mathbb{Z}_m$	Ring of integer modulo m
$\mathbb{C}$	Field of complex numbers
$\mathbb{F}_q$	Finite field with q elements
$\mathbb{F}_q^*$	All non-zero elements of $\mathbb{F}_q$
$\mathbb{F}_{2^m}$	Finite field of characteristic 2 with 2^m elements
$\mathbb{F}_{p^m}$	Finite field of characteristic p with p^m elements
$\mathbb{F}_q^n$	Vector space of dimension n over $\mathbb{F}_q$
dim C	Dimension of the vector space C
S_n	Symmetric group of n elements
$\mathbf{v}$	Vector of n elements
wt($\mathbf{v}$)	Total number of non-zero entries in $\mathbf{v}$
$\gcd(n, m)$	Greatest common divisor of n and m
$A_{n\times n}$	An $n \times n$ matrix A
a_{ij}	Entry at the i-th row and j-th column of the matrix $A = (a_{ij})$
$A(i, j)$	a_{ij}
R_i	The i-th row of the matrix A
C_j	The j-th column of the matrix A
A^{-1}	Inverse of the matrix A
A^T	Transpose of the matrix A
$\det A$	Determinant of the matrix A
trace A	Sum of diagonal elements of the matrix A
$A_{m\times n}(\mathcal{A})$	A $m \times n$ matrix A with entries from some algebraic structure $\mathcal{A}$
$i \oplus j$	Bitwise XOR of binary representation of i and j
Vand$(x_0, x_1, \cdots, x_{n-1})$	Vandermonde matrix $V(x_0, x_1, \cdots, x_{n-1}) = (x_i^{j-1})_{i,j=1}^r$
$\mathbb{V}(\mathbf{h}, Z)$	Generalized Vandermonde matrix with $\mathbf{h}$ is an increasing sequence of positive integers and Z is an increasing sequence of non-negative integers
$M_1 \sim_{P.E} M_2$	Matrices M_1 and M_2 are permutation equivalent

Contents

List of Figures

Chapter 1

Introduction

In today's digitally connected world, we share a lot of information through a wide range of online platforms and technologies. Sometimes this information is sensitive like our bank details, medical history, or some secret military details which need to be protected from third parties. Therefore, establishing a secure communication channel is the best option to protect the information. Block ciphers play a pivotal role in this scenario, ensuring the confidentiality, integrity, and authenticity of our transmitted information. Maximum Distance Separable (MDS) matrices stands as a crucial tool in the construction of a block cipher for enhancing security. In the present chapter, we provide a comprehensive insight into the utilization and diverse constructions of MDS matrices used in block ciphers which are relevant to our discussion, and some of them we shall discuss in upcoming chapters in detail.

1.1 Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of an adversary. The prefix "crypt" means "hidden" and the suffix "graphy" means "writing". Modern cryptography lies in the intersection of various fields including mathematics, computer science, electrical engineering, physics, and more. The basic idea of cryptography is to *encrypt* the message using a *key* to protect the information and then send it through an insecure channel. Anybody who has the corresponding key can *decrypt* the information and recover the original message. To any unauthorized observer, this encrypted information should appear as gibberish and unintelligible.

A *cryptosystem* consists of an encryption algorithm, a decryption algorithm, and a key generation algorithm. On the other hand, *cryptanalysis* is the technique to decrypt the encrypted text without knowing the original key. To design a cryptosystem, deep knowledge of cryptanalysis is required to protect the system from any attack. Therefore, cryptography and cryptanalysis are like the two sides of the same coin, inextricably intertwined with each other.

In modern days, two main approaches in the design of cryptosystems are *symmetric key cryptosystem* and *public key cryptosystem*. This division depends upon the number of keys used in the system. In a symmetric key setting, two parties share a key to communicate secretly. Using this shared key, one party encrypts a message or *plain text*, transforming it into *cipher text*. The other party uses the same key to decrypt the received cipher text and retrieve the original message.

The public key cryptosystem employs a pair of keys, a public key for encryption and a secret key for decryption. In this process, the sender encrypts the plain text using the recipient's public key and transmits it through an insecure channel. The receiver then decrypts the cipher text using their secret key. Even if the public key is available to adversaries, they cannot get the original message. In both scenarios, the security of the cryptosystem depends upon the key. Kerckhoffs's principle underscores this by asserting that "*The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.*"

1.1.1 Symmetric key cryptography

A symmetric key cryptography scheme consists of three fundamental components: a key space K, an encryption algorithm $\mathcal{E}$, and a decryption algorithm $\mathcal{D}$. The encryption algorithm chooses a key k from key space and a plain text m from the space of possible messages M, yielding a cipher text c that belongs to the set of possible cipher texts C. This process can be viewed as a function $\mathcal{E} : K \times M \to C$. Similarly, the decryption can be viewed as the function $\mathcal{D} : K \times C \to M$. For a successful cryptography scheme, the decryption and encryption functions must adhere to the condition

$$\mathcal{D}(k, \mathcal{E}(k, m)) = m,$$

for all $m \in M$ and $k \in K$. Symmetric key algorithms predominantly fall into two families: *block ciphers* and *stream ciphers*. While stream ciphers encrypt one byte of plain text at a time, block cipher encrypts a fixed size of data block at a time. Some well known block ciphers are Data Encryption Standard (DES) [1], Advanced Encryption Standard (AES) [2], Twofish [3] etc., and some well known stream ciphers are RC4 [4], ChaCha20 [5], Salsa20 [6] etc.

1.1.2 Block ciphers

Block ciphers are building blocks of many symmetric key protocols, playing a pivotal role in securing digital information. Given that, computers store data in binary format where each bit represents a value of either 0 or 1, block cipher algorithms operate on binary inputs. These algorithms take a key of length k bits and a message of size n bits as input and produce an output block of length n bit. Hence both the encryption and decryption of a block cipher are function

$$F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n,$$

where k is the key length and n is the block length. This function acts as a permutation of n bit binary digits. The challenge in the block cipher design is to construct a set of permutations with a concise key that mimics a random permutation. For this purpose, Claude Shannon introduced the idea of *confusion* and *diffusion* in his seminal paper [7].

The idea works as follows: Suppose we want to construct a random looking permutation F over a 64 bit input block. The key k of F will specify 8 permutations, say $f_1, f_2, \ldots, f_8$ such that each have 8 bit block length. For an input $x \in \{0,1\}^{64}$, we separate it as 8 bytes, say $x_1, x_2, \ldots, x_8$ and set

$$F(k, x) = f_1(x_1) \parallel f_2(x_2) \parallel \cdots \parallel f_8(x_8).$$

These f_i's introduce *confusion* into F.
In the *diffusion* step the bits of the output are permuted. This step spreads the local change that occurs in the diffusion layer throughout the entire 64 bit block. These two steps are together called a *round*.
Substitution-permutation networks: A substitution-permutation network (SPN) can be seen as a direct implementation of confusion - diffusion paradigm. It is a very simple and elegant structure with provable security against various attacks. The substitution layer employs a publicly defined "substitution function," known as an S-box. This layer utilizes multiple S-boxes, and the subsequent permutation layer rearranges the resulting output from the substitution layer. Figure 1.1 illustrates a single round of an SPN. The

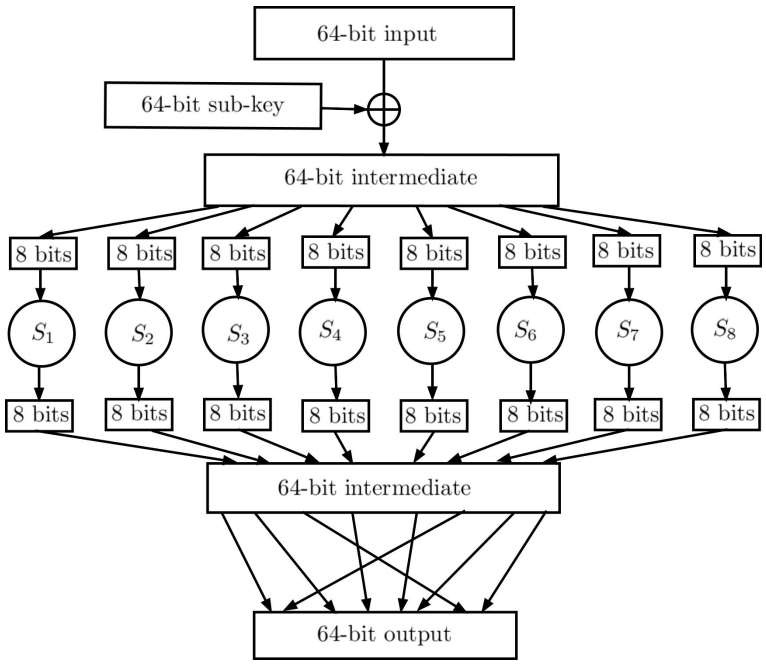

Figure 1.1: SPN struture

S-boxes induce confusion while mixing permutations introduce diffusion. The security of an SPN based block cipher depends on many factors like the number of rounds, choice of S-box, mixing permutations, key schedule, etc. A fundamental requirement for a block cipher is the presence of the "avalanche effect," which ensures that a small input change affects every output bit. Two primary methods to introduce avalanche effects in an SPN based block cipher are the following:

- The S-boxes are designed in such a way that one bit difference in the input of an

S-box should spread to at least two bits.

- The mixing permutations are designed so that the output bits of any given S-box are used as input to multiple S-boxes in the next round.

Heys and Tavares [8, 9, 10] demonstrated that choosing S-boxes with strong diffusion characteristics improves the avalanche behaviour of an SPN. In [11], Serge Vaudenay introduced multipermutations as a formalization of perfect diffusion.

Definition 1.1.1. *A (r, n)-multipermutation over an alphabet Z is a function f from Z^r to Z^n such that two different $(r+n)$-tuples of the form $(x, f(x))$ cannot collide in any r positions.*

An equivalent definition says that the set of all $(r+n)$-tuples of the form $(x, f(x))$ is an error correcting code with minimal distance $n+1$, which is the maximal possible. In the case of a linear function f, this aligns with the definition of MDS codes. Therefore, employing an appropriate linear transformation in place of a permutation between rounds of S-boxes offers an alternative approach for achieving optimal diffusion. The idea of using linear transformation found its inception in the diffusion layer of the block cipher SHARK [12] by Rijmen *et al.* in 1996. They choose a linear function $L : \mathbb{F}_{2^m}^n \to \mathbb{F}_{2^m}^n$ that maximize the value of $\mathcal{B}(L)$, where

$$\mathcal{B}(L) = \min_{\mathbf{a}\neq\mathbf{0}, \mathbf{a}\in\mathbb{F}_{2^m}^n} \{\mathrm{HW}(\mathbf{a}) + \mathrm{HW}(L(\mathbf{a}))\},$$

with $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_{2^m}^n$ and $\mathrm{HW}(\mathbf{a}) = |1 \leq i \leq n : a_i \neq 0|$ is the Hamming weight of $\mathbf{a}$. Since $\mathrm{HW}(\mathbf{a}) \leq n$ for all choice of L, if $\mathrm{HW}(\mathbf{a}) = 1$, then $\mathcal{B} \leq n+1$. An invertible linear mapping L is called *optimal* if $\mathcal{B} = n+1$. To achieve this optimal linear transformation, block cipher SHARK used the generator matrix of a $[2n, n, n+1]$ maximum distance separable code (see Definition 1.2.2). The following proposition of Rijmen *et al.* [12] proves the significance of using an MDS matrix.

Proposition 1.1.2. *Let $\mathcal{C}$ be a $[2n, n, n+1]$ linear code over the finite field $\mathbb{F}_{2^m}$. Let G be the generator matrix of $\mathcal{C}$ in echelon form, i.e., $G = [I_{n\times n}|B_{n\times n}]$. Then $\mathcal{C}$ defines an optimal invertible linear mapping $\gamma : (\mathbb{F}_{2^m})^n \to (\mathbb{F}_{2^m})^n$ by $\gamma(X) \to B \cdot X$.*

In 1997, Daemen *et al.* incorporated an MDS matrix into the block cipher SQUARE [13]. Subsequently, in 1998, Daemen and Rijmen used a circulant MDS matrix in the block cipher AES. Moreover, several SPN-based block ciphers, such as PRESENT [14], SQUARE [13], and Twofish [3] have integrated the MDS matrix into their diffusion layers, demonstrating the significance and effectiveness of MDS matrices in these ciphers.
The assessment of the diffusion power in the transformations within the diffusion layer of a block cipher is measured using the *Branch Number* (see [2], Chapter 9). For linear transformations, both the differential and linear branch numbers play crucial roles in determining the efficacy of these transformations.

Definition 1.1.3. *The differential branch number of a linear transformation ϕ over the finite field $\mathbb{F}_{2^m}$ is given by*

$$\mathcal{B}_d(\phi) = \min_{\boldsymbol{a}\neq\boldsymbol{0},\boldsymbol{a}\in\mathbb{F}_{2^m}^n} \{Wt(\boldsymbol{a}) + Wt(\phi(\boldsymbol{a}))\}.$$

Definition 1.1.4. *The linear branch number of a linear transformation ϕ over the finite field $\mathbb{F}_{2^m}$ is given by*

$$\mathcal{B}_l(\phi) = \min_{\boldsymbol{a}\neq\boldsymbol{0},\boldsymbol{a}\in\mathbb{F}_{2^m}^n} \{Wt(\boldsymbol{a}) + Wt(M^t\boldsymbol{a})\},$$

where $\phi(\boldsymbol{x}) = M \cdot \boldsymbol{x}$.

Note that the maximal value of $\mathcal{B}_d(\phi)$ and $\mathcal{B}_l(\phi)$ are $n+1$. In general $\mathcal{B}_d(\phi) \neq \mathcal{B}_l(\phi)$, but if a matrix achieves the maximum possible differential or linear branch number, then both branch numbers are equal. Consequently, for an MDS matrix M, $\mathcal{B}_d(\phi) = \mathcal{B}_l(\phi) = n+1$. This property accentuates the optimal diffusion characteristics inherent in MDS matrices. In general, SPN needs two different modules for the encryption and the decryption operations. The decryption process of an SPN is performed by running the data backward through the inverse network (i.e., applying the key scheduling algorithm in reverse and using the inverse S-boxes and the inverse linear transformation layer). In [15], Youssef *et al.* proposed a special class of SPNs that has the advantage that the same network can be used to perform both the encryption and the decryption operations. The basic idea is to use involutory substitution layers and involutory linear transformations. In the following section, we delve into the details of MDS codes and matrices, preceded by a brief overview of an alternative approach to block cipher design.

Fiestel Network: An alternative approach to construct a block cipher is the Fiestel Network. Figure 1.2 shows two rounds of a Feistel network. A Feistel network operates in a series of rounds. In each round, there is a keyed round function. In the initial round, the n-bit input is bifurcated into two halves L_0, R_0 and each consisting of $\frac{n}{2}$ bits. The resulting output L_1, R_1 determines as follows:

$$L_1 = R_0 \text{ and } R_1 = L_0 \oplus F_1(R_0),$$

where $F_1 : \{0,1\}^{\frac{n}{2}} \to \{0,1\}^{\frac{n}{2}}$ is a keyed function.

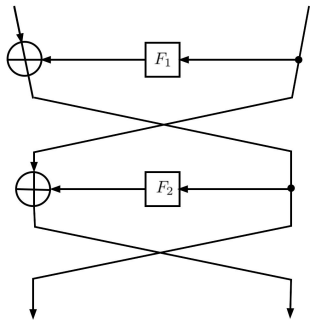

Figure 1.2: Two round Fiestel network

1.2 Maximum distance separable matrix

As discussed earlier, MDS matrices found their application in the diffusion layer of block ciphers and it has a direct connection with one of the most fascinating codes in coding theory, the maximum distance separable codes.
A linear code C is denoted by three parameters, n, k and d, where n and k are the length and dimension of the code and d is the minimum Hamming distance between the codewords. Richard Singleton established the following inequality between the parameters of a code, named Singleton bound:

Theorem 1.2.1. *Let C be an $[n, k, d]$ code, then $n - k \geq d - 1$.*

Codes that satisfy $d = n-k+1$ are called maximum distance separable codes, abbreviated as MDS codes. These codes achieve the maximum possible distance between the codewords. Reed-Solomon codes (see [16], Chapter 10) stand out as a prominent example of MDS codes. A characterization of MDS codes in terms of a systematic generator matrix is provided by the following theorem:

Theorem 1.2.2. *An $[n, k, d]$ code C with generator matrix $[I_{k\times k}|A]$ where A is a $k \times (n - k)$ matrix is MDS if and only if every square submatrix of A, formed by any i rows and i columns, for any $i = \{1, 2, \ldots, min(k, n - k)\}$, is non-singular.*

The matrix A in Theorem 1.2.2 is called an MDS matrix. Macwillams and Solane [16] highlighted Cauchy matrices as a prime example of MDS matrices under certain conditions. Specifically, they stated the following:

Corollary 1.2.3. *Let $\{x_1, x_2, \ldots, x_n\}$ and $\{y_1, y_2 \ldots, y_n\}$ be two sets of elements from a finite field $\mathbb{F}$, with x_i's and y_j's being distinct, and $x_i + y_j \neq 0$ for $1 \leq i, j \leq n$. Then every submatrix of the Cauchy matrix $A = (\frac{1}{x_i+y_j})$, $1 \leq i, j \leq n$ is non-singular over $\mathbb{F}$.*

In 1996, Youssef *et al.* [15] introduced the concept of using involutory linear transformations to perform encryption and decryption operations in the same network. They presented the following two methodologies for constructing involutory linear transformations.

- First construction is the matrix $\begin{bmatrix} A & A^{-1} \\ A^3 + A & A \end{bmatrix}$, which is an $n \times n$ involutory matrix over the finite field $\mathbb{F}_{2^m}$, where A is an $\frac{n}{2} \times \frac{n}{2}$ arbitrary non-singular matrix.
- Another construction utilizes a Cauchy matrix A to construct an MDS matrix that satisfies $A^2 = c^2 I$, where c is the sum of the entries of the first row of A.

In contrast, although any square submatrix of a Vandermonde matrix with real, positive entries is non-singular, the same cannot be guaranteed for Vandermonde matrices over finite fields. For example, see Fact 9 of [17]. Thus, while Cauchy matrices facilitate direct MDS matrix construction, Vandermonde matrices fail to achieve this property.

In 2004, Lacan and Fimes [18] first constructed systematic MDS erasure codes using two Vandermonde matrices. Their results established a direct method for constructing MDS matrices using two Vandermonde matrices. Let $V(a_1, a_2, \ldots, a_r) = (a_i^{j-1})_{i,j=1}^{r}$ represent a Vandermonde matrix. The result of Lacan and Fimes is the following regarding the characteristic of the submatrices of Vandermonde matrices:

Theorem 1.2.4. *Let $\{a_1, a_2, \ldots, a_r\}$ and $\{b_1, b_2, \ldots, b_r\}$ be $2r$ distinct elements over the finite field $\mathbb{F}_q$. Then every square submatrix of the matrix $V(a_1, a_2, \ldots, a_r)^{-1} \cdot V(b_1, b_2, \ldots, b_r)$ is non-singular.*

This theorem can be utilized to construct a systematic generator matrix of an MDS code, as stated in the following theorem:

Theorem 1.2.5. *Let $V(a_1, a_2, \ldots, a_k)$ be a $k \times k$ non-singular Vandermonde matrix and $V(b_1, b_2, \ldots, b_{n-k})$ be a $k \times (n-k)$ Vandermonde matrix. Then the code defined by the generator matrix*

$$G = [I_{k\times k} | V(a_1, a_2, \ldots, a_k)^{-1} \cdot V(b_1, b_2, \ldots, b_{n-k})]$$

is an MDS code if and only if a_j and b_j are n distinct elements.

These findings initiated a novel approach to directly constructing MDS matrices using Cauchy and Vandermonde matrices. Subsequent studies [18, 19, 20, 21] expanded upon this, providing diverse constructions of MDS matrices, which we will briefly discuss next.

1.2.1 Direct construction of MDS and involutory MDS matrices

The prevalence of MDS matrices in SPN-based block ciphers motivated various author to develop direct methods for constructing involutory MDS matrices. In 2012, Sajadieh *et al.* [19] showed that the Vandermonde based MDS matrix construction proposed by Lacan and Fimes in [18], could be transformed into an involutory matrix. This transformation involved a careful selection of the b_i's from the underlying finite field. Their work substantiated the following results:

Theorem 1.2.6. *Let $V_1 = Vand(a_0, a_1, \ldots, a_{n-1})$ and $V_2 = Vand(b_0, b_1, \ldots, b_{n-1})$ be two invertible Vandermonde matrices with $b_i = l + a_i$ for all $i = 0, 1, 2, \ldots, n-1$, and l is an arbitrary non-zero element. Then $V_1^{-1}V_2$ is an upper triangular matrix, and its non-zero elements are determined by the powers of l. Furthermore, the matrices V_1 and V_2 satisfy the equation $V_2V_1^{-1}V_2 = V_1$.*

An immediate application of this theorem yields the following corollary:

Corollary 1.2.7. *Let $V_1 = Vand(a_0, a_1, \ldots, a_{n-1})$ and $V_2 = Vand(b_0, b_1, \ldots, b_{n-1})$ be two invertible Vandermonde matrices over the finite field $\mathbb{F}_{2^m}$ with $b_i = l + a_i$, $l \in \mathbb{F}_{2^m}^*$ and $a_i \neq b_j$ for all $i, j = 0, 1, \ldots, n-1$. Then $V_2V_1^{-1}$ is an involutory MDS matrix.*

Sajadieh *et al.* ingeniously used the entries of the Vandermonde matrix from an additive subgroup of the finite field $\mathbb{F}_{2^m}$ to construct Hadamard MDS matrices.

A Hadamard matrix H adheres to the identity $H^2 = c^2 I$, where c denotes the sum of entries in any row and I represents the identity matrix. This property simplifies the determination of H^{-1}. Gupta and Ray restated this result in [20], as outlined below. Before that, we provide the definition of a *Special Vandermonde matrix*.

Definition 1.2.8. *Let $G = \{x_0, x_1, \ldots, x_{2^n-1}\}$ be an additive subgroup of order 2^n of the finite field $\mathbb{F}_{2^m}$, which is linear span of n linearly independent the elements $\{x_1, x_2, x_{2^2}, \ldots, x_{2^{n-1}}\}$. Each $x_i \in G, 0 \leq i \leq 2^n - 1$ is of the form $x_i = \sum_{i=0}^{n-1} b_i x_{2^i}$, where $(b_{n-1}, \ldots, b_1, b_0)$ is the binary representation of i. A Vandermonde matrix $V = Vand(y_0, y_1, y_2, \ldots, y_{2^n-1})$ is called Special Vandermonde matrix if $y_i = l + x_i$ for all $i = 1, 2, \ldots, 2^n - 1$.*

The construction of a Hadamard matrix using a Vandermonde matrix is as follows:

Theorem 1.2.9. *Let $V_1 = Vand(x_0, x_1, \ldots, x_{2^n-1})$ and $V_2 = Vand(y_0, y_1, \ldots, y_{2^n-1})$ be two Special Vandermonde matrices over the finite field $\mathbb{F}_{2^m}$ with $y_i = x_0 + y_0 + x_i$, and $y_0 \notin \{x_0, x_1, \ldots, x_{2^n-1}\}$. Then $V_1^{-1} V_2$ is a Hadamard involutory MDS matrix.*

In [20], the authors further studied Cauchy based MDS matrix construction. They constructed an MDS matrix of order a power of 2 using a Cauchy matrix A with entries from an additive subgroup of the finite field $\mathbb{F}_{2^m}$. The construction is as follows:

Theorem 1.2.10. *Let $G = \{x_0, x_1, \ldots, x_{n-1}\}$ be an additive subgroup of the finite field $\mathbb{F}_{2^m}$. Consider the coset $l + G, l \notin G$ with the elements $y_j = l + x_j, j = 0, 1, \ldots, n-1$. Then the $n \times n$ Cauchy matrix $A = (\frac{1}{x_i + y_j}), 0 \leq i, j \leq n - 1$ is an MDS matrix.*

The Cauchy matrix A constructed in Theorem 1.2.10 possesses the following interesting properties:

- The matrix A has exactly n distinct entries.
- The matrix A is symmetric and all rows are permutations of the first row.
- The matrix A satisfies $A^2 = a^2 I$, where $a = \sum_{j=0}^{n-1} \frac{1}{l + x_j}$.
- The matrix $a^{-1} A$ is an involutory MDS matrix, where a is the sum of all elements of any row.

Considering the ease of computing the inverses of Hadamard matrices, Gupta and Ray constructed Hadamard matrices using Cauchy based MDS matrix construction. Their result is as follows:

Theorem 1.2.11. *Let $G = \{x_0, x_1, \ldots, x_{2^n-1}\}$ be an additive subgroup of the finite field $\mathbb{F}_{2^m}$, which is a linear span of n linearly independent elements $\{x_1, x_2, x_{2^2}, \ldots, x_{2^{n-1}}\}$, such that $x_i = \sum_{i=0}^{n-1} b_i x_{2^i}$, where $(b_{n-1}, \ldots, b_1, b_0)$ is the binary representation of i. Let $y_i = l + x_i$ for $0 \leq i \leq 2^n - 1$, where $l \in \mathbb{F}_{2^m} \setminus G$. Then the Cauchy matrix $A = (a_{i,j}) = (\frac{1}{x_i + y_j}), 0 \leq i, j \leq 2^n - 1$ is a Hadamard MDS matrix.*

Note that, in both Theorem 1.2.10 and Theorem 1.2.11, the order of the matrices are power of 2. Therefore to obtain a matrix of a specific order k, we must initially generate a matrix of size 2^n where $k \leq 2^n$, followed by extracting a $k \times k$ submatrix from it. However, this process does not guarantee that the resulting submatrices will exhibit the desired involutory property.

Furthermore, in [21], Cui, Jin and Kong introduced another interesting class of Cauchy matrices, termed *compact Cauchy matrix*. These matrices exhibit the fewest distinct entries, rendering them particularly advantageous for implementation purposes. The definition of compact Cauchy matrix is the following:

Definition 1.2.12. *Let A be an $n \times n$ Cauchy matrix. If A has precisely n distinct entries, then A is a compact Cauchy matrix.*

It is worth noting that the Cauchy MDS matrix outlined in Theorem 1.2.10 qualifies as a compact Cauchy matrix. Additionally, in [21] Cui *et al.* presented an alternative condition for constructing compact Cauchy matrices in finite fields of characteristic 2.

Theorem 1.2.13. *The matrix A is an $n \times n$ compact Cauchy matrix over $\mathbb{F}_{2^m}$ generated by $X = (x_0, x_1, x_2, \ldots, x_{n-1}, x_n, \ldots, x_{2n-1})$ if and only if there exists an additive subgroup H of $\mathbb{F}_{2^m}$ with elements a, b such that $a + b \notin H$, $a + H = \{x_0, x_1, x_2, \ldots, x_{n-1}\}$ and $b + H = \{x_n, \ldots, x_{2n-1}\}$.*

In the next theorem, we note an alternative method to construct MDS matrices using the primitive elements of the finite field, as introduced by Roth and Seroussi in [22].

Theorem 1.2.14. *Let S be the following triangular array over the finite field $\mathbb{F}_q$:*

$$S_q = \begin{matrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 1 & a_1 & a_2 & \cdots & a_{q-3} & a_{q-2} & \\ 1 & a_2 & a_3 & \cdots & a_{q-2} & & \\ 1 & a_3 & a_4 & \cdots & & & \\ \vdots & \vdots & \vdots & & & & \\ 1 & a_{q-3} & a_{q-2} & & & & \\ 1 & a_{q-2} & & & & & \\ 1 & & & & & & \end{matrix},$$

where $a_i = \frac{1}{1-\gamma^i}, 1 \leq i \leq q-2$ for an arbitrary primitive element γ of $\mathbb{F}_q$. Then every square submatrix of S_q is non-singular.

In [20], a relation was established between the construction of Hadamard MDS matrices using Cauchy matrices and Vandermonde matrices. Let $G = \{\gamma_0, \gamma_1, \ldots, \gamma_{d-1}\}$ denote an additive subgroup of $\mathbb{F}_{2^m}$ of order d, where $\gamma_0 = 0$ and $\gamma_i + \gamma_j = \gamma_{i \oplus j}$. Consider two arbitrary elements r_1, r_2 from $\mathbb{F}_{2^m}$ such that $r_1 + r_2 \notin G$. Construct three cosets of G as

follows:

$$r_1 + G = \{\alpha_i = r_1 + \gamma_i, \text{ for } i = 0, 1, \ldots, d-1\},$$
$$r_2 + G = \{\beta_i = r_2 + \gamma_i, \text{ for } i = 0, 1, \ldots, d-1\},$$
$$r_1 + r_2 + G = \{\delta_i = r_1 + r_2 + \gamma_i, \text{ for } i = 0, 1, \ldots, d-1\}.$$

Let $V_1 = \text{Vand}(\alpha_0, \alpha_1, \ldots, \alpha_{d-1})$ and $V_2 = \text{Vand}(\beta_0, \beta_1, \ldots, \beta_{d-1})$ be two Vandermonde matrices and $M = (m_{i,j}) = (\frac{1}{\gamma_i + \delta_j})$, $1 \leq i, j \leq d-1$. Then the Vandermonde matrix AB^{-1} and the Cauchy matrix M satisfy the following relation:

Theorem 1.2.15. *$AB^{-1} = \frac{1}{c}M$, where $c = \sum_{k=0}^{d-1} \frac{1}{\delta_k}$.*

In 2019, the authors of [17] generalized the aforementioned relation, allowing entries of both Vandermonde and Cauchy matrices to be arbitrary elements of the finite field. Let $\{x_0, x_1, \ldots, x_{n-1}\}$ and $\{y_0, y_1, \ldots, y_{n-1}\}$ are $2n$ distinct elements from $\mathbb{F}_{2^m}$ such that $x_i + y_j \neq 0$ for all $0 \leq i, j \leq n-1$. Let $V_1 = \text{Vand}(x_0, x_1, \ldots, x_{n-1})$ and $V_2 = \text{Vand}(y_0, y_1, \ldots, y_{n-1})$ be two Vandermonde matrices and $M = (m_{i,j}) = (\frac{1}{x_i + y_j})$ be a Cauchy matrix. Then the matrices $V_1^{-1}V_2, V_2^{-1}V_1$ and M are MDS matrices. The result of Gupta *et al.* revealed a non-trivial relationship between these matrices, succinctly stated as follows:

Theorem 1.2.16. *Suppose V_1, V_2 and M are defined as above and $V_1^{-1} = (b_{i,j})$, $0 \leq i, j \leq n-1$. Then $D_1 M D_2 = V_1^{-1}V_2$, where*

$$D_1 = \textit{diag}(b_{0,n-1}, b_{1,n-1}, \ldots, b_{n-1,n-1}), \textit{ and}$$

$$D_2 = \textit{diag}(\prod_{k=0}^{n-1}(x_k + y_0), \prod_{k=0}^{n-1}(x_k + y_1), \ldots, \prod_{k=0}^{n-1}(x_k + y_{n-1})).$$

According to the MDS matrix construction described in Corollary 1.2.7, it is possible to construct involutory Vandermonde MDS matrix. Employing the similar construction, i.e., $y_i = l + x_i$ it is possible to construct a Cauchy matrix M, and the resultant Cauchy matrix is MDS but not necessarily involutory. Nevertheless, Theorem 1.2.16 asserts that this particular M can be transformed into an involutory MDS matrix through an appropriate choice of diagonal matrices D_1 and D_2.

We discussed the existence of MDS Cauchy matrices of order $n \times n$ with precisely n distinct entries. Additionally, in [17], the authors constructed Vandermonde MDS matrices with similar property. This construction is derived from Theorem 1.2.10 and stated in the following theorem.

Let $\{x_0, x_1, \ldots, x_{n-1}\}$ be an additive subgroup of $\mathbb{F}_{2^m}$ and $V = \text{Vand}(x_0, x_1, \ldots, x_{n-1})$. Let $V^{-1} = (b_{i,j})$ and $\gamma = \prod_{i=0}^{n-1} x_i$. Now the theorem is the following:

Theorem 1.2.17. *Let $V_1 = Vand(x_0, x_1, \ldots, x_{n-1})$ and $V_2 = Vand(y_0, y_1, \ldots, y_{n-1})$ be two Vandermonde matrices with $y_i = l + x_i, l \notin G$. Then $V_1^{-1}V_2$ is a compact involutory MDS matrix.*

From the aforementioned constructions, we can see that Hadamard matrices plays a significant role in the construction of involutory MDS matrices. In [23], the authors introduced Generalized Hadamard matrices (GHadamard) as a generalizations of Hadamard matrices.

Definition 1.2.18. *A matrix $GH = (h_{i,j})$ of order $2^t \times 2^t$ over the finite field $\mathbb{F}_{2^m}$ is called GHadamard matrix, if its entries are of the form $h_{i,j} = a_{i \oplus j} b_i^{-1} b_j$, $0 \leq i, j \leq 2^t - 1$, where a_i, b_j's are non-zero elements of $\mathbb{F}_{2^m}$ and $b_0 = 1$.*

In [17], the authors assert that GHadamard matrices arise from the multiplication of a Hadamard matrix H with a non-singular diagonal matrix D, leading to the expression DHD^{-1} for any GHadamard matrix. This multiplication preserves the involutory property of the Hadamard matrix.
Note that, a Hadamard matrix is uniquely determined by its first row, and any permutation of this row results in a different Hadamard matrix, possibly with a different branch number. Additionally, for an involutory Hadamard matrix, the sum of the entries of the first row must be 1. Moreover, to maintain the MDS characteristic, the first row cannot have repeated elements. This is crucial because, if $H(0, i) = H(0, j)$ for $i, j \in \{0, 1, \ldots, k-1\}$, then the $i \oplus j$-th row have $H(i \oplus j, i) = H(i \oplus j, j)$. This results to a singular submatrix of H. Consequently, there are $k!$ permutations available for the first row of a Hadamard matrix. In [24], Sim *et al.* studied the equivalence classes of Hadamard matrices based on Branch number.

Definition 1.2.19. *Given a Hadamard matrix H of order $k \times k$ and a permutation $\sigma \in S_k$, define a Hadamard matrix H^σ such that the first row of H^σ is the σ-permutation of the first row of H. Then H is said to be equivalent to H^σ if for any input vector $\mathbf{v}$, the output vectors $\mathbf{v}H$ and $\mathbf{v}^\sigma H^\sigma$ have the same set of elements, where $\mathbf{v}^\sigma$ is the σ-permutation of $\mathbf{v}$.*

Therefore, if two Hadamard matrices H_1, H_2 are equivalent, they belong to the same equivalence class and they have the same branch number. This is because, for every pair of input and output vector for H_1, there is a corresponding pair of vectors for H_2 with the same number of non-zero components. Sim *et al.* determined the specific form of the permutation σ that makes two Hadamard matrices equivalent when the entries of the first row belong to the same set. They proved that σ must be one of the following two permutations:

- Given a Hadamard matrix H, any Hadamard matrix H^α defined by the $(\alpha + 1)$-th row of H, with $\alpha = 0, 1, \ldots, k-1$, is equivalent to H.
- For any linear permutation σ, i.e., $\sigma(i \oplus j) = \sigma(i) \oplus \sigma(j)$, two Hadamard matrices H and H^σ are equivalent.

These permutations are referred as $\mathcal{H}$-permutations in [24]. The following theorem provides the total number of equivalence classes for Hadamard matrices of order $2^s \times 2^s$.

Theorem 1.2.20. *For a given a set of 2^s non-zero elements with $S = \{\alpha_0, \alpha_1, \ldots, \alpha_{2^s-1}\}$, there exists $\frac{(2^s-1)!}{\prod_{i=0}^{s-1}(2^s-2^i)}$ equivalence classes of Hadamard matrices of order $2^s \times 2^s$ defined by the elements of S.*

In [25], Liu and Sim gave an equivalent but slightly different description for the permutation σ. They proved that two Hadamard matrices H and H^σ belong to the same equivalence class, if the permutation σ has the following expression:

$$\sigma(i \oplus j) = \sigma(i) \oplus \sigma(j) \oplus \sigma(0), \text{ where } i, j \neq 0.$$

In [24], Sim *et al.* investigated the equivalence class of Hadamard-Cauchy matrices, initially introduced by Gupta *et al.* (see Theorem 1.2.11).

Definition 1.2.21. *Let HC_1 and HC_2 be two Hadamard-Cauchy matrices. They are permutation equivalent if one can be transformed to the other by either one or both of the following operations on the entries of the first row:*

- *multiply by a non-zero scalar.*
- *$\mathcal{H}$-permutation of the entries.*

The following theorem presents the total number of equivalence classes for Hadamard-Cauchy matrices of order $2^s \times 2^s$.

Theorem 1.2.22. *Given two positive integers s and r, there are $\prod_{i=0}^{s-1} \frac{2^{r-1}-2^i}{2^s-2^i}$ equivalence classes of involutory Hadamard-Cauchy matrices of order $2^s \times 2^s$ over $\mathbb{F}_{2^m}$.*

Over time, numerous researchers have counted the total numbers of MDS matrices for smaller dimensions under specific conditions within finite fields. The subsequent section is dedicated to exploring this particular theme.

1.2.2 Construction of general structure of MDS matrices

The preceding section explains diverse constructions and the significance of involutory MDS matrices. While MDS matrices of orders that are powers of 2 hold practical significance, the exploration of constructing MDS matrices for other orders remains an intriguing pursuit. For example, In 2007, Barreto *et al.* [26] introduced Curupira, an iterated block cipher designed specifically for constrained platforms. This cipher utilized a 3×3 MDS involutory matrix over the finite field $\mathbb{F}_{2^8}$. Building upon this work, in 2019, Gužel *et al.* explored the involutory MDS matrices of order 3×3 over the finite field $\mathbb{F}_{2^m}$ in more details. In [27], they established the following general structure of involutory matrices over the finite field of characteristic 2:

Theorem 1.2.23. *Let $A = (a_{ij}),\ 1 \leq i, j \leq 3$ be a 3×3 matrix over the finite field $\mathbb{F}_{2^m}$. If A is involutory, $a_{11} \neq a_{22}$ and $a_{11}, a_{22} \neq 1$, then the entries of A can be expressed by only two diagonal elements a_{11}, a_{22} and two arbitrary non-zero elements b_0, b_1 from the finite field in the following way:*

$$A = \begin{bmatrix} a_{11} & (a_{11}+1)b_0 & (a_{11}+1)b_1 \\ (a_{22}+1)b_0^{-1} & a_{22} & (a_{22}+1)b_0^{-1}b_1 \\ (a_{11}+a_{22})b_1^{-1} & (a_{11}+a_{22})b_1^{-1}b_0 & a_{11}+a_{22}+1 \end{bmatrix}. \tag{1.1}$$

Utilizing the structure of Theorem 1.2.23, they established the following proposition for constructing an MDS matrix:

Proposition 1.2.24. *Let A be a matrix in the general form described in Theorem 1.2.23. Then A is MDS over $\mathbb{F}_{2^m}$ if and only if $a_{11} \neq a_{22}, \{a_{11}, a_{22}\} \neq \{0, 1\}$ and $a_{11} + a_{22} \neq 1$.*

This proposition implies that a_{11} and a_{22} have total $(2^m - 2)$ and $(2^m - 4)$ choices respectively. Also the number of choice for b_1, b_2 are $(2^m - 1)^2$. Consequently, this leads to a total count of $(2^m - 1)^2(2^m - 2)(2^m - 4)$ involutory matrices of order 3×3 over a finite field of characteristic 2.
Following this, in 2020, Jian *et al.* [28] revisited the construction of 4×4 involutory MDS matrices over the finite field $\mathbb{F}_{2^m}$. Initially, they derived specific criteria governing the trace of the matrix.

Theorem 1.2.25. *Let A be an $n \times n$ matrix over the finite field $\mathbb{F}_{2^m}$. Then*

$$trace(A) = \begin{cases} 1, & \text{if } n \text{ is odd;} \\ 0, & \text{if } n \text{ is even .} \end{cases}$$

In the subsequent theorem, we highlight a key result from Jian *et al.* concerning the overall structure of 4×4 involutory MDS matrices. The theorem asserts that among the 16 entries within a 4×4 involutory MDS matrix, the values of 8 entries can be entirely deduced from the remaining 8. The theorem is as follows:

Theorem 1.2.26. *Let $A = (a_{ij}),\ 1 \leq i, j \leq 4$ be an involutory MDS matrix over the finite field $\mathbb{F}_{2^m}$. Then*

$$(a_{11} + a_{33})(a_{11} + a_{44}) = a_{12}a_{21} + a_{34}a_{43}.$$

Further if the eight entries $a_{11}, a_{12}, a_{21}, a_{22}, a_{33}, a_{34}, a_{43}, a_{44}$ are given, then the other eight entries, i.e., $(a_{13}, a_{14}, a_{23}, a_{24})^T$ and $(a_{42}, a_{32}, a_{41}, a_{31})^T$ are solutions of the system of linear equations $MX = 0$, where

$$M = \begin{bmatrix} a_{11}+a_{33} & a_{43} & a_{12} & 0 \\ a_{34} & a_{11}+a_{44} & 0 & a_{12} \\ a_{21} & 0 & a_{11}+a_{44} & a_{43} \\ 0 & a_{21} & a_{34} & a_{11}+a_{33} \end{bmatrix}$$

and $X = (x_1, x_2, x_3, x_4)^T$.

Continuing the exploration of even order involutory MDS matrices over $\mathbb{F}_{2^m}$, Yang *et al.* [29] introduced a novel method involving block matrices in 2021. Their result is as follows:

Theorem 1.2.27. *Let* $A = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}$ *be a* $2n \times 2n$ *involutory matrix over* $\mathbb{F}_{2^m}$ *where* $A_1, A_2, A_3, A_4 \in M_{n\times n}(\mathbb{F}_{2^m})$. *If the entries of* A_1 *and* A_2 *are given and the matrix* A_2 *is non-singular, then* A_3 *and* A_4 *can be uniquely determined.*

While this method involves an exhaustive search, however, in contrast to a direct search strategy, this construction overcomes the obstacle of the huge computational amount and reduces the search space to a great extent.
Yang *et al.* extended the construction method outlined in Theorem 1.2.27 for larger orders in the subsequent theorem. This result is a generalization of the 3×3 structure proposed by Gužel *et al.* to matrices of order $(2n + 1) \times (2n + 1)$ employing block matrices of size $n \times n$ along with specific row and column vectors.

Theorem 1.2.28. *Let*

$$A = \begin{bmatrix} A_1 & B_1 & A_2 \\ D_1 & c & D_2 \\ A_3 & B_2 & A_4 \end{bmatrix}$$

be a $(2n + 1) \times (2n + 1)$ *involutory matrix over* $\mathbb{F}_{2^m}$, *where* A_1, A_2, A_3, A_4 *are* $n \times n$ *matrices,* B_2, B_2 *are* n *dimensional column vectors,* D_1, D_2 *are* n *dimensional row vectors and* c *is an element of* $\mathbb{F}_{2^m}$. *If* A_1, A_2, B_1, D_1, c *are known and* A_2, A_3 *are non-singular, then the involutory matrix* A *can be uniquely determined.*

1.2.3 MDS matrix construction from circulant and circulant-like matrices

The renowned block cipher AES [2] uses the circulant MDS matrix circulant$(\alpha, \alpha+1, 1, 1)$ over the finite field $\mathbb{F}_{2^8}$ in its diffusion layer, where α is a root of $x^8 + x^4 + x^3 + x + 1$. This matrix is consists two 1's, offering an implementation advantage since multiplication by 1 implies no processing at all. However, its inverse does not exhibit the same favourable properties. In 2014, Gupta and Ray pioneered the study of circulant matrices with involutory and orthogonal properties over the finite field of characteristic 2. They demonstrated that, unlike Cauchy or Vandermonde matrices, these circulant matrices often lack the desirable properties of being involutory or orthogonal. In [30, 31], Gupta *et al.* established significant non-existence results regarding these circulant matrices.

Theorem 1.2.29. *Circulant orthogonal matrices of order* $2^d \times 2^d$ *over the finite field* $\mathbb{F}_{2^m}$ *cannot be MDS.*

It is worth noting that, in [30], the authors presented examples of 3×3 and 6×6 circulant MDS matrices over $\mathbb{F}_{2^8}$. However, in the case of involutory matrices, they proved the non-existence for matrices of all orders.

Theorem 1.2.30. *Circulant involutory matrices of order $n \times n, n \geq 3$ over the finite field $\mathbb{F}_{2^m}$ cannot be MDS.*

The absence of circulant MDS matrices with easily implementable inverse properties inspired the authors of [30] to generalized the circulant structure to an almost circulant structure. They introduced the definition of three types of almost circulant matrices.

- The $d \times d$ matrix of the form $\begin{bmatrix} a & \mathbf{1} \\ \mathbf{1}^t & A \end{bmatrix}$ is called *Type-I circulant-like matrix*, where $A = \text{circ}(1, a_1, a_2, \ldots, a_{d-2}), \mathbf{1} = (1, 1, \ldots, 1)$. Here 1 is the unit element, a_i's and a are any non-zero elements of the underlying field other than 1.
- The $d \times d$ matrix of the form $\begin{bmatrix} a & \mathbf{b} \\ \mathbf{b}^t & A \end{bmatrix}$ is called *almost Type-I circulant-like matrix*, where $A = \text{circ}(a_0, a_1, a_2, \ldots, a_{d-2}), \mathbf{b} = (b, b, \ldots, b)$. Here a, b and a_i's are any non-zero elements of the underlying field.
- The $2d \times 2d$ matrix f the form $\begin{bmatrix} A & A^{-1} \\ A^3 + A & A \end{bmatrix}$ is called *Type-II circulant-like matrix*, where $A = \text{circ}(a_0, a_1, a_2, \ldots, a_{d-1})$.

In both [30] and [17], the authors showed that Type-I circulant-like matrices have similar involutory properties with circulant matrices. Consequently, the following result holds true for these matrices.

Theorem 1.2.31. *Type-I circulant-like matrices of order $n \times n$ over the finite field $\mathbb{F}_{2^m}$ can not be involutory.*

They also proved that, for the orthogonal case, Type-I circulant-like matrices can never be MDS.

Theorem 1.2.32. *Type-I circulant-like matrices of order $n \times n$ over the finite field $\mathbb{F}_{2^m}$ can not be orthogonal.*

Based on Youssef *et al.*'s construction outlined in Section 1.2, it is clear that Type-II circulant-like matrices over $\mathbb{F}_{2^m}$ are involutory. However, it is noteworthy that they do not maintain the MDS property across all matrix orders, as established by Gupta and Ray in [30]. This leads to the following conclusion:

Theorem 1.2.33. *Any $2n \times 2n$ Type-II circulant-like matrix over $\mathbb{F}_{2^m}$ is non-MDS for even values of n.*

Note that, permutation equivalent matrices share the same branch number. Therefore, if matrix M is MDS, then PMQ is also MDS for any two permutation matrices P and Q. Keeping this in mind, in [25], Liu and Sim provided an equivalence relation between two circulant matrices C and C^σ of order $k \times k$, where σ is a k-cycle of the symmetric group S_k acting on the indices of the first row of C. This relation categorizes the $k!$ possible circulant matrices of order k into $\frac{(k-1)!}{\phi(k)}$ equivalence classes, with each circulant matrix in a class having the same branch number. The result is as follows:

Theorem 1.2.34. *Given two circulant matrices $C = circ(c_0, c_1, \ldots, c_{n-1})$ and $C^\sigma = circ(c_{\sigma(0)}, c_{\sigma(1)}, \ldots, c_{\sigma(n-1)})$, C is permutation equivalent to C^σ if and only if σ is some index permutation satisfying $\sigma(i) = bi + a \pmod n$, $\forall\, i \in \{0, 1, 2, \ldots, n-1\}$, where $a, b \in \mathbb{Z}_n$ and $\gcd(b, n) = 1$.*

Liu and Sim also generalized the circulant matrix structure and introduced *cyclic matrices* by changing the permutation.

Definition 1.2.35. *For a k-cycle $\rho \in S_k$, a matrix $\mathfrak{C}_\rho$ of order $k \times k$ is called cyclic matrix if each subsequent row is ρ-permutation of the previous row. We represent this matrix as $cyclic_\rho(c_0, c_1, c_2, \ldots, c_{k-1})$, where $(c_0, c_1, c_2, \ldots, c_{k-1})$ is the first row of the matrix. The (i, j)-th entry of $\mathfrak{C}_\rho$ can be expressed as $\mathfrak{C}_\rho(i, j) = c_{\rho^{-i}(j)}$.*

They also proved that, given a cyclic matrix and circulant matrix with entries from same set of k elements, there exists a permutation equivalence relation between them. However, they did not provide the structure of the permutation matrices. Based on the permutation equivalence, they derived the following corollary:

Corollary 1.2.36. *Any cyclic matrix corresponds to some circulant matrix, preserving the coefficients and the branch number.*

In [25], authors also established the non-existence of left-circulant MDS matrices with involutory property for order $2^d \times 2^d$ over the finite field of characteristic 2. Additionally, they asserted the following statement based on experimental findings.
Conjecture: No involutory MDS cyclic matrices exist for orders 4×4 and 8×8 over the finite field of characteristic 2.
It is important to note that a circulant matrix is a specialized form of a Toeplitz matrix. Defined by its initial row and column elements, a Toeplitz matrix can be represented by the vectors $\{a_0, a_1, \ldots, a_{n-1}, a_{-1}, a_{-1}, \ldots, a_{-(n-1)}\}$. The matrix is of the following form:

$$T = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{-(n-1)} & a_{-(n-1)} & a_{-(n-3)} & \cdots & a_0 \end{bmatrix}.$$

The study on circulant matrices with the MDS property inspired Sarkar and Syed [32, 33] to delve into Toeplitz matrices possessing MDS characteristics. Their results illustrate the similar behaviour of Toeplitz and circulant matrices. The first theorem of Sarkar *et al.* in this direction is the following:

Theorem 1.2.37. *Let T be an $n \times n$ Toeplitz matrix defined over $\mathbb{F}_{2^m}$. Then T cannot be both MDS and involutory.*

In a similar way, they encountered the following result regarding orthogonality:

Theorem 1.2.38. *Let T be an $2^d \times 2^d$ Toeplitz matrix defined over $\mathbb{F}_{2^m}$. Then T cannot be both MDS and orthogonal.*

Similar to circulant case, there exist Toeplitz matrices of orders other that $2^d \times 2^d$ that possess both MDS and orthogonal properties. In [17], the following two examples of Toeplitz orthogonal matrices over the finite field $\mathbb{F}_{2^8}$ with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$ were provided. The first example is a 3×3 matrix Toep$(\alpha, 1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^6, \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^6, \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^6, 1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^6)$, and the next example is a 6×6 matrix Toep$(1, 1, \alpha, 1 + \alpha^2 + \alpha^3 + \alpha^5 + \alpha^6 + \alpha^7, \alpha + \alpha^5, \alpha^2 + \alpha^3 + \alpha^6 + \alpha^7, \alpha + \alpha^5, \alpha^2 + \alpha^3 + \alpha^6 + \alpha^7, \alpha^2 + \alpha^3 + \alpha^6 + \alpha^7, \alpha + \alpha^5, 1 + \alpha^2 + \alpha^3 + \alpha^5 + \alpha^6 + \alpha^7, \alpha, 1)$. Both matrices also satisfy the MDS property.

In [17], the authors investigated Hankel matrices and explored their properties concerning MDS and involutory characteristics. Note that a left-circulant matrix is a special case of Hankel matrix. A Hankel matrix is defined by its first row and last column. It is also a symmetric matrix, therefore involutory and orthogonal are equivalent conditions. In [17], the authors proved the following result.

Theorem 1.2.39. *Let H be a $2^n \times 2^n, n \geq 2$ Hankel MDS matrix over $\mathbb{F}_{2^m}$. Then H is not an involutory matrix.*

The example of involutory Hankel matrices of orders other than powers of 2 is also presented in [17]. Recently, in 2019, Cauchois *et al.* [34] introduced a correspondence between a monic polynomial of degree m and a circulant matrix of order $m \times m$ through the following definition:

Definition 1.2.40. *Let $h(X) = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[x]$ be a monic polynomial of degree m. The circulant matrix associated with $h(X)$ is the matrix $\mathbb{C}_h = circulant(h_0, h_1, \ldots, h_{m-1})$.*

The matrix $\mathbb{C}_h$ can also be viewed as a matrix with respect to the basis $\{1, X, X^2, \ldots, X^{m-1}\}$ of the mapping

$$\phi : \mathbb{F}_q[X]/(X^m - 1) \to \mathbb{F}_q[X]/(X^m - 1)$$

defined by $\phi(Q(X)) = Q(X)h(X)$.

Using this algebraic framework, Cauchois *et al.* gave an alternative proof for Theorem 1.2.30 and extended this result for characteristic $p \geq 2$ for matrices of even order. The following two propositions play an important role in the generalization noted in Theorem 1.2.43.

Proposition 1.2.41. *Let $h(X) = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X]$ and $\mathbb{C}_h$ be the circulant matrix associated to $h(X)$. Then $\mathbb{C}_h$ is MDS if and only if for all $Q_1 \in \mathbb{F}_q[X]$ with degree$(Q_1(X)) \leq m - 1$, we have wt$(Q_1) +$ wt$(Q_1(X)h(X) \pmod{X^m - 1}) \geq m + 1$.*

Proposition 1.2.42. *Let $h(X) = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_q[X]$ and $\mathbb{C}_h$ be the circulant matrix associated to $h(X)$. Then $\mathbb{C}_h$ is involutory if and only if $h(X)^2 = 1 \pmod{X^m - 1}$.*

Theorem 1.2.43. *Let $d \geq 2$. Then involutory circulant MDS matrices of order $2d \times 2d$ do not exist over finite fields of characteristic $p \geq 2$.*

Cauchois *et al.* further extended this framework to θ-polynomial ring and define θ-circulant matrices over this ring.

Definition 1.2.44. *Let $h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_{q^m}[X, \theta]$ be a monic q-polynomial of degree m. The θ-circulant matrix associated with $h\langle X\rangle$ is the matrix defined by*

$$\mathbb{C}_{h,\theta} = \begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_{m-1} \\ h_{m-1}^{[1]} & h_0^{[1]} & h_1^{[1]} & \cdots & h_{m-2}^{[1]} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ h_1^{[m-1]} & h_2^{[m-1]} & h_3^{[m-1]} & \cdots & h_0^{[m-1]} \end{bmatrix},$$

where $h_i^{[j]} = \theta^j(h_i)$ and θ be an $\mathbb{F}_q$ automorphism of $\mathbb{F}_q^n$.

Analogous to propositions 1.2.42 and 1.2.42, Cauchois and Loidreau also established conditions for a θ-circulant matrix to be both involutory and MDS. An example of such a matrix was presented in [34].

Example 1.2.45. *Let $\mathbb{F}_{2^4}$ be a finite field with the irreducible polynomial X^4+X+1 and α is a root of this polynomial. The matrix $\mathbb{C}_{h,\theta}$ associated with $h\langle X\rangle = (X^4+1)+\alpha^7X^3+\alpha^{14}X^2+X+\alpha \in \mathbb{F}_{2^4}[X, \theta]$ is a θ-circulant involutory MDS matrix .*

Recently, Adhiguna *et al.* [35] studied the necessary and sufficient condition for the existence of orthogonal θ-circulant matrices using q-polynomial rings. They provided the following example of θ-circulant orthogonal MDS matrix.

Example 1.2.46. *Let $\mathbb{F}_{2^4}$ be a finite field with irreducible polynomial $X^4 + X + 1$ and α is a root of this polynomial. Let $\theta(\alpha) = \alpha^2$ and $\mathbb{C}_{h,\theta}$ is the matrix associated with $h\langle X\rangle = (X^4 - 1) + \alpha^{11} + \alpha X + \alpha^7X^2 + \alpha^5X^3 \in \mathbb{F}_{2^4}[X, \theta]$. Then $\mathbb{C}_{h,\theta}$ is a θ-circulant orthogonal MDS matrix.*

Thus far, our emphasis has been on the construction of MDS matrices through various matrix types. In the next section, we briefly explore the construction of MDS matrices using Gabidulin and BCH codes, along with the recursive construction of MDS matrices from a sparse matrix.

1.2.4 Recursive construction of MDS matrices

One significant challenge with the previously discussed construction of MDS matrices lies in their inefficient hardware implementation, notably in constrained setups like RFID systems and sensor networks. To address this limitation without compromising on the maximum branch number, a novel approach emerged in the in the document of PHOTON lightweight hash family [36] and subsequently applied in the diffusion layer of the LED lightweight block cipher [37]. These ciphers implemented an $m \times m$ MDS matrix

$\mathcal{B}^m$ derived from the companion matrix $\mathcal{B}$. This method of MDS matrix construction is termed as *recursive MDS matrix construction*.

Following these developments, in 2012, Sajadieh *et al.* [38] introduced a family of diffusion layer utilizing Feistel-like structures and linear round functions. Additionally, Wu *et al.* [39] created diffusion layers using matrix polynomials from the commutative ring $\mathbb{F}_2[L, L^{-1}]$, where L is a non-singular matrix over $\mathbb{F}_2$. In 2013, Thierry P. Berger [40] constructed an recursive MDS matrix using the generator matrix of Gabidulin codes. This matrix was constructed from the polynomial basis $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ of the field $\mathbb{F}_{2^m}$, where α is a root of an irreducible polynomial $P(X)$ of degree m. The generator matrix of the $[2r, r, r+1]$ Gabidulin code $\mathcal{G}_{\mathcal{B},r}$ is of the form

$$G_{\mathcal{B},r} = \begin{bmatrix} a_0 & a_1 & \cdots & a_{m-1} \\ a_0^{[1]} & a_1^{[1]} & \cdots & a_{m-1}^{[1]} \\ \vdots & \vdots & \cdots & \vdots \\ a_0^{[r-1]} & a_1^{[r-1]} & \cdots & a_{m-1}^{[r-1]} \end{bmatrix},$$

where $a_i = \alpha^i, a^{[i]} = a^{2^i}$ and $m = 2r$. This matrix can be expressed as $G_{\mathcal{B},r} = (U|S^rU)$ with S being the diagonal matrix diagonal$(a_1, a_1^{[1]}, a_1^{[2]}, \ldots, a_1^{[r-1]})$ and U is the matrix restricted to first r columns of $G_{\mathcal{B},r}$. Then the systematic generator matrix of $\mathcal{G}_{\mathcal{B},r}$ is $M = (I_{r\times r}|U^{-1}S^rU)$. Consider the MDS diffusion matrix $A = U^{-1}S^rU$. The subsequent theorem illustrates how the matrix A represents a recursive MDS construction derived from a companion matrix.

Theorem 1.2.47. *Consider the companion matrix*

$$C = \begin{bmatrix} 0 & 0 & 0 & \cdots & a_{0,0} \\ 1 & 0 & 0 & \cdots & a_{1,0} \\ 0 & 1 & 0 & \cdots & a_{2,0} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{r-1,0} \end{bmatrix},$$

where $a_{i,0}$ represents the entries of the matrix $A = U^{-1}S^rU$ for $i = 0, 1, \ldots, r-1$. Then $C^r = A$.

Subsequently, in 2014, Augot and Finiasz [41] used shortened BCH codes for the construction of recursive MDS matrices.

Definition 1.2.48. *Let $\mathbb{F}_q$ be a finite field and β be an element in some extension field of $\mathbb{F}_q$ with order$(\beta) = n$. Select integers l, d and consider the $d-1$ consecutive powers $\beta^l, \beta^{l+1}, \ldots, \beta^{l+d-2}$ of β. Let $g(x) = lcm\ (Min_{\mathbb{F}_q}(\beta^l), Min_{\mathbb{F}_q}(\beta^{l+1}), \ldots, Min_{\mathbb{F}_q}(\beta^{l+d-2}))$, where $Min_{\mathbb{F}_q}(\alpha)$ is the minimal polynomial of α over $\mathbb{F}_q$. The cyclic code defined by $g(x)$ is called a BCH code with length n, dimension $n - deg(g)$, and minimum distance at least d.*

Augot and Finiasz established a crucial condition on the roots of the polynomial $g(x)$ for a BCH code to be an MDS code, as outlined in the following theorem:

Theorem 1.2.49. *An BCH code over $\mathbb{F}_q$ defined by the k roots $\beta^l, \beta^{l+1}, \ldots, \beta^{l+k-1}$ with the actual distance $k+1$ is MDS if and only if $P(x) = \prod_{j=0}^{k-1}(x - \beta^{l+j}) \in \mathbb{F}_q[x]$. In this case, $g(x) = lcm\ (Min_{\mathbb{F}_q}(\beta^l), Min_{\mathbb{F}_q}(\beta^{l+1}), \ldots, Min_{\mathbb{F}_q}(\beta^{l+k-1}))$ is equal to $P(x)$.*

In [42], Gupta *et al.* introduced the notion of a *c-BCH* code over $\mathbb{F}_q$ as a specific type of BCH code. These codes are defined by generating polynomials whose roots can be represented as consecutive powers of an element β in an extension field of $\mathbb{F}_q$. Consequently, according to Theorem 1.2.49, a c-BCH code over $\mathbb{F}_q$ is also an MDS code. The MDS c-BCH code over $\mathbb{F}_q$ has length $n = \text{ord}(g)$ and dimension $k = n - \deg(g)$. Therefore, the generator matrix is of size $k \times \deg(g)$. For the use diffusion layer, a square matrix is necessary, i.e., $\deg(g) = k$ implying $n = 2k$. However, in the extensions of $\mathbb{F}_2$ all elements have odd orders. Hence, the solution involves seeking $[n = 2k + z, m = k + z, d = k + 1]$ MDS c-BCH codes, which are then shortened by z positions to yield the desired $[2k, k, k + 1]$ MDS codes, where z is an odd integer.
In [42] the authors presented results on the values of n and the corresponding values of l for which the constructed polynomials generate MDS c-BCH codes satisfying the conditions of Theorem 1.2.49. For integers $k \geq 2$ and $n = 2k + z(\leq q + 1)$ for some odd integer z, their theorem is following:

Theorem 1.2.50. *Let k and n be integers with $k \geq 2$ and $n > 2k$. Then there exists an MDS c-BCH code of length n and of dimension $(n - k)$ over $\mathbb{F}_q$ if and only if $q \equiv \pm 1 \pmod{n}$.*

Continuing the recursive MDS construction, in [43], the authors expanded the scope beyond the generator polynomials of BCH codes to identify arbitrary polynomials that generate recursive MDS matrices. Consider a monic polynomial $g(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1} + x^k \in \mathbb{F}_q[x]$ of degree k and $\mathbb{C}_g$ be the companion matrix associated with g. Then

$$\mathbb{C}_g = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_1 & \cdots & -a_{k-1} \end{bmatrix}.$$

If the matrix $M = \mathbb{C}_g^m$ is an MDS matrix, then we say that the polynomial $g(x)$ yields a recursive MDS matrix. In [43], Gupta *et al.* established the conditions for $M = \mathbb{C}_g^m$ to form an MDS matrix, which we outline here.

Theorem 1.2.51. *Let $g(x) \in \mathbb{F}_q[x]$ be a monic polynomial of degree k with $g(0) \neq 0$ and $ord(g) = n \geq 2$. Let $E = \{0, 1, \ldots, k-1, m, m+1, \ldots, m+k-1\}$ for some integer $m, k \leq m \leq n-k$. Then the matrix $M = \mathbb{C}_g^m$ is MDS if and only if the weight of any non-zero multiple $f(x)$ of $g(x)$ of the form $f(x) = \sum_{e \in E} f_e x^e \in \mathbb{F}_q[x]$ is greater than k.*

This theorem presents a direct method to construct recursive MDS matrices using the generator polynomial of a cyclic code. Consider a cyclic code $\tau = \langle g(x) \rangle$ defined by

$g(x) \in \mathbb{F}_q[x]$ of degree k with a minimum distance of $k+1$. When the condition of Theorem 1.2.51 is satisfied, τ becomes an MDS code. Consequently, for all m, where $k \leq m \leq \text{ord}(g) - k$, the matrix C_g^m derived from the polynomial $g(x)$ is MDS. Gupta *et al.* also established criteria to construct recursive MDS matrices based on the roots of the polynomial $g(x)$. The following result addresses this criterion.

Theorem 1.2.52. *Let $g(x) \in \mathbb{F}_q[x]$ be a monic polynomial of degree k with $g(0) \neq 0$ and ord$(g) = n$. Suppose that g has t distinct roots, say $\lambda_1, \lambda_2, \ldots, \lambda_t \in \overline{\mathbb{F}_q}$ with multiplicities $e_1, e_2, \ldots, e_t$ respectively. Let m be an integer with $k \leq m \leq n-k$. Then the matrix $M = \mathbb{C}_g^m$ is MDS if and only if any k columns of the matrix*

$$H' = \begin{bmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{k-1} & \lambda_1^m & \cdots & \lambda_1^{m+k-1} \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^{k-1} & \lambda_2^m & \cdots & \lambda_2^{m+k-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \lambda_k & \lambda_k^2 & \cdots & \lambda_k^{k-1} & \lambda_k^m & \cdots & \lambda_k^{m+k-1} \end{bmatrix}$$

are linearly independent over $\mathbb{F}_q$.

Building upon their work in [43], the authors introduced techniques to construct polynomials that generate recursive MDS matrices. This was accomplished by carefully choosing the roots and rigorous verification of the conditions specified in Theorem 1.2.49.

An alternative approach to construct recursive MDS matrices was extensively explored in [44], [45], [46]. Particularly, in [44], To *et al.* introduced a new class of serial-type matrices called Diagonal-Serial Invertible (DSI) matrices, known for their sparse characteristics. The definition of a DSI matrix is as follows:

Definition 1.2.53. *A Diagonal-Serial Invertible (DSI) matrix $D = (d_{i,j}), 1 \leq i, j \leq k$ with entries from the finite field $\mathbb{F}_{2^m}$ is determined by two vectors, $\boldsymbol{a} = (a_1, a_2, \ldots, a_k) \in (\mathbb{F}_{2^m}^*)^k$ and $\boldsymbol{b} = (b_1, b_2, \ldots, b_{k-1}) \in (\mathbb{F}_{2^m})^{k-1}$ as follows:*

$$D_{i,j} = \begin{cases} a_1, & \text{for } i = 1 \text{ and } j = k; \\ a_i, & \text{for } i = j+1; \\ b_i, & \text{for } i = j \leq k-1; \\ 0, & \text{otherwise.} \end{cases}$$

The initial observation concerning these matrices is that every DSI matrix $D = \text{DSI}(\mathbf{a},\mathbf{b})$ is indeed invertible. Consequently, the primary aim in constructing an MDS matrix from a power of D is to ascertain the minimum value of q where D^q contains only non-zero entries. To address this, To *et al.* calculated the entries of q-th power of the general DSI matrix $D = \text{DSI}(\mathbf{a},\mathbf{b})$ using graph theory. They represented D as a weighted adjacency matrix to a directed graph with vertices labeled 1 to k, and $D_{i,j}$ as the weight of the

directed edge from vertex i to vertex j. Then for any $q \in \mathbb{N}$, we have

$$(D^q)_{i,j} = \sum_{\text{length } q \text{ paths from } i \text{ to } j} (product\ of\ all\ weights\ along\ the\ path).$$

This unique construction led to the following consequential result:

Theorem 1.2.54. *Given a DSI matrix D of order $k \times k$, the minimum power of D for all entries to have a non-zero algebraic expression is k (and thus possibly MDS).*

They further reduced the number of non-zero entries and proposed the following subclass of DSI matrices:

Definition 1.2.55. *A DSI matrix $D = DSI(\boldsymbol{a,b})$ of order k is sparse if satisfies:*

$$\begin{cases} b_2 = b_4 = \cdots = b_{k-2} = 0, & \text{if } k \text{ is even;} \\ b_2 = b_4 = \cdots = b_{k-3} = 0, & \text{if } k \text{ is odd.} \end{cases}$$

Extending Theorem 1.2.54, the authors of [44] established that Sparse DSI matrices, with dimensions $k \times k$, have the potential to achieve k-MDS status.
Furthermore, in [46], DSI matrices were extended to Diagonal-Like Sparse (DLS) matrices through multiplication with a permutation matrix. The definition of DLS matrices is the following:

Definition 1.2.56. *Let $\rho = (i_1\ i_2\ \cdots\ i_n)$ be a permutation such that $i_k \neq k$ for $k = 1, 2, \ldots, n$, D_1 be a non-singular diagonal matrix, and D_2 be a diagonal matrix (may be singular). Then the matrix $B = PD_1 + D_2$ is the diagonal-like sparse (DLS) matrix, where P is the permutation matrix of order $n \times n$ related to the permutation ρ. These matrices are denoted by $DLS(\rho, D_1, D_2)$.*

In their work outlined in [46], the authors presented significant findings concerning DLS matrices in constructing recursive MDS matrices. They established that, in the case of a DLS matrix of order $n \times n$, the fundamental criterion for constructing a recursive MDS matrix is to elevate M to the n-th power. Their result in this regard is as follows:

Theorem 1.2.57. *Given a DLS matrix $M = DLS(\rho, D_1, D_2)$ of order $n \geq 2$, for $k < n - 1$, the number of non-zero elements in M^k is less than n^2 and hence M^k is not an MDS matrix.*

A bound on the number of non-zero entries in the matrix D_2 for a Diagonal-Serial Invertible (DSI) matrix of order $n \times n$ to qualify as recursive MDS is provided in [46]. Furthermore, they verified the essential condition that ρ must form an n-cycle, as outlined in the following theorem:

Theorem 1.2.58. *For an n-MDS DLS matrix $DLS(\rho, D_1, D_2)$ of order $n \times n$, D_2 must have at least $\lceil \frac{n}{2} \rceil$ non-zero elements and ρ will be an n-cycle.*

As a continuation of the work in [46], the authors delved introduced a further generalization of DLS matrices termed Generalized DLS matrices (GDLS). This extension involved an additional multiplication of the matrix D_2 with another permutation matrix. Moreover, they offered compelling instances of GDLS matrices with orders $4, 5, 6$, and 7 over the finite field $\mathbb{F}_{2^8}$ within the same paper.

In 2021, Kesarwani *et al.* presented a broader framework for constructing recursive MDS matrices within finite commutative rings in [47]. They first established that a companion matrix is similar to a diagonal matrix when the difference between roots of the associated polynomial are units within the ring. Leveraging this similarity criterion, they proved that for a polynomial $f(x)$ with roots from the units of a ring $\mathcal{R}$, the corresponding companion matrix of f provide a recursive MDS matrix, if the generalized Vandermonde matrix $\mathbb{V}$ constructed using the roots of f is non-singular under certain conditions on the entries of $\mathbb{V}$. Considering $\mathcal{U}(\mathcal{R})$ as the set of units of the ring $\mathcal{R}$, the theorem can be stated as follows:

Theorem 1.2.59. *Let $\boldsymbol{h} = (h_0, h_1, \ldots, h_{n-1})$ be an n-tuple over $\mathcal{U}(\mathcal{R})$ with $h_i - h_j \in \mathcal{U}(\mathcal{R})$ for all $i \neq j, i, j \in \{0, 1, \ldots, n-1\}$. Let $f(x) = \prod_{i=1}^{n-1}(x - h_i)$. The for $r \geq n$, the companion matrix of f, i.e., L_f^r is MDS if and only if $\mathbb{V}(\boldsymbol{h}, Z)$ is non-singular for all $Z = \{r_1, r_2, \ldots, r_n\} \subset \{0, 1, \ldots, n-1, r, r+1, \ldots, r+n-1\}$, where $\mathbb{V}(\boldsymbol{h}, Z) = (h_i^{r_j})\ \forall\ 0 \leq i \leq n-1, 1 \leq j \leq n$.*

The authors of [47] further investigated how the conditions governing $\mathbb{V}(\mathbf{h}, Z)$ change based on the types of roots found within the polynomial f.

Till now, we have outlined methodologies for constructing MDS matrices. However, for these matrices to be efficiently utilized in the diffusion layer, an additional crucial condition is necessary: the XOR-count of the matrix should be minimal. In the following section, we will offer a concise overview of how this condition works.

1.2.5 On implementation cost of MDS matrices

In the realm of MDS matrix implementations, a well-established principle is that lower Hamming weight typically results in more cost-effective hardware implementations of the matrix. This implementation cost is usually measured by the number of XORs required to implement the matrix. As a consequence, this principle motivates numerous researchers to construct MDS matrices with low XOR counts. For instance, the coefficients of the AES MDS matrix are $(0x01, 0x01, 0x02, 0x03)$ over $\mathbb{F}_{2^8}$, and this matrix is very lightweight due to the low Hamming weight of its entries. In [48], Khoo *et al.* introduced the following formula to determine the total number of XOR operations needed to implement an entire row within a matrix:

$$\text{XOR count for one row of } M = \sum_{i=1}^{k} \gamma_i + (n-1)r,$$

where γ_i is the XOR count of the i-th entry in the row of M, k being the order of the diffusion matrix, n denotes the number of non-zero elements in the row, and r is the dimension of the finite field. A detailed computation of XOR counts for circulant and serial matrices across different orders over finite fields with characteristic 2 is presented in [48]. After that, in 2015, Sim *et al.* [24] delved into the impact of irreducible polynomials on the XOR count. Specifically, they computed the XOR count of all elements in various finite fields of characteristic 2 and provided a formula for determining the total total XOR count for fields of characteristic 2.

Theorem 1.2.60. *The total XOR count for the field $\mathbb{F}_{2^m}$ is $\sum_{i=2}^{m} 2^{i-2}(i-1)$, where $m \geq 2$.*

Additionally, in [32], Sarkar and Syed explored the behaviour of the XOR count distributions under different bases of finite fields. They proved that total XOR count for the field $\mathbb{F}_{2^m}$ is invariant under the choice of irreducible polynomial and basis. Subsequently, they presented the following result.

Theorem 1.2.61. *The XOR count spectrum of $\mathbb{F}_{2^m}/(p(x))$ and $\mathbb{F}_{2^m}/(q(x))$ are the same.*

Moreover, in [49], Beierle *et al.* introduced the concept of s-XOR of a matrix. This allow the better estimate of the cost of hardware implementation.

Definition 1.2.62. *An invertible matrix A has an s-XOR count t, if t is the minimal number such that A can be written as $A = P\prod_{k=1}^{t}(I + E_{i,j})$ with $i_k \neq j_k$ for all k, where $E_{i,j}$ is the matrix that has exactly one 1 in the i-th row and j-th column and P is a permutation matrix.*

Beierle *et al.* characterized all elements of the finite field $\mathbb{F}_{2^m}$ with s-XOR count of 1. In [50], Lukas Kölsch generalized this and characterized all elements of the finite field $\mathbb{F}_{2^m}$ with s-XOR count of 2.

1.3 Format preserving encryption

Format preserving encryption is a cryptographic technique designed to encrypt data while retaining its original format. Traditional encryption methods inherently alter the input format, as doing otherwise would compromise the semantic security of the encryption algorithm. This behaviour was vividly described by Brightwell and Smith in [51] as "Ciphertext bears roughly the same resemblance to plaintext as a hamburger does to a T-bone steak".

Block cipher encryption algorithms, such as AES, encrypt data in blocks of a fixed size (e.g. 16 bytes in the case of AES) and treat this data as a sequence of binary digits. Moreover, most modes of operation used with block ciphers increase the length of the ciphertext by adding an extra block of initialization vector (IV). In many situations, it might be necessary to preserve the length as well as the format of the plaintext. However, a standard block cipher would require a fixed size input and produce a (possibly longer

than the plaintext) fixed size output. This gap in what was available versus what was needed in some practical situations led to the study and design of encryption schemes which preserve both the length as well as the format of the input. The first formal study of such schemes, which are called Format Preserving Encryption (FPE) schemes, was initiated by Bellare *et al.* in 2009 [52]. Many FPE schemes, such as FFX, FFSEM, BPS etc., were proposed in the last two decades and the US government's standards body National Institute of Standards and Technology (NIST) has now standardized some FPE schemes via Special publication 38-G [53].

In 2002, Black and Rogaway [54] explore the problem of encrypting plain text of specified format into cipher text of the same format. They introduced three approaches, namely Prefix Cipher, Cycle-Walking Cipher, and Generalized-Fiestel Cipher.

Prefix Cipher: Fix an integer k and consider the set $\mathcal{M} = \{0, 1, \ldots, k-1\}$. The Prefix cipher, denoted as P, utilizes an existing block cipher E, having a key space $\mathcal{K}$ and a domain that is a superset of $\mathcal{M}$. The key space for P also remains $\mathcal{K}$. To compute $P_K(m)$ for some $m \in \mathcal{M}$ and $K \in \mathcal{K}$, first compute the tuple $I = (E_K(0), E_K(1), \ldots, E_K(k-1))$. Since each element of I is a distinct string, replace each element in I with its ordinal position (starting from zero) to produce the tuple J. Then, $P_K(m)$ correspond to the m-th component of J.

Cycle-walking cipher: Let $\mathcal{M} = \{0, 1, \ldots, k-1\}$ denote the message space, with k being a fixed integer. Let N be the smallest power of 2 greater or equals to k, and E_K be an n-bit block cipher, where $n = \log N$. Then it is possible to construct an FPE Cy_K on the set $\mathcal{M}$ by computing $c = E_K(m)$ and iterating if $c \notin \mathcal{M}$.

Generalized-Fiestel Cipher: In this method first decompose all the numbers in $\mathcal{M}$ into pairs of "similarly sized" numbers and then apply the well-known Feistel construction (see Section 1.1.2) to produce a cipher.

Combining Cycle-Walking with AES based balanced Feistel network, Terrance Spices proposed FFSEM [55] in 2008. From then many FPE schemes were proposed, for example FFX (based on Feistel network) [56], BPS [57], VFPE [58]. In 2016, Chang *et al.* [59] proposed a new FPE algorithm SPF, based on the substitution permutation network (SPN) strategy. Each round of SPF consists of some basic transformations namely, Format Preserving SubBytes, Shift Rows, Format Preserving MixColumns, Format Preserving Key Addition, and Format Preserving Tweak Addition. In the MixColumn transformation, i.e. in the diffusion layer they used the following binary matrix

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

However, this matrix does not provide optimal branch number which is necessary to prevent differential attacks against the FPE design.

In 2016, Gupta, Pandey and Ray first introduce the concept of Format Preserving Set

(FPS) in [60] in the diffusion layer of an FPE. The concept is the following:
Let M be the matrix corresponding to the diffusion layer with entries from some algebraic structure $\mathbb{A}$. Let X be any set with the desired input size and $\phi : X \to \mathbb{A}$ be an injective map. Then $\phi(X)$ is a format preserving set with respect to M if $M\mathbf{v} \in \phi(X)^n$ for all $\mathbf{v} \in \phi(X)^n$. This notion of FPS plays a fundamental role in constructing FPE from a block cipher, as demonstrated by Gupta *et al.* in their illustrative credit card encryption example presented in [60].
In the encryption of credit card numbers, the desired format for both input and output are the digits 0 to 9. To achieve this, first consider an injective map ϕ from the set $X = \{0, 1, \ldots, 9\}$ to $Y = \{0, 1\}^m$. To preserve the format of plaintext and its corresponding ciphertext, one way to encrypt an element $X_1 \parallel X_2 \parallel \cdots \parallel X_l$ from X^l is the following:

- First encode the element $X_1 \parallel X_2 \parallel \cdots \parallel X_l$ using the map ϕ. Let the output is $\phi(X_1) \parallel \phi(X_2) \parallel \cdots \parallel \phi(X_l) = Y_1 \parallel Y_2 \parallel \cdots \parallel Y_l$ an element of Y^l.
- Use an block cipher encryption algorithm $\mathcal{E}$ and get the ciphertext $\bar{Y_1} \parallel \bar{Y_2} \parallel \cdots \parallel \bar{Y_l}$.
- Apply ϕ^{-1} to decode the ciphertext and get $\phi^{-1}(\bar{Y_1}) \parallel \phi^{-1}(\bar{Y_2}) \parallel \cdots \parallel \phi^{-1}(\bar{Y_l})$.

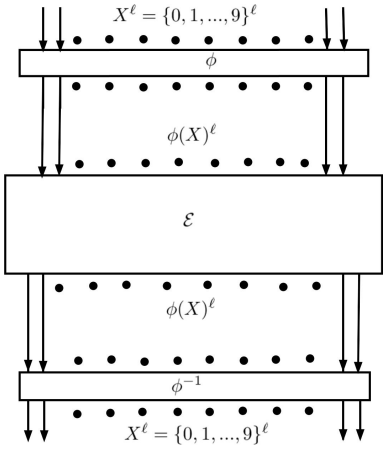

Figure 1.3: FPS structure

For successful decoding, ensuring that each $\bar{Y_i}$ belongs to $\phi(X)$ for all $i = 1, 2, \ldots, l$ is crucial. Therefore, this method provides a solution for format preserving encryption if and only if $\mathcal{E}(\phi(X)^l) = \phi(X)^l$. A model of this construction is presented in Figure 1.3. Therefore, when using an SPN-based block cipher, two primary questions arise:

- Can an S-box be constructed which maps $\phi(X)^l$ to $\phi(X)^l$, and
- Can an $n \times n$ matrix be constructed which given any input vector from $\phi(X)^l$ outputs a vector from $\phi(X)^l$ only?

In their work, Gupta *et al.* [60], delved into answering this question by constructing format preserving sets and investigating their characteristics under different conditions concerning the set and the associated matrix. Their definition of a Format Preserving Set (FPS) over a finite field is as follows:

Definition 1.3.1. *A non-empty set $S \subseteq \mathbb{F}_q$ is said to be a format preserving set with respect to an $n \times n$ matrix $M(\mathbb{F}_q)$ if $M\boldsymbol{v} \in S^n$ for all $\boldsymbol{v} \in S^n$.*

In particular, when the additive identity $0 \in S$, Gupta *et al.* proved that the possible cardinality of an FPS is always a prime power. This conclusion stems directly from the following theorem:
Consider an $n \times n$ matrix $M = (m_{i,j})$ with entries from $\mathbb{F}_q$ and $Z = \{m_{i,j} : m_{i,j} \in \mathbb{F}_q^*\}$. Consider the subgroup $\mathbb{F}_q^*$ of generated by the element of the set Z and denote it by $\langle Z \rangle$. Now define the set $\mathbb{K} = \{k_1\alpha_1 + k_2\alpha_2 + \cdots + k_r\alpha_r : r \geq 0, k_i \geq 1, \alpha_i \in \langle Z \rangle\}$. This set $\mathbb{K}$ is the smallest field containing entries of the matrix M.

Theorem 1.3.2. *Let $0 \in S$. Suppose M has at least one row which contains at least two non-zero entries. Then, S is an FPS with respect to M if and only if S is a vector space over the field $\mathbb{K}$.*

By keeping in mind that MDS matrix provides optimal diffusion, in 2017 Chang *et al.* [61] constructed a new efficient format preserving encryption scheme named e-SPF. To construct an FPE on a set of cardinality 10, they considered the Galois field $GF(11)$ and they used the following MDS matrix in the permutation layer

$$\begin{bmatrix} 1 & 1 & 2 & 5 \\ 5 & 1 & 1 & 2 \\ 2 & 5 & 1 & 1 \\ 1 & 2 & 5 & 1 \end{bmatrix}.$$

Since size of the field (which is 11) is greater than the alphabet size 10, each state of encryption needs some discarding algorithm to maintain the format. Therefore an immediate question pops up: why not instead of the finite field search for format preserving sets over some other algebraic structure where cardinality 10 or other important alphabet size is possible. Also, can we construct some MDS matrix simultaneously over those algebraic structure?
In this direction, Barua *et al.* [62] investigated the existence of an FPS over finite commutative ring with identity under the restriction that S is closed under addition. They proved that, under these conditions, S acquires a unital module structure over the ring. Interestingly, within the same paper, they presented an example that diverges from the aforementioned restrictions yet still constitutes an FPS.

Example 1.3.3. *Consider the ring $\mathcal{R} = \mathbb{Z}_{10}$, and a 3×3 matrix M with entries from the set $\{1, 3, 5, 7, 9\} \subset \mathbb{Z}_{10}$. Consider the set $S = \{1, 3, 5, 7, 9\}$. S is not closed under addition, since $3 + 5 = 8 \notin S$. However, S is an FPS with respect to M over the ring $\mathbb{Z}_{10}$.*

FPS of multiple different cardinalities which are not prime power were also constructed in [62]. They showed how to construct an FPS of cardinality 20 with respect to a 3×3 MDS matrix, cardinality 10^3 with respect to a 4×4 MDS matrix, and cardinality 26^3 with respect to a 4×4 MDS matrix. Their method involves the structure of certain finite rings which are direct products of finite fields.

1.4 Main results

In this section, we provide motivation and outline the main results of this thesis, which we will substantiate in subsequent chapters. Our initial set of results is inspired by the construction of Maximum Distance Separable (MDS) matrices utilizing Cauchy matrices over finite fields. In [20], Gupta and Ray introduced a construction of MDS matrices from the Cauchy matrix with entries from an additive subgroup of the finite field $\mathbb{F}_{2^m}$. This innovative construction yields MDS matrices of order powers of 2. Furthermore, these matrices exhibit Hadamard matrix properties, simplifying the inversion process significantly. This construction method extends to producing MDS matrices of any order smaller than the original matrix, as submatrices of a Cauchy matrix retain the Cauchy property. Thus, it becomes feasible to create MDS matrices of orders that are not strictly powers of 2 by utilizing submatrices from this construction. However, it is important to note that this approach does not guarantee the preservation of the straightforward inverse characteristic.

Therefore, it seems natural to ask whether it is feasible to devise a construction method for MDS matrices using the Cauchy matrix that ensures a straightforward inverse with the property that its submatrices also yield MDS matrices with easily invertible characteristics.

In [63], we address this question by presenting a construction of the MDS Cauchy matrix over a finite field of characteristic $p \geq 2$, as detailed in Theorem 1.4.3. This construction relies on the semi-orthogonal characteristic of Cauchy matrices, a concept introduced by Miroslav Fiedler and Frank J. Hall in 2012 [64]. Before delving further into our results, it is pertinent to define a semi-orthogonal matrix.

Definition 1.4.1. *A non-singular matrix M is semi-orthogonal if there exist non-singular diagonal matrices D_1 and D_2 such that $M^{-T} = D_1 M D_2$, where M^{-T} denotes the transpose of the matrix M^{-1}.*

This is a generalization of the orthogonal property of a matrix. Although Fiedler and Hall termed this property as "G-matrices", in this thesis, we adopt the term "semi-orthogonal property" to refer to it consistently.

If the matrix M of Definition 1.4.1 is symmetric, then the inverse matrix is of the form $M^{-1} = D_2 M D_1$, where D_1 and D_2 are non-singular diagonal matrices. Matrices with this characterization are termed as semi-involutory matrices. This concept was introduced by Cheon *et al.* in 2021 as a generalization of involutory property. The definition of semi-involutory matrix is as follows:

Definition 1.4.2. *A non-singular matrix M is semi-involutory if there exist non-singular diagonal matrices D_1 and D_2 such that $M^{-1} = D_1 M D_2$.*

The diagonal matrices D_1 and D_2 are referred as associated diagonal matrices of a semi-involutorty (semi-orthogonal) matrix throughout the thesis.

Now, we proceed to present the theorem that provides an MDS matrix of any order, featuring a straightforward inverse matrix for all the submatrices also.

Theorem 1.4.3. *Let $G = \{x_0, x_1, \ldots, x_{d-1}\}$ be a proper subfield of the finite field $\mathbb{F}_{p^n}$ and let $r \notin G$. Consider the coset $r + G = \{y_0, y_1, \ldots, y_{d-1}\}$. Then $A = (\frac{1}{x_i + y_j})$, $1 \leq i, j \leq d-1$ is an MDS Cauchy matrix. Further, there exist diagonal matrices $D_1 = \frac{1}{c^2} I$ and $D_2 = I$ such that $A^{-1} = D_1 A D_2$, where $c = \sum_{k=0}^{d-1} \frac{1}{r + x_k}$.*

Therefore, it is evident that constructing MDS matrices possessing semi-involutory property is achievable. In [63], we further explore MDS matrices characterized by both semi-involutory an semi-orthogonal properties. Initially, we demonstrate the feasibility of constructing MDS matrices of smaller orders, such as 2×2 and 3×3, while possessing both semi-involutory and semi-orthogonal properties. We begin by presenting the results for the 2×2 case.

Theorem 1.4.4. *Let $A = (a_{ij})$ be a 2×2 semi-involutory matrix. Then A is MDS if and only if $a_{ij} \neq 0$ for all $1 \leq i, j \leq 2$.*

Theorem 1.4.5. *Let $A = (a_{ij})$ be a 2×2 semi-orthogonal matrix. Then A is MDS if and only if $a_{ij} \neq 0$ for all $1 \leq i, j \leq 2$.*

For the construction of 3×3 semi-involutory MDS matrices, we rely on the characterization of semi-involutory matrices established in [65]. This result establishes a connection between the entries of a semi-involutory matrix and the submatrix formed by excluding the row and column containing that entry.

Theorem 1.4.6. *Let $A = (a_{ij})$ be a semi-involutory matrix of order $m \times m$. Then $\det A(j|i) = 0$ if and only if $a_{ij} = 0$.*

Leveraging Theorem 1.4.6, we establish the following characterization for 3×3 semi-involutory matrices.

Theorem 1.4.7. *Let $A = (a_{ij})$ be a 3×3 semi-involutory matrix over a finite field. Then A is an MDS matrix if and only if $a_{ij} \neq 0$ for all $1 \leq i, j \leq 3$.*

To construct semi-orthogonal MDS matrices of order 3×3, we first present a result analogues to Theorem 1.4.6 in the semi-orthogonal context.

Theorem 1.4.8. *Let $A = (a_{ij})$ be a semi-orthogonal matrix of order $m \times m$. Then $\det A(j|i) = 0$ if and only if $a_{ji} = 0$.*

This result offers a direct method for constructing 3×3 MDS matrices over finite fields, ensuring they possess the semi-orthogonal property.

Corollary 1.4.9. *Let $A = (a_{ij})$ be a 3×3 semi-orthogonal matrix over a finite field. Then A is an MDS matrix if and only if $a_{ij} \neq 0$ for all $1 \leq i, j \leq 3$.*

Our subsequent results focus on the circulant matrices with semi-involutory and semi-orthogonal properties. This study is significant due to the non-existence results of Gupta *et al.* in [31] for finite fields of characteristic 2. They proved that circulant MDS matrices of order $n \geq 3$ cannot be involutory. Furthermore, circulant MDS matrices fail to achieve orthogonality, particularly when the order of the matrix is $2^d \times 2^d$. Consequently, investigating the behavior of circulant matrices concerning both semi-involutory and semi-orthogonal properties is an interesting area to study.
In [63], we specifically investigate this question concerning circulant matrices over finite fields. In this direction, we first establish that for circulant semi-involutory matrices over a finite field, the diagonal matrices exhibit intriguing and noteworthy properties. The result is as follows.

Theorem 1.4.10. *Let A be an $n \times n$ circulant matrix over a finite field $\mathbb{F}$. Then A is semi-involutory if and only if there exist non-singular diagonal matrices D_1, D_2 such that $D_1^n = k_1 I$ and $D_2^n = k_2 I$ for non-zero scalars k_1, k_2 in the finite field, and $A^{-1} = D_1 A D_2$.*

An interesting corollary of the preceding theorem provides a correlation between the scalars k_1, k_2 and an eigenvalue of the circulant matrix.

Corollary 1.4.11. *Let A be an $n \times n$ circulant, semi-involutory matrix over $\mathbb{F}_{p^m}$ where $n = p^k$ for some k. Then there exists diagonal matrices D_1 and D_2 with $D_1^n = k_1 I$ and $D_2^n = k_2 I$ for some non-zero scalars k_1, k_2 in the finite field with $k_1 k_2 = \frac{1}{\lambda^{2n}}$ where λ is the sum of the entries of the first row, which is an eigenvalue value of A.*

The next two results are analogues to the previous two for the semi-orthogonal case.

Theorem 1.4.12. *Let A be an $n \times n$ circulant matrix over a finite field $\mathbb{F}$. Then A is semi-orthogonal if and only if there exist non-singular diagonal matrices D_1 and D_2 such that $D_1^n = k_1 I$ and $D_2^n = k_2 I$ for non-zero scalars $k_1, k_2 \in \mathbb{F}$, and $A^{-T} = D_1 A D_2$.*

Corollary 1.4.13. *Let A be an $n \times n$ circulant, semi-orthogonal matrix over $\mathbb{F}_{p^m}$ where $n = p^k$ for some k. Then there exists diagonal matrices D_1 and D_2 with $D_1^n = k_1 I$ and $D_2^n = k_2 I$ for some non-zero scalars k_1, k_2 in the finite field with $k_1 k_2 = \frac{1}{\lambda^{2n}}$ where λ is the sum of the entries of the first row, which is an eigenvalue value of A.*

In our subsequent finding, we establish the non-existence of MDS property for a particular class of circulant semi-orthogonal matrices. These matrices are named sesqui-semi-orthogonal matrices in [63] and for these matrices either D_1 or D_2 is an identity matrix. This result mirrors Gupta *et al.* findings concerning the non-existence of circulant MDS matrices (see Section 1.2.3).

Theorem 1.4.14. *Let p be a prime, and A be a $2p \times 2p$ circulant sesqui-semi-orthogonal matrix over the field $\mathbb{F}_{p^m}$. Then A is not an MDS matrix.*

In the last section of [63], we present a necessary and sufficient condition for a 4×4 matrix with all non-zero entries to be semi-involutory. This result extends the characterization for 3×3 matrices proved by Cheon *et al.* in [65]. First we need the following definition.

Definition 1.4.15. *Let $A = (a_{ij}), 1 \leq i, j \leq n$ be an $n \times n$ matrix. The upper G-discriminant of A is the $\binom{n}{2} \times n$ matrix $G(A_u) = (a_{ik}a_{kj})$, and the lower G-discriminant of A is $G(A_l) = (a_{ki}a_{jk})$, where $1 \leq i < j \leq n$ and $k \in \{1, 2, \ldots, n\}$.*

Theorem 1.4.16. *Let* $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$ *be a 4×4 non-singular matrix over some field $\mathbb{F}$ with $a_{ij} \neq 0$ for all i, j, and $a_{32}a_{24}a_{43} = a_{23}a_{34}a_{42}$. Then A is semi-involutory if and only if the following conditions are satisfied:*

1. *Entries of A satisfy*

$$a_{12}a_{23}a_{31} = a_{21}a_{32}a_{13},\ a_{21}a_{14}a_{42} = a_{12}a_{24}a_{41},\ a_{13}a_{34}a_{41} = a_{31}a_{14}a_{43}.$$

2. *Determinant of X_1, X_2 and X_3 are zero where*

$$X_1 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{21}a_{13} & a_{22}a_{23} & a_{23}a_{33} & a_{24}a_{43} \end{bmatrix} X_2 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{14}a_{21} & a_{22}a_{24} & a_{23}a_{34} & a_{24}a_{44} \end{bmatrix},$$

$$\text{and } X_3 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{14}a_{31} & a_{24}a_{32} & a_{33}a_{34} & a_{34}a_{44} \end{bmatrix}.$$

3. *Rank of $G(A_u)$ and $G(A_l)$ is at most 3.*

4. *The submatrix B of A formed by removing the first column of A (i.e., $B = A[1, 2, 3, 4|2, 3, 4]$) has 'totally the rank' 3.*

In [63], we have demonstrated the feasibility of constructing 3×3 semi-involutory MDS matrices over a finite field. Our next goal is to study the general structure of 3×3 semi-involutory MDS matrices. This is a similar line of work done by Güzel *et al.* in [27] in 2019. To begin with, we rely on the theorem proved in [65] which provides a relation between the corresponding diagonal matrices of an irreducible semi-involutory matrix. Note that, a matrix A of order $n \times n$ is said to be *reducible*, if there exists permutation matrix P such that

$$P^T AP = \begin{bmatrix} A_1 & A_2 \\ 0 & A_3 \end{bmatrix},$$

where A_1, A_2 are square matrices of order at least 1. A matrix is said to be *irreducible* if it is not reducible. The result for irreducible matrices is as follows.

Theorem 1.4.17. *Let A be an irreducible semi-involutory matrix of order $n \times n$ such that $A^{-1} = D_1 A D_2$, where D_1 and D_2 are non-singular diagonal matrices. Then $D_1 = cD_2$ for some non-zero constant c.*

Using this characteristic of irreducible matrices, we establish the following structure for 3×3 semi-involutory matrices in [66].

Theorem 1.4.18. *Let $A = (a_{ij}), 1 \leq i, j \leq 3$ be a 3×3 irreducible, semi-involutory matrix with an associated diagonal matrix D =diagonal(d_1, d_2, d_3) over the finite field $\mathbb{F}_{2^m}$. Then the entries of A can be expressed in terms of the diagonal entries of A and entries of D as follows:*

$$\left.\begin{aligned} a_{12} &= (a_{11}d_1 + a_{33}d_3)d_2^{-1}x, \\ a_{13} &= (a_{11}d_1 + a_{22}d_2)d_3^{-1}xy, \\ a_{21} &= (a_{22}d_2 + a_{33}d_3)d_1^{-1}x^{-1}, \\ a_{23} &= (a_{22}d_2 + a_{11}d_1)d_3^{-1}y, \\ a_{31} &= (a_{33}d_3 + a_{22}d_2)d_1^{-1}(xy)^{-1}, \\ a_{32} &= (a_{33}d_3 + a_{11}d_1)d_2^{-1}y^{-1}, \end{aligned}\right\} \tag{1.2}$$

where x, y are some non-zero elements of $\mathbb{F}_{2^m}$.

In the specific scenario where $d_1 = d_2 = d_3 = 1$ and $c = 1$, where c is the constant from Theorem 1.4.17, the aforementioned theorem simplifies to the result established by Güzel *et al.*, as stated in Theorem 1.2.23.
We also establish the converse of Theorem 1.4.18 under certain conditions in the subsequent theorem.

Theorem 1.4.19. *Let $A = (a_{i,j})$ be a 3×3 matrix over $\mathbb{F}_{2^m}$. Suppose $d_1, d_2, d_3, x, y \in \mathbb{F}_{2^m}^*$ are any elements that satisfy Equation (1.2). If $a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0$, then A is semi-involutory. Moreover, if any two of $a_{11}d_1 + a_{22}d_2$, $a_{22}d_2 + a_{33}d_3$ and $a_{11}d_1 + a_{33}d_3$ are non-zero, then A is irreducible.*

The irreducible property of MDS matrices allow us to prove the following result.

Theorem 1.4.20. *Let $A = (a_{i,j})$ be a 3×3 matrix over $\mathbb{F}_{2^m}$ following the form described in Equation (1.2), where $a_{11}, a_{22}, a_{33}, d_1, d_2, d_3, x, y$ are non-zero. Then A is semi-involutory and MDS if and only if $a_{11}d_1 + a_{22}d_2, a_{11}d_1 + a_{33}d_3, a_{22}d_2 + a_{33}d_3$ and $a_{11}d_1 + a_{22}d_2 + a_{33}d_3$ are non-zero elements of $\mathbb{F}_{2^m}$.*

This result is a generalization of Proposition 1.2.24. By using Theorem 1.4.20, we enumerate the total number of semi-involutory MDS matrices over the finite field $\mathbb{F}_{2^m}$ in [66]. For this purpose, consider the following construction of a set S of 6-tuples that satisfy the conditions presented in Theorem 1.4.20 over the finite field $\mathbb{F}_{2^m}$: $S = \{(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}$. Using the cardinality of S, we ascertain the total number of semi-involutory MDS matrices over the finite field $\mathbb{F}_{2^m}$.

Theorem 1.4.21. *The number of 3×3 semi-involutory MDS matrix over the finite field $\mathbb{F}_{2^m}, m \geq 2$ is $(2^m-1)^4(2^m-2)(2^{3m}-6.2^{2m}+9.2^m-4)$.*

Our subsequent goal is to study the characteristics of cyclic matrices as introduced by Liu and Sim in [25]. These cyclic matrices are generalization of circulant matrices. Before delving into the properties of cyclic matrices, let us revisit the definition of g-circulant matrices introduced by Friedman in [67], which stands as a generalization of circulant matrices in specific scenarios.

Definition 1.4.22. *A g-circulant matrix of order $k \times k$ is a matrix of the form $A = g\text{-circulant}(c_0, c_1, \ldots, c_{k-1}) = \begin{bmatrix} c_0 & c_1 & \cdots & c_{k-1} \\ c_{k-g} & c_{k-g+1} & \cdots & c_{k-1-g} \\ c_{k-2g} & c_{k-2g+1} & \cdots & c_{k-1-2g} \\ \vdots & \vdots & \cdots & \vdots \\ c_g & c_{g+1} & \cdots & c_{g-1} \end{bmatrix}$, where all subscripts are taken modulo k.*

In literature, the g-circulant matrices are explored vastly and one can see these references [68],[67]. A representation of g-circulant matrices utilizing permutation matrices is established in Theorem 5.1.7 of [68], which is the following.

Theorem 1.4.23. *Let $A = g\text{-circulant}(c_0, c_1, \ldots, c_{k-1})$ with $\gcd(k, g) = 1$. Then A can be expressed as $A = \sum_{i=0}^{k-1} a_i Q_g P^i$, where $P = \text{circulant}(0, 1, 0, \ldots, 0)$ and $Q_g = g\text{-circulant}(1, 0, 0, \ldots, 0)$.*

In [69], we extend this representation to cyclic matrices. To proceed, we first revisit the definition of cyclic matrices.

Definition 1.4.24. *For a k-cycle $\rho \in S_k$, a matrix $\mathfrak{C}_\rho$ of order $k \times k$ is called cyclic matrix if each subsequent row is ρ-permutation of the previous row. We represent this matrix as $\text{cyclic}_\rho(c_0, c_1, c_2, \ldots, c_{k-1})$, where $(c_0, c_1, c_2, \ldots, c_{k-1})$ is the first row of the matrix. The (i, j)-th entry of $\mathfrak{C}_\rho$ can be expressed as $\mathfrak{C}_\rho(i, j) = c_{\rho^{-i}(j)}$.*

Liu and Sim established a significant correspondence between cyclic and circulant matrices, a result highlighted in Corollary 1.2.36. Building upon this, in [69], we furthered this notion by proving a permutation equivalence between a circulant matrix and a cyclic matrix. Additionally, we explicitly determined the permutation matrices involved in this equivalence.

Theorem 1.4.25. *Let $\mathfrak{C}_\rho(c_0, c_1, \ldots, c_{k-1})$ be a cyclic matrix. Then there exists a unique permutation matrix Q such that $\mathfrak{C}Q = \text{circulant}(c_0, c_{\rho(0)}, c_{\rho^2(0)}, c_{\rho^3(0)}, \ldots, c_{\rho^{k-1}(0)})$.*

This result provides the following generalization of Theorem 1.4.23 to cyclic matrices.

Theorem 1.4.26. *Let $\mathfrak{C}_\rho(c_0, c_1, c_2, \ldots, c_{k-1})$ be a cyclic matrix. Then $\mathfrak{C}_\rho = \sum_{i=0}^{k-1} a_{\rho^i(0)} P^i Q_\rho$, where $Q_\rho = \text{cyclic}_\rho(1, 0, 0, \ldots, 0)$ corresponding to the k-cycle ρ and P =circulant $(0, 1, 0, \ldots, 0)$.*

Our subsequent objective is to study the g-circulant matrices with MDS property over the finite field of characteristic 2. We commence with the following result on the determinant of g-circulant matrices of order $2^d \times 2^d$ over the finite field $\mathbb{F}_{2^m}$.

Lemma 1.4.27. *Let $A = g\text{-circulant}(c_0, c_1, c_2, \ldots, c_{2^d-1})$ be a matrix with entries from the finite field $\mathbb{F}_{2^m}$ and g be an odd integer. Then $\det(A) = (\sum_{i=0}^{2^d-1} c_i)^{2^d}$.*

Using this lemma, we establish the non-existence of g-circulant orthogonal MDS matrices of order $2^d \times 2^d$ over the finite field of characteristic 2. This result represents a generalized version of the outcome observed for circulant matrices, as presented in Section 1.2.3.

Theorem 1.4.28. *Let $A = g\text{-circulant}(c_0, c_1, c_2, \ldots, c_{2^d-1})$ be a matrix with entries from the finite field $\mathbb{F}_{2^m}$ and g be an odd integer. Then A is not an MDS matrix.*

Note that, this result holds for a more general class, i.e., for cyclic matrices using Theorem 1.4.25.

Theorem 1.4.29. *Let $\mathfrak{C}$ be a $2^d \times 2^d$ cyclic orthogonal matrix over $\mathbb{F}_{2^m}$. Then $\mathfrak{C}$ is not an MDS matrix.*

In addition to the study of g-circulant orthogonal matrices, in [70], we explore g-circulant matrices with involutory property. These findings represent an extension of the earlier exploration of the involutory and MDS properties of circulant and left-circulant matrices, as initiated in [17, 25, 30, 31]. Our initial result establishes the pivotal reason behind focusing on the condition $g^2 \equiv 1 \pmod{k}$ for constructing an involutory MDS matrix.

Theorem 1.4.30. *Let A be a g-circulant matrix of order $k \times k$ and $\gcd(k, g) = 1$. If $g^2 \not\equiv 1 \pmod{k}$, then A cannot be involutory.*

Our subsequent aim is to investigate solutions to the equation $g^2 \equiv 1 \pmod{k}$ focusing on those that lead to an involutory MDS g-circulant matrix. In this direction, first observation is that when the order of the matrix is $2^d \times 2^d$, a g-circulant involutory matrix cannot be MDS over the finite field $\mathbb{F}_{2^m}$. The result stands as follows.

Theorem 1.4.31. *Let A be a g-circulant matrix of order $2^d \times 2^d$ over a finite field of characteristic 2 and g is odd. Let $(c_0, c_1, c_2, \ldots, c_{2^d-1})$ be the first row of A and $g^2 \equiv 1 \pmod{2^d}$. If A is an involutory matrix, then A can not be MDS.*

This aforementioned result is a partial affirmative answer to the conjecture proposed by Liu and Sim in [25] noted in Section 1.2.3.
Our subsequent result focus on the case where the order of the matrix is of the form $2^m \prod_{i=1}^{l} p_i^{m_i}, m \geq 0, m_i \geq 1$ and p_i's are odd primes. Our initial finding affirm that a g-circulant involutory matrix cannot be MDS if the value of g is strictly less than $k - 1$.

Theorem 1.4.32. *Let A be a g-circulant matrix of order $k \times k$ with $\gcd(k, g) = 1$ over a finite field of characteristic 2 with $k = 2^m \prod_{i=1}^{l} p_i^{m_i}, m \geq 0, m_i \geq 1$ and p_i's are odd primes. Let $(c_0, c_1, c_2, \ldots, c_{k-1})$ be the first row of A and $g^2 \equiv 1 \pmod{k}$. If A is an involutory matrix and $1 \leq g < k - 1$, then A is not an MDS matrix.*

The next result is on the remaining case, i.e., $g = k - 1$. In this scenario, the matrix becomes left-circulant. Our following findings prove the possibility of constructing left-circulant involutory MDS matrices under specific conditions. This outcome aligns with Proposition 6 outlined in [25], and we offer an alternate proof leveraging the structure of the matrix A^2.

Theorem 1.4.33. *Let A be a left-circulant matrix of order k over the finite field of characteristic 2 with $k > 2, k = 2^m \prod_{i=1}^{l} p_i^{m_i}, m \geq 0, m_i \geq 1$ and p_i's are primes. Let $(c_0, c_1, c_2, \ldots, c_{k-1})$ be the first row of A. Then A is involutory and MDS if and only if the following conditions holds:*

1. $\sum_{i=0}^{k-1} c_i = 1,$
2. $\sum_{\substack{i,j=0, \\ gi+j=l \pmod{k}}}^{k-1} c_i c_j = 0,\ 1 \leq l \leq \lfloor \frac{k-1}{2} \rfloor,$
3. *All submatrices of A have non-zero determinant.*

We also investigate g-circulant matrices endowed with semi-orthogonal and semi-involutory properties. These findings naturally extend the results presented in Theorems 1.4.10 and 1.4.12. The results are as follows:

Theorem 1.4.34. *Let A be a g-circulant matrix of order $k \times k$ over a finite field $\mathbb{F}$ with $\gcd(g, k) = 1$. Then A is semi-orthogonal if and only if there exist non-singular diagonal matrices D_1, D_2 such that $D_1^k = k_1 I$ and $D_2^k = k_2 I$ for non-zero scalars k_1, k_2 in the finite field and $A^{-T} = D_1 A D_2$.*

Theorem 1.4.35. *Let A be a g-circulant matrix of order $k \times k$ over a finite field $\mathbb{F}$ with $\gcd(g, k) = 1$. Then A is semi-involutory if and only if there exist non-singular diagonal matrices D_1, D_2 such that $D_1^k = k_1 I$ and $D_2^k = k_2 I$ for non-zero scalars k_1, k_2 in the finite field and $A^{-1} = D_1 A D_2$.*

In [71], we further investigate the circulant MDS matrices with semi-orthogonal property over a finite field of characteristic 2. Leveraging Theorem 1.4.12, we establish that for circulant semi-orthogonal matrices of order $2^d \times 2^d$, the trace of the associated diagonal matrices is zero over a finite field of characteristic 2.

Proposition 1.4.36. *Let A be a circulant, semi-orthogonal matrix of order $2^d \times 2^d$ over the finite field $\mathbb{F}_{2^m}$ with associated diagonal matrices D_1 and D_2. Then the trace of D_1 and D_2 is zero.*

Additionally, we establish a correlation between the trace of associated diagonal matrices and the MDS property for even order circulant matrices. The initial matrix order we investigate is $2^i n \times 2^i n, i > 1$ and $n \geq 3$, an odd integer. The result is as follows.

Theorem 1.4.37. *Let A be a circulant, semi-orthogonal matrix of order $k \times k$ over the finite field $\mathbb{F}_{2^m}$ with associated diagonal matrices D_1 and D_2, where $k = 2^i n, i > 1$ and $n \geq 3$, an odd integer. Then A is MDS implies both the matrices D_1 and D_2 have trace zero.*

For other even numbers, i.e., numbers in the form of $2n$, where n is an odd number, an additional condition on the entries of at least one of the corresponding diagonal matrices becomes necessary. Any diagonal matrix of even order meeting this criterion is termed as non-periodic diagonal matrix. Specifically, we define a diagonal matrix $D = \text{diagonal}(d_0, d_1, d_2, \ldots, d_{2n-1})$ as a non-periodic diagonal matrix, if the entries satisfy $d_i \neq d_{i+n}, i = 0, 1, 2, \ldots, n-1$. The result under this condition is as follows.

Theorem 1.4.38. *Let A be a circulant, semi-orthogonal matrix of order $2n \times 2n, n \geq 3$ be an odd number, over $\mathbb{F}_{2^m}$ with associated diagonal matrices D_1 and D_2. If A is an MDS matrix and at least one of the associated diagonal matrix is non-periodic, then trace of that non-periodic diagonal matrix is zero.*

We also provides examples of semi-orthogonal MDS matrices with odd orders in [71]. The conclusive finding in this chapter pertains to the analogous characteristics of previous results concerning circulant semi-involutory matrices. The theorem is as follows.

Theorem 1.4.39. *Let A be an $n \times n, n \geq 3, n \neq 2^i$ circulant, semi-involutory matrix over the finite field $\mathbb{F}_{2^m}$ with associated diagonal matrices D_1 and D_2. Then A is MDS implies both the matrices D_1 and D_2 have trace zero.*

This result can be perceived as an extension of the result of Gupta *et al.* presented in [30], where it was proved that circulant involutory matrices of order $n \geq 3$ cannot be MDS.

The last part of this thesis addresses the construction of format preserving sets over rings and modules. We show that it is possible to construct format preserving sets over a finite commutative ring which are not closed under addition. This result provide the general theory behind the Example 1.3.3.

Theorem 1.4.40. *Let $\mathcal{I} = \langle a \rangle$ be a proper ideal of $\mathcal{R} = \mathbb{Z}_n$, where n is a composite positive integer and $S = \mathcal{I} + 1 \subseteq \mathcal{R}$. Then S is an FPS with respect to a matrix $M_{r\times r}(S)$ if and only if the order of the matrix $r \equiv 1 (mod\ a)$.*

We further study the similar construction of format preserving sets over Galois rings, summarized as follows.

Theorem 1.4.41. *Let $\mathcal{R} = GR(p^n, r)$ and $\mathcal{I}_i$ be a principal ideal of $\mathcal{R}$. Consider $S = \mathcal{I}_i + 1 \subseteq \mathcal{R}$. Then S is an FPS with respect to a matrix $M_{r\times r}$ with entries from S if and only if $r \equiv 1 (mod\ p^i)$.*

Moreover, we establish a construction of FPS over arbitrary rings by showing that ideals are natural source of format preserving sets.

Theorem 1.4.42. *Let S be an ideal of the ring $\mathcal{R}$, then S is a format preserving set with respect to any matrix $M_{n\times n}(\mathcal{R})$.*

The subsequent construction of FPS for torsoin modules over PID relies on the fundamental theorem of finitely generated modules over PID.

Theorem 1.4.43. *Let N be a finite module over a PID $\mathcal{R}$ with invariant factors $a_1, a_2, \ldots, a_m$. A subset S of N is an FPS with respect to $M_{n\times n}(\mathcal{R})$ if and only if there exists $S_i \subseteq \mathcal{R}/(a_i)$, such that each S_i is an FPS with respect to $M_{n\times n}(\mathcal{R})$ for all $i = 1, 2, \ldots, m$.*

These constructions of FPS within modules prompt an intriguing question: is it feasible to construct MDS matrices over algebraic structures beyond finite fields? In this direction, many authors [72, 73, 74] explored the construction MDS codes and corresponding generator matrices over cyclic groups, Abelian groups, and elementary Abelian groups as a module over $\mathbb{Z}_p$. In [75], we consider the construction of MDS matrix by considering $\mathbb{Z}_m$ as a $\mathbb{Z}$ module.

Theorem 1.4.44. *Let $N = \mathbb{Z}_m$ be a $\mathbb{Z}$-module, where $m = p_1^{d_1}p_2^{d_2}\cdots p_r^{d_r}$, and p_i's are distinct primes, $1 \leq i \leq r$. Suppose $M = (a_{ij})_{r\times k}$ is a matrix with entries from $\mathbb{Z}$. Then M cannot be MDS if $max\{r, k\} \geq p = min\{p_1, p_2, \ldots, p_r\}$.*

1.5 Organization of the thesis

We now give a brief outline of the work done in each chapter for the convenience of reader.

Chapter 1. In this chapter, we give a brief introduction to the construction of maximum distance separable (MDS) matrices and format preserving sets (FPS) using various methods. For motivation, we describe some of the classical background as well as recent results which lead to this work. In this chapter we also give the layout of the thesis and the statement of the main results established in this thesis.

Chapter 2. In this chapter, we give the necessary prerequisites which are important in order to understand the statement of the results and their proofs. We also recall some of the recent work done by various authors which will be used in our discussion.

Chapter 3. In this chapter, we introduce the construction of MDS matrices possessing both semi-involutory and semi-orthogonal properties. These properties represent a generalization of the classical involutory and orthogonal properties of matrices. We prove that some classical direct construction of MDS matrices over the finite fields satisfy these properties which makes their inverse matrices easy to calculate. Additionally, we provide a characterization of 4×4 semi-involutory matrices and characterize 3×3 semi-involutory and semi-orthogonal matrices with MDS property.

Chapter 4. In this chapter, we present the general structure of 3×3 semi-involutory matrices over the finite field of characteristic 2. We also characterize these matrices with the MDS property. Furthermore, we enumerate the total count of 3×3 semi-involutory

MDS matrices over the finite field of characteristic 2.

Chapter 5. In this chapter, we introduce the general structure of cyclic matrices using permutation matrices. We establish that cyclic matrices encompass a broader class compared to both the g-circulant matrices introduced by Friedman and the traditional circulant matrices. Additionally, we explore the properties of g-circulant and cyclic orthogonal matrices exhibiting the MDS property.

Chapter 6. In this chapter, we explore g-circulant matrices with involutory and MDS properties for various orders over the finite field of characteristic 2. Our initial contribution involves providing an affirmative answer for Liu and Sim's conjecture for a subclass of cyclic matrices. Additionally, we explore g-circulant matrices with semi-involutory and semi-orthogonal properties.

Chapter 7. In this chapter, we delve into the connection between the trace of the associated diagonal matrices of circulant semi-orthogonal matrices of even orders with the MDS property over the finite field $\mathbb{F}_{2^m}$. Additionally, we present examples of circulant, semi-orthogonal MDS matrices for odd orders. Analogous results for circulant semi-involutory matrices of order $n \geq 3$ are also demonstrated.

Chapter 8. In this chapter, we investigate the cardinality of format preserving sets (FPS) over rings and modules. We specifically construct FPS of cardinalities 26 and 52 over torsion modules and rings. These cardinalities are interesting because they correspond to the set of English alphabets, without and with capitalization.

Chapter 9. In this chapter, we study the construction of maximum distance separable (MDS) matrices over $\mathbb{Z}$ modules. Utilizing the concept of MDS codes over modules introduced by Dong, Soh, and Gunawan, we establish that a matrix M with entries from the PID is MDS if and only if M is MDS under the projection map on the same Abelian group.

Chapter 2

Preliminaries

To make our discussion reasonably self-sufficient, we recall some of the basic definitions and related results which shall be used frequently in the later chapters.

2.1 Algebraic structures and their properties

The definitions and the proof of the results mentioned in this section can be found in the textbook [76].

Definition 2.1.1. *A **group** is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms:*

- $(a * b) * c = a * (b * c)$ *for all* $a, b, c \in G$,
- *There exists an element e in G, called an **identity** of G, such that for all $a \in G$ we have $a * e = e * a = a$,*
- *For each $a \in G$ there is an element a^{-1} of G, called an **inverse** of a, such that $a * a^{-1} = a^{-1} * a = e$.*

A *semigroup* is a set G together with a binary operation $*$ that satisfies the associative property i.e., for all $a, b, c \in G$ the equation $(a * b) * c = a * (b * c)$ holds.

Definition 2.1.2. *A group $(G, *)$ is called **Abelian** (or commutative) if $a * b = b * a$ for all $a, b \in G$.*

Definition 2.1.3. *A group G is **cyclic** if G can be generated by a single element, i.e., there is some element $x \in G$ such that $G = \{x^n \mid n \in \mathbb{Z}\}$.*

Definition 2.1.4. *Let Σ be any non-empty set and let S_Σ be the set of all bijections from Σ to itself. The set $(S_\Sigma, \circ)$ is called **symmetric group** where the operation $\circ$ is function composition. If $\Sigma = \{1, 2, \ldots, n\}$, the symmetric group on Σ is denoted S_n, the symmetric group of degree n.*

Note that, the order of S_n is $n!$, because there are precisely $n!$ permutations of $\{1, 2, \cdots, n\}$. A *cycle* is a string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers). The cycle $(x_1\ x_2\ \cdots\ x_m)$ is the permutation which sends x_i to x_{i+1} for all $1 \leq i \leq m-1$ and sends x_m to x_1.

Definition 2.1.5. *Let $(G, *)$ and $(H, \circ)$ be groups. A map $\phi : G \to H$ such that $\phi(x \star y) = \phi(x) \circ \phi(y)$ is called a homomorphism.*

If the domain and range of the homomorphism ϕ are the same set, the it is called *endomorphism*. Again if the map ϕ is a bijection, then it is called an *isomorphism* between G and H.

Definition 2.1.6. *A **ring** is a non empty set $\mathcal{R}$ together with two binary operations addition $(+)$ and multiplication $(\cdot)$ satisfying following axioms:*

1. *$(\mathcal{R}, +)$ is an abelian group.*
2. *$(\mathcal{R}, \cdot)$ is semigroup.*
3. *$(r + s) \cdot t = r \cdot s + s \cdot t$ and $r \cdot (s + t) = r \cdot s + r \cdot t$ for all r, s, t in $\mathcal{R}$.*

A ring $\mathcal{R}$ is said to be commutative if it is commutative with respect to multiplication. We sometimes simply write ab instead of $a \cdot b$ for $a, b \in \mathcal{R}$. The additive identity of the ring is denoted by 0 and the multiplicative identity, if it exists, is denoted by 1. Multiplicative inverse of any element a is denoted by a^{-1}. Characteristic of ring $\mathcal{R}$ is the smallest integer n such that $n \cdot 1 = 0$. If no such n exists, then we say $\mathcal{R}$ is of characteristics 0.

Definition 2.1.7. *(i) A non-zero element a of a ring $\mathcal{R}$ is called a **zero divisor** if there is a non-zero element b in $\mathcal{R}$ such that $ab = 0$ or $ba = 0$.*

*(ii) An element u in the ring $\mathcal{R}$ is called a **unit** if there exists v in $\mathcal{R}$ such that $uv = vu = 1$.*

For example, every non zero element in the ring $\mathbb{Z}_n$ is either a unit or a zero divisor. The ideal of a ring plays a very important in this thesis. We define it next.

Definition 2.1.8. *A (two sided) **ideal** $\mathcal{I}$ of a ring $\mathcal{R}$ is a subset of $\mathcal{R}$ with the following properties:*

(i) For any $r_1, r_2 \in \mathcal{I},\ (r_1 - r_2) \in \mathcal{I}$.

(ii) For any $r \in \mathcal{R}$ and $r_1 \in \mathcal{I},\ r \cdot r_1 \in \mathcal{I}$ and $r_1 \cdot r \in \mathcal{I}$.

If an ideal $\mathcal{I}$ is a proper subset of the ring it is called a **proper ideal**. If an ideal $\mathcal{I}$ is generated by a single element α, it is called a **principal ideal**. We denote it by $\mathcal{I} = \langle \alpha \rangle$.

Definition 2.1.9. *A **Principal Ideal Domain** (P.I.D.) is an integral domain in which every ideal is principal.*

Two families of ring we discuss now are ring of integers modulo n and Galois ring. The set of integers modulo n, equipped with the operations of addition and multiplication, constitutes a ring denoted as $\mathbb{Z}_n$ in this thesis. A few notable properties of $\mathbb{Z}_n$ are outlined below.

1. $(\mathbb{Z}_n, \oplus, \odot)$ is a commutative ring with unity. The operation $\oplus$ is addition modulo n and $\odot$ is multiplication modulo n. The element 1 is the multiplicative identity and 0 is the additive identity of this ring.
2. Every ideal of $\mathbb{Z}_n$ is principal ideal.

3. Every non-zero element of $\mathbb{Z}_n$ is either a unit or a zero divisor.

Galois rings are finite extensions of the ring $\mathbb{Z}_{p^n}$, where p is a prime number. Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}_{p^n}[x]$. Consider the ring homomorphism $\psi : \mathbb{Z}_{p^n}[x] \to \mathbb{Z}_p[x]$, where $\psi(c_0 + c_1x + \cdots + c_nx^n) = \bar{c_0} + \bar{c_1}x + \cdots + \bar{c_n}x^n$. Consider the image of $f(x)$ under the mapping ψ in $\mathbb{Z}_p[x]$. If the image $\overline{f(x)}$ in $\mathbb{Z}_p[x]$ is irreducible in $\mathbb{Z}_p$, then $f(x)$ is called a monic, basic, irreducible polynomial.
Let $f(x)$ is a monic, basic, irreducible polynomial of degree m over the ring $\mathbb{Z}_{p^n}$. Then the residue class ring $\mathbb{Z}_{p^n}[x]/\langle f(x)\rangle$ is a Galois ring, denoted by $GR(p^n, m)$. This ring is of characteristic p^n and of cardinality p^{nm}. Some properties of the Galois ring $GR(p^n, m)$ are as follows:

- $GR(p^n, m)$ is a finite, commutative, local ring, i.e., rings with a unique maximal ideal.
- The unique maximal ideal of $GR(p^n, m)$ is the principal ideal $(p) = pGR(p^n, m)$. It consists all elements which are multiple of p. Also $GR(p^n, m)/(p)$ is isomorphic to the finite field $\mathbb{F}_{p^m}$.
- Other principal ideals of $GR(p^n, m)$ are $\mathcal{I}_i = (p^i), 0 \leq i \leq n$ and the elements are of the form $\mathcal{I}_i = \{c_0 + c_1x + \cdots + c_{m-1}x^{m-1} : c_j \in (p^i),\ 1 \leq j \leq m-1\}$.

Definition 2.1.10. *Let $\mathcal{R}$ be a ring. A triple $(N, +, \cdot)$, where $(N, +)$ is an Abelian group together with an action of $\mathcal{R}$ on N, is called an $\mathcal{R}$-**module** if it satisfies the following conditions:*

(i) $(r + s) \cdot n = r \cdot n + s \cdot n$, *for all* $r, s \in \mathcal{R}, n \in N$.

(ii) $(rs) \cdot n = r(s \cdot n)$, *for all* $r, s \in \mathcal{R}, n \in N$.

(iii) $r \cdot (n_1 + n_2) = r \cdot n_1 + r \cdot n_2$, *for all* $r \in \mathcal{R}, n_1, n_2 \in N$.

(iv) Further, if the ring $\mathcal{R}$ has 1, *then* $1 \cdot n = n$, *for all* $n \in N$.

If N satisfies the above conditions over a field $\mathcal{R}$ then it becomes a vector space over $\mathcal{R}$. Further, every ring $\mathcal{R}$ has a module structure over itself.

Definition 2.1.11. *Let $\mathcal{R}$ be a ring and N be an $\mathcal{R}$-module. A subset N' of N is a **submodule** of N if and only if*

(i) $N' \neq \phi$ *and,*

(ii) $x + ry \in N'$ *for all* $r \in \mathcal{R}$ *and* $x, y \in N'$.

For example, if we consider a ring $\mathcal{R}$ as a module over itself, ideals are submodules of $\mathcal{R}$. An element $n \in N$ of the $\mathcal{R}$-module is called a **torsion** element if $rn = 0$ for some non-zero element $r \in \mathcal{R}$. The set of torsion elements is denoted by $\text{Tor}(N) = \{n \in N : rn = 0 \text{ for some non-zero } r \in \mathcal{R}\}$.

Definition 2.1.12. *An $\mathcal{R}$-module N is said to be a **torsion module** if every element of N is a torsion element.*

For example, any finite Abelian group is a torsion module over $\mathbb{Z}$. For any submodule N' of N, the **annihilator** of N' is the ideal of $\mathcal{R}$ defined by $\text{Ann}(N') = \{r \in \mathcal{R} : rn = 0 \text{ for all } n \in N'\}$.

Definition 2.1.13. *An $\mathcal{R}$-module N is said to be **free module** on the subset A of N if for every non-zero element x of N, there exist unique non-zero elements $r_1, r_2, \ldots, r_n$ of $\mathcal{R}$ and unique $a_1, a_2, \ldots, a_n$ in A such that $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$ for some positive integer n.*

The fundamental theorem of finitely generated modules over PID is following:

Theorem 2.1.14. *Let $\mathcal{R}$ be a PID and N be a finitely generated $\mathcal{R}$-module. Then*

(i) N is isomorphic to the direct sum of finitely many cyclic modules. More precisely,

$$N \cong \mathcal{R}^r \bigoplus \mathcal{R}/(a_1) \bigoplus \mathcal{R}/(a_2) \bigoplus \cdots \bigoplus \mathcal{R}/(a_m)$$

for some integer $r \geq 0$ and non-zero elements $a_1, a_2, \ldots, a_m$ of $\mathcal{R}$ which are not units in $\mathcal{R}$ and satisfy the divisibility relations $a_1|a_2| \cdots |a_m$.

(ii) N is torsion free if and only if N is free.

(iii) $Tor(N) \cong \mathcal{R}/(a_1) \bigoplus \mathcal{R}/(a_2) \bigoplus \cdots \bigoplus \mathcal{R}/(a_m)$.

The elements $a_1, a_2, \ldots, a_m$ in Theorem 2.1.14 are known as the invariant factors of N. Since $\mathcal{R}$ is a PID, for each $1 \leq i \leq m$, $\mathcal{R}/(a_i)$ is a cyclic module and its elements are of the form $r + (a_i)$, which we denote as $\bar{r}$.
A **field** $\mathbb{F}$ is a commutative ring with identity in which every non-zero element has an inverse. The **characteristic** of a field $\mathbb{F}$ is the smallest positive integer p such that $p \cdot 1_{\mathbb{F}} = 0$, where $1_{\mathbb{F}}$ is the multiplicative identity of $\mathbb{F}$.

Proposition 2.1.15. *The characteristic of a field $\mathbb{F}$ is either 0 or a prime p.*

For example, the finite field $\mathbb{F}_p = \mathbb{Z}_p$ has characteristic p for any prime p. Also $\mathbb{F}_p$ has p elements. The field $\mathbb{F}_{p^n}$ is an finite extension of $\mathbb{F}_p$ with degree of extension n. Also $\mathbb{F}_{p^n} \simeq \mathbb{F}_p/\langle f(x) \rangle$, where $f(x)$ is an irreducible polynomial of degree n in $\mathbb{F}_p[x]$. For the finite field $\mathbb{F}_q$ with $q = p^m$, p prime, $\mathbb{F}_q^*$ is the set of non-zero elements of $\mathbb{F}_q$ and $|\mathbb{F}_q^*| = q - 1$.

Theorem 2.1.16. *$\mathbb{F}_q^*$ is a cyclic multiplicative group of order $p^m - 1$.*

Therefore, if α is a generator of the cyclic group $\mathbb{F}_q^*$, then all elements are of the form $\{1, \alpha, \alpha^2, \cdots, \alpha^{p^m-1}\}$ with $\alpha^{p^m} = 1$.
In the finite field of characteristic 2, elements can be expressed in binary and hexadecimal forms. For instance, consider the finite field $\mathbb{F}_{2^4}$ with irreducible polynomial $x^4 + x + 1$. If $\beta \in \mathbb{F}_{2^4}$, it can be written as $\beta_0 + \beta_1 a + \beta_2 a^2 + \beta_3 a^3$, where a is a root of the polynomial $x^4 + x + 1$. Then $\beta = (\beta_0, \beta_1, \beta_2, \beta_3)_2$ is the binary representation of the element. For example, the binary form of the element $a^3 + a^2 + 1$ is $(1101)_2$ and the hexadecimal form is D.

2.2 Some important results on matrices

In this section, we concentrate on specific classes of matrices and their properties, which play a significant role in this thesis. A matrix, denoted as $M = (m_{i,j})$, has entries $m_{i,j}$ representing the element in the i-th row and j-th column. Alternatively, we may use m_{ij}. The inverse and transpose are represented as M^{-1} and M^T throughout the thesis.

Definition 2.2.1. *Let $\{x_0, x_1, \ldots, x_{n-1}\}$ and $\{y_0, y_1, \ldots, y_{n-1}\}$ be two sets of elements from a finite field $\mathbb{F}$ such that $x_i + y_j \neq 0$ for $0 \leq i, j \leq n-1$. Then the matrix $A = \left(\frac{1}{x_i+y_j}\right), 0 \leq i, j \leq n-1$ is called a **Cauchy matrix**.*

The determinant of a Cauchy matrix is

$$\det A = \frac{\prod_{1\leq i<j\leq n}(x_j - x_i)(y_j - y_i)}{\prod_{1\leq i,j\leq n}(x_i + y_j)}.$$

Also for the case $x_i \neq x_j$ and $y_i \neq y_j$ for all $1 \leq i, j \leq n$, the determinant is always non-zero and hence in this case square Cauchy matrices are invertible. Let $A^{-1} = (\gamma_{ij}), 1 \leq i, j \leq n$. Then the general form of γ_{ij} is

$$\gamma_{ij} = (x_j + y_i)\frac{\prod_{l\neq i}(x_j + y_l)\prod_{k\neq j}(y_i + x_k)}{\prod_{l\neq j}(x_j - x_l)\prod_{k\neq i}(y_i - y_k)}. \tag{2.1}$$

Definition 2.2.2. *The matrix*

$$V = vand(v_0, v_1, \cdots, v_{m-1}) = \begin{bmatrix} 1 & v_0 & v_0^2 & \cdots & v_0^n \\ 1 & v_1 & v_1^2 & \cdots & v_1^n \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & v_{m-1} & v_{m-1}^2 & \cdots & v_{m-1}^n \end{bmatrix}$$

*is called a **Vandermonde matrix** of order $m \times n$.*

The (i, j)-th entry of a Vandermonde matrix is is denoted as $V(i, j) = v_i^j$, considering zero-based indices for both i, j. Most authors define the Vandermonde matrix as the transpose of the aforementioned matrix.
The determinant of a square Vandermonde matrix is $\det V = \prod_{0\leq i<j\leq n}(v_i - v_j)$. While over the real field, the square submatrices of Vandermonde matrices are nonsingular, this property does not hold over finite fields, as pointed out by MacWilliams and Sloane in [16]. Therefore, an interesting remark regarding Vandermonde matrices over finite field is the following:

Remark 2.2.3. *There exists Vandermonde matrices over finite field with singular submatrices. For example, the matrix Vandermonde$(1, \alpha, \alpha^4, \alpha^5)$, where α is a primitive element of the finite field $\mathbb{F}_{2^4}$ defined by the polynomial $x^4 + x + 1$ has a singular submatrix. This matrix was shown to have a singular submatrix, as demonstrated in [17].*

Definition 2.2.4. *A finite field Hadamard matrix, denoted as H, is of order $2^t \times 2^t,\ t > 0$ with entries from $\mathbb{F}_{2^m}$ can be expressed as follows: $H = \begin{bmatrix} A_0 & A_1 \\ A_1 & A_0 \end{bmatrix}$ where A_0 and A_1 are $2^{t-1} \times 2^{t-1}$ Hadamard matrices.*

A 2×2 Hadamard matrix H with entries of the first row (h_0, h_1) has the form $\begin{bmatrix} h_0 & h_1 \\ h_1 & h_0 \end{bmatrix}$. Similarly, for a 4×4 Hadamard matrix with entries in the first row as (h_0, h_1, h_2, h_3) has the following form:

$$\begin{bmatrix} h_0 & h_1 & h_2 & h_3 \\ h_1 & h_0 & h_3 & h_2 \\ h_2 & h_3 & h_0 & h_1 \\ h_3 & h_2 & h_1 & h_0 \end{bmatrix}.$$

It is important to note that a Hadamard matrix H over a field of characteristic 2 satisfies $H^2 = c^2 I$, where c is the sum of the elements in the first row of H. Consequently, if $c^2 = 1$, the matrix H becomes involutory. If the entries of a Hadamard matrix are taken from a finite field of characteristic 2, they adhere to the following lemma.

Lemma 2.2.5. *Let $H = (h_{i,j}), 0 \leq i, j \leq 2^n - 1$ be a $2^n \times 2^n$ matrix with in the first row given by $(h_0, h_1, \ldots, h_{2^n-1})$. Then H is a Hadamard if and only if $h_{i,j} = h_{i \oplus j}$, where $i \oplus j$ represents the bitwise XOR of the n-bit binary representations of i and j, respectively.*

We now turn our attention to circulant matrices and their generalizations, and these are the next class of matrices in our discussion. To start, let us define circulant matrices.

Definition 2.2.6. *The $k \times k$ matrix of the form $\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{k-1} \\ c_{k-1} & c_0 & c_1 & \cdots & c_{k-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}$ is called a **circulant matrix** and is denoted by $\mathcal{C} = circulant(c_0, c_1, c_2, \ldots, c_{k-1})$.*

The entire circulant matrix is clearly defined by its first row (or column). Notably, we represent the entry at the (i, j)-th position of this matrix as $\mathcal{C}(i, j)$. The entries of $\mathcal{C}$ can be expressed as $\mathcal{C}(i, j) = c_{j-i \pmod k}$. Moreover, the entries of $\mathcal{C}$ adhere to the relationship $\mathcal{C}(i, j) = \mathcal{C}(i + 1, j + 1)$. Utilizing the property of the permutation matrix $P = \text{circulant}(0, 1, 0, \ldots, 0)$, a circulant matrix $\mathcal{C}$ can be represented as:

$$\mathcal{C} = \text{circulant}(c_0, c_1, c_2, \ldots, c_{k-1}) = c_0 I + c_1 P + c_2 P^2 + \cdots + c_{k-1} P^{k-1}, \tag{2.2}$$

where I denotes the identity matrix of order $k \times k$.

A comprehensive expression for the determinant of a circulant matrix is provided in [68]. For any circulant matrix $A = c_0 I + c_1 P + c_2 P^2 + \cdots + c_{k-1} P^{k-1}$ of a fixed order k, where $c_0, c_1, \cdots, c_{k-1}$ are arbitrary integers in $\mathbb{Z}$ and $P = \text{circulant}(0, 1, 0, \ldots, 0)$, the

determinant $\det(A)$ can be expressed as:

$$\det(A) = \prod_{j=0}^{k-1}(\sum_{i=0}^{k-1} c_i \omega_k^{ji}), \tag{2.3}$$

where $\omega_k = e^{\frac{2\pi i}{k}} \in \mathbb{C}$.

Definition 2.2.7. *The square matrix of the form* $\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{k-1} \\ c_1 & c_2 & c_3 & \cdots & c_0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ c_{k-1} & c_0 & c_1 & \cdots & c_{k-2} \end{bmatrix}$ *is said to be left-circulant matrix and denoted by left-circulant*$(c_0, c_1, c_2, \ldots, c_{k-1})$.

Next we discuss permutation matrices and some of its properties. By a permutation σ belongs to the symmetric group S_n,we means one-to-one mapping from the set $N = \{1, 2, \ldots, n\}$ to itself. A permutation can be written as $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}$ and this means $\sigma(1) = i_1, \sigma(2) = i_2, \cdots, \sigma(n) = i_n$. The inverse permutation is denoted by σ^{-1} and $\sigma^{-1}(i_k) = k$. Let E_i denote the row vector on n-components with 1 at i-th positions and 0 at all other positions.

Definition 2.2.8. *A* ***permutation matrix*** P *of order* $n \times n$ *is a matrix of the form*

$$P = P_\sigma = \begin{bmatrix} E_{i_1} \\ E_{i_2} \\ \vdots \\ E_{i_n} \end{bmatrix}.$$

It can be written as $P = (a_{ij})$ where $\begin{cases} a_{i,\sigma(i)} = 1, & \text{for } i = 1, 2, \cdots, n. \\ a_{ij} = 0, & \text{otherwise.} \end{cases}$

Some properties of permutations matrices are as follows:

- $P_\sigma P_\tau = P_{\sigma\tau}$,
- $P_\sigma^{-1} = P_{\sigma^{-1}} = P_\sigma^T$,
- If $A = (a_{i,j})$ is a $m \times n$ matrix, then $P_\sigma A = A_{\sigma(i),j}$ and $AP_\sigma = A_{i,\sigma^{-1}(j)}$. That is, $P_\sigma A$ is A with row permuted by σ and AP_σ is A with column permuted by σ.
- A matrix A is said to be **permutation similar** to another matrix B if $B = PAP^T$ for some permutation matrix P.
- A matrix A is said to be **permutation equivalent** to another matrix B if $B = PAQ$ for some permutation matrices P and Q.

B. Friedman further expanded the theory of circulant matrices in 1961 by introducing g-circulant matrices [67]. The definition of a g-circulant matrix is as follows:

Definition 2.2.9. *A g-circulant matrix of order $k \times k$ is a matrix of the form* $A = g\text{-circulant}(c_0, c_1, \ldots, c_{k-1}) = \begin{bmatrix} c_0 & c_1 & \cdots & c_{k-1} \\ c_{k-g} & c_{k-g+1} & \cdots & c_{k-1-g} \\ c_{k-2g} & c_{k-2g+1} & \cdots & c_{k-1-2g} \\ \vdots & \vdots & \cdots & \vdots \\ c_g & c_{g+1} & \cdots & c_{g-1} \end{bmatrix}$, *where all subscripts are taken modulo k.*

For $g = 1$, it represents a circulant matrix, and for $g \equiv -1 \pmod{k}$, it takes the form of a left-circulant matrix. Here are some noteworthy properties of g-circulant matrices, with details provided in [68], [77].

Lemma 2.2.10. *Let A be g-circulant and B h-circulant. Then AB is gh-circulant.*

Lemma 2.2.11. *If A and B are both g-circulant matrices then AB^T forms a circulant matrix.*

Lemma 2.2.12. *A is g-circulant if and only if $PA = AP^g$ where P is the permutation matrix $P = circulant(0, 1, 0, \ldots, 0)$.*

For the case $\gcd(k, g) = 1$, the solution to the equation $gx \equiv 1 \pmod{k}$ is unique modulo k. Then the following result regarding the inverse of a non-singular g-circulant matrix is proved in [68].

Lemma 2.2.13. *Let A be a non-singular g-circulant matrix of order $k \times k$ with $\gcd(g, k) = 1$. Then A^{-1} is g^{-1}-circulant.*

The next theorem extends the structure defined in Equation 2.2 to g-circulant matrices. Let $P = \text{circulant}(0, 1, 0, \ldots, 0)$ and $Q_g = g\text{-circulant}(1, 0, 0, \ldots, 0)$. The representation of g-circulant matrices is established by the following theorem [[68], Theorem 5.1.7].

Theorem 2.2.14. *Let $A = g\text{-circulant}(c_0, c_1, \ldots, c_{k-1})$ with $\gcd(k, g) = 1$. Then A can be expressed as $A = \sum_{i=0}^{k-1} c_i Q_g P^i$ where $P = circulant(0, 1, 0, \ldots, 0)$ and $Q_g = g\text{-circulant}(1, 0, 0, \ldots, 0)$.*

The notion of cyclic matrix was introduced by Liu and Sim [25] as a generalization of the circulant matrix in 2016. Cyclic matrices of order $k \times k$ are defined using a k-cycle permutation ρ of its first row where $\rho \in S_k$, the permutation group on k elements. The definition of cyclic matrix is the following:

Definition 2.2.15. *For a k-cycle $\rho \in S_k$, a matrix $\mathfrak{C}_\rho$ of order $k \times k$ is called cyclic matrix if each subsequent row is ρ-permutation of the previous row. We represent this matrix as $cyclic_\rho(c_0, c_1, c_2, \ldots, c_{k-1})$, where $(c_0, c_1, c_2, \ldots, c_{k-1})$ is the first row of the matrix. The (i, j)-th entry of $\mathfrak{C}_\rho$ can be expressed as $\mathfrak{C}_\rho(i, j) = c_{\rho^{-i}(j)}$.*

2.3 Semi-involutory and semi-orthogonal matrices

Two intriguing properties of a matrix are its involutory and orthogonal characteristics.

Definition 2.3.1. *A square matrix A is said to be involutory if $A^2 = I$ and orthogonal if $AA^T = A^TA = I$.*

Therefore, for a symmetric matrix $A = A^T$, both properties become equivalent.
Recently, in 2012, Fiedler *et al.* [64] generalised orthogonal matrices and named them *G-matrices*, which we refer as *semi-orthogonal matrices* throughout this thesis. The definition of a semi-orthogonal matrix is as follows:

Definition 2.3.2. *A non-singular matrix A is **semi-orthogonal** if there exist non-singular diagonal matrices D_1 and D_2 such that $A^{-T} = D_1AD_2$, where A^{-T} denotes the transpose of the matrix A^{-1}.*

Some equivalent definitions of semi-orthogonal matrices are the following:

1. A is semi-orthogonal.
2. A^{-1} and A^T are semi-orthogonal.
3. If A is semi-orthogonal and D is a non-singular diagonal matrix, then both AD and DA are semi-orthogonal.
4. If A is semi-orthogonal and P is a permutation matrix, then both PA and AP are semi-orthogonal.
5. ADA^T is non singular and diagonal for some diagonal matrix D.

We refer to the matrices D_1 and D_2 in definition as "associated diagonal matrices" for the semi-orthogonal matrix A. The authors of [64] further provided a characterization of all 2×2 semi-orthogonal matrices in the following theorem:

Theorem 2.3.3. *A 2×2 matrix is semi-orthogonal if and only if it is non-singular and has four or two non-zero entries.*

After that, in 2021, Cheon, Curtis and Kim [65] expanded the idea of an involutory matrix and defined a semi-involutory matrix as follows:

Definition 2.3.4. *A non-singular matrix A is said to be **semi-involutory** if there exist non-singular diagonal matrices D_1 and D_2 such that $A^{-1} = D_1AD_2$.*

Some equivalent definitions of semi-involutory matrices are given as follows:

1. A is semi-involutory.
2. A^{-1} and A^T are semi-involutory.
3. DAD' is semi-involutory for any non-singular diagonal matrices D and D'.

4. P^TAP is semi-involutory for any permutation matrix P.

5. ADA is non-singular and diagonal for some diagonal matrix D.

We refer the matrices D_1 and D_2 in the definition as "associated diagonal matrices" for the semi-involutory matrix A.
Cheon et al. [65] provided a characterization of 2×2 semi-involutory matrices by utilizing the "zero non-zero pattern" of the matrix. The "*zero non-zero pattern*" of a matrix $A = (a_{ij})$ is the $(0,1)$-matrix whose (i,j)-th entry is non-zero if and only if a_{ij} is non-zero. Furthermore, Cheon et al. [65] characterize 2×2 semi-involutory matrices based on this property.

Theorem 2.3.5. *Let A be a non-singular matrix of order 2. Then A is semi-involutory if and only if the zero non-zero pattern of A is not permutation similar to* $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$.

A connection between the entries and submatrices of a semi-involutory matrix is established in [65]. To articulate this result, we introduce specific notations. Let α and β be subsets of the set $[n] = \{1, 2, \ldots, n\}$. For a matrix A of order n, $A[\alpha|\beta]$ denotes the $|\alpha| \times |\beta|$ submatrix of A formed by the rows indexed by α and the columns indexed by β. Let $\alpha^c = [n] \setminus \alpha$ and $\beta^c = [n] \setminus \beta$. Then $A(\alpha|\beta)$ denotes the matrix $A[\alpha^c|\beta^c]$. The result is as follows:

Theorem 2.3.6. *Let $A = (a_{ij})$ be a semi-involutory matrix of order $n \times n$. Then $\det A(j|i) = 0$ if and only if $a_{ij} = 0$.*

Proof. For proof, see Theorem 2.11 of [65]. □

Before proceeding to the next characterization, we introduce another class of matrices.

Definition 2.3.7. *A square matrix A is said to be reducible if it is permutation similar to an upper triangular matrix. The matrix A is called irreducible if it is not reducible.*

A comprehensive characterization of 3×3 semi-involutory matrices was also established by Cheon *et al.* The characterization is outlined as follows:

Theorem 2.3.8. *Let $A = (a_{ij})$ be a real matrix of order 3×3. Then A is semi-involutory if and only if A is non-singular and one of the following holds.*

- *Up to permutation similarity A is a reducible matrix of the form*

$$A = \begin{bmatrix} B & \boldsymbol{x} \\ \boldsymbol{0}^T & c \end{bmatrix}$$

  such that $B^{-1} = D_1BD_2$ for some non-singular diagonal matrices D_1 and D_2, and $\boldsymbol{x} = \boldsymbol{0}$ or $\boldsymbol{x}$ is an eigenvector of BD_1.

- *Up to permutation similarity $a_{11} = 0$ is the only zero entry in A, $\det A(1|1) = 0$ and $a_{12}a_{23}a_{31} = a_{13}a_{21}a_{32}$.*

- *A is nowhere zero,* $a_{12}a_{23}a_{31} = a_{13}a_{21}a_{32}$*, and* $\det X = 0$ *where*

$$X = \begin{bmatrix} a_{11}a_{22} & a_{21}a_{22} & a_{23}a_{31} \\ a_{11}a_{31} & a_{21}a_{32} & a_{31}a_{33} \\ a_{12}a_{31} & a_{22}a_{32} & a_{32}a_{33} \end{bmatrix}.$$

Proof. For proof, see Theorem 2.10 of [65]. □

Additionally, another characterization of irreducible semi-involutory matrices was proven by Cheon *et al.*, stated as follows:

Theorem 2.3.9. *Let* A *be an irreducible semi-involutory matrix of order* $n \times n$ *such that* $A^{-1} = D_1AD_2$*, where* D_1 *and* D_2 *are non-singular diagonal matrices. Then* $D_1 = cD_2$ *for some non-zero constant* c*.*

2.4 Linear codes

In this section, we revisit some definitions and results from coding theory, essential for various proofs in our discussion.
In coding theory, a linear code C of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. If dimension of C over $\mathbb{F}_q$ is k, then it is denoted as a $[n, k]$ code. Here n is the *length* of the code and k is the *dimension*. An element of C is called a codeword. Another important parameter of a linear code is minimum distance. The Hamming distance between two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ is the number of positions where the differ, denoted by $d(\mathbf{x}, \mathbf{y})$. Additionally, the Hamming weight $wt(\mathbf{x})$ of a vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is the count of non-zero x_i's in $\mathbf{x}$. Thus, the minimum distance d of a linear code is defined by

$$d = \min d(\mathbf{u}, \mathbf{v}) = \min wt(\mathbf{u} - \mathbf{v}),$$

where $\mathbf{u}, \mathbf{v} \in C, \mathbf{u} \neq \mathbf{v}$.
Hence, a linear code C of length n, dimension k, and minimum distance d is referred as an $[n, k, d]$ code. The minimum distance of a linear code is the minimum weight of any non-zero codeword.

Definition 2.4.1. *Let* C *be a linear code over* $\mathbb{F}_q^n$*. The dual code of* C *is the orthogonal complement of the subspace* C *of* $\mathbb{F}_q^n$*, and is denoted by* $C^\perp$*.*

Proposition 2.4.2. $C^\perp$ *is a linear code and dim* C*+ dim* $C^\perp = n$*.*

Two important matrices associated to a linear codes are generator matrix and parity check matrix.

Definition 2.4.3. *A* ***generator matrix*** *of a* $[n, k]$ *linear code* C *is a* $k \times n$ *matrix* G *whose rows form a basis of* C*.*

The standard from of a generator matrix is $[I|A]$, where I is the $k \times k$ identity matrix and A is a $k \times (n-k)$ matrix.

Definition 2.4.4. *A **parity check matrix** H of a linear code C is the generator matrix of the dual code $C^{\perp}$.*

The parity check matrix of C is a $(n-k) \times k$ matrix, and the standard from of H is $[B|I]$ where I is the $(n-k) \times (n-k)$ identity matrix and B is a $(n-k) \times k$ matrix. The generator matrix of a code C can be obtained from the standard form of the parity check matrix, and it is $[I|-B^T]$. They are related by the identity $GH^T = 0$ or $HG^T = 0$. Some essential properties of linear codes are following:

Theorem 2.4.5. *If H is the parity check matrix of a code C of length n, then the code has dimension $n-k$ if and only if some k columns of H are linearly independent but no $k+1$ columns are.*

Proof. For proof, see Theorem 9 of Chapter 1 of [16]. □

Theorem 2.4.6. *If H is the parity check matrix of a code of length n, then the code has minimum distance d if and only if every $d-1$ columns of H are linearly independent and some d columns are linearly dependent.*

Proof. For proof, see Theorem 10 of Chapter 1 of [16]. □

Theorem 2.4.7. *(**Singleton bound**) If C is an $[n,k,d]$ code, then $n-k \geq d-1$.*

Proof. For proof, see Theorem 11 of Chapter 1 of [16]. □

Codes with $d = n-k+1$ are called Maximum distance Separable (MDS) codes. It is one of the most important class of codes. Reed-Solomon codes are an important example of this class. Some key properties of MDS codes are following:

Theorem 2.4.8. *A $[n,k,d]$ code C is an MDS code if and only if every $n-k$ columns of the parity check matrix H are linearly independent.*

Proof. For proof, see Theorem 1 of Chapter 11 of [16]. □

Theorem 2.4.9. *If C is an MDS code, then $C^{\perp}$ is also MDS.*

Proof. For proof, see Theorem 2 of Chapter 11 of [16]. □

Corollary 2.4.10. *Let C be an $[n,k,d]$ code over the finite field $\mathbb{F}_q$. Then the following statements are equivalent:*

- *C is MDS.*
- *Every k columns of a generator matrix G are linearly independent.*
- *Every $n-k$ columns of a parity check matrix H are linearly independent.*

Proof. For proof, see Corollary 3 of Chapter 11 of [16]. □

Theorem 2.4.11. *An $[n, k, d]$ code C with generator matrix $[I_{k\times k}|A]$, where A is a $k \times (n-k)$ matrix is MDS if and only if every square submatrix of A, formed from any i rows and i columns, for any $i = \{1, 2, \ldots, min(k, n-k)\}$, is non-singular.*

Proof. For proof, see Theorem 8 of Chapter 11 of [16]. □

The following result is a direct application of Theorem 2.4.11.

Proposition 2.4.12. *A square matrix A is an MDS matrix if and only if every square submatrix of A is non-singular.*

Some properties of MDS matrices are as follows:

Corollary 2.4.13. *If A is an MDS matrix, then for any non-singular diagonal matrices D_1 and D_2, D_1AD_2 is also an MDS matrix.*

Proof. For proof, see Corollary 1 of [17]. □

Corollary 2.4.14. *If A is an MDS matrix, then A^T and A^{-1} are also MDS matrices.*

Proof. For proof, see Corollary 2 and Corollary 3 of [17]. □

Corollary 2.4.15. *For any permutation matrices P and Q, the branch numbers of the two matrices M and PMQ are same.*

Proof. For proof, see Proposition 1 of [17]. □

As an immediate application of this corollary, the following result holds.

Corollary 2.4.16. *If A is an MDS matrix, then for any permutation matrices P and Q, PAQ is also an MDS matrix.*

Proof. For proof, see Corollary 4 of [17]. □

Chapter 3

Semi-orthogonal and semi-involutory MDS matrices

In this chapter we first introduce the construction of Maximum Distance Separable (MDS) matrices with semi-involutory and semi-orthogonal properties. Subsequently, we propose a construction method for MDS matrices using Cauchy matrices, ensuring a straightforward inverse operation. This construction method maintains the property that submatrices also exhibit the MDS property with easily invertible characteristics. In the last part we provide a characterization of 4×4 semi-involutory matrices with all non-zero entries over some field. The findings presented in this chapter have been published and can be referenced in [63].

3.1 Introduction

The significance of constructing MDS matrices endowed with either involutory or orthogonal properties becomes apparent through our discussion from Chapter 1. These constructions have been studied by various authors. For instance, in [19], Sajadieh *et al.* constructed involutory MDS matrices using Vandermonde matrices. Additionally, in [20], the authors focused on Cauchy matrices to construct MDS involutory matrices. In the Cauchy based construction, matrices are derived from an additive subgroup of the finite field $\mathbb{F}_{2^m}$, resulting in the orders of the matrices consistently being powers of 2. Therefore, even if it is possible to construct an involutory MDS matrix with order as a power of 2 over the finite field $\mathbb{F}_{2^m}$, the construction of an MDS Cauchy matrix of any order with easily implementable inverse remains an open question. Recently, in 2012, Fiedler and Hall [64] proved that Cauchy matrices are semi-orthogonal. The semi-orthogonal property is a generalization of the orthogonal property of a matrix. We recall (see Definition 2.3.2) the definition of semi-orthogonal matrices here for the convenience of the reader.

Definition 3.1.1. *A non-singular matrix M is **semi-orthogonal** if there exist non-singular diagonal matrices D_1 and D_2 such that $M^{-T} = D_1 M D_2$, where M^{-T} denotes the transpose of the matrix M^{-1}.*

If the matrix M of Definition 3.1.1 is symmetric, then the inverse matrix is of the form $M^{-1} = D_1 M D_2$. Matrices with this characterization are termed semi-involutory

matrices. This concept was introduced by Cheon *et al.* in 2021 as a generalization of involutory property. We recall (see Definition 2.3.4) the definition here.

Definition 3.1.2. *A non-singular matrix M is said to be **semi-involutory** if there exist non-singular diagonal matrices D_1 and D_2 such that $M^{-1} = D_1 M D_2$.*

Significantly, in both of these generalizations, the authors aimed to construct matrices with computationally simple inverses. Leveraging these properties, we proceed to construct MDS matrices with a 'nice inverse' over finite fields. We initiate this process by constructing MDS matrices of small orders.

3.2 Semi-involutory and semi-orthogonal MDS matrices of small orders

In this section, our initial focus is to construct 2×2 MDS matrices with semi-involutory and semi-orthogonal properties. Subsequently, we do the same for 3×3 matrices and prove that some well-known constructions of MDS matrices exhibit either semi-involutory or semi-orthogonal characteristics. We begin with matrices of order 2×2. Utilizing the result of Cheon *et al.* noted in Theorem 2.3.5, we establish the criteria for a 2×2 semi-involutory matrix to be MDS.

Theorem 3.2.1. *Let $A = (a_{ij}), 1 \leq i, j \leq 2$ be a 2×2 semi-involutory matrix over a finite field. Then A is MDS if and only if $a_{ij} \neq 0$ for all $1 \leq i, j \leq 2$.*

Proof. Since A is a semi-involutory matrix, A^{-1} exists. Hence $\det(A)$ is a non-zero element and the zero non-zero pattern of A is permutation similar to either $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. For A being MDS, all entries must be non-zero. Therefore, only the first pattern is possible. Hence it is required that $a_{ij} \neq 0$ for all the entries of A.
Conversely, assume that $a_{ij} \neq 0$ for all $1 \leq i, j \leq 2$. Since A is a 2×2 matrix, for being MDS, it is enough to show that A is invertible and that is obvious from the fact that A is semi-involutory. □

Remark 3.2.2. *For a 2×2 semi-involutory MDS matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, it is possible to construct diagonal matrices D_1 and D_2 such that $A^{-1} = D_1 A D_2$. Let $\det A = \triangle$ and consider $D_1 = \begin{bmatrix} \frac{1}{\triangle a} & 0 \\ 0 & -\frac{1}{\triangle d} \end{bmatrix}$ and $D_2 = \begin{bmatrix} d & 0 \\ 0 & -a \end{bmatrix}$. Note that D_1 and D_2 need not be unique, since for any non-zero element c of the finite field, $\frac{1}{c} D_1$ and $c D_2$ also works.*

Next, we show an application of Theorem 3.2.1.

Example 3.2.3. *Consider the finite field $\mathbb{F}_{11}$ and $A = \begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix}$. Here $\det(A) = 2$. Using Remark 3.2.2, we get $D_1 = \begin{bmatrix} 4 & 0 \\ 0 & 8 \end{bmatrix}$ and $D_2 = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$. Then $A^{-1} = D_1 A D_2$. Again by considering*

$c = 4$, we can get another set of diagonal matrices, which are $D_1 = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ and $D_2 = \begin{bmatrix} 8 & 0 \\ 0 & 5 \end{bmatrix}$. These D_1, D_2 also satisfy $A^{-1} = D_1 A D_2$. This shows that A is semi-involutory and MDS.

From the equivalent Definition 5 of semi-involutory matrices noted in Section 2.3 , we know that if A is semi-involutory then ADA is a diagonal matrix, for some non-singular diagonal matrix D. This property allows us to state that each 2×2 MDS matrix is semi-involutory.

Proposition 3.2.4. *Let $A = (a_{ij}), 1 \leq i, j \leq 2$ be a 2×2 MDS matrix over a finite field. Then A is semi-involutory.*

Proof. Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ be a 2×2 MDS matrix. Then $\det(A) = a_{11}a_{22} - a_{21}a_{12}$ is unit and entries of A are non-zero. First, consider the case when a_{11} and a_{22} are additive inverse in the field, i.e., $a_{11} + a_{22} = 0$. Then for $D = I_2$, the matrix ADA is diagonal.
In the other case, let d_2 be the additive inverse of a_{22}. If $d_1 = a_{11}^{-1} d_2^2$ then $a_{11} = d_2^2 d_1^{-1}$. Hence $a_{11}d_1 + a_{22}d_2 = d_2^2 - d_2^2 = 0$. For $D = \text{diagonal}(d_1, d_2)$, we can see that ADA is a non-singular diagonal matrix. Hence, A semi-involutory. □

We now turn our attention to semi-orthogonal matrices of order 2×2. Utilizing Theorem 2.3.3 of Fiedler and Hall [65], the next result establishes the conditions for semi-orthogonal matrices to be MDS. The proof of this result follows a similar logic to that of Theorem 3.2.1.

Theorem 3.2.5. *Let $A = (a_{ij}), 1 \leq i, j \leq 2$ be a 2×2 semi-orthogonal matrix over a finite field. Then A is MDS if and only if $a_{ij} \neq 0$ for all $1 \leq i, j \leq 2$.*

Proof. Since A is a semi-orthogonal matrix, A^{-1} exists. Hence $\det(A)$ is a non-zero element and the zero non-zero pattern of A has four or two non-zero entries. For A being MDS, all entries must be non-zero. Therefore, only four non-zero entries are possible. Hence it is required that $a_{ij} \neq 0$ for all the entries of A.
Conversely, assume that $a_{ij} \neq 0$ for all $1 \leq i, j \leq 2$. Since A is a 2×2 matrix, for being MDS, it is enough to show that A is invertible and that is obvious from the fact that A is semi-orthogonal. □

Using properties of semi-orthogonal matrices, we demonstrate that each 2×2 MDS matrix matrix inherently exhibits a semi-orthogonal structure.

Theorem 3.2.6. *Let $A = (a_{ij}), 1 \leq i, j \leq 2$ be a 2×2 MDS matrix over a finite field. Then A is semi-orthogonal.*

Proof. Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ be a 2×2 MDS matrix. Let $c_1 = a_{11}a_{21}$ and $c_2 = a_{12}a_{22}$. Both c_1, c_2 are non-zero elements of the finite field since $a_{ij} \neq 0$ in A. Then there exists d_1 such that $c_1 + d_1 = 0$. Take $d_2 = c_2^{-1} c_1^2$ and $D =$diagonal(d_1, d_2). Hence $ADA^T =$

$\begin{bmatrix} a_{11}^2 d_1 + a_{12}^2 d_2 & a_{11}a_{21}d_1 + a_{22}a_{12}d_2 \\ a_{11}a_{21}d_1 + a_{22}a_{12}d_2 & a_{21}^2 d_1 + a_{22}^2 d_2 \end{bmatrix}$. Observe that $a_{11}a_{21}d_1 + a_{22}a_{12}d_2 = c_1 d_1 + c_2 d_2 = -c_1^2 + c_2 c_2^{-1} c_1^2 = 0$. This shows that ADA^T is a non-singular diagonal matrix and A is semi-orthogonal. □

Though 2×2 matrices have some nice properties, they have limited application in the diffusion layer of real-life block ciphers. Therefore, we shift our discussion for the case of 3×3 semi-involutory and semi-orthogonal matrices being MDS. Using the characterization of semi-involutory matrices noted in Theorem 2.3.6, we can prove the following statement.

Theorem 3.2.7. *Let $A = (a_{ij}), 1 \leq i, j \leq 3$ be a 3×3 semi-involutory matrix over a finite field. Then A is an MDS matrix if and only if $a_{ij} \neq 0$ for all $1 \leq i, j \leq 3$.*

Proof. Let A be semi-involutory and $a_{ij} \neq 0$ for all $1 \leq i, j \leq 3$. Then $A^{-1} = D_1 A D_2$ where $D_1 = \text{diagonal}(d_1, d_2, d_3)$ and $D_2 = \text{diagonal}(d_1', d_2', d_3')$ are non-singular diagonal matrices. Let $A^{-1} = (b_{ij})$. Then $b_{ij} = (-1)^{i+j} \frac{\det A(j|i)}{\det A}$ and this equals to $d_i a_{ij} d_j'$. Since $d_i, d_j' \neq 0$ and $a_{ij} \neq 0$, we have $\det A(j|i) \neq 0$. For a 3×3 matrix A, this implies determinant of all 2×2 submatrices are non-zero. Hence A is an MDS matrix.
Conversely, let A be an MDS matrix. Then it is obvious that $a_{ij} \neq 0$ for all $1 \leq i, j \leq 3$. □

Example 3.2.8. *Consider the finite field $\mathbb{F}_{2^4}$ constructed by the irreducible polynomial $x^4 + x + 1$. Let α be a primitive element of the field. Consider the matrix*

$$M = \begin{bmatrix} \alpha + 1 & 1 & \alpha^2 \\ \alpha^3 + 1 & \alpha^3 + \alpha + 1 & \alpha \\ \alpha & \alpha & \alpha^3 + \alpha \end{bmatrix}.$$

It is easy to see that

$$M^{-1} = \begin{bmatrix} \alpha^2 & \alpha^3 + \alpha^2 + 1 & 1 \\ \alpha^3 + \alpha^2 + \alpha + 1 & \alpha^2 + \alpha & \alpha^3 + 1 \\ \alpha^3 + 1 & \alpha^3 + 1 & \alpha^3 + \alpha + 1 \end{bmatrix} = DMD,$$

where $D = \begin{bmatrix} \alpha^3 + 1 & 0 & 0 \\ 0 & \alpha^3 + 1 & 0 \\ 0 & 0 & \alpha^3 + 1 \end{bmatrix}$. By Theorem 3.2.7, M is also an MDS matrix.

Next, we prove a similar result of Theorem 2.3.6 for semi-orthogonal matrices.

Theorem 3.2.9. *Let $A = (a_{ij})$ be a semi-orthogonal matrix of order $n \times n$. Then $\det A(j|i) = 0$ if and only if $a_{ji} = 0$.*

Proof. Let A be a semi-orthogonal matrix. Then $A^{-T} = D_1 A D_2$ for some non-singular diagonal matrices $D_1 = \text{diagonal}(d_1, d_2, \ldots, d_n)$ and $D_2 = \text{diagonal}(d_1', d_2', \ldots, d_n')$. Let $A^{-1} = (b_{ij})$. Then $b_{ij} = \frac{(-1)^{i+j} \det A(j|i)}{\det A}$ and this is equal to the (i, j)-th entry of $D_2 A^T D_1$.

Hence $\frac{(-1)^{i+j}\det A(j|i)}{\det A} = d'_i a_{ji} d_j$. This implies that $\det A(j|i) = 0$ if and only if $a_{ji} = 0$ since $d'_i, d_j \neq 0$. □

Using Theorem 3.2.9, we state a result for 3×3 semi-orthogonal matrices.

Theorem 3.2.10. *Let $A = (a_{ij}), 1 \leq i, j \leq 3$ be a 3×3 semi-orthogonal matrix over a finite field. Then A is an MDS matrix if and only if $a_{ij} \neq 0$ for all $1 \leq i, j \leq 3$.*

Proof. A is semi-orthogonal and $a_{ij} \neq 0$ for all $1 \leq i, j \leq 3$. Then $A^{-T} = D_1 A D_2$, where $D_1 = \text{diagonal}(d_1, d_2, d_3)$ and $D_2 = \text{diagonal}(d'_1, d'_2, d'_3)$ are non-singular diagonal matrices. Let $A^{-1} = (b_{ij})$, then $A^{-T} = (b_{ji})$. Then $b_{ji} = (-1)^{i+j}\frac{\det A(j|i)}{\det A}$, and this equals to $d_i a_{ij} d'_j$. Since $d_i, d'_j \neq 0$ and $a_{ji} \neq 0$, we have $\det A(j|i) \neq 0$. For a 3×3 matrix A, this implies determinant of all 2×2 submatrices are non-zero. Hence A is an MDS matrix. Conversely, let A be an MDS matrix. Then it is obvious that $a_{ij} \neq 0$ for all $1 \leq i, j \leq 3$. □

In the next section, we discuss some MDS matrix constructions which satisfy semi-involutory and semi-orthogonal properties.

3.3 Cauchy matrices with semi-involutory and semi-orthogonal properties

Macwillams and Solane [16] first observed that Cauchy matrices with entries over a finite field offered a very interesting property that directly allows us to construct MDS matrices as discussed in Theorem 1.2.3. Their construction is called Cauchy based construction of Type-I. Based upon this technique, Gupta and Ray [20] introduced three more direct constructions of MDS matrices from Cauchy matrices over a finite field of characteristic 2.

Constructon II: Let $\{x_1, x_2, \ldots, x_n\}$ are elements from the finite field $\mathbb{F}_{2^m}$ and $y_i = l + x_i, 1 \leq i \leq n$ for some arbitrary non-zero element $l \in \mathbb{F}_{2^m}$. Then the Cauchy matrix $C = \left(\frac{1}{x_i + y_j}\right), 1 \leq i, j \leq n$ is an MDS matrix.

Construction III: Let $G = \{x_1, x_2, \ldots, x_n\}$ be an additive subgroup of the finite field $\mathbb{F}_{2^m}$. Consider the set $l + G = \{l + x_j = y_j, 1 \leq j \leq n\}, l \notin G$. Then the Cauchy matrix $C = \left(\frac{1}{x_i + y_j}\right), 1 \leq i, j \leq n$ is an MDS matrix.

Construction IV: Let $G = \{x_1, x_2, \ldots, x_{2^n-1}\}$ be an additive subgroup of the finite field $\mathbb{F}_{2^m}$ constructed by the linear combination of n linearly independent elements label as $x_1, x_2, x_{2^2}, \ldots, x_{2^{n-1}}$. Let $y_i = l + x_i, 1 \leq i \leq 2^n - 1, l \notin G$. Then the Cauchy matrix $C = \left(\frac{1}{x_i + y_j}\right), 1 \leq i, j \leq 2^n - 1$ is a Hadamard MDS matrix.

For a detailed proof of these statements, please refer to [20]. Note that, in Construction III, the matrix C satisfies $C^2 = a^2 I$, where $a = \sum_{k=1}^{n} \frac{1}{l + x_k}$. In Construction IV, although the matrix C may not inherently exhibit involutory properties, the matrix $\frac{1}{a}C$ is a Hadamard involutory matrix, where a is the sum of any row of C. Hence none of these constructions directly exhibit involutory property but they do become involutory MDS matrices under specific conditions.

Another noteworthy constraint of these constructions relates to the size of the matrices. The matrices produced through Constructions III and IV always have an order that is a power of 2. Consequently, when aiming to construct an MDS Cauchy matrix of some arbitrary order n, the initial step involves constructing an MDS Cauchy matrix of order 2^β where $2^\beta \geq n$. Subsequently, a submatrix of size $n \times n$ is extracted from this larger matrix. However, the resulting submatrix does not guarantee the preservation of involutory or orthogonal properties.

Fiedler *et al.* [64, 78] established the semi-orthogonality of Cauchy matrices and formulated diagonal matrices D_1 and D_2 such that $A^{-T} = D_1 A D_2$. The construction is outlined as follows:

Consider a Cauchy matrix $A = \left(\frac{1}{x_i+y_j}\right), 1 \leq i,j \leq n$, and let $A^{-1} = (\gamma_{ij})$ where γ_{ij} adheres to the form detailed in Equation 2.1. Then A^{-1} can be written as $\gamma_{ij} = \frac{1}{x_j+y_i} U_j V_i$, where

$$U_j = (x_j + y_j) \prod_{k \neq j} \frac{x_j + y_k}{x_j - x_k} \tag{3.1}$$

and

$$V_i = (x_i + y_i) \prod_{k \neq i} \frac{y_i + x_k}{y_i - y_k}. \tag{3.2}$$

Considering $D_1 = \text{diagonal}(U_1, \ldots, U_n)$ and $D_2 = \text{diagonal}(V_1, \ldots, V_n)$, we get $A^{-T} = D_1 A D_2$. Using this construction we can state the following result.

Lemma 3.3.1. *Type-I MDS Cauchy matrices are semi-orthogonal.*

In [17], an example of a MDS Cauchy matrix is provided, and notably, it does not exhibit involutory property. Employing Lemma 3.3.1, we demonstrate that this particular matrix possesses a semi-orthogonal nature.

Example 3.3.2. *Consider the finite field $\mathbb{F}_{2^4}$ with constructing polynomial $x^4 + x + 1$ and primitive element α. Let $\{x_0 = 0, x_1 = \alpha^4, x_2 = \alpha^8\}$ and $\{y_0 = 1, y_1 = \alpha^3, y_2 = \alpha^5\}$. Then the Cauchy matrix*

$$A = \begin{bmatrix} 1 & \frac{1}{\alpha^3} & \frac{1}{\alpha^5} \\ \frac{1}{\alpha^4+1} & \frac{1}{\alpha^4+\alpha^3} & \frac{1}{\alpha^4+\alpha^5} \\ \frac{1}{\alpha^8+1} & \frac{1}{\alpha^8+\alpha^3} & \frac{1}{\alpha^8+\alpha^3} \end{bmatrix} = \begin{bmatrix} 1 & \alpha^3+\alpha^2+\alpha+1 & \alpha^2+\alpha+1 \\ \alpha^3+1 & \alpha^2+1 & \alpha^3+\alpha+1 \\ \alpha^3+\alpha^2+1 & \alpha^2 & \alpha^3+\alpha^2+\alpha \end{bmatrix}.$$

Calculating $U_1, U_2, U_3, V_1, V_2, V_3$ using formula 3.1 and 3.2, we can write

$$D_1 = \begin{bmatrix} \alpha^3+\alpha^2+\alpha & 0 & 0 \\ 0 & \alpha^3+\alpha+1 & 0 \\ 0 & 0 & \alpha^3+\alpha^2 \end{bmatrix} \text{ and } D_2 = \begin{bmatrix} \alpha^3+\alpha & 0 & 0 \\ 0 & \alpha^3+\alpha^2+1 & 0 \\ 0 & 0 & \alpha^3+\alpha^2+\alpha \end{bmatrix}.$$

Since A is semi-orthogonal, $A^{-T} = D_1 A D_2$. This implies A^{-1} should be equal to $D_2 A^T D_1$. We

can verify that this is indeed so for the given matrices, with

$$A^{-1} = \begin{bmatrix} \alpha^2+\alpha & 1 & \alpha^3+\alpha^2+1 \\ \alpha^3+\alpha^2 & \alpha^3+\alpha^2+1 & \alpha^3+\alpha^2 \\ \alpha^2 & \alpha^2+\alpha+1 & \alpha^3+\alpha^2+1 \end{bmatrix}.$$

If a matrix A is symmetric and semi-orthogonal then it is semi-involutory. Since Type-II MDS Cauchy matrices are symmetric, hence by Lemma 3.3.1, they are semi-involutory. We note this result as the following lemma.

Lemma 3.3.3. *Let A be symmetric Cauchy matrix. Then A is semi-involutory.*

In Example 2 of [17], an MDS Cauchy matrix of type-II is given. We show that it is semi-involutory.

Example 3.3.4. *Consider the finite field $\mathbb{F}_{2^4}$ with constructing polynomial x^4+x+1 and primitive element α. Let $\{x_0 = \alpha, x_1 = \alpha^2, x_2 = \alpha^3\}$ and $y_i = l + x_i, 1 \leq i \leq 3$ where $l = 1$. Then Cauchy matrix*

$$A = \begin{bmatrix} 1 & \frac{1}{1+\alpha+\alpha^2} & \frac{1}{1+\alpha+\alpha^3} \\ \frac{1}{1+\alpha+\alpha^2} & 1 & \frac{1}{1+\alpha^2+\alpha^3} \\ \frac{1}{1+\alpha+\alpha^3} & \frac{1}{1+\alpha^2+\alpha^3} & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha^2+\alpha & \alpha^2+1 \\ \alpha^2+\alpha & 1 & \alpha^2 \\ \alpha^2+1 & \alpha^2 & 1 \end{bmatrix}.$$

Hence, by Lemma 3.3.3, we can say

$$A^{-1} = D_2 A D_1 = \begin{bmatrix} \alpha^3+\alpha^2 & \alpha^2+\alpha & \alpha \\ \alpha^2+\alpha & \alpha^3+\alpha & \alpha+1 \\ \alpha & \alpha+1 & \alpha^2+\alpha+1 \end{bmatrix} \text{ where}$$

$$D_1 = \begin{bmatrix} \alpha^3 & 0 & 0 \\ 0 & \alpha^3+\alpha^2+\alpha+1 & 0 \\ 0 & 0 & \alpha^2+\alpha \end{bmatrix} \text{ and } D_2 = \begin{bmatrix} \alpha^3 & 0 & 0 \\ 0 & \alpha^3+\alpha^2+\alpha+1 & 0 \\ 0 & 0 & \alpha^2+\alpha \end{bmatrix}.$$

In the Construction-III by Gupta and Ray [20], the Cauchy matrix $C = \left(\frac{1}{x_i+y_j}\right)$ satisfies $C^2 = a^2 I$, where $a = \sum_{k=0}^{n} \frac{1}{r+x_k}$ over the finite field of characteristic 2. However, in the case of a finite field with characteristic $p > 2$, we have the following analogues result.

Lemma 3.3.5. *Let $G = (x_0, x_1, \ldots, x_{d-1})$ be an additive subgroup of $\mathbb{F}_{p^n}, p > 2$. Let us consider the coset $r+G, r \notin G$ of G having elements $y_j = r + x_j, j = 0, \ldots, d-1$. Then the $d \times d$ matrix $A = (a_{ij})$, where $a_{ij} = \frac{1}{x_i+y_j} = \frac{1}{r+x_i+x_j}$, for all $0 \leq i, j \leq d-1$ is a symmetric MDS matrix. Also $A^2 = \beta I$ where $\beta = \sum_{k=0}^{d-1} \frac{1}{(r+x_k)^2}$.*

Proof. The symmetry of A is clear from the fact that $a_{ij} = \frac{1}{x_i+y_j} = \frac{1}{r+x_i+x_j} = a_{ji}$. Since $x_i + y_j = r + x_i + x_j \in r + G$, it is non-zero for all $0 \leq i, j \leq d-1$. Thus

from Theorem 1.2.3. , A is an MDS matrix. Let $A^2 = (h_{ij})$. Then the diagonal entries of A^2 are $h_{ii} = \sum_{k=0}^{d-1} \frac{1}{(r+x_i+x_k)^2} = \sum_{k=0}^{d-1} \frac{1}{(r+x_k)^2} = \beta$. The non diagonal entries are $h_{ij} = \sum_{k=0}^{d-1} \frac{1}{r+x_i+x_k} \cdot \frac{1}{r+x_j+x_k} = \sum_{k=0}^{d-1} \frac{1}{x_j-x_i}\left(\frac{1}{r+x_i+x_k} - \frac{1}{r+x_j+x_k}\right) = \frac{1}{x_j-x_i}\sum_{k=0}^{d-1}\left(\frac{1}{r+x_i+x_k} - \frac{1}{r+x_j+x_k}\right) = \frac{1}{x_j-x_i}\left(\sum_{l=0}^{d-1}\frac{1}{r+x_l} - \sum_{l'=0}^{d-1}\frac{1}{r+x_{l'}}\right) = 0,$ since the set $\{r+x_l, 0 \le l \le d-1\} = \{r+x_{l'}, 0 \le l' \le d-1\}$. This implies that $A^2 = \beta I$. □

It is important to highlight that the choice of a field with characteristic 2 in [20] guarantees that the value of a derived from Construction-III is invariably a square element. However, it is not always possible for fields of characteristic $p > 2$, since there exist non-square elements (see [79]). Subsequently, we introduce an alternative approach in Theorem 3.3.7 over a finite field of characteristic p for constructing MDS matrices with 'nice inverse', leveraging the semi-involutory property of symmetric Cauchy matrices. To facilitate this, we first establish the following result over a finite field.

Proposition 3.3.6. *Let $\mathbb{F}$ be a finite field of cardinality p^n and K be a subfield of cardinality p^m where $m|n$. Let $K = \{x_0 = 0, x_1, x_2, \ldots, x_{p^m-1}\}$. Then all the elementary symmetric polynomials in terms of $\{x_1, x_2, \ldots, x_{p^m-1}\}$ are zero.*

Proof. Let K^* denote the group of non-zero elements of field K under multiplication. Then all the elements of K^* satisfy the equation $x^{p^m-1} = 1$. Therefore K^* is the set of all roots of the polynomial $x^{p^m-1} - 1$. Hence, all non-zero elements of K are roots of the polynomial $x^{p^m-1} - 1$. Since it is a monic polynomial of degree $p^m - 1$, we can write the sum of all its roots as the the coefficient of x^{p^m-2} which is 0. Similarly the sum of product of any two roots will be the coefficient of x^{p^m-3} and is also 0. Continuing this process we find that the sum of product of any $p^m - 2$ roots is the coefficient of x and is also 0. This implies $\sum_{i=1}^{p^m-1} x_i = 0, \sum_{1\le i<j\le p^m-1} x_i x_j = 0, \ldots, \sum_{i=1}^{p^m-1} \prod_{j=1,\, i\neq j}^{p^m-1} x_j = 0.$ □

Now, we are ready to give the proof of Theorem 1.4.3.

Theorem 3.3.7. *Let $G = \{x_0, x_1, \ldots, x_{d-1}\}$ be a proper subfield of the finite field $\mathbb{F}_{p^n}$ and let $r \notin G$. Consider the coset $r + G = \{y_0, y_1, \ldots, y_{d-1}\}$. Then $A = \left(\frac{1}{x_i+y_j}\right), 1 \le i, j \le d-1$ is an MDS Cauchy matrix. Further, there exist diagonal matrices $D_1 = \frac{1}{c^2}I$ and $D_2 = I$ such that $A^{-1} = D_1 A D_2$, where $c = \sum_{k=0}^{d-1} \frac{1}{r+x_k}$.*

Proof. Let $G = \{x_0 = 0, x_1, x_2, x_3, \ldots, x_{d-1}\}$ be a subfield of $\mathbb{F}_{p^n}$ and the coset $r + G = \{r+x_0, r+x_1, r+x_2, r+x_3, \ldots, r+x_{d-1}\} = \{y_0, y_1, y_2, y_3, \ldots, y_{d-1}\}$. Then $x_i + y_j = r + x_i + x_j = r + x_l \in r + G$ for some l, since G is closed under addition. Therefore $x_i + y_j$ is non-zero because $0 \notin r + G$. This implies the elements y_j's are all distinct since x_j's are distinct. Hence, by Theorem 1.2.3 , A is an MDS Cauchy matrix.

By the construction above, A is a symmetric MDS matrix. From Equation 2.1, 3.1 and 3.2 A^{-1} can be written as $A^{-1} = (\gamma_{ij}) = \left(\frac{1}{x_j+y_i}U_jV_i\right), 1 \leq i,j \leq d-1$, where $U_j = (x_j+y_j)\prod_{k\neq j}\frac{x_j+y_k}{x_j-x_k}$, $V_i = (x_i+y_i)\prod_{k\neq i}\frac{y_i+x_k}{y_i-y_k}$. Hence $A^{-1} = (U_j a_{ji} V_i) = (U_j a_{ij} V_i)$. Therefore it is enough to show that $U_jV_i = \frac{1}{c^2}$ for all $1 \leq i,j \leq d-1$.

We consider two cases, when $i = j$ or $i \neq j$.

Case 1. *When $i = j$*

$$\begin{aligned}
U_iV_i &= (x_i+y_i)\prod_{k\neq i}(\frac{x_i+y_k}{x_i-x_k})(x_i+y_i)\prod_{k\neq i}(\frac{y_i+x_k}{y_i-y_k}) \\
&= (r+x_i+x_i)\prod_{k\neq i}(\frac{r+x_i+x_k}{x_i-x_k})(r+x_i+x_i)\prod_{k\neq i}(\frac{r+x_i+x_k}{x_i-x_k}) \\
&= \frac{(r+x_i+x_0)^2(r+x_i+x_1)^2\cdots(r+x_i+x_i)^2\cdots(r+x_i+x_{d-1})^2}{\prod_{k\neq i}(x_i-x_k)^2}.
\end{aligned}$$

Case 2. *When $i \neq j$*

$$\begin{aligned}
U_jV_i &= (x_j+y_j)\prod_{k\neq j}(\frac{x_j+y_k}{x_j-x_k})(x_i+y_i)\prod_{k\neq i}(\frac{y_i+x_k}{y_i-y_k}) \\
&= (r+x_j+x_j)\prod_{k\neq j}(\frac{r+x_j+x_k}{x_j-x_k})(r+x_i+x_i)\prod_{k\neq i}(\frac{r+x_i+x_k}{x_i-x_k}) \\
&= \frac{(r+x_j+x_0)\cdots(r+x_j+x_j)\cdots(r+x_j+x_{d-1})}{\prod_{k\neq j}(x_j-x_k)} \\
&\quad\times\frac{(r+x_i+x_0)\cdots(r+x_i+x_i)\cdots(r+x_i+x_{d-1})}{\prod_{k\neq i}(x_i-x_k)} \\
&= \frac{(r+x_i+x_0)^2(r+x_i+x_2)^2\cdots(r+x_i+x_i)^2\cdots(r+x_i+x_{d-1})^2}{\prod_{k\neq j}(x_j-x_k)\prod_{k\neq i}(x_i-x_k)}.
\end{aligned}$$

Since G is a subfield, it is closed under addition. Hence, for a fixed i, $\{x_i+x_j, 0 \leq j \leq d-1\} = \{x_0, x_1, \ldots, x_{d-1}\}$. Thus $\{(r+x_i+x_0), \ldots, (r+x_i+x_i), \ldots, (r+x_i+x_{d-1})\} = \{(r+x_j+x_0), \ldots, (r+x_j+x_j)\ldots, (r+x_j+x_{d-1})\}$.

Further, for a fixed i,

$$\prod_{k\neq i}(x_i-x_k)^2 = (x_i-x_0)^2\cdots(x_i-x_{i-1})^2(x_i-x_{i+1})^2\cdots(x_i-x_{d-1})^2 \quad = x_1^2x_2^2x_3^2\cdots x_{d-1}^2.$$

The previous statement is true since for any two distinct elements $x_k, x_l \in G$, $(x_i-x_k) \neq (x_i-x_l)$. Hence, the set $\{(x_i-x_0), (x_i-x_1), \ldots, (x_i-x_{i-1}), (x_i-x_{i+1}), \ldots, (x_i-x_{d-1})\} = \{x_1, x_2, x_3, \ldots, x_{d-1}\}$.

Similarly,

$$\prod_{k\neq j}(x_j - x_k)\prod_{k\neq i}(x_i - x_k) = (x_j - x_0)\cdots(x_j - x_{j-1})(x_j - x_{j+1})\cdots(x_j - x_{d-1})(x_i - x_0)$$
$$\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_{d-1})$$
$$= x_1^2x_2^2x_3^2\cdots x_{d-1}^2.$$

Hence, for all $0 \leq i, j \leq d-1$, $U_jV_i = \frac{(r+x_0)^2(r+x_1)^2(r+x_2)^2\cdots(r+x_{d-1})^2}{x_1^2x_2^2x_3^2\cdots x_{d-1}^2}$.
Further, $c = \frac{1}{r+x_0} + \frac{1}{r+x_1} + \frac{1}{r+x_2} + \cdots + \frac{1}{r+x_{d-1}} = \frac{1}{y_0} + \frac{1}{y_1} + \frac{1}{y_2} + \cdots + \frac{1}{y_{d-1}}$ and this implies

$$\frac{1}{c^2} = \frac{(y_0y_1y_2\cdots y_{d-1})^2}{(\prod_{i\neq 0} y_i + \prod_{i\neq 1} y_i + \cdots + \prod_{i\neq(d-1)} y_i)^2}.$$

The numerator of $\frac{1}{c^2}$ is $(y_0y_1y_2\cdots y_{d-1})^2 = (r+x_0)^2(r+x_1)^2(r+x_2)^2\cdots(r+x_{d-1})^2$, which is the same as the numerator of U_jV_i for all $0 \leq i, j \leq d-1$. On the other hand, the denominator of $\frac{1}{c^2}$ is $(\prod_{i\neq 0} y_i + \prod_{i\neq 1} y_i + \cdots + \prod_{i\neq(d-1)} y_i)^2$ which we calculate next.
Notice that $\prod_{i\neq 0} y_i = y_1y_2y_3\cdots y_{d-1}$ which can be simplified as follows.

$$\prod_{i\neq 0} y_i = (r+x_1)(r+x_2)(r+x_3)\cdots(r+x_{d-1})$$
$$= r^{d-1} + r^{d-2}(\sum_{i=1}^{d-1} x_i) + r^{d-3}(\sum_{i,j=1,i\neq j}^{d-1} x_ix_j) + \cdots + r(x_1x_2\cdots x_{d-2} + x_2x_3\cdots x_{d-1})$$
$$+ x_1x_2x_3\cdots x_{d-1}.$$

Hence, $\prod_{i\neq 0} y_i + \prod_{i\neq 1} y_i + \cdots + \prod_{i\neq(d-1)} y_i$ can be simplified as follows.

$$\prod_{i\neq 0} y_i + \prod_{i\neq 1} y_i + \cdots + \prod_{i\neq(d-1)} y_i$$
$$= \{r^{d-1} + r^{d-2}(\sum_{i=1}^{d-1} x_i) + r^{d-3}(\sum_{i,j=1,i\neq j}^{d-1} x_ix_j) + \cdots + r(x_1x_2\cdots x_{d-2} + x_2x_3\cdots x_{d-1}) +$$
$$x_1x_2x_3\cdots x_{d-1}\} + \{r^{d-1} + r^{d-2}(\sum_{i=0,i\neq 1}^{d-1} x_i) + r^{d-3}(\sum_{i,j=0,i,j\neq 1,i<j}^{d-1} x_ix_j) + \cdots$$
$$+ r(x_0x_2\cdots x_{d-2} + x_2x_3\cdots x_{d-1}) + x_0x_2x_3\cdots x_{d-1}\} + \cdots + \{r^{d-1} + r^{d-2}(\sum_{i=0}^{d-2} x_i)$$
$$+ r^{d-3}(\sum_{i,j=0,i\neq j,i<j}^{d-2} x_ix_j) + \cdots + r(x_0x_1\cdots x_{d-3} + x_1x_2\cdots x_{d-2}) + x_0x_1x_2x_3\cdots x_{d-2}\}$$

In the above expression, the coefficient of r^{d-1} is d and hence 0. Next, in the coefficient

of r^{d-2}, we can see that each x_i will appear exactly $d-1$ time. Therefore, the coefficient of r^{d-2} is $(d-1)(x_0+x_1+\cdots+x_{d-1})=0$ by Proposition 3.3.6. In the coefficient of r^{d-3}, each x_ix_j will appear $d-2$ times and hence the coefficient is $(d-2)(\sum_{i,j=0,i<j}^{d-1} x_ix_j)=0$ by Proposition 3.3.6. Continuing this process and using Proposition 3.3.6, the coefficient of r is $2(x_0x_1\cdots x_{d-3}+\cdots+x_2x_3\cdots x_{d-1})=0$. Finally, the constant term is $x_1x_2x_3\cdots x_{d-1}+x_0x_2x_3\cdots x_{d-1}+\cdots+x_0x_1x_2x_3\cdots x_{d-2}=x_1x_2x_3\cdots x_{d-1}$ since $x_0=0$.
This implies that $(\prod_{i\neq 0} y_i+\prod_{i\neq 1} y_i+\cdots+\prod_{i\neq(d-1)} y_i)^2=(x_1x_2\cdots x_{d-1})^2$. Therefore, the denominator of $\frac{1}{c^2}$ is $x_1^2x_2^2\cdots x_{d-1}^2$.
Hence, $\frac{1}{c^2}=\frac{(r+x_0)^2(r+x_1)^2(r+x_2)^2\cdots(r+x_{d-1})^2}{x_1^2x_2^2\cdots x_{d-1}^2}=U_jV_i$. This completes the proof. □

The construction of any $n\times n$ MDS matrix from the submatrices of a Cauchy matrix of Type-III over $\mathbb{F}_{2^m}$ was given in Remark 5 of [17]. By using Theorem 3.3.7, it is possible to construct a semi-involutory MDS Cauchy matrix of any prime power order by choosing a proper finite field and its subfield. It is also possible to construct an MDS Cauchy matrix from the submatrices of previous construction over any finite field. These submatrices are also Cauchy matrix. Therefore from Lemma 3.3.1, they are semi-orthogonal. Notably, if the submatrix is also symmetric, it becomes semi-involutory. For illustration, we provide an example of a semi-involutory MDS Cauchy matrix of order 5×5.

Example 3.3.8. *Consider the finite field $\mathbb{F}_{5^2}$ with generating polynomial x^2+4x+2. Let α be the primitive element. Consider the subfield $G=\{0,1,2,3,4\}$ and $r=2\alpha+1$. Then the Cauchy matrix*

$$M=\begin{bmatrix} \frac{1}{2\alpha+1} & \frac{1}{2\alpha+2} & \frac{1}{2\alpha+3} & \frac{1}{2\alpha+4} & \frac{1}{2\alpha} \\ \frac{1}{2\alpha+2} & \frac{1}{2\alpha+3} & \frac{1}{2\alpha+4} & \frac{1}{2\alpha} & \frac{1}{2\alpha+1} \\ \frac{1}{2\alpha+3} & \frac{1}{2\alpha+4} & \frac{1}{2\alpha} & \frac{1}{2\alpha+1} & \frac{1}{2\alpha+2} \\ \frac{1}{2\alpha+4} & \frac{1}{2\alpha} & \frac{1}{2\alpha+1} & \frac{1}{2\alpha+2} & \frac{1}{2\alpha+3} \\ \frac{1}{2\alpha} & \frac{1}{2\alpha+1} & \frac{1}{2\alpha+2} & \frac{1}{2\alpha+3} & \frac{1}{2\alpha+4} \end{bmatrix}=\begin{bmatrix} 3\alpha+3 & 3\alpha+4 & \alpha & 4\alpha+3 & \alpha+4 \\ 3\alpha+4 & \alpha & 4\alpha+3 & \alpha+4 & 3\alpha+3 \\ \alpha & 4\alpha+3 & \alpha+4 & 3\alpha+3 & 3\alpha+4 \\ 4\alpha+3 & \alpha+4 & 3\alpha+3 & 3\alpha+4 & \alpha \\ \alpha+4 & 3\alpha+3 & 3\alpha+4 & \alpha & 4\alpha+3 \end{bmatrix}.$$

Now $c=(3\alpha+3)+(3\alpha+4)+\alpha+(4\alpha+3)+(\alpha+4)=2\alpha+4$ and $\frac{1}{c^2}=2$. Hence $D_1=2I$ and $M^{-1}=D_1\cdot M=\begin{bmatrix} \alpha+1 & \alpha+3 & 2\alpha & 3\alpha+1 & 2\alpha+3 \\ \alpha+3 & 2\alpha & 3\alpha+1 & 2\alpha+3 & \alpha+1 \\ 2\alpha & 3\alpha+1 & 2\alpha+3 & \alpha+1 & \alpha+3 \\ 3\alpha+1 & 2\alpha+3 & \alpha+1 & \alpha+3 & 2\alpha \\ 2\alpha+3 & \alpha+1 & \alpha+3 & 2\alpha & 3\alpha+1 \end{bmatrix}$.

In Algorithm 1 of [20], another construction of Cauchy based MDS matrix was provided which is a Hadamard matrix. In [80], authors proved that Hadamard matrices are also semi-involutory.

In Section 1.2.2 we explained the non-trivial relationships between MDS matrices constructed using the Cauchy based constructions and Vandermonde based constructions. The detailed explanation of this connection is provided in Theorem 5.1 of [17], referenced as Theorem 1.2.16. For ease of reference, we reiterate it here.

Theorem 3.3.9. *Let* $\{x_0, x_1, \ldots, x_{n-1}\}$ *and* $\{y_0, y_1, \ldots, y_{n-1}\}$ *be* $2n$ *distinct elements from* $\mathbb{F}_{2^m}$ *such that* $x_i + y_j \neq 0$ *for all* $0 \leq i, j \leq n-1$. *Consider the matrices* $V_1 = Vand(x_0, x_1, \ldots, x_{n-1}), V_2 = Vand(y_0, y_1, \ldots, y_{n-1})$ *and* $M = (m_{i,j})$, *where* $m_{ij} = \frac{1}{x_i + y_j}$. *Let* $V_1^{-1} = (b_{i,j}), 0 \leq i, j \leq n-1$. *Then* $D_1 M D_2 = V_1^{-1} V_2$, *where* $D_1 = diagonal(b_{0,n-1}, b_{1,n-1}, b_{2,n-1}, \ldots, b_{n-1,n-1})$ *and* $D_2 = diagonal(\prod_{k=0}^{n-1}(x_k + y_0), \prod_{k=0}^{n-1}(x_k + y_1), \ldots, \prod_{k=0}^{n-1}(x_k + y_{n-1}))$.

Proof. For proof see Theorem 5.1 of [17]. □

Now using Theorem 3.3.9 and Lemma 3.3.1 we can say that $V_1^{-1}V_2$ is semi-orthogonal.

Lemma 3.3.10. *Vandermonde based MDS matrices constructed by Theorem 3.3.9 are semi-orthogonal.*

Proof. Let V_1 and V_2 be two Vandermonde matrices as stated in Theorem 3.3.9. Hence, there exist diagonal matrices D_1, D_2 such that $V_1^{-1}V_2 = D_1 M D_2$. Since M is semi-orthogonal, $M^{-1} = D_3 M^T D_4$ for some non-singular diagonal matrices D_3, D_4. Therefore $(V_1^{-1}V_2)^{-1} = D_2^{-1} M^{-1} D_1^{-1} = D_2^{-1} D_3 M^T D_4 D_1^{-1} = D_2^{-1} D_3 D_2^{-1} (V_1^{-1}V_2)^T D_1^{-1} D_4 D_1^{-1} = D'(V_1^{-1}V_2)^T D''$, where D', D'' are non-singular diagonal matrices. Hence, $V_1^{-1}V_2$ is semi-orthogonal. □

3.4 Circulant matrices with semi-involutory and semi-orthogonal properties

Circulant MDS matrices have gained a lot of attention ([25, 30, 31, 34]) because of their application in lightweight cryptography. A comprehensive study of the current findings on circulant orthogonal and involutory matrices is presented in Section 1.2.3. Within this section, our focus shifts to characterizing circulant matrices endowed with both semi-involutory and semi-orthogonal properties, with entries from a finite field. We begin with circulant semi-involutory matrices.

Theorem 3.4.1. *Let* A *be an* $n \times n$ *circulant matrix over a finite field* $\mathbb{F}$. *Then* A *is semi-involutory if and only if there exist non-singular diagonal matrices* D_1, D_2 *such that* $D_1^n = k_1 I$ *and* $D_2^n = k_2 I$ *for non-zero scalars* k_1, k_2 *in the finite field and* $A^{-1} = D_1 A D_2$.

Proof. Let $A = \text{circulant}(a_1, a_2, \ldots, a_n)$ be semi-involutory. By definition there exist non-singular diagonal matrices D_1 and D_2 such that $A^{-1} = D_1 A D_2$. Let $D_1 = \text{diagonal}(d_1, d_2, \ldots, d_n)$ and $D_2 = \text{diagonal}(d_1', d_2', \ldots, d_n')$. Then the matrix A^{-1} is of the form

$$A^{-1} = \begin{bmatrix} d_1 a_1 d_1' & d_1 a_2 d_2' & \cdots & d_1 a_n d_n' \\ d_2 a_n d_1' & d_2 a_1 d_2' & \cdots & d_2 a_{n-1} d_n' \\ \vdots & \vdots & \cdots & \vdots \\ d_n a_2 d_1' & d_n a_3 d_2' & \cdots & d_n a_1 d_n' \end{bmatrix}.$$

Since inverse of a circulant matrix is also circulant, entries of the second row of A^{-1} are the same as the entries of the first row shifted right by one. Therefore,

$$\begin{aligned} d_1 a_1 d_1' &= d_2 a_1 d_2' \\ d_1 a_2 d_2' &= d_2 a_2 d_3' \\ &\vdots \\ d_1 a_n d_n' &= d_2 a_n d_1'. \end{aligned}$$

This implies that $d_1 d_1' = d_2 d_2'$, $d_1 d_2' = d_2 d_3'$, $\ldots$, $d_1 d_n' = d_2 d_1'$. Multiplying all these equalities, we get $d_1^n = d_2^n$. Similarly, entries of the third row are the same as entries of the second row right shifted by one, and that implies $d_2 a_i d_i' = d_3 a_i d_{i+1}'$ for $i = 1, \ldots, n$, and the indices are reduced modulo n, which leads to $d_2^n = d_3^n$. Continuing this process, we get $d_1^n = d_2^n = d_3^n = d_4^n = \cdots = d_n^n$.
Similarly, in a circulant matrix, the second column is nothing but a circular shifted version of the first column. This implies that, $d_1 a_1 d_1' = d_2 a_1 d_2'$, $d_2 a_n d_1' = d_3 a_n d_2'$, $\ldots$, $d_n a_2 d_1' = d_1 a_2 d_2'$ and multiplying these, we get $d_1'^n = d_2'^n$. Applying the same reasoning for the second and the third columns, we get $d_2'^n = d_3'^n$. Continuing similar reasoning, we get $d_1^n = d_2'^n = d_3'^n = \cdots = d_n'^n$.
Conversely, if there exists non-singular diagonal matrices D_1, D_2 such that $D_1^n = k_1 I$ and $D_2^n = k_2 I$ for non-zero scalars k_1, k_2 in the finite field and $A^{-1} = D_1 A D_2$, then by the definition A is semi-involutory. □

Further, if the order of the matrix is some power of the characteristic if the finite field, then we have the following corollary.

Corollary 3.4.2. *Let A be an $n \times n$ circulant, semi-involutory matrix over $\mathbb{F}_{p^m}$ where $n = p^k$ for some k. Then there exists diagonal matrices D_1 and D_2 with $D_1^n = k_1 I$ and $D_2^n = k_2 I$ for some non-zero scalars k_1, k_2 in the finite field with $k_1 k_2 = \frac{1}{\lambda^{2n}}$ where λ is the sum of the entries of the first row, which is an eigenvalue value of A.*

Proof. Let $A = \text{circulant}(c_1, c_2, \ldots, c_n)$ be an $n \times n$ circulant, semi-involutory matrix. Then there exist diagonal matrices $D_1 = \text{diagonal}(d_1, d_2, \ldots, d_n)$ and $D_2 = \text{diagonal}(d_1', d_2', \ldots, d_n')$ such that $A^{-1} = D_1 A D_2$. This implies $A D_1 A = D_2^{-1}$, where $D_1^n = k_1 I$ and $D_2^n = k_2 I$ for some $k_1, k_2 \in \mathbb{F}_{p^m}$ by Theorem 3.4.1. Using the form of matrices A and D_1, we can write the structure of AD_1 as follows.

$$AD_1 = \begin{bmatrix} c_1 d_1 & c_2 d_2 & c_3 d_3 & \cdots & c_n d_n \\ c_n d_1 & c_1 d_2 & c_2 d_3 & \cdots & c_{n-1} d_n \\ c_{n-1} d_1 & c_n d_2 & c_1 d_3 & \cdots & c_{n-2} d_n \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ c_2 d_1 & c_3 d_2 & c_4 d_3 & \cdots & c_1 d_n \end{bmatrix}.$$

Let $\lambda = c_1 + c_2 + \cdots + c_n$ and r_i denote the sum of the entries of the i-th row of AD_1.

Adding the entries in the first row of AD_1A, we get the following:

$$(c_1 + c_2 + \cdots + c_n)(c_1d_1 + c_2d_2 + c_3d_3 + \cdots + c_nd_n) = \lambda r_1.$$

Continuing in the same argument, we get the sum of entries of the i-th row of AD_1A as follows:

$$\lambda r_i = (c_1 + c_2 + \cdots + c_n)(c_1d_i + \cdots + c_nd_{i-1}).$$

From the equality $AD_1A = D_2^{-1}$, we observe that the entries of the diagonal matrix D_2^{-1} satisfy $\frac{1}{d_i'} = \lambda r_i$ for $i = 1, \ldots, n$. Taking the n-th power on both sides of this equality, we get $\frac{1}{d_i'^n} = \lambda^n r_i^n$. Observe that $\lambda^n r_i^n = (c_1 + c_2 + \cdots + c_n)^n(c_1d_i + c_2d_{i+1} + \cdots + c_nd_{i-1})^n = \lambda^n k_1(c_1^n + c_2^n + \cdots + c_n^n) = \lambda^{2n}k_1$. This holds because n is a power of p and our finite field is of characteristic p. The previous equality implies that $k_1k_2 = \frac{1}{\lambda^{2n}}$. Hence the proof is complete. □

A result similar to Theorem 3.4.1 holds for circulant semi-orthogonal matrices which we record here.

Theorem 3.4.3. *A be an $n \times n$ circulant matrix over a finite field $\mathbb{F}$. Then A is semi-orthogonal if and only if there exist non-singular diagonal matrices D_1 and D_2 such that $D_1^n = k_1I$ and $D_2^n = k_2I$ for non-zero scalars $k_1, k_2 \in \mathbb{F}$ and $A^{-T} = D_1AD_2$.*

Proof. Let $A = \text{circulant}(a_1, a_2, \ldots, a_n)$ be semi-orthogonal. By definition there exist non-singular diagonal matrices D_1 and D_2 such that $A^{-T} = D_1AD_2$. Let $D_1 = \text{diagonal}(d_1, d_2, \ldots, d_n)$ and $D_2 = \text{diagonal}(d_1', d_2', \ldots, d_n')$.Then the matrix A^{-T} is of the form

$$A^{-T} = \begin{bmatrix} d_1a_1d_1' & d_1a_2d_2' & \cdots & d_1a_nd_n' \\ d_2a_nd_1' & d_2a_1d_2' & \cdots & d_2a_{n-1}d_n' \\ \vdots & \vdots & \cdots & \vdots \\ d_na_2d_1' & d_na_3d_2' & \cdots & d_na_1d_n' \end{bmatrix}.$$

Since inverse and transpose of a circulant matrix is also circulant, entries of the second row of A^{-T} are the same as the entries of the first row shifted right by one. Therefore,

$$\begin{aligned} d_1a_1d_1' &= d_2a_1d_2' \\ d_1a_2d_2' &= d_2a_2d_3' \\ &\vdots \\ d_1a_nd_n' &= d_2a_nd_1'. \end{aligned}$$

This implies that $d_1d_1' = d_2d_2'$, $d_1d_2' = d_2d_3'$, $\cdots$, $d_1d_n' = d_2d_1'$. Multiplying all these equalities, we get $d_1^n = d_2^n$. Similarly, entries of the third row are the same as entries of the second row right shifted by one, and that implies $d_2a_id_i' = d_3a_id_{i+1}'$ for $i = 1, \ldots, n$, and the indices are reduced modulo n, which leads to $d_2^n = d_3^n$. Continuing this process, we get $d_1^n = d_2^n = d_3^n = d_4^n = \cdots = d_n^n$.

Similarly, in a circulant matrix, the second column is nothing but a circular shifted version of the first column. This implies that, $d_1a_1d'_1 = d_2a_1d'_2$, $d_2a_nd'_1 = d_3a_nd'_2, \ldots, d_na_2d'_1 = d_1a_2d'_2$ and multiplying these, we get $d'^n_1 = d'^n_2$. Applying the same reasoning for the second and the third columns, we get $d'^n_2 = d'^n_3$. Continuing similar reasoning, we get $d^n_1 = d'^n_2 = d'^n_3 = \cdots = d'^n_n$.
Conversely, if there exists non-singular diagonal matrices D_1, D_2 such that $D^n_1 = k_1I$ and $D^n_2 = k_2I$ for non-zero scalars k_1, k_2 in the finite field and $A^{-T} = D_1AD_2$, then by the definition A is semi-involutory. □

An immediate corollary of Theorem 3.4.3 which is analogues to Corollary 3.4.2 is following.

Corollary 3.4.4. *Let A be an $n \times n$ circulant, semi-orthogonal matrix over $\mathbb{F}_{p^m}$ where $n = p^k$ for some k. Then there exists diagonal matrices D_1 and D_2 with $D^n_1 = k_1I$ and $D^n_2 = k_2I$ for some non-zero scalars k_1, k_2 in the finite field with $k_1k_2 = \frac{1}{\lambda^{2n}}$ where λ is the sum of the entries of the first row, which is an eigenvalue value of A.*

Proof. Since $A = \text{circulant}(c_1, c_2, \ldots, c_n)$ is an $n \times n$ circulant, semi-orthogonal matrix. Then there exist diagonal matrices $D_1 = \text{diagonal}(d_1, d_2, \ldots, d_n)$ and $D_2 = \text{diagonal}(d'_1, d'_2, \ldots, d'_n)$ such that $A^{-T} = D_1AD_2$. This implies $AD_1A^T = D_2^{-1}$, where $D^n_1 = k_1I$ and $D^n_2 = k_2I$ for some $k_1, k_2 \in \mathbb{F}_{p^m}$ by Theorem 3.4.1. Using the form of matrices A and D_1, we can write the structure of AD_1 as follows.

$$AD_1 = \begin{bmatrix} c_1d_1 & c_2d_2 & c_3d_3 & \cdots & c_nd_n \\ c_nd_1 & c_1d_2 & c_2d_3 & \cdots & c_{n-1}d_n \\ c_{n-1}d_1 & c_nd_2 & c_1d_3 & \cdots & c_{n-2}d_n \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ c_2d_1 & c_3d_2 & c_4d_3 & \cdots & c_1d_n \end{bmatrix}.$$

Let $\lambda = c_1 + c_2 + \cdots + c_n$, and let r_i denote the sum of the entries of the i-th row of AD_1. Adding the entries in the first row of AD_1A^T, we get the following:

$$(c_1 + c_2 + \cdots + c_n)(c_1d_1 + c_2d_2 + c_3d_3 + \cdots + c_nd_n) = \lambda r_1.$$

Continuing in the same argument, we get the sum of entries of the i-th row of AD_1A^T as follows:

$$\lambda r_i = (c_1 + c_2 + \cdots + c_n)(c_1d_i + \cdots + c_nd_{i-1}).$$

From the equality $AD_1A^T = D_2^{-1}$, we observe that the entries of the diagonal matrix D_2^{-1} satisfy $\frac{1}{d'_i} = \lambda r_i$ for $i = 1, \cdots, n$. Taking the n-th power on both sides of this equality, we get $\frac{1}{d'^n_i} = \lambda^n r^n_i$. Observe that $\lambda^n r^n_i = (c_1 + c_2 + \cdots + c_n)^n(c_1d_i + c_2d_{i+1} + \cdots + c_nd_{i-1})^n = \lambda^n k_1(c^n_1 + c^n_2 + \cdots + c^n_n) = \lambda^{2n}k_1$. This holds because n is a power of p and our finite field is of characteristic p. The previous equality implies that $k_1k_2 = \frac{1}{\lambda^{2n}}$. Hence the proof is complete. □

An example of circulant semi-orthogonal matrix is the following.

Example 3.4.5. *Consider the finite field $\mathbb{F}_{2^4}$ with generating polynomial $x^4 + x + 1$ and α be a primitive element. Let $C = circulant(\alpha^3, \alpha^2, \alpha^3 + 1)$. Then $C^{-T} = CD$ where $D = diagonal(\alpha^3 + 1, \alpha^3 + 1, \alpha^3 + 1)$ and C^{-T}= circulant$(\alpha^2, \alpha, \alpha^3 + \alpha^2 + 1)$. Note that, C is an MDS matrix.*

In Chapter 1, as outlined in Theorem 1.2.29, Gupta and Ray [30] proved that circulant orthogonal matrices of order $2^d \times 2^d$ cannot be MDS. We prove a similar result for a subclass of circulant semi-orthogonal matrix. This subclass is named *sesqui-semi-orthogonal* matrices. It contains the semi-orthogonal matrices A such that $A^{-T} = D_1 A D_2$ with either D_1 or D_2 being an identity matrix. For this class of matrices, we prove the non-existence of MDS property using the general expression for the determinant of a circulant matrix. This result can be found in [68] and discussed in Chapter 2, Section 2.2, Equation 2.3.

Theorem 3.4.6. *Let p be a prime, and A be a $2p \times 2p$ circulant sesqui-semi-orthogonal matrix over the field $\mathbb{F}_{p^n}$. Then A is not an MDS matrix.*

Proof. Let $A = \text{circulant}(c_0, c_1, \ldots, c_{2p-1})$ be a $2p \times 2p$ circulant semi-orthogonal matrix over $\mathbb{F}_{p^n}$. Without loss of generality, assume that $D_2 = I$. Then $AA^T = D$ for some non-singular diagonal matrix D.
Since non-diagonal entries of AA^T are zero, we get the following $2p - 1$ equations from the first row of AA^T.

$$\left.\begin{aligned} \sum_{i=0}^{2p-1} c_i c_{i+1} &= 0, \\ \sum_{i=0}^{2p-1} c_i c_{i+2} &= 0, \\ \sum_{i=0}^{2p-1} c_i c_{i+3} &= 0, \\ &\vdots \\ \sum_{i=0}^{2p-1} c_i c_{i+2p-1} &= 0, \end{aligned}\right\} \tag{3.3}$$

where suffixes of c_i's are taken modulo $2p$. Adding alternate equations from (3.3) starting with the first one, we get $(c_0 + c_2 + \cdots + c_{2p-2})(c_1 + c_3 + \cdots + c_{2p-1}) = 0$. Then either $(c_0 + c_2 + \cdots + c_{2p-2}) = 0$ or $(c_1 + c_3 + \cdots + c_{2p-1}) = 0$. Without loss of generality, assume that $(c_0 + c_2 + \cdots + c_{2p-2}) = 0$.
Consider the $p \times p$ circulant sub-matrix formed by the odd numbered rows and odd numbered columns of A. Let $B = \text{circulant}(c_0, c_2, \ldots, c_{2p-2})$ and $\det B = \triangle$. Let $Q_{p\times p} = \text{circulant}(0, 1, 0, \ldots, 0)$ and $Q^p = I$. The matrix B can be written as $B = c_0 I + c_2 Q + c_4 Q^2 + \cdots + c_{2p-2} Q^{p-1}$. Hence $\triangle = \prod_{j=0}^{n-1}(c_0 + c_2\omega^j + c_4\omega^{2j} \cdots + c_{2p-2}\omega^{pj}) = 0$, where ω is a p-th root of unity. This implies that A is not MDS. □

3.5 Characterisation of some 4×4 semi-involutory matrices

In this section, we study some properties of a class of 4×4 semi-involutory matrices and provide a necessary and sufficient condition for an arbitrary matrix of this class to be semi-involutory. We prove Theorem 1.4.16 in this section. First we need the following definition from [78].

Definition 3.5.1. *Let $A = (a_{ij})$ be an $n \times n$ matrix. The upper G-discriminant of A is the $\binom{n}{2} \times n$ matrix $G(A_u) = (a_{ik}a_{kj})$, and the lower G-discriminant of A is $G(A_l) = (a_{ki}a_{jk})$, where $1 \leq i < j \leq n$ and $k \in \{1, 2, \ldots, n\}$.*

Theorem 3.5.2. *Let A be a 4×4 matrix. If A is semi-involutory then the matrices $G(A_u)$ and $G(A_l)$ are not of full rank.*

Proof. Let $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$ be a semi-involutory matrix. Then there exists a non-singular diagonal matrix $D = \text{diagonal}(d_1, d_2, d_3, d_4)$ such that ADA is a diagonal matrix. Since the off-diagonal entries of ADA are zero, we have the following 12 equations

$$\begin{aligned} a_{i1}a_{1j}d_1 + a_{i2}a_{2j}d_2 + a_{i3}a_{3j}d_3 + a_{i4}a_{4j}d_4 &= 0 \text{ where } 1 \leqslant i < j \leqslant 4, \text{ and} \\ a_{1i}a_{j1}d_1 + a_{2i}a_{j2}d_2 + a_{3i}a_{j3}d_3 + a_{4i}a_{j4}d_4 &= 0 \text{ where } 1 \leqslant i < j \leqslant 4. \end{aligned}$$

Consider the 6×4 matrix formed by the first six equations. It is denoted by

$$G(A_u) = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{21}a_{13} & a_{22}a_{23} & a_{23}a_{33} & a_{24}a_{43} \\ a_{21}a_{14} & a_{22}a_{24} & a_{23}a_{34} & a_{24}a_{44} \\ a_{31}a_{14} & a_{32}a_{24} & a_{33}a_{34} & a_{34}a_{44} \end{bmatrix}.$$

Notice that the non-zero vector $d = (d_1, d_2, d_3, d_4)$ satisfies $G(A_u) \cdot d^T = 0$. Thus for any 4×4 sub-matrix of $G(A_u)$, the non-zero vector (d_1, d_2, d_3, d_4) belongs to its null space. Therefore, rank$(G(A_u)) \neq 4$. Similarly $G(A_l)$ is constructed from the last six equations and its rank is also not equal to 4. □

Using Theorem 3.5.2 and Theorem 3.2.7, we provide some necessary and sufficient conditions for a particular class of 4×4 matrices to be semi-involutory. We start by recalling the definition of "totally the rank" from [78].

Definition 3.5.3. *Let A be an $m \times n$ matrix. Then A has 'totally the rank' r if the rank of A is r, and all $r \times r$ submatrices of A are non-singular.*

Theorem 3.5.4. *Let* $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$ *be a* 4×4 *non-singular matrix over some field* $\mathbb{F}$ *with* $a_{ij} \neq 0$ *for all* i, j*, and* $a_{32}a_{24}a_{43} = a_{23}a_{34}a_{42}$*. Then* A *is semi-involutory if and only if the following conditions are satisfied:*

1. *Entries of* A *satisfy*

$$a_{12}a_{23}a_{31} = a_{21}a_{32}a_{13} \tag{3.4}$$

$$a_{21}a_{14}a_{42} = a_{12}a_{24}a_{41} \tag{3.5}$$

$$a_{13}a_{34}a_{41} = a_{31}a_{14}a_{43}. \tag{3.6}$$

2. *Determinant of* X_1*,* X_2 *and* X_3 *are zero where*

$$X_1 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{21}a_{13} & a_{22}a_{23} & a_{23}a_{33} & a_{24}a_{43} \end{bmatrix}, X_2 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{14}a_{21} & a_{22}a_{24} & a_{23}a_{34} & a_{24}a_{44} \end{bmatrix},$$

$$\text{and } X_3 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{14}a_{31} & a_{24}a_{32} & a_{33}a_{34} & a_{34}a_{44} \end{bmatrix}.$$

3. *Rank of* $G(A_u)$ *and* $G(A_l)$ *is at most* 3*.*

4. *The submatrix* B *of* A *formed by removing the first column of* A *(i.e.,* $B = A[1, 2, 3, 4|2, 3, 4]$*) has 'totally the rank'* 3*.*

Proof. Let A be semi-involutory. Then there exists a non-singular diagonal matrix D such that ADA is diagonal. Then the off-diagonal entries of ADA are zero giving us the following 12 equations:

$$a_{i1}a_{1j}d_1 + a_{i2}a_{2j}d_2 + a_{i3}a_{3j}d_3 + a_{i4}a_{4j}d_4 = 0 \text{ where } 1 \leqslant i < j \leqslant 4, \tag{3.7}$$

$$a_{1i}a_{j1}d_1 + a_{2i}a_{j2}d_2 + a_{3i}a_{j3}d_3 + a_{4i}a_{j4}d_4 = 0 \text{ where } 1 \leqslant i < j \leqslant 4. \tag{3.8}$$

Using the condition $a_{ij} \neq 0$ and Theorem 2.3.6, we get that all 3×3 submatrices of A have non-zero determinants. Since $a_{11} \neq 0$, $\det A(1|1) = \det A[\{2, 3, 4\}|\{2, 3, 4\}] \neq 0$. Similarly, $a_{12} \neq 0$ implies $\det A(2|1) = \det A[\{1, 3, 4\}|\{2, 3, 4\}] \neq 0$. Other 3×3 submatrices can also be shown to have non-zero determinants in the same manner.

Consider the following two 4×4 submatrices constructed using Equations 3.7 and 3.8.

$$X_1 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{21}a_{13} & a_{22}a_{23} & a_{23}a_{33} & a_{24}a_{43} \end{bmatrix} \text{ and } Y_1 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{12}a_{31} & a_{22}a_{32} & a_{32}a_{33} & a_{42}a_{34} \end{bmatrix}.$$

Let x_i denote the i-th row of X_1 and y_j denote the j-th row of Y_1. Let x_{ij} and y_{ij} denote the j-th entry of the i-th row of X_1 and Y_1, respectively. Observe that the first three rows of X_1 and Y_1 are the same. Since A is semi-involutory, there exists a non-zero vector d such that $X_1 d^T = 0$ and $Y_1 d^T = 0$. Hence, ranks of X_1 and Y_1 are ≤ 3. Further, note that the sub-matrix $X_1[\{1,2,3\}|\{1,2,3\}]$ is the same as the sub-matrix $Y_1[\{1,2,3\}|\{1,2,3\}]$. The determinant of this submatrix is $a_{11}a_{12}a_{13} \cdot \det A[\{1,2,3\}|\{2,3,4\}] \neq 0$. Hence, the ranks of X_1 and Y_1 are 3. This implies that x_4 and y_4 are linear combinations of x_1, x_2, x_3. Let $x_4 = ax_1 + bx_2 + cx_3$ and $y_4 = dx_1 + ex_2 + fx_3$ where a, b, c, d, e, f are some non-zero scalars.

Consider $t = a_{23}^{-1}a_{32}$. Then $y_{42} = tx_{42}$ and $y_{43} = tx_{43}$. By the given condition $a_{32}a_{24}a_{43} = a_{23}a_{34}a_{42}$, we get $y_{44} = t\ x_{44}$. Since A is semi-involutory, we have $d_1x_{41} + d_2x_{42} + d_3x_{43} + d_4x_{44} = 0$ and $d_1y_{41} + d_2y_{42} + d_3y_{43} + d_4y_{44} = 0$ where $d_i \neq 0$ for $1 \leq i \leq 4$. Therefore, $td_1x_{41}+td_2x_{42}+td_3x_{43}+td_4x_{44} = td_1x_{41}+d_2y_{42}+d_3y_{43}+d_4y_{44} = 0$, i.e., $td_1x_{41}-d_1y_{41} = 0$. Since $d_1 \neq 0$, we have $y_{41} = tx_{41}$ implies $a_{12}a_{31}a_{23} = a_{13}a_{21}a_{32}$.

Next consider the following two 4×4 sub matrices X_2 and Y_2 constructed from Equations 3.7 and 3.8 with the same first three rows and different last row.

$$X_2 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{14}a_{21} & a_{22}a_{24} & a_{23}a_{34} & a_{24}a_{44} \end{bmatrix} \text{ and } Y_2 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{12}a_{41} & a_{22}a_{42} & a_{32}a_{43} & a_{42}a_{44} \end{bmatrix}$$

Then, by the same argument as before, the ranks of X_2 and Y_2 are 3. Let p_i's and q_i's denote i-th row of X_2 and Y_2, respectively. Then $p_4 = a'p_1 + b'p_2 + c'p_3$ and $q_4 = d'q_1 + e'q_2 + f'q_3$ for some non-zero scalars a', b', c', d', e', f'. Let $t = a_{24}^{-1}a_{42}$, then $tp_{42} = q_{42}, tp_{44} = q_{44}$. Using the given condition $a_{32}a_{24}a_{43} = a_{23}a_{34}a_{42}$, we get $tp_{43} = q_{43}$. Using semi-involutory property of A, we get $d_1p_{41} + d_2p_{42} + d_3p_{43} + d_4p_{44} = 0$ and $d_1q_{41} + d_2q_{42} + d_3q_{43} + d_4q_{44} = 0$ where $d_i \neq 0$ for $1 \leq i \leq 4$. This implies that $td_1p_{41}+td_2p_{42}+td_3p_{43}+td_4p_{44} = td_1p_{41}+d_2q_{42}+d_3q_{43}+d_4q_{44} = 0$, i.e., $td_1p_{41}-d_1q_{41} = 0$. Since $d_1 \neq 0$, $q_{41} = tp_{41}$ and $a_{21}a_{14}a_{42} = a_{12}a_{24}a_{41}$.

Next consider the following two 4×4 submatrices formed by Equations 3.7 and 3.8.

$$X_3 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{14}a_{31} & a_{24}a_{32} & a_{33}a_{34} & a_{34}a_{44} \end{bmatrix} \text{ and } Y_3 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{13}a_{41} & a_{23}a_{42} & a_{33}a_{43} & a_{43}a_{44} \end{bmatrix}$$

Using the same argument as earlier, the ranks of X_3 and Y_3 are 3. Let r_i and s_i denote the i-th row of X_3 and Y_3 respectively. Then $r_4 = a''r_1 + b''r_2 + c''r_3$ and $s_4 = d''s_1 + e''s_2 + f''s_3$ for some non-zero scalars $a'', b'', c'', d'', e'', f''$. Let $t = a_{34}^{-1}a_{43}$. Then $tr_{43} = s_{43}, tr_{44} = s_{44}$. Using the given condition $a_{32}a_{24}a_{43} = a_{23}a_{34}a_{42}$, we get $ta_{24}a_{32} = a_{23}a_{42}$, i.e., $tr_{43} = s_{43}$. Using the semi-involutory property of A again, we get $r_{41} = ts_{41}$ and $a_{13}a_{34}a_{41} = a_{31}a_{14}a_{43}$.

Observe that X_1, X_2 and X_3 are 4×4 submatrices of $G(A_u)$ of rank 3. Since $G(A_u)$ is a 6×4 matrix, its rank is ≤ 4. However, all 4×4 submatrices of $G(A_u)$ have rank 3. This implies rank of $G(A_u)$ is at most 3. Similarly, the proof of the rank of $G(A_l)$ holds from the argument that Y_1, Y_2 and Y_3 have rank 3.

Consider the matrix $B = \begin{bmatrix} a_{12} & a_{13} & a_{14} \\ a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \end{bmatrix}$. Since B is a 4×3 matrix, it's rank is at most 3. From the semi-involuotry property of A, determinant of all 3×3 submatrices of B is non-zero. Therefore, B has 'totally the rank' 3.

Conversely, assume entries of A satisfy the given conditions. To show that A is semi-involutory, we need to show the existence of a non-singular diagonal matrix D such that ADA is diagonal. Consider the following two 6×4 matrices:

$$G(A_u) = M_1 = \begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \\ a_{21}a_{13} & a_{22}a_{23} & a_{23}a_{33} & a_{24}a_{43} \\ a_{21}a_{14} & a_{22}a_{24} & a_{23}a_{34} & a_{24}a_{44} \\ a_{31}a_{14} & a_{32}a_{24} & a_{33}a_{34} & a_{34}a_{44} \end{bmatrix} \text{ and}$$

$$G(A_l) = M_2 = \begin{bmatrix} a_{11}a_{21} & a_{21}a_{22} & a_{31}a_{23} & a_{41}a_{24} \\ a_{11}a_{31} & a_{21}a_{32} & a_{31}a_{33} & a_{41}a_{34} \\ a_{11}a_{41} & a_{21}a_{42} & a_{31}a_{43} & a_{41}a_{44} \\ a_{12}a_{31} & a_{22}a_{32} & a_{32}a_{33} & a_{42}a_{34} \\ a_{12}a_{41} & a_{22}a_{42} & a_{32}a_{43} & a_{42}a_{44} \\ a_{13}a_{41} & a_{23}a_{42} & a_{33}a_{43} & a_{43}a_{44} \end{bmatrix}.$$

To show that ADA is diagonal, it is enough to show that there exists a vector $d = (d_1, d_2, d_3, d_4)$ with all non-zero entries such that $M_1 d^T$ and $M_2 d^T$ are zero, i.e., they share a null vector. Since the rank of M_1 and M_2 are ≤ 3, there exists a non-zero null vector in the null space of M_1 and M_2 by the rank-nullity theorem. Using the

given conditions, and the Equations 3.4, 3.5 and 3.6, it is easy to show that $\text{row}1_{M2} = (a_{21}a_{12}^{-1})\text{row}1_{M1}$, $\text{row}2_{M2} = (a_{31}a_{13}^{-1})\text{row}2_{M1}$, $\text{row}3_{M2} = (a_{41}a_{14}^{-1})\text{row}3_{M1}$, $\text{row}4_{M2} = (a_{32}a_{23}^{-1})\text{row}4_{M1}$, $\text{row}5_{M2} = (a_{42}a_{24}^{-1})\text{row}5_{M1}$, and $\text{row}6_{M2} = (a_{43}a_{34}^{-1})\text{row}6_{M1}$. Hence the row space of M_1 and M_2 are the same, and they share a non-zero null vector. To complete the proof, we only need to show that all d_i's are non-zero for $1 \leq i \leq 4$.

On the contrary, let us assume that at least one d_i is zero. Without loss of generality, let $d_1 = 0$. Then $M_1 d^T = 0$ implies that $d_2C_2 + d_3C_3 + d_4C_4 = 0$ where C_i denotes the i-th column of M_1. This means that C_2, C_3, and C_4 are linearly dependent. Consider the 6×3 matrix $M_3 = \begin{bmatrix} C_2 & C_3 & C_4 \end{bmatrix}$. The rank of M_3 is at most 2.

Now consider the following 3×3 submatrix of M_3: $\begin{bmatrix} a_{12}a_{22} & a_{13}a_{32} & a_{14}a_{42} \\ a_{12}a_{23} & a_{13}a_{33} & a_{14}a_{43} \\ a_{12}a_{24} & a_{13}a_{34} & a_{14}a_{44} \end{bmatrix}$. The determinant of this matrix is $(a_{12}a_{13}a_{14} \cdot \det A[\{2,3,4\}|\{2,3,4\}])$, which is non-zero by condition 4. Hence $d_1 \neq 0$. Similarly, if $d_2 = 0$ then $d_1C_1 + d_3C_3 + d_4C_4 = 0$ and this implies that the rank of the 6×3 matrix $\begin{bmatrix} C_1 & C_3 & C_4 \end{bmatrix}$ is at most 2. Consider the following 3×3 submatrix: $\begin{bmatrix} a_{11}a_{12} & a_{13}a_{32} & a_{14}a_{42} \\ a_{11}a_{13} & a_{13}a_{33} & a_{14}a_{43} \\ a_{11}a_{14} & a_{13}a_{34} & a_{14}a_{44}. \end{bmatrix}$. The determinant of this matrix is $(a_{11}a_{13}a_{14} \cdot \det A[\{1,3,4\}|\{2,3,4\}])$ and this is non-zero by condition 4. Thus d_2 is also non-zero. If $d_3 = 0$, then the rank of the 6×3 matrix $\begin{bmatrix} C_1 & C_2 & C_4 \end{bmatrix}$ is at most 2. However, the determinant of the matrix $\begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{14}a_{42} \\ a_{11}a_{13} & a_{12}a_{23} & a_{14}a_{43} \\ a_{11}a_{14} & a_{12}a_{24} & a_{14}a_{44}. \end{bmatrix}$ is $(a_{11}a_{12}a_{14} \cdot \det A[\{1,2,4\}|\{2,3,4\}]) \neq 0$ by condition 4. Thus d_3 is also non-zero. Similarly, if $d_4 = 0$ then the rank of $\begin{bmatrix} C_1 & C_2 & C_3 \end{bmatrix}$ is at most 2. However, the determinant of the matrix $\begin{bmatrix} a_{11}a_{12} & a_{12}a_{22} & a_{13}a_{32} \\ a_{11}a_{13} & a_{12}a_{23} & a_{13}a_{33} \\ a_{11}a_{14} & a_{12}a_{24} & a_{13}a_{34}. \end{bmatrix}$ is $(a_{11}a_{12}a_{13} \cdot \det A[\{1,2,3\}|\{2,3,4\}]) \neq 0$ by condition 4. Thus d_4 is also non-zero.

Therefore, there exists a non-singular diagonal matrix $D = \text{diagonal}(d_1, d_2, d_3, d_4)$ such that ADA is diagonal. This completes the proof that A is semi-involutory. □

3.6 Conclusion

This chapter explored MDS matrices characterized by semi-involutory and semi-orthogonal properties, and also Cauchy, Vandermonde, and circulant matrices within this framework. While the characterization of semi-involutory matrices of order 4×4 with all non-zero entries has been proved, the impact of the MDS property on this characterization remains an open question. Furthermore, investigating circulant MDS matrices of odd orders over finite fields, while considering their semi-involutory and semi-orthogonal properties, introduces a compelling direction for future research.

Chapter 4

Characterization of semi-involutory MDS matrices

In the previous chapter, we have characterized 3×3 semi-involutory MDS matrices over finite fields. In this chapter we provide a general structure of these matrices, motivated by the work on 3×3 MDS involutory matrices done by Gužel *et al.* in [27]. In first section, we recall some results on the general structure of MDS involutory matrices and semi-involutory matrices which will be useful for our discussion. Then we give a characterization for 3×3 semi-involutory matrices and prove a necessary and sufficient condition to construct MDS matrices using the characterization. In the last section, we count the number of 3×3 semi-involutory MDS matrices over the finite fields of characteristic 2. The work presented in this chapter is given in [66].

4.1 Introduction

Involutory MDS matrices play an important role in the design of lightweight cryptography primitives. Recently, in 2019, Gužel *et al.* introduced a general construction of MDS involutory matrices of order 3×3 using only two arbitrary elements of the finite field $\mathbb{F}_{2^m}$. Their work was motivated by the use of MDS involutory matrix in the diffusion layer of the block cipher Curupira. They established the following general format of involutory matrices:

$$\begin{bmatrix} a_1 & (a_1+1)b_0 & (a_1+1)b_1 \\ (a_2+1)b_0^{-1} & a_2 & (a_2+1)b_0^{-1}b_1 \\ (a_1+a_2)b_1^{-1} & (a_1+a_2)b_1^{-1}b_0 & a_1+a_2+1 \end{bmatrix}, \tag{4.1}$$

where a_1, a_2 are arbitrary elements from the finite field $\mathbb{F}_{2^m}$ with $a_1 \neq a_2, \{a_1, a_2\} \neq 1$ and $b_0, b_1 \in \mathbb{F}_{2^m}^*$. Using the structure 4.1 , they proved the following proposition to construct an MDS matrix:

Proposition 4.1.1. *A matrix in the form of Equation 4.1 is MDS over $\mathbb{F}_{2^m}, m > 2$ if and only if $a_1, a_2 \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ and $a_1 + a_2 \neq 1$.*

Proof. For proof see Proposition 1 of [27]. □

This proposition implies that there exists total $(2^m-1)^2(2^m-2)(2^m-4)$ involutory MDS matrices of order 3×3 over the finite field $\mathbb{F}_{2^m}$. Subsequently, in the following section, we

generalize these results for irreducible semi-involutory matrices. Additionally, we rely on certain properties of irreducible semi-involutory matrices which are noted in Section 2.3 of Chapter 2.

4.2 Structure of 3×3 semi-involutory MDS matrices

We begin this section with the proof of Theorem 1.2.

Theorem 4.2.1. *Let $A = (a_{ij}), 1 \leq i, j \leq 3$ be a 3×3 irreducible, semi-involutory matrix with an associated diagonal matrix $D = diagonal(d_1, d_2, d_3)$ over the finite field $\mathbb{F}_{2^m}$. Then*

$$\begin{aligned} a_{12} = (a_{11}d_1 + a_{33}d_3)d_2^{-1}x, a_{13} = (a_{11}d_1 + a_{22}d_2)d_3^{-1}xy, \\ a_{21} = (a_{22}d_2 + a_{33}d_3)d_1^{-1}x^{-1}, a_{23} = (a_{22}d_2 + a_{11}d_1)d_3^{-1}y, \\ a_{31} = (a_{33}d_3 + a_{22}d_2)d_1^{-1}(xy)^{-1}, a_{32} = (a_{33}d_3 + a_{11}d_1)d_2^{-1}y^{-1}, \end{aligned} \tag{4.2}$$

where x, y are non-zero elements of $\mathbb{F}_{2^m}$.

Proof. Since $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ is an irreducible, semi-involutory matrix, by Theorem 2.3.9, we have $A^{-1} = cDAD$. This implies that $(DA)^2 = c^{-1}I$. Let $c^{-1} = a \in \mathbb{F}_{2^m}$. The diagonal and non-diagonal entries of $(DA)^2$ satisfy the following conditions:

$$a_{11}^2d_1^2 + a_{12}a_{21}d_1d_2 + a_{13}a_{31}d_1d_3 = a \tag{4.3}$$
$$a_{22}^2d_2^2 + a_{12}a_{21}d_1d_2 + a_{23}a_{32}d_2d_3 = a \tag{4.4}$$
$$a_{33}^2d_3^2 + a_{13}a_{31}d_1d_3 + a_{23}a_{32}d_2d_3 = a \tag{4.5}$$
$$a_{11}a_{12}d_1^2 + a_{12}a_{22}d_1d_2 + a_{13}a_{32}d_1d_3 = 0 \tag{4.6}$$
$$a_{11}a_{13}d_1^2 + a_{12}a_{23}d_1d_3 + a_{13}a_{33}d_1d_3 = 0 \tag{4.7}$$
$$a_{11}a_{21}d_1d_2 + a_{12}a_{22}d_2^2 + a_{23}a_{31}d_2d_3 = 0 \tag{4.8}$$
$$a_{13}a_{21}d_1d_2 + a_{22}a_{23}d_2^2 + a_{23}a_{33}d_2d_3 = 0 \tag{4.9}$$
$$a_{11}a_{31}d_1d_3 + a_{21}a_{32}d_2d_3 + a_{31}a_{33}d_3^2 = 0 \tag{4.10}$$
$$a_{12}a_{31}d_1d_3 + a_{22}a_{32}d_2d_3 + a_{32}a_{33}d_3^2 = 0 \tag{4.11}$$

Adding (4.3), (4.4) and (4.5) we get

$$a_{11}^2d_1^2 + a_{22}^2d_2^2 + a_{33}^2d_3^2 = a. \tag{4.12}$$

Equation (4.6), (4.7), (4.8), (4.9), (4.10) and (4.11) can be re-written in the following form

thanks to an idea follows from Theorem 1 in [27]:

$$(a_{11}d_1 + a_{33}d_3)(a_{22}d_2 + a_{33}d_3) = a_{12}a_{21}d_1d_2 \tag{4.13}$$

$$(a_{11}d_1 + a_{22}d_2)(a_{11}d_1 + a_{33}d_3) = a_{23}a_{32}d_3d_2 \tag{4.14}$$

$$(a_{11}d_1 + a_{22}d_2)(a_{22}d_2 + a_{33}d_3) = a_{13}a_{31}d_3d_1. \tag{4.15}$$

Multiply the first term in the product by d_2^{-1} and second term by d_1^{-1} in the left hand side of Equation (4.13), we can write $a_{12} = (a_{11}d_1+a_{33}d_3)d_2^{-1}x$ and $a_{21} = (a_{22}d_2+a_{33}d_3)d_1^{-1}x^{-1}$ where x is an non-zero element of $\mathbb{F}_{2^m}$. Similarly, form (4.14), we get $a_{23} = (a_{22}d_2 + a_{11}d_1)d_3^{-1}y$ and $a_{32} = (a_{33}d_3 + a_{11}d_1)d_2^{-1}y^{-1}$, where y is an non-zero element of $\mathbb{F}_{2^m}$. Finally, from (4.15) we get $a_{13} = (a_{11}d_1 + a_{22}d_2)d_3^{-1}z$ and $a_{31} = (a_{33}d_3 + a_{22}d_2)d_1^{-1}z^{-1}$ where z is an non-zero element of $\mathbb{F}_{2^m}$. Since A is semi-involutory and irreducible, entries of A satisfy $a_{12}a_{23}a_{31} = a_{13}a_{21}a_{32}$ from Theorem 2.3.8. This implies x, y and z satisfy $xyz^{-1} = x^{-1}y^{-1}z$. By choosing $z = xy$ we get desired a_{13} and a_{31}. □

Remark 4.2.2. *Irreducible semi-involutory matrices may not be involutory. Thus Theorem 4.2.1 holds for a more general class of matrices. For example, consider the finite field $\mathbb{F}_{2^3}$ with generating polynomial $x^3 + x^2 + 1$. Let α be a primitive element of the finite field . Consider the matrix $A = \begin{bmatrix} \alpha^2+\alpha & 1 & \alpha^2+1 \\ 1 & \alpha^2+\alpha & \alpha+1 \\ \alpha^2+1 & \alpha+1 & \alpha^2+\alpha \end{bmatrix}$. Then A is semi-involutory and irreducible with D = diagonal $(\alpha^2+\alpha+1, \alpha^2+\alpha, \alpha+1)$ and $c = 1$ but $A^2 \neq I$.*

The converse of Theorem 4.2.1 is not necessarily true. For example,

Example 4.2.3. *Consider the finite field $\mathbb{F}_{2^2}$ with generating polynomial $x^2 + x + 1$. Let β be a primitive element and $a_{11} = 1, a_{22} = \beta, a_{33} = \beta + 1, d_1 = \beta, d_2 = \beta + 1$ and $d_3 = 1$. Take $x = \beta, y = \beta + 1$. Then the matrix*

$$A = \begin{bmatrix} a_{11} & (a_{11}d_1 + a_{33}d_3)d_2^{-1}x & (a_{11}d_1 + a_{22}d_2)d_3^{-1}xy \\ (a_{22}d_2 + a_{33}d_3)d_1^{-1}x^{-1} & a_{22} & (a_{11}d_1 + a_{22}d_2)d_3^{-1}y \\ (a_{22}d_2 + a_{33}d_3)d_1^{-1}(xy)^{-1} & (a_{11}d_1 + a_{33}d_3)d_2^{-1}y^{-1} & a_{33} \end{bmatrix} \tag{4.16}$$

is equal to $\begin{bmatrix} 1 & \beta+1 & \beta+1 \\ \beta+1 & \beta & \beta \\ 1 & \beta+1 & \beta+1 \end{bmatrix}$ *with* $\det A$ *is zero. Hence A is not semi-involutory.*

Observe that Equation (4.16) is the generalized form of the matrix provided in Theorem 1 of [27]. Substituting $d_1 = d_2 = d_3 = 1$ and $a = 1$ in equation (4.12), we can deduce to the generalized form of 3×3 involutory matrix which is noted in Equation 4.1.

Under certain condition we prove the converse of Theorem 4.2.1 in the following theorem.

Theorem 4.2.4. *Let A be a 3×3 matrix over $\mathbb{F}_{2^m}$ as described in Equation (4.16) and $d_1, d_2, d_3, x, y \in \mathbb{F}_{2^m}^*$. If $a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0$, then A is semi-involutory. Moreover, if any two of $a_{11}d_1 + a_{22}d_2, a_{22}d_2 + a_{33}d_3$ and $a_{11}d_1 + a_{33}d_3$ are non-zero, then A is irreducible.*

Proof. Consider the diagonal matrix D with d_1, d_2, d_3 as consecutive diagonal entries. Then D is a non-singular diagonal matrix and $ADA = \text{diagonal}(d_1^{-1}a, d_2^{-1}a, d_3^{-1}a)$ where a satisfies Equation (4.12), i.e., $a = (a_{11}d_1 + a_{22}d_2 + a_{33}d_3)^2$. Therefore by the given condition ADA is a non-singular diagonal matrix. Since $\det A = (a_{11}d_1 + a_{22}d_2 + a_{33}d_3)^3(d_1d_2d_3)^{-1}$, by the given condition $\det A \neq 0$. Hence from the equivalent condition of semi-involutory matrix A is semi-involutory. Observe that if at least two of $a_{11}d_1 + a_{22}d_2, a_{22}d_2 + a_{33}d_3$ and $a_{11}d_1 + a_{33}d_3$ are non-zero, then A cannot be permutation similar to a upper triangular matrix as a 3×3 upper triangular matrix must have at least three zeros, but by the given conditions, there can be at most two zero elements in A. Therefore, A cannot be permutation similar to an upper triangular matrix. Thus, A is irreducible. □

Note that, MDS matrices are irreducible. Using this property we prove the following result.

Theorem 4.2.5. *Let A be a 3×3 matrix over $\mathbb{F}_{2^m}$ as described in Equation (4.16), where $a_{11}, a_{22}, a_{33}, d_1, d_2, d_3, x, y$ are non-zero. Then A is semi-involutory MDS matrix if and only if $a_{11}d_1 + a_{22}d_2, a_{11}d_1 + a_{33}d_3, a_{22}d_2 + a_{33}d_3$ and $a_{11}d_1 + a_{22}d_2 + a_{33}d_3$ are non-zero elements of the finite field.*

Proof. Let A be a semi-involutory MDS matrix. Then A^{-1} exists and $\det A = (a_{11}d_1 + a_{22}d_2 + a_{33}d_3)^3(d_1d_2d_3)^{-1}$. This implies $a_{11}d_1 + a_{22}d_2 + a_{33}d_3$ is non-zero. Observe that, over the finite field $\mathbb{F}_{2^m}$, Equation (4.12) can be written as $(a_{11}d_1 + a_{22}d_2 + a_{33}d_3)^2 = a$ and there exists a non-zero element b such that $b^2 = a$. Hence $a_{11}d_1 + a_{22}d_2 + a_{33}d_3 = b$. The determinant of all 2×2 sub-matrices of A are following:

$$\begin{vmatrix} a_{11} & (a_{11}d_1 + a_{33}d_3)d_2^{-1}x \\ (a_{22}d_2 + a_{33}d_3)d_1^{-1}x^{-1} & a_{22} \end{vmatrix} = a_{33}bd_3d_1^{-1}d_2^{-1},$$

$$\begin{vmatrix} a_{11} & (a_{11}d_1 + a_{22}d_2)d_3^{-1}xy \\ (a_{22}d_2 + a_{33}d_3)d_1^{-1}x^{-1} & (a_{11}d_1 + a_{22}d_2)d_3^{-1}y \end{vmatrix} = (a_{11}d_1 + a_{22}d_2)byd_3^{-1}d_1^{-1},$$

$$\begin{vmatrix} (a_{11}d_1 + a_{33}d_3)d_2^{-1}x & (a_{11}d_1 + a_{22}d_2)d_3^{-1}xy \\ a_{22} & (a_{11}d_1 + a_{22}d_2)d_3^{-1}y \end{vmatrix} = (a_{11}d_1 + a_{22}d_2)bxyd_2^{-1}d_3^{-1},$$

$$\begin{vmatrix} a_{11} & (a_{11}d_1 + a_{33}d_3)d_2^{-1}x \\ (a_{22}d_2 + a_{33}d_3)d_1^{-1}(xy)^{-1} & (a_{11}d_1 + a_{33}d_3)d_2^{-1}y^{-1} \end{vmatrix} = (a_{11}d_1 + a_{33}d_3)by^{-1}d_1^{-1}d_2^{-1},$$

$$\begin{vmatrix} a_{11} & (a_{11}d_1 + a_{22}d_2)d_3^{-1}xy \\ (a_{22}d_2 + a_{33}d_3)d_1^{-1}(xy)^{-1} & a_{33} \end{vmatrix} = a_{22}bd_2d_1^{-1}d_3^{-1},$$

$$\begin{vmatrix} (a_{11}d_1 + a_{33}d_3)d_2^{-1}x & (a_{11}d_1 + a_{22}d_2)d_3^{-1}xy \\ (a_{11}d_1 + a_{33}d_3)d_2^{-1}y^{-1} & a_{33} \end{vmatrix} = (a_{11}d_1 + a_{33}d_3)bxd_2^{-1}d_3^{-1},$$

$$\begin{vmatrix} (a_{22}d_2 + a_{33}d_3)d_1^{-1}x^{-1} & a_{22} \\ (a_{22}d_2 + a_{33}d_3)d_1^{-1}(xy)^{-1} & (a_{11}d_1 + a_{33}d_3)d_2^{-1}y^{-1} \end{vmatrix} = (a_{22}d_2 + a_{33}d_3)bx^{-1}y^{-1}d_1^{-1}d_2^{-1},$$

$$\begin{vmatrix} (a_{22}d_2 + a_{33}d_3)d_1^{-1}x^{-1} & (a_{11}d_1 + a_{22}d_2)d_3^{-1}y \\ (a_{22}d_2 + a_{33}d_3)d_1^{-1}(xy)^{-1} & a_{33} \end{vmatrix} = (a_{22}d_2 + a_{33}d_3)bxd_1^{-1}d_3^{-1},$$

$$\begin{vmatrix} a_{22} & (a_{11}d_1 + a_{22}d_2)d_3^{-1}y \\ (a_{11}d_1 + a_{33}d_3)d_2^{-1}y^{-1} & a_{33} \end{vmatrix} = a_{11}bd_1d_2^{-1}d_3^{-1}.$$

Since A is an MDS matrix and d_1, d_2, d_3, x, y, b are non-zero elements of the finite field, then the condition holds.

Conversely, let $a_{11}d_1 + a_{22}d_2, a_{11}d_1 + a_{33}d_3, a_{22}d_2 + a_{33}d_3$ and $a_{11}d_1 + a_{22}d_2 + a_{33}d_3$ are non-zero elements of the finite field. Then we have all the entries of the matrix A and all 2×2 sub-matrices have non-zero determinant. Since $a_{11}d_1+a_{22}d_2+a_{33}d_3 \neq 0, \det A$ is also non-zero. Therefore A is an MDS matrix. By some easy calculation we have $ADA = D'$ with $D = \text{diagonal}(d_1, d_2, d_3)$ and $D' = \text{diagonal}(d_1^{-1}a, d_2^{-1}a, d_3^{-1}a)$, with $a = (a_{11}d_1 + a_{22}d_2+a_{33}d_3)^2$. Since a is a non-zero element of the finite field and D, D' are non-singular matrices, A is semi-involutory. □

4.3 A counting problem

In this section, we count the number of semi-involutory MDS matrices of order 3×3 over the finite field $\mathbb{F}_{2^m}$. We start with the following construction of a set S of 6-tuples that satisfy the conditions presented in Theorem 4.2.5 over the finite field $\mathbb{F}_{2^m}$: $S = \{(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}$. Using the cardinality of S, we count the number of semi-involutory MDS matrices in Theorem 4.3.5. To determine the cardinality of S, we first prove a series of lemmas.

Lemma 4.3.1. *Let* $S_1 = \{(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{ii} \neq a_{jj}, 1 \leq i < j \leq 3, a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}$. *Then* $|S_1| = (2^m - 1)^2(2^m - 2)(2^{3m} - 9 \cdot 2^{2m} + 26 \cdot 2^m - 24)$.

Proof. Let $a_{ii} \neq a_{jj}, 1 \leq i < j \leq 3$. We consider three sub-cases based on the choice of d_1, d_2, d_3. As a result, let consider the following three sets:

$$\begin{aligned} S_1' = \{&(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{ii} \neq a_{jj}, d_i = d_j, 1 \leq i < j \leq 3, \\ &a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}, \\ S_1'' = \{&(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{ii} \neq a_{jj}, 1 \leq i < j \leq 3, d_i = d_j \text{ for} \\ &(i, j) \in \{(1, 2), (1, 3), (2, 3)\}, a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, \\ &a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}, \\ S_1''' = \{&(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{ii} \neq a_{jj}, d_i \neq d_j, 1 \leq i < j \leq 3, \\ &a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}. \end{aligned}$$

Case I. First consider the set S_1'. In this case we have $d_i = d_j$ for $1 \leq i < j \leq 3$. This

implies that $a_{11}d_1 + a_{22}d_2, a_{11}d_1 + a_{33}d_3, a_{22}d_2 + a_{33}d_3$ are non-zero. Since $d_i \in \mathbb{F}_{2^m}^*$, the equation $a_{11}d_1 + a_{22}d_2 + a_{33}d_3 = 0$ holds if $a_{11} + a_{22} + a_{33} = 0$. Consider the sets $A_1 = \{(a_{11}, a_{22}, a_{33}) : a_{11} + a_{22} + a_{33} = 0\}$ and $A_2 = \{(a_{11}, a_{22}, a_{33}) : a_{11} + a_{22} + a_{33} \neq 0\}$. Any non-zero $d_i \in \mathbb{F}_{2^m}$ satisfy all the four conditions of S_1' for each element of A_2. Clearly,

$$|A_2| = (2^m - 1)(2^m - 2)(2^m - 3) - (2^m - 1)(2^m - 2) = (2^m - 1)(2^m - 2)(2^m - 4).$$

Hence cardinality of S_1' is

$$\begin{aligned} |S_1'| &= \{(2^m - 1)(2^m - 2)(2^m - 3) - (2^m - 1)(2^m - 2)\}(2^m - 1) \\ &= (2^m - 1)^2(2^m - 2)(2^m - 4). \end{aligned}$$

Case II. Next consider the set S_1''. Then exactly one pair of d_i is equal. We give the proof for the case $d_1 = d_2, d_1 \neq d_3, d_2 \neq d_3$. The other two cases will follow similarly.

Let $d_1 = d_2, d_1 \neq d_3, d_2 \neq d_3$. Then $a_{11}d_1 + a_{22}d_2$ is non-zero. To determine the cardinality of S_1'', we count the cardinality of non-zero 3-tuple (d_1, d_1, d_3) such that $a_{11}d_1 + a_{33}d_3, a_{22}d_1 + a_{33}d_3, a_{11}d_1 + a_{22}d_1 + a_{33}d_3$ are non-zero.

First we choose an arbitrary (a_{11}, a_{22}, a_{33}) such that $a_{33} \neq a_{11} + a_{22}$ and fix it. There are $(2^m - 1)$ and $(2^m - 2)$ ways to choose a_{11} and a_{22} respectively. Since a_{33} is different from $a_{11} + a_{22}$, we have $(2^m - 4)$ many options for a_{33}. Therefore (a_{11}, a_{22}, a_{33}) can be chosen in total $(2^m - 1)(2^m - 2)(2^m - 4)$ ways. Let define the following two sets:

$$\begin{aligned} &T = \{(d_1, d_3) \neq (0, 0) : d_1 \neq d_3\} \text{ and} \\ &X = \{(d_1, d_3) \in T : a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_1 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_1 + a_{33}d_3 \neq 0\}. \end{aligned}$$

Clearly, $|T| = (2^m - 1)(2^m - 2)$. To count the cardinality of X, consider three sets

$$\begin{aligned} X_1 &= \{(d_1, d_3) \in T : a_{11}d_1 + a_{33}d_3 = 0\}, \\ X_2 &= \{(d_1, d_3) \in T : a_{22}d_1 + a_{33}d_3 = 0\}, \\ \text{and } X_3 &= \{(d_1, d_3) \in T : (a_{11} + a_{22})d_1 + a_{33}d_3 = 0\}. \end{aligned}$$

Observe that $|X| = |T| \setminus |X_1 \cup X_2 \cup X_3|$. To calculate the cardinality of $X_i, 1 \leq i \leq 3$, we construct three sets Y_1, Y_2 and Y_3 defined as follows:

$$\begin{aligned} Y_1 &= \{(xa_{33}, xa_{11}) : x \in \mathbb{F}_{2^m}^*\}, \\ Y_2 &= \{(ya_{33}, ya_{22}) : y \in \mathbb{F}_{2^m}^*\}, \\ \text{and } Y_3 &= \{(za_{33}, z(a_{11} + a_{22}) : z \in \mathbb{F}_{2^m}^*\}. \end{aligned}$$

We prove that $X_i = Y_i, 1 \leq i \leq 3$. It is easy to observe that, $Y_1 \subseteq X_1, Y_2 \subseteq X_2$ and $Y_3 \subseteq X_3$.

To prove the other side of inclusion, i.e., $X_1 \subseteq Y_1$, consider an arbitrary element $(\alpha_1, \alpha_2) \in X_1$. Therefore $a_{11}\alpha_1 + a_{33}\alpha_2 = 0$. Moreover, there exist non-zero elements β_1, β_2 in $\mathbb{F}_{2^m}^*$

such that $\alpha_1 = \beta_1 a_{33}$ and $\alpha_2 = \beta_2 a_{11}$. Hence $a_{11}a_{33}(\beta_1 + \beta_2) = 0$ implies $\beta_1 = \beta_2$. Thus $(\alpha_1, \alpha_2) \in Y_1$ and this implies $X_1 = Y_1$. Similarly, $Y_2 = X_2$ and $Y_3 = X_3$ and $|X_1| = |X_2| = |X_3| = (2^m - 1)$.

Next assume that $X_1 \cap X_2 \neq \phi$. This implies $a_{11} = a_{22}$, which is not possible. Similarly, if $X_1 \cap X_3 \neq \phi$, that implies $a_{11} = a_{11} + a_{22}$, which is not possible. Also, if $X_2 \cap X_3 \neq \phi$, then $a_{22} = a_{11} + a_{22}$, which is not possible. Therefore,

$$\begin{aligned} |X_1 \cup X_2 \cup X_3| &= 3(2^m - 1) \text{ and} \\ |X| = |T| \setminus |X_1 \cup X_2 \cup X_3| &= (2^m - 1)(2^m - 2) - 3(2^m - 1) = (2^m - 1)(2^m - 5). \end{aligned}$$

For the case $a_{33} = a_{11} + a_{22}$, first we choose arbitrary a_{11}, a_{22} and fix them. Then $a_{11}d_1 + a_{22}d_1 + a_{33}d_3 = (d_1 + d_3)a_{33} \neq 0$. Hence, in this situation the set X is defined as $X = \{(d_1, d_3) \in T : a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_1 + a_{33}d_3 \neq 0\}$. Following a similar approach as in previous case, construct the sets X_1, X_2, Y_1, Y_2 and obtain $|X|$. Then

$$|X| = (2^m - 1)(2^m - 2) - 2(2^m - 1) = (2^m - 1)(2^m - 4).$$

Combining both cases for $d_1 = d_2, d_1 \neq d_3, d_2 \neq d_3$ and considering the remaining two cases for d_i's, we have

$$\begin{aligned} |S_1''| &= 3\{(2^m - 1)^2(2^m - 2)(2^m - 4)(2^m - 5) + (2^m - 1)^2(2^m - 2)(2^m - 4)\} \\ &= 3(2^m - 1)^2(2^m - 2)(2^m - 4)^2. \end{aligned}$$

Case III. Lastly, consider S_1'''. First choose an arbitrary triplet (a_{11}, a_{22}, a_{33}) and fix it. First we define the following two sets:

$$\begin{aligned} T &= \{(d_1, d_2, d_3) \neq (0, 0, 0) : d_i \neq d_j, 1 \leq i < j \leq 3\}, \\ X &= \{(d_1, d_2, d_3) \in T : a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, \\ &\quad a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}. \end{aligned}$$

Clearly, $|T| = (2^m - 1)(2^m - 2)(2^m - 3)$. Consider the sets

$$\begin{aligned} X_1 &= \{(d_1, d_2, d_3) \in T : a_{11}d_1 + a_{22}d_2 = 0\}, \\ X_2 &= \{(d_1, d_2, d_3) \in T : a_{11}d_1 + a_{33}d_3 = 0\}, \\ X_3 &= \{(d_1, d_2, d_3) \in T : a_{22}d_2 + a_{33}d_3 = 0\}, \\ \text{and } X_4 &= \{(d_1, d_2, d_3) \in T : a_{11}d_1 + a_{22}d_2 + a_{33}d_3 = 0\}. \end{aligned}$$

First we calculate $|X_1 \cup X_2 \cup X_3 \cup X_4|$. We begin with defining the following sets

$$\begin{aligned}
Y_1 &= \{(xa_{22}, xa_{11}, d_3) : x \in \mathbb{F}_{2^m}^*, d_3 \neq (0, xa_{22}, xa_{11})\},\\
Y_2 &= \{(ya_{33}, d_2, ya_{11}) : y \in \mathbb{F}_{2^m}^*, d_2 \neq (0, ya_{33}, ya_{11})\},\\
Y_3 &= \{(d_1, za_{33}, za_{22}) : d_1 \in \mathbb{F}_{2^m}^*, z \in \mathbb{F}_{2^m}^*, za_{33} \neq d_1, za_{11} \neq d_1\}\\
&= \{(d_1, za_{33}, za_{22}) : d_1 \in \mathbb{F}_{2^m}^*, z \in \mathbb{F}_{2^m}^*, z \neq (d_1a_{33}^{-1}, d_1a_{22}^{-1})\},\\
\text{and } Y_4 &= \{(d_1, d_2, d_3) : d_1 \in \mathbb{F}_{2^m}^*, d_2 \neq (0, d_1, a_{22}^{-1}a_{11}d_1, (a_{11}+a_{33})a_{22}^{-1}d_1, (a_{22}+a_{33})^{-1}a_{11}d_1),\\
&\quad d_3 \neq 0, d_3 = a_{33}^{-1}(a_{11}d_1 + a_{22}d_2)\}.
\end{aligned}$$

We prove that $X_i = Y_i, 1 \leq i \leq 4$. For the case $a_{33} = a_{11} + a_{22}$, Y_4 is denoted by

$$Y_4^0 = \{(d_1, d_2, d_3) : d_1 \in \mathbb{F}_{2^m}^*, d_2 \neq (0, d_1, a_{22}^{-1}a_{11}d_1), d_3 \neq 0, d_3 = a_{33}^{-1}(a_{11}d_1 + a_{22}d_2)\}.$$

The cardinality of Y_4^0 and Y_4 are $|Y_4^0| = (2^m - 1)(2^m - 3)$ and $|Y_4| = (2^m - 1)(2^m - 5)$.
Clearly, $Y_1 \subseteq X_1, Y_2 \subseteq X_2$ and $Y_3 \subseteq X_3$. We now prove the reverse inclusion starting with the case $X_1 \subseteq Y_1$, and the other two cases are similar.
Let $(d_1', d_2', d_3') \in X_1$. From the construction of X_1 this implies $a_{11}d_1' + a_{22}d_2' = 0$ and $d_3' \neq \{d_1', d_2'\}$. There exists non-zero elements $\beta_1, \beta_2 \in \mathbb{F}_{2^m}^*$ such that $d_1' = \beta_1 a_{22}, d_2' = \beta_2 a_{11}$. Since $a_{11}d_1' + a_{22}d_2' = 0$, we have $a_{11}a_{22}(\beta_1 + \beta_2) = 0$. Since a_{11}, a_{22} are non-zero element, this implies $\beta_1 = \beta_2$. Therefore $d_3' \neq \{\beta_1 a_{22}, \beta_1 a_{11}\}$ and $X_1 = Y_1$. Hence, cardinality of the set Y_1 is $(2^m - 1)(2^m - 3)$ because, we need to choose x from $\mathbb{F}_{2^m}^*$ and d_3 from $\mathbb{F}_{2^m}^* \setminus \{0, xa_{22}, xa_{11}\}$.
Likewise, $X_2 = Y_2$ and $X_3 = Y_3$. Hence $|X_1| = |X_2| = |X_3| = (2^m - 1)(2^m - 3)$.
We now prove that $Y_4 = X_4$ for the case $a_{33} \neq a_{11} + a_{22}$. Let $(d_1', d_2', d_3') \in Y_4$. Then $d_3' = a_{33}^{-1}(a_{11}d_1' + a_{22}d_2')$ and this implies $a_{11}d_1' + a_{22}d_2' + a_{33}d_3' = 0$. Also $d_3' \neq 0$ implies $a_{11}d_1' \neq a_{22}d_2'$ i.e., $d_2' \neq a_{22}^{-1}a_{11}d_1'$.
To prove $(d_1', d_2', d_3') \in X_4$, we need to show $d_3' \neq \{d_1', d_2'\}$. If $d_3' = d_1'$ then $d_1' = a_{33}^{-1}(a_{11}d_1' + a_{22}d_2')$, which implies $d_2' = (a_{11} + a_{33})a_{22}^{-1}d_1'$, which is not possible from the construction of Y_4. Similarly, if $d_3' = d_2'$, then $d_2' = a_{33}^{-1}(a_{11}d_1' + a_{22}d_2')$, which implies $d_2' = (a_{22} + a_{33})^{-1}a_{11}d_1'$, which is also not possible from the construction of Y_4. Therefore, $(d_1', d_2', d_3') \in T$ and $Y_4 \subseteq X_4$.
Conversely , let $(d_1', d_2', d_3') \in X_4$. Then $d_1' \neq d_2', d_1' \neq d_3', d_1' \neq d_2'$ and $a_{11}d_1' + a_{22}d_2' + a_{33}d_3' = 0$. Since $a_{33}d_3' \neq 0$, we have $a_{11}d_1' \neq a_{22}d_2'$ and this implies $d_2' \neq a_{22}^{-1}a_{11}d_1'$. Furthermore, since $d_3' \neq d_1', d_2'$, it follows that $a_{11}d_1' + a_{22}d_2' \neq a_{33}d_1'$ and $a_{11}d_1' + a_{22}d_2' \neq a_{33}d_2'$. This implies $d_2' \neq (a_{11} + a_{33})a_{22}^{-1}d_1'$ and $d_2' \neq (a_{22} + a_{33})^{-1}a_{11}d_1'$ respectively. Therefore $(d_1', d_2', d_3') \in Y_4$.
Similarly it can be proved that $Y_4^0 = X_4$ when $a_{33} = a_{11} + a_{22}$.
Next, we calculate the cardinality of $X_i \cap X_j, 1 \leq i, j \leq 4$. We start with calculating $X_1 \cap X_2$ and $X_1 \cap X_4$, and the others cases are similar.
Let $(d_1', d_2', d_3') \in X_1 \cap X_2$. This implies $d_1' = xa_{22} = ya_{33}, d_2' = xa_{11}, d_3' = ya_{11}$. Since $a_{22} \neq a_{33}$, and $xa_{22} = ya_{33} = d_1'$ then $x = d_1'a_{22}^{-1}$ and $y = d_1'a_{33}^{-1}$. Therefore

$\{(d_1', d_1'a_{22}^{-1}a_{11}, d_1'a_{33}^{-1}a_{11}) : d_1' \in \mathbb{F}_{2^m}^*\} = X_1 \cap X_2$. Then $|X_1 \cap X_2| = (2^m - 1)$. Similar to this, $|X_1 \cap X_3| = |X_2 \cap X_3| = (2^m - 1)$.
Let $(d_1', d_2', d_3') \in X_1 \cap X_4$. Then $a_{11}d_1' + a_{22}d_2' = 0$ and $a_{11}d_1' + a_{22}d_2' + a_{33}d_3' = 0$. This implies $a_{33}d_3' = 0$, which is not possible. Thus $|X_1 \cap X_4| = \phi$. Similarly, $|X_2 \cap X_4| = |X_3 \cap X_4| = \phi$.
Lastly, we calculate the cardinality of the set $X_1 \cap X_2 \cap X_3$. For that, we prove that $X_1 \cap X_2 \cap X_3 = X_1 \cap X_2$.
Let $(d_1', d_2', d_3') \in X_1 \cap X_2$. then $a_{11}d_1' + a_{22}d_2' = 0$ and $a_{11}d_1' + a_{33}d_3' = 0$. Adding these, we have $a_{22}d_2' + a_{33}d_3' = 0$. Thus $(d_1', d_2', d_3') \in X_1 \cap X_2 \cap X_3$. Other side of the inclusion follow easily. Thus $|X_1 \cap X_2 \cap X_3| = (2^m - 1)$.
Therefore $|X_1 \cup X_2 \cup X_3 \cup X_4| = \begin{cases} 2(2^m - 1)(2.2^m - 7), & \text{for } a_{11} + a_{22} = a_{33} \\ (2^m - 1)(4.2^m - 16), & \text{for } a_{11} + a_{22} \neq a_{33} \end{cases}$
and $|X| = \begin{cases} (2^m - 1)(2^{2m} - 9.2^m + 20), & \text{for } a_{11} + a_{22} = a_{33} \\ (2^m - 1)(2^{2m} - 9.2^m + 22), & \text{for } a_{11} + a_{22} \neq a_{33}. \end{cases}$
Cardinality of S_1''' in this case is $(2^m - 1)^2(2^m - 2)\{(2^m - 4)(2^{2m} - 9.2^m + 22) + (2^{2m} - 9.2^m + 20)\}$. Since any two of S_1', S_1'' and S_1''' have empty intersection, cardinality of S_1 is:

$$\begin{aligned} |S_1| &= (2^m - 1)^2(2^m - 2)(2^m - 4) + 3(2^m - 1)^2(2^m - 2)(2^m - 4)^2 + (2^m - 1)^2(2^m - 2) \\ &\quad \cdot \{(2^m - 4)(2^{2m} - 9.2^m + 22) + (2^{2m} - 9.2^m + 20)\} \\ &= (2^m - 1)^2(2^m - 2)(2^{3m} - 9 \cdot 2^{2m} + 26 \cdot 2^m - 24). \end{aligned}$$

□

In the next lemma, we consider another condition on the a_{ii}'s and determine the cardinality of the set S_2 derived from S.

Lemma 4.3.2. *Let* $S_2 = \{(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : \ a_{ii} = a_{jj}, 1 \leq i < j \leq 3, a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}$. *Then* $|S_2| = (2^m - 1)^2(2^m - 2)(2^m - 4)$.

Proof. Assume that $a_{ii} = a_{jj}, 1 \leq i < j \leq 3$. In this case, the only possible choice for d_i's are $d_i \neq d_j, 1 \leq i < j \leq 3$.
As a result $a_{11}d_1 + a_{22}d_2, a_{11}d_1 + a_{33}d_3, a_{22}d_2 + a_{33}d_3$ are never zero. Additionally, the elements in the set S_2 satisfy the condition $a_{11}d_1 + a_{22}d_2 + a_{33}d_3 = a_{11}(d_1 + d_2 + d_3) \neq 0$. Since a_{11} in non-zero, we need $d_1 + d_2 + d_3$ cannot be zero i.e., $d_3 \neq d_1 + d_2$. Then for the triplet (d_1, d_2, d_3), we have

$$(2^m - 1)(2^m - 2)(2^m - 3) - (2^m - 1)(2^m - 2) = (2^m - 1)(2^m - 2)(2^m - 4)$$

many choices. Therefore cardinality of S_2 is $(2^m - 1)^2(2^m - 2)(2^m - 4)$. □

For the last case, let us assume at most one pair of a_{ii}'s are equal i.e., $a_{ii} = a_{jj}$ for $(i, j) \in \{(1, 2), (1, 3), (2, 3)\}$. We prove for the case $a_{11} = a_{22}, a_{11} \neq a_{33}$ and the other two cases

follow similarly.

Lemma 4.3.3. *Let* $S_3 = \{(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{11} = a_{22}, a_{11} \neq a_{33}, a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}$. *Then* $|S_3| = (2^m - 1)^2(2^m - 2)(2^{2m} - 6 \cdot 2^m + 8)$.

Proof. Let $a_{11} = a_{22}, a_{11} \neq a_{33}, a_{22} \neq a_{33}$. We study each sub-cases of d_i separately. Let

$$\begin{aligned}
S_3' &= \{(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{11} = a_{22}, a_{11} \neq a_{33}, d_1 = d_2, d_2 \neq d_3,\\
&\quad d_1 \neq d_3, a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0,\\
&\quad a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\},\\
S_3'' &= \{(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{11} = a_{22}, a_{11} \neq a_{33}, d_1 \neq d_2, d_2 = d_3,\\
&\quad d_1 \neq d_3, a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0,\\
&\quad a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\},\\
S_3''' &= \{(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{11} = a_{22}, a_{11} \neq a_{33}, d_1 \neq d_2, d_2 \neq d_3,\\
&\quad d_1 = d_3, a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0,\\
&\quad a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\},\\
S_3'''' &= \{(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{11} = a_{22}, a_{11} \neq a_{33}, d_1 \neq d_2, d_2 \neq d_3,\\
&\quad d_1 \neq d_3, a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0,\\
&\quad a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}.
\end{aligned}$$

Case I. Consider the set S_3'. In this set, we have $d_1 = d_2, d_2 \neq d_3, d_1 \neq d_3$. Therefore $a_{11}d_1 + a_{22}d_2$ is always zero and this case will never occur.
Case II. Consider the set S_3''. Then $d_1 \neq d_2, d_2 = d_3, d_1 \neq d_3$.
For each value of d_i's with $1 \leq i \leq 3$, both $a_{22}d_2 + a_{33}d_3$ and $a_{11}d_1 + a_{22}d_2$ are always non-zero in this case.
Furthermore, the elements of the set S_3'' satisfy $a_{11}d_1 + a_{33}d_3, a_{11}d_1 + a_{22}d_2 + a_{33}d_3$ are non-zero. To find the cardinality of S_3'', we first fix an arbitrary 3-tuple $(a_{11}, a_{22}, a_{33}) \in (\mathbb{F}_{2^m}^*)^3$ with $a_{11} = a_{22}$. Let us define the following sets:

$T = \{(d_1, d_3) \neq (0, 0) : d_1 \neq d_3\}$ and
$X = \{(d_1, d_3) \in T : a_{11}d_1 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 = a_{11}d_1 + a_{11}d_3 + a_{33}d_3 \neq 0\}$

Clearly, $|T| = (2^m - 1)(2^m - 2)$. To determine the cardinality of X, we first count the cardinality of the following sets. Let

$$\begin{aligned}
X_1 &= \{(d_1, d_3) \in T : a_{11}d_1 + a_{33}d_3 = 0\},\\
X_2 &= \{(d_1, d_3) \in T : a_{11}d_1 + (a_{11} + a_{33})d_3 = 0\},\\
\text{and } Y_1 &= \{(xa_{33}, xa_{11}) : x \in \mathbb{F}_{2^m}^*\},\\
Y_2 &= \{(z(a_{11} + a_{33}), z(a_{11}) : z \in \mathbb{F}_{2^m}^*\}.
\end{aligned}$$

Our claim is that $X_i = Y_i$ for $i = 1, 2$. One side of the inclusion is evident, i.e., $Y_1 \subseteq X_1, Y_2 \subseteq X_2$. For the converse part, consider an arbitrary element $(\alpha_1, \alpha_2) \in X_1$. Then $a_{11}\alpha_1 + a_{33}\alpha_2 = 0$. There exists non-zero elements β_1, β_2 over $\mathbb{F}_{2^m}^*$ such that $\alpha_1 = \beta_1 a_{33}$ and $\alpha_2 = \beta_2 a_{11}$. Consequently, we get $a_{11}a_{33}(\beta_1 + \beta_2) = 0$ which implies $\beta_1 = \beta_2$. Thus $X_1 = Y_1$. Similarly, $X_2 = Y_2$ and $|X_1| = |X_2| = (2^m - 1)$.
Next we calculate $|X_1 \cup X_2|$. If $X_1 \cap X_2 \neq \phi$ then $a_{33} = a_{11} + a_{33}$, which is contradiction to $a_{11} \neq 0$. Therefore

$$|X_1 \cup X_2| = 2(2^m - 1) \text{ and}$$
$$|X| = |T| \setminus |X_1 \cup X_2| = (2^m - 1)(2^m - 2) - 2(2^m - 1) = (2^m - 1)(2^m - 4).$$

Thus $|S_3''| = (2^m - 1)^2(2^m - 2)(2^m - 4)$.
Case III. Consider the set S_3'''. Then $d_1 \neq d_2, d_2 \neq d_3, d_1 = d_3$.
Proving similarly as Case II of Lemma 4.3.3, we will get $|S_3'''| = (2^m - 1)^2(2^m - 2)(2^m - 4)$.
Case IV. Consider the set S_3''''. Then $d_1 \neq d_2, d_2 \neq d_3, d_1 \neq d_3$.
First fix an arbitrary triple $(a_{11}, a_{22}, a_{33}) \in (\mathbb{F}_{2^m}^*)^3$ with $a_{11} = a_{22}$. Let define the following sets:

$$T = \{(d_1, d_2, d_3) \neq (0, 0, 0) : d_i \neq d_j, 1 \leq i < j \leq 3\},$$
$$\text{and } X = \{(d_1, d_2, d_3) \in T : a_{11}d_1 + a_{22}d_2 = a_{11}(d_1 + d_2) \neq 0,$$
$$a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}.$$

Clearly, $|T| = (2^m - 1)(2^m - 2)(2^m - 3)$. To determine the cardinality of X, we begin with the following four subsets of X.

$$X_1 = \{(d_1, d_2, d_3) \in T : a_{11}d_1 + a_{22}d_2 = 0\},$$
$$X_2 = \{(d_1, d_2, d_3) \in T : a_{11}d_1 + a_{33}d_3 = 0\},$$
$$X_3 = \{(d_1, d_2, d_3) \in T : a_{11}d_2 + a_{33}d_3 = 0\},$$
$$\text{and } X_4 = \{(d_1, d_2, d_3) \in T : a_{11}d_1 + a_{22}d_2 + a_{33}d_3 = 0\}.$$

Observe that $|X| = |T| \setminus |X_1 \cup X_2 \cup X_3 \cup X_4|$. Since $d_1 \neq d_2$ and $a_{11} = a_{22},\ a_{11}d_1 + a_{22}d_2 = a_{11}(d_1 + d_2)$ is always non-zero for all (d_1, d_2, d_3). Therefore $|X_1| = 0$.
Consider the following three sets:

$$Y_2 = \{(ya_{33}, d_2, ya_{11}) : y \in \mathbb{F}_{2^3}^*, d_2 \neq \{0, ya_{33}, ya_{11}\}\},$$
$$Y_3 = \{(d_1, za_{33}, za_{11}) : d_1 \in \mathbb{F}_{2^3}^*, z \in \mathbb{F}_{2^3}^*, d_1 \neq \{za_{33}, za_{11}\}\}$$
$$= \{(d_1, za_{33}, za_{11}) : d_1 \in \mathbb{F}_{2^3}^*, z \in \mathbb{F}_{2^3}^*, z \neq \{d_1a_{33}^{-1}, d_1a_{22}^{-1}\}\},$$
$$\text{and } Y_4 = \{(d_1, d_2, d_3) : d_1 \in \mathbb{F}_{2^3}^*, d_2 \neq \{0, d_1, (a_{11} + a_{33})a_{22}^{-1}d_1, (a_{22} + a_{33})^{-1}a_{11}d_1\}, d_3 \neq 0,$$
$$d_3 = a_{33}^{-1}(a_{11}d_1 + a_{22}d_2)\}.$$

Using the same argument as previous cases, we have $Y_2 = X_2, Y_3 = X_3$. Then $|X_2| =$

$|X_3| = (2^m - 1)(2^m - 3)$.

Next we prove that $Y_4 = X_4$. Let $(d_1', d_2', d_3') \in Y_4$. Then $d_3' = a_{33}^{-1}(a_{11}d_1' + a_{22}d_2')$ implies $a_{11}d_1' + a_{22}d_2' + a_{33}d_3' = 0$. Additionally, since $d_3' \neq 0$ it follows that $a_{11}d_1' \neq a_{22}d_2'$ i.e., $d_2' \neq a_{22}^{-1}a_{11}d_1' = d_1'$. To prove $(d_1', d_2', d_3') \in X_4$, we need to show $d_3' \neq \{d_1', d_2'\}$. If we assume $d_3' = d_1'$ then $d_1' = a_{33}^{-1}(a_{11}d_1' + a_{22}d_2')$ which implies $d_2' = (a_{11}+a_{33})a_{22}^{-1}d_1'$, which is not possible. Also, if $d_3' = d_2'$, then $d_2' = a_{33}^{-1}(a_{11}d_1' + a_{22}d_2')$ implies $d_2' = (a_{22}+a_{33})^{-1}a_{11}d_1'$, also not possible. Therefore $(d_1', d_2', d_3') \in T$ and $Y_4 \subseteq X_4$.

Conversely , let $(d_1', d_2', d_3') \in X_4$. Then $d_1' \neq d_2', d_1' \neq d_3', d_1' \neq d_2'$ and $a_{11}d_1' + a_{22}d_2' + a_{33}d_3' = 0$. Since $a_{33}d_3' \neq 0$, we have $a_{11}d_1' \neq a_{22}d_2'$. This implies $d_2' \neq a_{22}^{-1}a_{11}d_1' = d_1'$. Since $d_3' \neq \{d_1', d_2'\}$, then $a_{11}d_1' + a_{22}d_2' \neq a_{33}d_1'$ and $a_{11}d_1' + a_{22}d_2' \neq a_{33}d_2'$. This implies $d_2' \neq (a_{11} + a_{33})a_{22}^{-1}d_1'$ and $d_2' \neq (a_{22} + a_{33})^{-1}a_{11}d_1'$ respectively. Thus $(d_1', d_2', d_3') \in Y_4$. Thus $|Y_4| = (2^m - 1)(2^m - 4) = |X_4|$.

Observe that $X_1 \cap X_2 = X_1 \cap X_3 = X_1 \cap X_4 = \phi$. Now we calculate cardinality of $X_2 \cap X_3$. If $(d_1', d_2', d_3') \in X_2 \cap X_3$, then $a_{11}d_1' + a_{33}d_3' = 0$ and $a_{11}d_2' + a_{33}d_3' = 0$. Adding these two equations, we obtain, $a_{11}d_1' + a_{11}d_2' = 0$ which is not possible since $d_1' \neq d_2'$. Therefore we conclude that $X_2 \cap X_3 = \phi$.

Similarly, for the set $X_2 \cap X_4$, assume that $(d_1', d_2', d_3') \in X_2 \cap X_4$. Then $a_{11}d_1' + a_{33}d_3' = 0$ and $a_{11}d_1' + a_{22}d_2' + a_{33}d_3' = 0$. These two equations imply $a_{33}d_3' = 0$ which is not possible. For similar reasons, $X_3 \cap X_4$ is also empty. Therefore,

$$\begin{aligned} |X_1 \cup X_2 \cup X_3 \cup X_4| &= |X_1| + |X_2| + |X_3| + |X_4| \\ &= 2(2^m - 1)(2^m - 3) + (2^m - 1)(2^m - 4) \\ &= (2^m - 1)(3.2^m - 10) \\ \text{and } |X| &= (2^m - 1)(2^m - 2)(2^m - 3) - (2^m - 1)(3.2^m - 10) \\ &= (2^m - 1)(2^{2m} - 8.2^m + 16). \end{aligned}$$

Hence cardinality of S_3'''' is $(2^m - 1)^2(2^m - 2)(2^{2m} - 8.2^m + 16)$. Since the intersection of any two of S_3', S_3'', S_3''' and S_3'''' are empty, cardinality of S_3 is

$$\begin{aligned} |S_3| &= 2(2^m - 1)^2(2^m - 2)(2^m - 4) + (2^m - 1)^2(2^m - 2)(2^{2m} - 8.2^m + 16) \\ &= (2^m - 1)^2(2^m - 2)(2^{2m} - 6 \cdot 2^m + 8). \end{aligned}$$

□

Consider the other two cases similar to S_3 and named them as follows:

$$\begin{aligned} S_4 = \{&(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{11} = a_{33}, a_{22} \neq a_{33}, a_{11}d_1 + a_{22}d_2 \neq 0, \\ &a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\} \end{aligned}$$

$$\begin{aligned} \text{and } S_5 = \{&(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{22} = a_{33}, a_{11} \neq a_{33}, a_{11}d_1 + a_{22}d_2 \neq 0, \\ &a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}. \end{aligned}$$

Then, we have

$$\begin{aligned}|S_3 \cup S_4 \cup S_5| =& 6(2^m-1)^2(2^m-2)(2^m-4) + 3(2^m-1)^2(2^m-2)(2^{2m}-8.2^m+16)\\ =& 3(2^m-1)^2(2^m-2)(2^{2m}-6.2^m+8).\end{aligned}$$

Theorem 4.3.4. *Let S be the set $S = \{(a_{11}, a_{22}, a_{33}, d_1, d_2, d_3) \in (\mathbb{F}_{2^m}^*)^6, m \geq 2 : a_{11}d_1 + a_{22}d_2 \neq 0, a_{11}d_1 + a_{33}d_3 \neq 0, a_{22}d_2 + a_{33}d_3 \neq 0, a_{11}d_1 + a_{22}d_2 + a_{33}d_3 \neq 0\}$. Then cardinality of S is $(2^m-1)^2(2^m-2)(2^{3m}-6.2^{2m}+9.2^m-4)$.*

Proof. Note that, the set S is the disjoint union of S_1, S_2, S_3, S_4 and S_5 i.e., $S_i \cap S_j = \phi$ for all $1 \leq i < j \leq 5$. Therefore, from lemma 4.3.1, 4.3.2 and 4.3.3, we have $|S| = |S_1| + |S_2| + |S_3| + |S_4| + |S_5| = (2^m-1)^2(2^m-2)(2^{3m}-6.2^{2m}+9.2^m-4)$. □

Theorem 4.3.5. *The number of 3×3 semi-involutory MDS matrix over the finite field $\mathbb{F}_{2^m}, m \geq 2$ is $(2^m-1)^4(2^m-2)(2^{3m}-6.2^{2m}+9.2^m-4)$.*

Proof. An MDS semi-involutory matrix is expressed in general form given by the equation (4.16) using only diagonal entries of the matrix and the entries of an associated diagonal matrix. Let $a_{11}, a_{22}, a_{33}, d_1, d_2, d_3$ are those entries and x, y are arbitrary. Since $x, y \in \mathbb{F}_{2^m}^*$, then the number of choices for x and y is $(2^m-1)^2$. Using Theorem 4.2.5 and Theorem 4.3.4, the number of choices for $a_{11}, a_{22}, a_{33}, d_1, d_2$ and d_3 are $(2^m-1)^2(2^m-2)(2^{3m}-6.2^{2m}+9.2^m-4)$. Therefore total number of MDS semi-involutory matrix is $(2^m-1)^4(2^m-2)(2^{3m}-6.2^{2m}+9.2^m-4)$. □

Remark 4.3.6. *In [27] it was proved that the number of 3×3 involutory MDS matrices over $\mathbb{F}_{2^m}, m > 2$ is $(2^m-1)^2(2^m-2)(2^m-4)$. Therefore, there exists total 1176 and 37800, 3×3 involutory MDS matrices over $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^4}$ respectively. However, Theorem 4.3.5 states that there does not exist any 3×3 semi-involutory MDS matrix over $\mathbb{F}_{2^2}$ and the number of 3×3 semi-involutory MDS matrices over $\mathbb{F}_{2^3}$ is 2832576, and over $\mathbb{F}_{2^4}$ is 1913625000.*

4.4 Conclusion

In conclusion, this chapter demonstrates the construction of 3×3 semi-involutory MDS matrices over the finite field $\mathbb{F}_{2^m}$ by using only three diagonal elements and the entries of an associated diagonal matrix. However, the fundamental structure of involutory and semi-involutory MDS matrices of orders greater than four over finite fields of characteristic 2 still poses an unresolved question.

Chapter 5

Cyclic non-MDS matrices

In 1998, Daemen *et al.* introduced a circulant Maximum Distance Separable (MDS) matrix in the diffusion layer of the Rijndael block cipher, drawing significant attention to circulant MDS matrices. This block cipher is now universally acclaimed as the AES block cipher. After that, in 2016, Liu and Sim introduced cyclic matrices by changing the permutation of circulant matrices. While circulant matrices have been well-studied in literature, the properties of cyclic matrices are not. Back in 1961, Friedman introduced the notion of g-circulant matrices to study the eigenvalues of composite matrices. This chapter studies the properties of circulant and g-circulant matrices, generalizing them to cyclic matrices. We also establish a permutation equivalence between cyclic and circulant matrices and provide a detailed structure of the associated permutation matrices. In the last section, we find the determinant of g-circulant matrices of order $2^d \times 2^d$ and prove that they cannot be simultaneously orthogonal and MDS over a finite field of characteristic 2. Furthermore, we prove that this result holds for any cyclic matrix. The work presented in this chapter is given in [69].

5.1 Introduction

One significant limitation of the AES circulant matrix lies in the complexity of implementing its inverse. Therefore, construction of a circulant MDS matrix with orthogonal or involutory properties has become an important research topic. In this direction, Gupta and Ray [30, 31] proved the non-existence of MDS property in circulant orthogonal matrices of order $2^d \times 2^d$ (Theorem 1.2.29) over the finite field $\mathbb{F}_{2^m}$. They also established the non-existence of circulant involutory matrices of order $n \geq 3$ (Theorem 1.2.30) over the finite fields of characteristic 2.
Consequently, many researchers have sought to extend the circulant matrix property for constructing MDS matrices with involutory or orthogonal characteristics. In [32, 33], Sarkar and Syed studied Toeplitz matrices with orthogonal and involutory properties and found some non-existence results. Following that, in 2016, Liu and Sim [25] introduced cyclic matrices as an extension of circulant matrices. Their initial proof showcased the existence of left-circulant involutory matrices with the MDS property, noting that left-circulant matrices form a subclass of cyclic matrices. We revisit the definition of cyclic matrices from Definition 2.2.15.

Definition 5.1.1. *For a k-cycle $\rho \in S_k$, a matrix $\mathfrak{C}_\rho$ of order $k \times k$ is called cyclic matrix if each subsequent row is ρ-permutation of the previous row. We represent this matrix as*

cyclic$_\rho(c_0, c_1, c_2, \ldots, c_{k-1})$*, where* $(c_0, c_1, c_2, \ldots, c_{k-1})$ *is the first row of the matrix. The* (i, j)*-th entry of* $\mathfrak{C}_\rho$ *can be expressed as* $\mathfrak{C}_\rho(i, j) = c_{\rho^{-i}(j)}$.

For example, the matrix $cyclic_\rho(c_0, c_1, c_2, \ldots, c_{k-1})$, where $\rho = (0\ 1\ 2 \cdots\ k-1) \in S_k$ results in a circulant matrix. Similarly, if we use $\rho = (0\ k-1\ 1\ 2 \cdots k-2) \in S_k$, we obtain a left-circulant matrix. Note that, a k-cycle of the form $\begin{pmatrix} 0 & 1 & 2 & \cdots & k-1 \\ g & g+1 & g+2 & \cdots & g+k-1 \end{pmatrix}$, where $g+i$ is calculated modulo k and $\gcd(g, k) = 1$ can be written as $(0 \quad g \pmod k \quad 2g \pmod k \quad 3g \pmod k \cdots (k-1)g \pmod k)$. This gives a complete k-cycle because of the next lemma.

Lemma 5.1.2. *Let* $S = \{\alpha g \pmod k,\ \alpha = 0, 1, \ldots, k-1\}$*. Then* S *is a complete residue system modulo* k *if and only if* $\gcd(g, k) = 1$.

Proof. Consider the mapping $\phi : \mathbb{Z}_k \to S$ defined as $\phi(\alpha) = \alpha g \pmod k$. Take arbitrary elements $\alpha_1, \alpha_2 \in \mathbb{Z}_k$ and assume that $\phi(\alpha_1) = \phi(\alpha_2)$. This implies $\alpha_1 g \pmod k = \alpha_2 g \pmod k$ and hence k divides $(\alpha_1 - \alpha_2)g$. Since $\gcd(g, k) = 1$, this implies $\alpha_1 - \alpha_2 = 0 \pmod k$, yielding $\alpha_1 = \alpha_2$. Therefore ϕ is injective and a bijection. Hence proved. □

We now recall the definition of g-circulant matrices from Definition 2.2.9.

Definition 5.1.3. *A* g*-circulant matrix of order* $k \times k$ *is a matrix of the form* $A =$ g*-circulant*$(c_0, c_1, \ldots, c_{k-1}) = \begin{bmatrix} c_0 & c_1 & \cdots & c_{k-1} \\ c_{k-g} & c_{k-g+1} & \cdots & c_{k-1-g} \\ c_{k-2g} & c_{k-2g+1} & \cdots & c_{k-1-2g} \\ \vdots & \vdots & \cdots & \vdots \\ c_g & c_{g+1} & \cdots & c_{g-1} \end{bmatrix}$, *where all subscripts are taken modulo* k.

For $g = 1$, it represents a circulant matrix, and for $g \equiv -1 \pmod k$, it takes the form of a left-circulant matrix. For the case $\gcd(g, k) = 1$, g-circulant matrices represent a subclass of cyclic matrices and otherwise it is not. In this case, the k-cycle of S_k associated with a g-circulant matrix of order $k \times k$ is $\rho = (0 \quad g \pmod k \quad 2g \pmod k \quad 3g \pmod k \cdots (k-1)g \pmod k)$, and ρ^{-1} is of the form $\rho^{-1} = \begin{pmatrix} 0 & 1 & 2 & \cdots & k-1 \\ k-g & k-g+1 & k-g+2 & \cdots & k-1-g \end{pmatrix}$. Thus cyclic matrices corresponding to these cycles are g-circulant matrices.
Consider the following example of cyclic and g-circulant matrix.

Example 5.1.4. *Consider two* 5*-cycles* $\rho_1 = (0\ 2\ 3\ 1\ 4)$ *and* $\rho_2 = (0\ 3\ 1\ 4\ 2)$ *in* S_5*. Then*

$$cyclic_{\rho_1}(c_0, c_1, c_2, c_3, c_4) = \begin{bmatrix} c_0 & c_1 & c_2 & c_3 & c_4 \\ c_4 & c_3 & c_0 & c_2 & c_1 \\ c_1 & c_2 & c_4 & c_0 & c_3 \\ c_3 & c_0 & c_1 & c_4 & c_2 \\ c_2 & c_4 & c_3 & c_1 & c_0 \end{bmatrix},$$

$$\textit{cyclic}_{\rho_2}(c_0, c_1, c_2, c_3, c_4) = \begin{bmatrix} c_0 & c_1 & c_2 & c_3 & c_4 \\ c_2 & c_3 & c_4 & c_0 & c_1 \\ c_4 & c_0 & c_1 & c_2 & c_3 \\ c_1 & c_2 & c_3 & c_4 & c_0 \\ c_3 & c_4 & c_0 & c_1 & c_2 \end{bmatrix}.$$

Observe that $\textit{cyclic}_{\rho_2}(c_0, c_1, c_2, c_3, c_4)$ *is a* 3*-circulant matrix.*

5.2 Structure of cyclic matrices and their connection with g-circulant matrices

In this section we first show that we are only interested in the case $\gcd(k, g) = 1$. This restriction is vital because if $\gcd(k, g) > 1$, these g-circulant matrices are singular and hence never be MDS. To justify this, we use Lemma 5.1.2.

Theorem 5.2.1. *Let* A *be a* g*-circulant matrix of order* $k \times k$*. If* $\gcd(g, k) > 1$*, then* A *cannot be an MDS matrix.*

Proof. Let $A = (a_{i,j})$ be a g-circulant matrix and $\gcd(k, g) = d$. Then there exists k_1, k_2 such that $k = dk_1, g = dk_2$ and $\gcd(k_1, k_2) = 1$. In a g-circulant matrix, the entries satisfy the relation $a_{i,j} = a_{i+1,j+g}$ for $0 \leq i, j \leq k-1$, with suffixes calculated modulo k. The entries of the first row of A are $(a_{0,0}, a_{0,1}, a_{0,2}, \ldots, a_{0,n-1})$. According to Lemma 5.1.2, there exits an integer $\alpha, 1 < \alpha \leq k-1$ such that $\alpha g = 0 \pmod{k}$. Consequently, we have

$A(0,0) = A(1,g) = A(2,2g) = \cdots = A(\alpha, 0) = a_{0,0}$, and
$A(0,j) = A(1,g+i) = A(2,2g+j) = \cdots = A(\alpha, \alpha g + j) = a_{0,j}$, for all $j = 0, 1, \ldots, k-1$.

Therefore, first row and α-th row are identical and A cannot be an MDS matrix. □

We revisit the representation of g-circulant matrices using permutation matrices from Theorem 2.2.14.

Theorem 5.2.2. *Let* $A = g\textit{-circulant}(c_0, c_1, \ldots, c_{k-1})$ *with* $\gcd(k, g) = 1$*. Then* A *can be expressed as* $A = \sum_{i=0}^{k-1} c_i Q_g P^i$*, where* $P = \textit{circulant}(0, 1, 0, \ldots, 0)$ *and* $Q_g = g\textit{-circulant}(1, 0, 0, \ldots, 0)$.

Our subsequent objective is to establish an analogue of Theorem 5.2.2 for cyclic matrices. To achieve this, we first prove a permutation equivalence between a cyclic and a circulant matrix in the following theorem.

Theorem 5.2.3. *Let* $\mathfrak{C}_\rho(c_0, c_1, \ldots, c_{k-1})$ *be a cyclic matrix. Then there exists a unique permutation matrix* Q *such that* $\mathfrak{C}Q = \textit{circulant}(c_0, c_{\rho(0)}, c_{\rho^2(0)}, c_{\rho^3(0)}, \ldots, c_{\rho^{k-1}(0)})$.

Proof. Let $\mathfrak{C}_\rho = \text{cyclic}(c_0, c_1, c_2, \ldots, c_{k-1})$. Then by Definition 5.1.1, we have

$$\mathfrak{C}_\rho = (c_{\rho^{-i}(j)}) = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{k-1} \\ c_{\rho^{-1}(0)} & c_{\rho^{-1}(1)} & c_{\rho^{-1}(2)} & \cdots & c_{\rho^{-1}(k-1)} \\ c_{\rho^{-2}(0)} & c_{\rho^{-2}(1)} & c_{\rho^{-2}(2)} & \cdots & c_{\rho^{-2}(k-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ c_{\rho^{-(k-1)}(0)} & c_{\rho^{-(k-1)}(1)} & c_{\rho^{-(k-1)}(2)} & \cdots & c_{\rho^{-(k-1)}(k-1)} \end{bmatrix}.$$

Consider the permutation matrix Q with $(i,j)-$th entry is given by the rule

$$Q(i,j) = \begin{cases} 1, & \text{if } i = \rho^j(0), j = 0, 1, \ldots, k-1\ ; \\ 0, & \text{otherwise.} \end{cases}$$

Since ρ is a cycle of length k, we have $\rho^i(0) \neq \rho^l(0)$ for $i, l = \{0, 1, 2, \ldots, k-1\}, i \neq l$. Therefore Q is a permutation matrix.

Let $\mathfrak{C}Q = \mathcal{C}$. We prove that $\mathcal{C}$ is a circulant matrix by showing that i-th row of $\mathcal{C}$ is a right shift of $(i-1)$-th row for $i = 0, 1, \ldots, k-1$, i.e., $\mathcal{C}(i,j) = \mathcal{C}(i-1, j-1)$ for $1 \leq i, j \leq k-1$. We will establish this property through induction on i.

For the base case, consider $i = 0$. Evaluating $\mathcal{C}(0,0)$ we get, $\mathcal{C}(0,0) = \sum_{l=0}^{k-1} \mathfrak{C}_\rho(0,l)Q(l,0) = \mathfrak{C}_\rho(0,0)Q(0,0) = c_0$, since $Q(0,0) = 1$ and $Q(l,0) = 0$ for $l = 2, 3, \ldots, k-1$.

Calculating similarly the other entries of this row, we get $\mathcal{C}(0,j) = \sum_{l=0}^{k-1} \mathfrak{C}_\rho(0,l)Q(l,j) = \mathfrak{C}_\rho(0, \rho^j(0))Q(\rho^j(0), j) = c_{\rho^j(0)}$. This holds because $Q(\rho^j(0), j) = 1$ and the other entries of the j-th column of Q are 0. Consequently, the first row (which is row-0) of the matrix $\mathcal{C}$ is given by $(c_0, c_{\rho(0)}, c_{\rho^2(0)}, c_{\rho^3(0)}, \ldots, c_{\rho^{k-1}(0)})$.

Next we prove the statement for $i = 1$.

Evaluating $\mathcal{C}(1,j)$ for $j = 0, 1, \ldots, k-1$, we get $\mathcal{C}(1,j) = \sum_{l=0}^{k-1} \mathfrak{C}_\rho(1,l)Q(l,j) = \mathfrak{C}_\rho(1, \rho^j(0))Q(\rho^j(0), j) = c_{\rho^{-1}(\rho^j(0))} = c_{\rho^{j-1}(0)} = \mathcal{C}(0, j-1)$. This relationship holds true due to the definitions of both Q and $\mathfrak{C}_\rho$. Therefore the row R_1 of $\mathcal{C}$ is $(c_{\rho^{k-1}(0)}, c_0, c_{\rho(0)}, c_{\rho^2(0)}, c_{\rho^3(1)}, \ldots, c_{\rho^{k-2}(0)})$.

With this, the validity of the induction hypothesis for both $i = 0, 1$ are proved. Using induction hypothesis, we assume that the i-th row can be represented as $(c_{\rho^{k-i}(0)}, c_{\rho^{k-i+1}(0)}, \ldots, c_{\rho^{k-i+j-1}(0)}, c_{\rho^{k-i+j}(0)}, \ldots, c_{\rho^{k-i-1}(0)})$.

Calculating the first entry of the $(i+1)$-th row, we get $\mathcal{C}(i+1, 0) = \sum_{l=0}^{k-1} \mathfrak{C}_\rho(i+1, l)Q(l,0) = \mathfrak{C}(i+1, 0)Q(0,0) = c_{\rho^{-(i+1)}(0)} = c_{\rho^{k-i-1}(0)} = \mathcal{C}(i, k-1)$. This holds because $Q(0,0) = 1$ and $Q(l,0) = 0$ for $l = 2, 3, \ldots, k-1$. Similarly, by calculating the other entries of the $(i+1)$-th row, we get $\mathcal{C}(i+1, j) = \sum_{l=0}^{k-1} \mathcal{C}(i+1, l)Q(l,j) = \mathfrak{C}(i+1, \rho^j(0))Q(\rho^j(0), j) = c_{\rho^{-(i+1)}(\rho^j(0))} = c_{\rho^{-(i+1)+j}(0)} = c_{\rho^{k-(i+1)+j}(0)} = \mathcal{C}(i, j-1)$ for $j = 1, 2, \ldots, k-1$ by induction hypothesis. Therefore $\mathcal{C}$ is a circulant matrix .

To establish uniqueness, suppose there exists another permutation matrix Q' defined using k-cycle ρ' such that $\mathfrak{C}Q' = \text{circulant}\ (c_0, c_{\rho(0)}, c_{\rho^2(0)}, c_{\rho^3(0)}, \ldots, c_{\rho^{k-1}(0)})$. This implies $\rho^i(0) = \rho'^i(0)$ for $i = 1, \ldots, k-1$. Since both ρ and ρ' are k-cycle permutation, we can

conclude that $\rho = \rho'$ and $Q = Q'$. □

The matrix circulant$(c_0, c_{\rho(0)}, c_{\rho^2(0)}, c_{\rho^3(0)}, \ldots, c_{\rho^{k-1}(0)})$ is referred as the *circulant matrix associated with the cyclic matrix* $\mathfrak{C}_\rho$ throughout the thesis. In the forthcoming result, we establish a noteworthy structure of the permutation matrix Q.

Lemma 5.2.4. *Consider the permutation matrix Q of order $k \times k$ defined as*

$$Q(i,j) = \begin{cases} 1, & \text{if } i = \rho^j(0), j = 0, 1, \ldots, k-1\ ; \\ 0, & \text{otherwise.} \end{cases}$$

Then $Q^{-1} = \text{cyclic}_\rho(1, 0, 0, \ldots, 0)$.

Proof. Since $Q^{-1} = Q^T$, we can express Q^{-1} as follows:

$$Q^{-1}(i,j) = \begin{cases} 1, & \text{if } j = \rho^i(0), i = 0, 1, \cdots, k-1\ ; \\ 0, & \text{otherwise.} \end{cases}$$

Therefore Q^{-1} has 1 at the positions $\{(0,0), (1, \rho(0)), (2, \rho^2(0)), \cdots, (k-1, \rho^{k-1}(0))\}$. Also from Definition 5.1.1, the cyclic matrix $\text{cyclic}_\rho(1, 0, 0, \ldots, 0)$ has 1 at positions $\{(0,0), (1, \rho(0)), (2, \rho^2(0)), \ldots, (k-1, \rho^{k-1}(0))\}$. Hence they are equal. □

Note that, the matrix $Q_\rho = \text{cyclic}_\rho(1, 0, 0, \ldots, 0)$ satisfy $Q_\rho Q_\rho^T = I$ as described in Section 2.2. Next, we prove one of the main theorem of this chapter which is Theorem 1.4.26 and this is a generalization of Theorem 5.2.2.

Theorem 5.2.5. *Let $\mathfrak{C}_\rho(c_0, c_1, c_2, \ldots, c_{k-1})$ be a cyclic matrix. Then $\mathfrak{C}_\rho = \sum_{i=0}^{k-1} a_{\rho^i(0)} P^i Q_\rho$, where $Q_\rho = \text{cyclic}_\rho(1, 0, 0, \ldots, 0)$ corresponding to the k-cycle ρ and $P = \text{circulant}(0, 1, 0, \ldots, 0)$.*

Proof. Since $\mathfrak{C}_\rho$ is a cyclic matrix, applying Theorem 5.2.3 we get a circulant matrix $\mathcal{C} = \text{circulant}(c_0, c_{\rho(0)}, c_{\rho^2(0)}, c_{\rho^3(0)}, \ldots, c_{\rho^{k-1}(0)})$ corresponding to $\mathfrak{C}$. The circulant matrix $\mathcal{C}$ can be written as $\mathcal{C} = c_0 I + c_{\rho(0)} P + c_{\rho^2(0)} P^2 + \cdots + c_{\rho^{k-1}(0)} P^{k-1}$, where $P = \text{circulant}(0, 1, 0, \ldots, 0)$. Therefore, $\mathfrak{C} = c_0 Q^{-1} + c_{\rho(0)} P Q^{-1} + c_{\rho^2(0)} P^2 Q^{-1} + \ldots + c_{\rho^{k-1}(0)} P^{k-1} Q^{-1}$. By using Lemma 5.2.4, we get $Q^{-1} = Q_\rho$. Hence proved. □

An illustration of Theorem 5.2.5 is the following.

Example 5.2.6. *Consider the matrix $\mathfrak{C} = \text{cyclic}_{\rho_1}(c_0, c_1, c_2, c_3, c_4)$ with $\rho_1 = (0\ 2\ 3\ 1\ 4)$ from Example 5.1.4. Then $\mathfrak{C} = c_0 Q_{\rho_1} + c_2 P Q_{\rho_1} + c_3 P^2 Q_{\rho_1} + c_1 P^3 Q_{\rho_1} + c_4 P^4 Q_{\rho_1}$ with Q_{ρ_1} is the matrix*

$$Q_{\rho_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Since g-circulant matrices with $\gcd(k, g) = 1$ are cyclic matrices, we prove that Theorem 5.2.5 is essentially reduced to Theorem 5.2.2 for the k-cycle $(0 \quad g \pmod k \quad 2g \pmod k \quad 3g \pmod k \cdots (k-1)g \pmod k)$ in the following corollary.

Corollary 5.2.7. *Let $\mathfrak{C}_\rho = \text{cyclic}(c_0, c_1, c_2, \ldots, c_{k-1})$ where ρ is the k-cycle permutation $(0 \quad g \pmod k \quad 2g \pmod k \quad 3g \pmod k \cdots (k-1)g \pmod k)$ with $\gcd(g, k) = 1$. Then $\mathfrak{C}_\rho = \sum_{i=0}^{k-1} a_i Q_g P^i$, where $P = \text{circulant}(0, 1, 0, \ldots, 0)$ and $Q_g = g\text{-circulant}(1, 0, 0, \ldots, 0)$.*

Proof. Since $\mathfrak{C}_\rho = \text{cyclic } (c_0, c_1, c_2, \ldots, c_{k-1})$, applying Theorem 5.2.5 we get

$$\mathfrak{C}_\rho = c_0 Q_\rho + c_{\rho(0)} P Q_\rho + c_{\rho^2(0)} P^2 Q_\rho + \cdots + c_{\rho^{k-1}(0)} P^{k-1} Q_\rho,$$

where $Q_\rho = \text{cyclic}_\rho(1, 0, 0, \ldots, 0)$. Note that $Q_\rho = Q_g$. Using Lemma 2.2.12 and substituting $\rho(0) = g, \rho^i(0) = ig, 1 \leq i \leq k-1$ we get

$$\mathfrak{C}_\rho = c_0 Q_g + c_g Q_g P^g + c_{2g} Q_g P^{2g} + c_{3g} Q_g P^{3g} + \cdots + c_{(k-1)g} Q_g P^{(k-1)g},$$

where $\{ig, 1 \leq i \leq k-1\}$ are calculated modulo k. Using Lemma 5.1.2, we can simply it further to

$$\mathfrak{C}_\rho = c_0 Q_g + c_1 Q_g P + c_2 Q_g P^2 + \cdots + c_{(k-1)} Q_g P^{(k-1)}.$$

This completes the proof. □

To determine the number of circulant matrices with same branch number, Liu and Sim [25] introduced an equivalence relation between two circulant matrices $\mathcal{C} = \text{circulant}(c_0, c_1, \ldots, c_{k-1})$ and $\mathcal{C}_\sigma = \text{circulant}(c_{\sigma(0)}, c_{\sigma(1)}, \ldots, c_{\sigma(k-1)})$. Their result is noted in Theorem 1.2.34.

In Theorem 5.2.3, we established a permutation equivalence between the cyclic matrix $\mathfrak{C}_\rho$ and the circulant matrix $\mathcal{C} = \text{circulant}(c_0, c_{\rho(0)}, c_{\rho^2(0)}, c_{\rho^3(0)}, \ldots, c_{\rho^{k-1}(0)})$, where $\rho \in S_k$ is a cycle of length k. Therefore these two matrices have same branch number by Theorem 2.4.15. To determine when two cyclic matrices have the same branch number, we need to prove an equivalence relation between them. This is accomplished in the following theorem.

Theorem 5.2.8. *Let $\mathfrak{C}_{\rho_1}$ and $\mathfrak{C}_{\rho_2}$ be two cyclic matrices with first row $(c_0, c_1, \ldots, c_{k-1})$. Then $\mathfrak{C}_{\rho_1} \sim_{P.E} \mathfrak{C}_{\rho_2}$ if and only if their corresponding circulant matrices are permutation equivalent.*

Proof. Let $\mathfrak{C}_{\rho_1}$ be permutation equivalent $\mathfrak{C}_{\rho_2}$. Then there exists permutation matrices P_1, P_2 such that $P_1 \mathfrak{C}_{\rho_1} P_2 = \mathfrak{C}_{\rho_2}$. From Theorem 5.2.3, we get two permutation matrices Q_{ρ_1} and Q_{ρ_2} such that $\mathfrak{C}_{\rho_1} Q_{\rho_1} = \mathcal{C}_1$ and $\mathfrak{C}_{\rho_2} Q_{\rho_2} = \mathcal{C}_2$. This implies $P_1 \mathcal{C}_1 Q_{\rho_1}^{-1} P_2 = \mathcal{C}_2 Q_{\rho_2}^{-1}$. This can be written as $P_1 \mathcal{C}_1 P_3 = \mathcal{C}_2$ where $P_3 = Q_{\rho_1}^{-1} P_2 Q_{\rho_2}$. Since P_3 is also a permutation matrix, we get $\mathcal{C}_1 \sim_{P.E} \mathcal{C}_2$.

Conversely, let $\mathcal{C}_1 \sim_{P.E} \mathcal{C}_2$. Then there exists permutation matrices P_1, P_2 such that $P_1 \mathcal{C}_1 P_2 = \mathcal{C}_2$. Since $\mathcal{C}_1$ and $\mathcal{C}_2$ corresponds to $\mathfrak{C}_{\rho_1}$ and $\mathfrak{C}_{\rho_2}$ respectively, we have $P_1 \mathfrak{C}_{\rho_1} Q_{\rho_1} P_2 = \mathfrak{C}_{\rho_2} Q_{\rho_2}$. This implies $P_1 \mathfrak{C}_{\rho_1} P_3 = \mathfrak{C}_{\rho_2}$ where $P_3 = Q_{\rho_1} P_2 Q_{\rho_2}^{-1}$. □

This theorem is illustrated in the following example.

Example 5.2.9. *Let* $\mathfrak{C}_{\rho_1}$ = *cyclic* $(c_0, c_1, c_2, c_3, c_4)$ *with* $\rho_1 = (0\ 2\ 4\ 1\ 3)$ *and* $\mathfrak{C}_{\rho_2}$ = *cyclic* $(c_0, c_1, c_2, c_3, c_4)$ *with* $\rho_2 = (0\ 3\ 1\ 4\ 2)$.
Then

$$\mathfrak{C}_{\rho_1} = \begin{bmatrix} c_0 & c_1 & c_2 & c_3 & c_4 \\ c_3 & c_4 & c_0 & c_1 & c_2 \\ c_1 & c_2 & c_3 & c_4 & c_0 \\ c_4 & c_0 & c_1 & c_2 & c_3 \\ c_2 & c_3 & c_4 & c_0 & c_1 \end{bmatrix} \text{ and } \mathfrak{C}_{\rho_2} = \begin{bmatrix} c_0 & c_1 & c_2 & c_3 & c_4 \\ c_2 & c_2 & c_4 & c_0 & c_1 \\ c_4 & c_0 & c_1 & c_2 & c_3 \\ c_1 & c_2 & c_3 & c_4 & c_0 \\ c_3 & c_4 & c_0 & c_1 & c_2 \end{bmatrix}.$$

Here $P_1\mathfrak{C}_{\rho_1}P_2 = \mathfrak{C}_{\rho_2}$ *where* $P_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$ *and* $P_2 = I_5$.
Circulant matrices corresponding to $\mathfrak{C}_{\rho_1}$ *and* $\mathfrak{C}_{\rho_2}$ *are* $\mathcal{C}_1$ = *circulant*$(c_0, c_2, c_4, c_1, c_3)$ *and* $\mathcal{C}_2$ = *circulant*$(c_0, c_3, c_1, c_4, c_2)$ *respectively. Calculating* $P_1\mathcal{C}_1P_3$ *where* $P_3 = Q_{\rho_1}^{-1}Q_{\rho_2}$, *where* Q_{ρ_1} *and* Q_{ρ_2} *are as defined in Theorem 5.2.3, we get* $\mathcal{C}_2$. *This implies* $\mathcal{C}_1 \sim_{P.E} \mathcal{C}_2$.
On the other way, $\mathcal{C}_1 = \begin{bmatrix} c_0 & c_2 & c_4 & c_1 & c_3 \\ c_3 & c_0 & c_2 & c_4 & c_1 \\ c_1 & c_3 & c_0 & c_2 & c_4 \\ c_4 & c_1 & c_3 & c_0 & c_2 \\ c_2 & c_4 & c_1 & c_3 & c_0 \end{bmatrix}$ *and* $\mathcal{C}_2 = \begin{bmatrix} c_0 & c_3 & c_1 & c_4 & c_2 \\ c_2 & c_0 & c_3 & c_1 & c_4 \\ c_4 & c_2 & c_0 & c_3 & c_1 \\ c_1 & c_4 & c_2 & c_0 & c_3 \\ c_3 & c_1 & c_4 & c_2 & c_0 \end{bmatrix}$.
Consider $P_1 = P_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$. *Then we get* $P_1\mathcal{C}_1P_2 = \mathcal{C}_2$. *It is easy to check that* $P_3 = Q_{\rho_1}P_2Q_{\rho_2}^{-1} = I_5$. *Thus* $P_1\mathfrak{C}_{\rho_1}I_5 = \mathfrak{C}_{\rho_2}$ *and this implies* $\mathfrak{C}_{\rho_1} \sim_{P.E} \mathfrak{C}_{\rho_2}$.

5.3 g-Circulant matrices with orthogonal property

To investigate the orthogonal property of $2^d \times 2^d$ circulant MDS matrices over the finite fields of characteristic 2, Gupta and Ray [30] proved that A^{2^d} is a scaler matrix, where A is a circulant matrix. Subsequently, Liu and Sim extended these findings to the left-circulant case in [25]. Given that left-circulant matrices exhibit symmetry, the properties of being involutory and orthogonal are synonymous. However, that is not the case for all other g-circulant matrices. Therefore, this section is dedicated to the examination of g-circulant matrices of order $2^d \times 2^d$, with a specific focus on their orthogonal attributes, as outlined in Theorem 1.4.28. Preceding the theorem, we prove three intermediate lemmas.

Lemma 5.3.1. *For any odd integer* $g > 1$, *and for any positive integer* d, 2^d *divides* $\frac{g^{2^d}-1}{g-1}$.

Proof. $\frac{g^{2^d}-1}{g-1} = (g+1)(g^2+1)(g^{2^2}+1)\cdots(g^{2^{d-1}}+1)$. Since g is an odd number, $(g+1), (g^2+1), \ldots, (g^{2^{d-1}}+1)$ are all even numbers. Hence, each term is divisible by 2 and there are d such terms. Therefore 2^d divides the product. □

Lemma 5.3.2. *Let $A = g$-circulant$(c_0, c_1, c_2, \ldots, c_{2^d-1})$ be a matrix with entries from the finite field $\mathbb{F}_{2^m}$, where g is an odd integer greater than 1. Then $A^{2^d} = (c_0^{2^d} + c_1^{2^d} + c_2^{2^d} + \cdots + c_{2^d-1}^{2^d})I$.*

Proof. Let $A = g$-circulant$(c_0, c_1, c_2, \ldots, c_{2^d-1})$. Applying Theorem 5.2.2, we express A as

$$A = c_0 Q_g + c_1 Q_g P + c_2 Q_g P^2 + \cdots + c_{2^d-1} Q_g P^{2^d-1}.$$

Consequently,

$$\begin{aligned} A^{2^d} &= (c_0 Q_g + c_1 Q_g P + c_2 Q_g P^2 + \cdots + c_{2^d-1} Q_g P^{2^d-1})^{2^d} \\ &= c_0^{2^d} Q_g^{2^d} + c_1^{2^d} (Q_g P)^{2^d} + c_2^{2^d} (Q_g P^2)^{2^d} + \cdots + c_{k-1}^{2^d} (Q_g P^{k-1})^{2^d}. \end{aligned}$$

Since $P = $ circulant$(0, 1, 0, \ldots, 0)$ is a $2^d \times 2^d$ permutation matrix, we can easily see that $P^{2^d} = I$. Additionally, $Q_g = g$-circulant$(1, 0, 0, \ldots, 0)$ is a $2^d \times 2^d$ matrix. By applying Lemma 2.2.10, we can say $Q_g^{2^d}$ is a g^{2^d}-circulant matrix. Since $g^{\phi(2^d)} = g^{2^{d-1}} \equiv 1 \pmod{2^d}$, where ϕ is the phi-function, we have $g^{2^d} \equiv 1 \pmod{2^d}$ by squaring both sides. This implies, $Q_g^{2^d} = I$. Therefore,

$$\begin{aligned} A^{2^d} = c_0^{2^d} Q_g^{2^d} &+ c_1^{2^d} Q_g^{2^d} P^{\frac{g^{2^d}-1}{g-1}} + c_2^{2^d} Q_g^{2^d} P^{\frac{2(g^{2^d}-1)}{g-1}} + c_3^{2^d} Q_g^{2^d} P^{\frac{3(g^{2^d}-1)}{g-1}} + \cdots \\ &+ c_{k-1}^{2^d} Q_g^{2^d} P^{\frac{(k-1)(g^{2^d}-1)}{g-1}}. \end{aligned}$$

Since $\frac{n(g^{2^d}-1)}{g-1} \equiv 0 \pmod{2^d}$, we get $P^{\frac{n(g^{2^d}-1)}{g-1}} = I$. Therefore $A^{2^d} = (c_0^{2^d} + c_1^{2^d} + c_2^{2^d} + \cdots + c_{2^d-1}^{2^d})I$. □

Using this lemma we can say about determinant of g-circulant matrices.

Lemma 5.3.3. *Let $A = g$-circulant$(c_0, c_1, c_2, \ldots, c_{2^d-1})$ be a matrix with entries from the finite field $\mathbb{F}_{2^m}$ and g be an odd integer. Then $\det(A) = (\sum_{i=0}^{2^d-1} c_i)^{2^d}$.*

Proof. Let A be g-circulant$(c_0, c_1, \ldots, c_{2^d-1})$ and $\det A = \triangle$. Then $\triangle^{2^d} = (\det A)^{2^d} = \det(A^{2^d})$. From Lemma 5.3.2 and Lemma 4 of [31], $A^{2^d} = (\sum_{i=0}^{2^d-1} c_i^{2^d})I$. So, $\triangle^{2^d} = (\sum_{i=0}^{2^d-1} c_i^{2^d})^{2^d}$. This implies, $\triangle = \sum_{i=0}^{2^d-1} c_i^{2^d} = (\sum_{i=0}^{2^d-1} c_i)^{2^d}$. □

Now we are ready to give the proof of Theorem 1.4.28.

Theorem 5.3.4. *Let A be a $2^d \times 2^d$ g-circulant orthogonal matrix over $\mathbb{F}_{2^m}$ and g be an odd integer. Then A is not an MDS matrix.*

Proof. Let $A = g\text{-circulant}(c_0, c_1, \ldots, c_{2^d-1})$. Let the rows of A are denoted as $R_0, R_1, \ldots, R_{2^d-1}$ with R_0 being same for all of them. Since A is orthogonal, $R_0 \cdot R_j = 0$ for $j = 1, 2, \cdots, 2^d - 1$. Consider the product $R_0 \cdot R_j = 0$ for $j = \{(2k+1)g \pmod{2^d},\ k = 0, 1, \ldots, 2^{d-2} - 1\}$. These products lead to the following equations:

$$\sum_{i=0}^{2^d-1} c_i c_{i+1} = 0, \sum_{i=0}^{2^d-1} c_i c_{i+3} = 0, \sum_{i=0}^{2^d-1} c_i c_{i+5} = 0, \cdots, \sum_{i=0}^{2^d-1} c_i c_{i+2^{d-1}-1} = 0,$$

where suffixes are modulo 2^d. Adding these equations yields

$$(c_0 + c_2 + \cdots + c_{2^d-2})(c_1 + c_3 + \cdots + c_{2^d-1}) = 0$$

Note that g-circulant$(c_0, c_2, \ldots, c_{2^d-2})$ and g-circulant$(c_1, c_3, \ldots, c_{2^d-1})$ are two $2^{d-1} \times 2^{d-1}$ submatrices of A. Therefore according to Lemma 5.3.3, either one of two submatrices is singular. Therefore A is not MDS. □

In the case of order 4×4, there are only two distinct g-circulant matrices: the circulant and the left-circulant matrices. However, when the order is $2^d \times 2^d, d > 2$, total 2^{d-1} different g-circulant matrices exists, corresponding to $g = 1, 3, 5, \ldots, 2^d - 1$. Notably, for $g = 1$ we obtain a circulant matrix, and for this, our findings are reduced to the first three results presented in Section 3 of [31]. On the other hand, for the case $g = 2^d - 1$, resulting matrix is left-circulant. In this scenario, Theorem 5.3.4 provide a more general proof of the results presented in Section 5.2 of [25].
In the next section, we discuss about cyclic matrices with orthogonal property.

5.4 Cyclic matrices with orthogonal property

We begin this section with an alternative proof of theorem 5.3.4 using the fact that the permutation matrices are orthogonal. This proof holds for a more general class, i.e., for cyclic matrices. Although this proof is compact, it does not describe any properties of cyclic matrices like the determinant or scaler structure. But for the sake of completeness, we record the proof here.

Theorem 5.4.1. *Let $\mathfrak{C}$ be a $2^d \times 2^d$ cyclic orthogonal matrix over $\mathbb{F}_{2^m}$. Then $\mathfrak{C}$ is not MDS.*

Proof. Let $\mathfrak{C}$ be a $2^d \times 2^d$ cyclic orthogonal MDS matrix over $\mathbb{F}_{2^m}$. Then $\mathfrak{C}\mathfrak{C}^T = I$. From Theorem 5.2.3 there exists a permutation matrix Q such that $\mathfrak{C}Q = \mathcal{C}$, where $\mathcal{C}$ is a circulant matrix. Using the fact $Q^{-1} = Q_\rho$, we get $\mathfrak{C} = \mathcal{C}Q_\rho$. Since Q_ρ is a permutation matrix, it is orthogonal. Therefore $\mathfrak{C}\mathfrak{C}^T = \mathcal{C}Q_\rho(\mathcal{C}Q_\rho)^T = \mathcal{C}Q_\rho Q_\rho^T \mathcal{C}^T = \mathcal{C}\mathcal{C}^T = I$. Therefore $\mathcal{C}$ is a $2^d \times 2^d$ circulant orthogonal matrix over $\mathbb{F}_{2^m}$. It is also MDS from Corollary 2.4.16. This leads to a contradiction. □

According to Remark 5 in [31], circulant orthogonal MDS matrices of orders other than $2^d \times 2^d$ exist over the finite fields of characteristic 2. For example, $\mathcal{C}_1 = \text{circulant}(a, 1 +$

$a^2+a^3+a^4+a^6, a+a^2+a^3+a^4+a^6)$ and $\mathcal{C}_2 =$ circulant$(1, 1, a, 1+a^2+a^3+a^5+a^6+a^7, a+a^5, a^2+a^3+a^6+a^7)$ are two examples of circulant MDS matrices with orthogonal property over the finite field $\mathbb{F}_{2^8}$ with the irreducible polynomial $x^8+x^4+x^3+x+1$.
Similarly cyclic MDS matrices with orthogonal property can be found for orders other than $2^d \times 2^d$. For instance, in the symmetric group S_3, only two cycles of order 3 exist, which are $\rho_1 = (0\ 1\ 2)$ and $\rho = (0\ 2\ 1)$. This cycle ρ_1 produce the circulant matrix $\mathcal{C}_1$, while the cycle ρ_2 yields the left-circulant matrix $\mathfrak{C}_{\rho_2} =$ left-circulant $(a, 1+a^2+a^3+a^4+a^6, a+a^2+a^3+a^4+a^6)$. This matrix is an orthogonal (involutory) MDS matrix.
In the symmetric group S_6, consider the 6-cycle $\rho = (0\ 2\ 4\ 3\ 5\ 1)$. Consider the cyclic matrix $\mathfrak{C}_\rho$ with first row $(1, a^2+a^3+a^6+a^7, 1, 1+a^2+a^3+a^5+a^6+a^7, a, a^5+a)$. Then the matrix is $\mathfrak{C}_\rho =$

$$\begin{bmatrix} 1 & a^2+a^3+a^6+a^7 & 1 & 1+a^2+a^3+a^5+a^6+a^7 & a & a^5+a \\ a^2+a^3+a^6+a^7 & a^5+a & 1 & a & 1 & 1+a^2+a^3+a^5+a^6+a^7 \\ a^5+a & 1+a^2+a^3+a^5+a^6+a^7 & a^2+a^3+a^6+a^7 & 1 & 1 & a \\ 1+a^2+a^3+a^5+a^6+a^7 & a & a^5+a & 1 & a^2+a^3+a^6+a^7 & 1 \\ a & 1 & 1+a^2+a^3+a^5+a^6+a^7 & a^2+a^3+a^6+a^7 & a^5+a & 1 \\ 1 & 1 & a & a^5+a & 1+a^2+a^3+a^5+a^6+a^7 & a^2+a^3+a^6+a^7 \end{bmatrix}.$$

According to Theorem 5.2.3, the circulant matrix corresponding to $\mathfrak{C}_\rho$ is $\mathcal{C} =$ circulant $(1, 1, a, 1+a^2+a^3+a^5+a^6+a^7, a+a^5, a^2+a^3+a^6+a^7)$. This matrix is orthogonal and MDS. Therefore $\mathfrak{C}_\rho$ is also orthogonal and MDS.
The general result is presented in the following theorem and the proof is straightforward using the identity $PP^T = I$ for any permutation matrix P.

Theorem 5.4.2. *Let $\mathfrak{C}$ be a cyclic matrix of order k, $k \neq 2^d$. Then $\mathfrak{C}$ is an MDS orthogonal matrix if and only if the corresponding circulant matrix is an MDS orthogonal matrix.*

Proof. Let $\mathfrak{C}$ be a cyclic MDS matrix and $\mathfrak{C}\mathfrak{C}^T = I$. From Theorem 5.2.3, there exists a permutation matrix Q such that $\mathfrak{C}Q$ is a circulant matrix say $\mathcal{C}$. Then $\mathfrak{C} = \mathcal{C}Q^{-1} = \mathcal{C}Q^T$, since Q is a permutation matrix. Therefore $\mathcal{C}\mathcal{C}^T = \mathfrak{C}Q(\mathfrak{C}Q)^T = \mathfrak{C}QQ^T\mathfrak{C} = \mathfrak{C}\mathfrak{C}^T = I$. Also $\mathcal{C}$ is MDS by Corollary 2.4.16 . □

5.5 Conclusion

In conclusion, this chapter has offered a comprehensive exploration of cyclic matrices and their connection with g-circulant and circulant matrices. Additionally, cyclic orthogonal matrices with the MDS property have been investigated. An open area for further investigation lies in studying the properties of g-circulant and cyclic matrices with orders other than $2^d \times 2^d$ over finite fields.

Chapter 6

MDS property of g-circulant matrices

In the previous chapter, we explored a generalized form of circulant matrices known as cyclic matrices, and a specific subclass referred to as g-circulant matrices. In this chapter, we undertake a more comprehensive study of g-circulant matrices. In the initial section, our focus is on g-circulant matrices endowed with MDS and involutory properties. Additionally, we provide an affirmative answer to the conjecture raised by Liu and Sim in [25] for g-circulant matrices. In the last section, we present some properties of the associated diagonal matrices of a g-circulant matrix with semi-orthogonal and semi-involutory characteristics. The work presented in this chapter can be found in [70].

6.1 Introduction

In 2016, Liu and Sim [25] conjectured that, there are no involutory MDS cyclic matrices of order $4, 8$ over $\mathbb{F}_{2^m}$. In this chapter, we prove this conjecture for g-circulant matrices, a subclass of cyclic matrices as established in Chapter 5. The permutation $\rho \in S_k$ corresponding to a g-circulant matrix of order $k \times k$ is $(0 \quad g \pmod k \quad 2g \pmod k \quad 3g \pmod k \cdots (k-1)g \pmod k)$. We reiterate the formal definition of a g-circulant matrix here.

Definition 6.1.1. *A g-circulant matrix of order $k \times k$ is a matrix of the form* $A = g\text{-circulant}(c_0, c_1, \ldots, c_{k-1}) = \begin{bmatrix} c_0 & c_1 & \cdots & c_{k-1} \\ c_{k-g} & c_{k-g+1} & \cdots & c_{k-1-g} \\ c_{k-2g} & c_{k-2g+1} & \cdots & c_{k-1-2g} \\ \vdots & \vdots & \cdots & \vdots \\ c_g & c_{g+1} & \cdots & c_{g-1} \end{bmatrix}$, *where all subscripts are taken modulo k.*

Entries of a g-circulant matrix satisfy the relation $A(i,j) = A(i+1, j+g)$, where subscripts are calculated modulo k. Moreover, for a g-circulant matrix $A = (a_{i,j})$, $0 \leq i, j \leq k-1$ with first row $(c_0, c_1, \ldots, c_{k-1})$, we have $A(i,j) = c_{j-ig \pmod k}$.
In the previous chapter, we explained that to construct an MDS g-circulant matrix, we consider only the case $\gcd(g,k) = 1$, as emphasized in Theorem 5.2.1. The general structure of g-circulant matrices of order $k \times k$ in terms of permutation matrices under the condition $\gcd(g,k) = 1$, is detailed in Theorem 2.2.14, presented as follows.

Theorem 6.1.2. *Let $A = g\text{-circulant}(c_0, c_1, \ldots, c_{k-1})$ with $\gcd(k,g) = 1$. Then A*

can be expressed as $A = \sum_{i=0}^{k-1} c_i Q_g P^i$, *where* $P = circulant(0, 1, 0, \ldots, 0)$ *and* $Q_g = g\text{-}circulant(1, 0, 0, \ldots, 0)$.

In the case of $\gcd(g, k) = 1$, the inverse of a non-singular g-circulant matrix demonstrates a specific characteristic, as established by [68], Theorem 5.1.4. For completeness, we record the proof here.

Lemma 6.1.3. *Let A be a non-singular g-circulant matrix of order $k \times k$ with $\gcd(g, k) = 1$. Then A^{-1} is g^{-1}-circulant.*

Proof. Since $\gcd(g, k) = 1$, there exists g^{-1} with $gg^{-1} = 1 \pmod{k}$. Now, from Lemma 2.2.12, we have $PA = AP^g$ and thus $A^{-1}P^{-1} = P^{-g}A^{-1}$. Hence

$$\begin{aligned} PA^{-1} &= P^{-g+1}A^{-1}P = P^{-g+1}(A^{-1}P^{-1})P^2 \\ &= P^{-g+1}(P^{-g}A^{-1})P^2 = P^{-2g+1}A^{-1}P^2. \end{aligned}$$

Repeating this s times, we get $PA^{-1} = P^{-sg+1}A^{-1}P^s$. Choosing $s = g^{-1}$, we get $PA^{-1} = A^{-1}P^{g^{-1}}$. Thus A^{-1} is g^{-1}-circulant. □

The transpose of a g-circulant matrix exhibits similar characteristics.

Lemma 6.1.4. *Let A be a g-circulant matrix of order $k \times k$ with $\gcd(g, k) = 1$. Then A^T is g^{-1}-circulant.*

Proof. Given that $A = (a_{i,j}), 0 \leq i, j \leq k-1$ is g-circulant matrix, we have $A(i, j) = A(i + 1, j + g)$, i.e., $a_{i,j} = a_{i+1,j+g}\ \forall\ 0 \leq, i, j \leq k-1$, considering subscripts modulo k. Using this property, the entries of A exhibit the following pattern:

$$a_{i,j} = A(i, j) = A(i + 1, j + g) = A(i + 2, j + 2g) = \cdots = A(i + l, j + lg) = a_{i+l,j+lg},$$

where subscripts are calculated modulo k. Consequently, the entry at the i-th row and j-th column repeats at the $j+1$-th column when $j+lg = j+1 \pmod{k}$. Since $\gcd(g, k) = 1$, we have $l = g^{-1}$. Then entries of A^T are $A(j, i)$ and they satisfy $A(j, i) = A(j + 1, i + g^{-1})$ for all $0 \leq j, i \leq k-1$. Thus A^T is g^{-1}-circulant. □

6.2 g-Circulant matrices with MDS and involutory properties

We begin this section with a structure of A^2 where A is a g-circulant matrix.

Theorem 6.2.1. *Let A be a g-circulant matrix of order $k \times k$ with the first row $(c_0, c_1, \ldots, c_{k-1})$ and $\gcd(k, g) = 1$. Then A^2 can be expressed as*

$$A^2 = \sum_{l=0}^{k-1} \left(\sum_{\substack{i,j=0 \\ gi+j=l \pmod{k}}}^{k-1} c_i c_j \right) Q_g^2 P^l,$$

where $Q_g^2 = g^2$*-circulant*$(1, 0, 0, \ldots, 0)$ *and* $P =$ *circulant*$(0, 1, 0, \ldots, 0)$ *are permutation matrices of order* $k \times k$*.*

Proof. Let $A = g$-circulant$(c_0, c_1, \ldots, c_{k-1})$ with $\gcd(k, g) = 1$. Then by Theorem 6.1.2, A can be expressed as $A = \sum_{k=0}^{k-1} c_i Q_g P^i$, where Q_g is a g-circulant matrix. Therefore A^2 an be written as

$$\begin{aligned} A^2 &= (c_0 Q_g + c_1 Q_g P + c_2 Q_g P^2 + c_3 Q_g P^3 + \cdots + c_{k-1} Q_g P^{k-1})^2 \\ &= c_0^2 Q_g^2 + c_1^2 (Q_g P)^2 + \cdots + c_{k-1}^2 (Q_g P^{k-1})^2 + c_0 c_1 Q_g Q_g P + c_0 c_2 Q_g Q_g P^2 + \cdots \\ &\quad + c_{k-2} c_{k-1} Q_g P^{k-2} Q_g P^{k-1} \end{aligned}$$

Using the identity $PQ_g = Q_g P^g$ and $P^k = I$, we can derive that $Q_g P^i Q_g P^{k-ig} = Q_g^2 P^k = Q_g^2$. Therefore, the coefficient of Q_g^2 in A^2 is:

$$\sum_{\substack{i,j=0, \\ gi+j=0 \pmod k}}^{k-1} c_i c_j = c_0^2 + c_1 c_{k-g} + c_2 c_{k-2g} + \cdots + c_{k-1} c_{k-(k-1)g}.$$

Similarly, the coefficient of $Q_g^2 P$ in A^2 can be written as

$$\sum_{\substack{i,j=0, \\ gi+j=1 \pmod k}}^{k-1} c_i c_j = c_0 c_1 + c_1 c_{1+k-g} + c_2 c_{1+k-2g} + \cdots + c_{k-1} c_{1+k-(k-1)g}.$$

Thus using induction, we get the coefficient of $Q_g^2 P^l$ is $\sum_{\substack{i,j=0, \\ gi+j=l \pmod k}}^{k-1} c_i c_j$. Therefore, we can conclude that $A^2 = \sum_{l=0}^{k-1} \left(\sum_{\substack{i,j=0 \\ gi+j=l \pmod k}}^{k-1} c_i c_j \right) Q_g^2 P^l$. □

Utilizing the structure of A^2 from Theorem 6.2.1, we discuss the existence of g-circulant matrices over the finite field $\mathbb{F}_{2^m}$ with both involutory and MDS properties. To begin with, we show the non-existence of g-circulant involutory matrices when $g^2 \not\equiv 1 \pmod k$. The theorem is as follows.

Theorem 6.2.2. *Let* A *be a* g*-circulant matrix of order* $k \times k$ *and* $\gcd(k, g) = 1$*. If* $g^2 \not\equiv 1 \pmod k$*, then* A *cannot be involutory.*

Proof. Let A be a g-circulant matrix of order $k \times k$ and $\gcd(k, g) = 1$. Then A^2 is a g^2-circulant matrix. Therefore $A^2(0, 0) = A^2(1, g^2)$. If A is involutory then $A^2(0, 0) = 1$. But $A^2(1, g^2) = 0$ since $g^2 \not\equiv 1 \pmod k$. This is a contradiction. □

An example illustrating Theorem 6.2.2 is as follows.

Example 6.2.3. *Consider the finite field $\mathbb{F}_{2^8}$ defined by the irreducible polynomial $1+x^2+x^5+x^6+x^8$. Let a be a primitive element of this field. Consider the 3-circulant matrix of order 5×5 with the first row $(1, a, 1+a+a^4+a^5+a^7, 1+a+a^3+a^4+a^5+a^7, a+a^3)$. Here $3^2 \equiv 4 \pmod 5$. The matrix A^2 is a 4-circulant matrix. Then $A^2(0,0) = a^6+1 = A^2(1,4)$. For A to be involutory, we must have $A^2(0,0) = 1$ and $A^2(1,4) = 0$, which is not possible. Consequently, it is evident that A is never involutory.*

The above theorem implies that, to construct a g-circulant matrix with MDS and involutory properties, we only need to focus on the case $g^2 \equiv 1 \pmod k$. First we prove some lemmas and a theorem to determine the number of solutions of the equivalence relation $x^2 \equiv 1 \pmod k$.

Lemma 6.2.4. *Let $k = 2^m$, m positive integer. Then, the number of solutions to the congruence relation $x^2 \equiv 1 \pmod k$ in the residue modulo k is*

$$\begin{cases} 1, & \text{if } m = 1\ ; \\ 2, & \text{if } m = 2\ ; \\ 4, & \text{if } m \geq 3. \end{cases}$$

Proof. For $k = 2$ the only solution of the congruence relation is 1. When $k = 4$ there are two solutions, namely $x = 1, 3$.
Consider the case $k = 2^m, m \geq 3$. It is apparent that $\pm 1 \pmod{2^m}$ are solutions. We will now prove that $2^{m-1} \pm 1 \pmod{2^m}$ also solutions. Consider the square of $2^{m-1} \pm 1$. Then $(2^{m-1} \pm 1)^2 = 2^{2(m-1)} + 1 \pm 2^m = 1 \pmod{2^m}$, since $2^{2(m-1)} \pm 2^m \equiv 0 \pmod{2^m}$.
To establish that these are the only solutions, we will assume that there exists an α such that $\alpha^2 \equiv 1 \pmod{2^m}$ and $\alpha \neq \{\pm 1, 2^{m-1} \pm 1\}$. Furthermore, α must be an odd number and assume $\alpha < 2^{m-1}$. Then α can be expressed as $\alpha = 2^{m-i} \pm 1$ for some i in range $2 \leq i \leq m-1$. Then $\alpha^2 = 2^{2(m-i)} + 1 \pm 2^{m-i+1} = 2^{m-i+1}(2^{m-i+1} \pm 1) + 1 < 2^{m-1}(2^{m-1} \pm 1) + 1$ and therefore α^2 not congruent to 1 modulo 2^m. □

Next, consider the case for an odd prime power in the following lemma.

Lemma 6.2.5. *Let $k = p^m$ where $p \geq 3$ be a prime number. Then the solutions to the congruence $x^2 \equiv 1 \pmod k$ in the residue modulo k are given by $x \equiv \pm 1 \pmod k$.*

Proof. Let $x^2 \equiv 1 \pmod{p^m}$. This implies $p^m | (x+1)(x-1)$. Suppose that $x \neq \pm 1 \pmod{p^m}$. In this case, both $x+1$ and $x-1$ are less than p^m. This implies p divides both $x+1$ and $x-1$. Therefore $p|2$, which is a contradiction to p is an odd prime . □

Applying the Chinese Remainder Theorem one can prove the following theorem.

Theorem 6.2.6. *Let $k = 2^m p_1^{m_1} \cdots p_l^{m_l}$ where p_i's are odd primes and $m, m_i \geq 0$ for $1 \leq i \leq l$.*

Then the number of solutions of the equation $x^2 = 1 \pmod{k}$ *in residue modulo* k *is*

$$\begin{cases} 2^l, & \text{if } m = 0, 1 \text{ ;} \\ 2^{l+1}, & \text{if } m = 2 \text{ ;} \\ 2^{l+2}, & \text{if } m \geq 3. \end{cases}$$

Proof. Using Chinese Remainder Theorem, Lemma 6.2.4 and Lemma 6.2.5 the number of solutions of $x^2 \equiv 1 \pmod{k}$ is $2^i \cdot 2^l$ where

$$i = \begin{cases} 0, & \text{if } m = 0, 1 \text{ ;} \\ 1, & \text{if } m = 2 \text{ ;} \\ 2, & \text{if } m \geq 3. \end{cases}$$

□

In [25], the authors conjectured that cyclic matrices of order $4, 8$ over the finite field $\mathbb{F}_{2^m}$ does not exists. In the following theorem, we substantiate their conjecture within a specific subclass of cyclic matrices. Specifically, we show that g-circulant involutory matrices of order $2^d \times 2^d$ cannot be MDS by proving the existence of a singular submatrix. To establish this, we first demonstrate the presence of a left-circulant matrix as a submatrix in a g-circulant matrix of order $2^d \times 2^d$ for a particular g.

Lemma 6.2.7. *Let* A *be a* g*-circulant matrix of order* $2^d \times 2^d$ *and* $g = 2^{d-1} - 1$. *Let* $(c_0, c_1, c_2, \ldots, c_{2^d-1})$ *be the first row of* A. *Then* A *has two left-circulant submatrices of order* $2^{d-1} \times 2^{d-1}$.

Proof. Let $(c_0, c_1, c_2, \ldots, c_{2^d-1})$ be the first row of A. We denote the i-th row of A by R_i, j-th column by C_j and $A(0, j) = c_j$ for $0 \leq j \leq 2^d - 1$. Consider the entries of the row R_2:

$$A(2, 0) = c_{2^d-2g \pmod{2^d}} = c_{2^d-2(2^{d-1}-1)} = c_2, A(2, 1) = c_3,$$
$$A(2, 2) = c_4, \ldots, A(2, 2^d - 1) = c_{2+2^d-1 \pmod{2^d}} = c_1.$$

Similarly, the entries of the row R_4 are:

$$A(4, 0) = c_{2^d-4g \pmod{2^d}} = c_4, A(4, 1) = c_5,$$
$$A(4, 2) = c_6, \ldots, A(4, 2^d - 1) = c_{4+2^d-1 \pmod{2^d}} = c_3.$$

Continuing this process, we find the entries of row R_{2^d-2} are :

$$A(2^d - 2, 0) = c_{2^d-2}, A(2^d - 2, 1) = c_{2^d-1}, \ldots, A(2^d - 2, 2^d - 1) = c_{2^d-3}.$$

Therefore the rows $R_0, R_2, R_4, \ldots, R_{2^d-1}$ and the columns $C_0, C_2, C_4, \ldots, C_{2^d-2}$ form the left-circulant matrix with the entries of first row $c_0, c_2, c_4, \ldots, c_{2^d-2}$. Similarly, the rows

$R_0, R_2, R_4, \ldots, R_{2^d-1}$ and the columns $C_1, C_3, C_5, \ldots, C_{2^d-1}$ form the left-circulant matrix with the entries of the first row $c_1, c_3, c_5, \ldots, c_{2^d-1}$. □

Note that, if $\mathcal{C}_1$ is a circulant matrix with first row $(c_0, c_1, c_2, \ldots, c_{k-1})$ and $\mathcal{C}_2$ is a left-circulant matrix with same first row, then their determinant is same over the finite field of characteristic 2. We are now ready to prove the theorem.

Theorem 6.2.8. *Let A be a g-circulant matrix of order $2^d \times 2^d$ over a finite field of characteristic 2, where g is odd. Let $(c_0, c_1, c_2, \ldots, c_{2^d-1})$ be the first row of A and $g^2 \equiv 1 \pmod{2^d}$. If A is an involutory matrix, then A can not be an MDS matrix.*

Proof. Consider the g-circulant matrix A of order $2^d \times 2^d$ over $\mathbb{F}_{2^m}$ with first row $(c_0, c_1, c_2, \ldots, c_{2^d-1})$. Given that $g^2 \equiv 1 \pmod{2^d}$, we consider the following cases for the possible values of g:

Case I. For the case $g = 1$, A is a circulant matrix. If A is involutory, then from Lemma 9 of [30] (see Theorem 1.2.30), A can not be MDS.

Case II. For the case $g = 2^d - 1$ the matrix A becomes a left-circulant matrix. Let A be involutory. Since left-circulant matrices are symmetric, which implies they are orthogonal. Therefore A is a $2^d \times 2^d$ left-circulant, orthogonal matrix. Therefore A cannot be MDS follows by the Theorem 5.3.4 of Chapter 5.

Case III. From the Lemma 6.2.4, there exist values of g in the range $1 < g < 2^d - 1$ satisfying $g^2 \equiv 1 \pmod{2^d}$. Note that g is an odd number.

Moreover, A^2 is a circulant matrix according to Theorem 2.2.10. Let A be involutory. Since Q_g^2 is a g^2-circulant matrix and $g^2 \equiv 1 \pmod{2^d}$, we have $Q_g^2 = I$. This implies $Q_g^2 P^l = P^l$ for $0 \leq l \leq k-1$. By utilizing Theorem 6.2.1 and the involutory property, we can deduce that $A^2(0,0) = 1$ and $A^2(0,l) = 0$ for $1 \leq l \leq 2^d - 1$. We calculate the coefficient of $A^2(0, 2^{d-1})$.

$$\begin{aligned} A^2(0, 2^{d-1}) &= \sum_{\substack{i,j=0,\\ gi+j=2^{d-1} \pmod{2^d}}}^{k-1} c_i c_j \\ &= \sum_{\substack{i=0,\\ gi+i=2^{d-1} \pmod{2^d}}}^{k-1} c_i^2 + \sum_{\substack{i\neq j,\ i,j=0,\\ gi+j=2^{d-1} \pmod{2^d}}}^{k-1} c_i c_j \end{aligned}$$

Consider the equation $gi + j = 2^{d-1} \pmod{2^d}$. Since g is invertible, multiply this equation by g^{-1} and using that g has self-inverse, we get $i + gj = g^{-1}2^{d-1} = g2^{d-1} = (2k_1 + 1)2^{d-1} = 2^d k_1 + 2^{d-1} = 2^{d-1} \pmod{2^d}$. Therefore the set $\{(i,j) : gi + j = 2^{d-1} \pmod{2^d}\}$

is same as the set $\{(i,j) : i+gj = 2^{d-1} \pmod{2^d}\}$. Thus, the equation reduces as follows:

$$\begin{aligned} A^2(0, 2^{d-1}) &= \sum_{\substack{i=0, \\ gi+i=2^{d-1} \pmod{2^d}}}^{k-1} c_i^2 + \sum_{\substack{i<j,\ i,j=0, \\ gi+j=2^{d-1} \pmod{2^d}}}^{k-1} 2c_ic_j \\ &= \sum_{\substack{i=0, \\ (g+1)i=2^{d-1} \pmod{2^d}}}^{k-1} c_i^2 \end{aligned}$$

Consider the set $S = \{i : (g+1)i = 2^{d-1} \pmod{2^d}\}$. Note that, if $\alpha \in S$, then the additive inverse of α also belongs to S because $(g+1)(2^d - \alpha) = -(g+1)\alpha = 2^d - 2^{d-1} = 2^{d-1} \pmod{2^d}$. As a result, $|S|$ is even.

From Lemma 6.2.4, the only possibilities for g are $2^{d-1} \pm 1$. First we prove that for $g = 2^{d-1}-1$, if $\alpha \in S$ then $\alpha+2 \in S$. This is evident because $(g+1)(\alpha+2) = 2^{d-1}+2(g+1) = 2^{d-1}+2^d = 2^{d-1} \pmod{2^d}$. Since $1 \in S$ in this scenario, we get $1, 1+2 = 3, 5, \ldots, 2^d-1 \in S$. Also, $2 \notin S$. Hence,

$$A^2(0, 2^{d-1}) = (c_1 + c_3 + \cdots + c_{2^d-1})^2$$

Since A is involutory, this implies $c_1 + c_3 + \cdots + c_{2^d-1} = 0$.

Therefore by Lemma 6.2.7, we get a left-circulant submatrix of order $2^{d-1} \times 2^{d-1}$ with determinant 0 and this implies A is not an MDS matrix.

Next consider the case for $g = 2^{d-1}+1$. First we prove that if $\alpha \in S$ then $\alpha + 2^{d-1} \in S$. This hold because $(g+1)(\alpha + 2^{d-1}) = 2^{d-1} + 2^{d-1}(g+1) = 2^{d-1} + 2^{d-1}(2^{d-1}+2) = 2^{d-1} + 2^d(2^{d-2}+1) = 2^{d-1} \pmod{2^d}$. Furthermore, $2^{d-2} \in S$ because $(g+1)2^{d-2} = (2^{d-1}+2)2^{d-2} = 2^{d-1}(2^{d-1}+1) = 2^{d-1} \pmod{2^d}$. Consequently $2^{d-2}, 2^{d-2}+2^{d-1} \in S$. Thus

$$A^2(0, 2^{d-1}) = (c_{2^{d-2}} + c_{3\cdot 2^{d-2}})^2$$

Since A is involutory, this implies $(c_{2^{d-2}} + c_{3\cdot 2^{d-2}}) = 0$. Consider the 2×2 submatrix of A with entries $A(0, 2^{d-2}), A(0, 3\cdot 2^{d-2}), A(2^{d-1}, 2^{d-2})$ and $A(2^{d-1}, 3\cdot 2^{d-2})$. The entries in the first rows are $A(0, 2^{d-2}) = c_{2^{d-2}}$ and $A(0, 3\cdot 2^{d-2}) = c_{3\cdot 2^{d-2}}$. By calculating the entries of 2^{d-1}-th row, we get

$$\begin{aligned} A(2^{d-1}, 2^{d-2}) &= c_{2^d - 2^{d-1}g + 2^{d-2}} \pmod{2^d} \\ &= c_{2^d - 2^{d-1}(2^{d-1}+1) + 2^{d-2}} \pmod{2^d} = c_{3\cdot 2^{d-2}}, \\ A(2^{d-1}, 3\cdot 2^{d-2}) &= c_{2^d - 2^{d-1}g + 3\cdot 2^{d-2}} \pmod{2^d} \\ &= c_{2^{d-2}(2^2 - 2^d - 2 + 3)} \pmod{2^d} = c_{2^{d-2}} \end{aligned}$$

Hence there exists a 2×2 submatrix of A with determinant 0. Thus A is not MDS. □

Next we consider g-circulant matrices of order other than $2^d \times 2^d$. Let $k = 2^m \prod_{i=1}^{l} p_i^{m_i}, m \geq 0, m_i \geq 1$ and p_i's are odd primes.

Theorem 6.2.9. *Let A be a g-circulant matrix of order $k \times k$ with $\gcd(g,k) = 1$ over a finite field of characteristic 2 with $k = 2^m \prod_{i=1}^{l} p_i^{m_i}, m \geq 0, m_i \geq 1$ and p_i's are odd primes. Let $(c_0, c_1, c_2, \ldots, c_{k-1})$ be the first row of A and $g^2 \equiv 1 \pmod{k}$. If A is an involutory matrix and $1 \leq g < k-1$, then A is not an MDS matrix.*

Proof. **Case I.** Let $g = 1$ i.e., A is a circulant matrix. Then from Lemma 9 of [30] (see Theorem 1.2.30), A is not MDS.

Case II. Let consider the case $1 < g < k-1$. According to Theorem 6.2.6, there exists g in this range with $g^2 \equiv 1 \pmod{k}$.Therefore A^2 is a circulant matrix by Theorem 2.2.10. We now calculate the entry $A^2(0, g+1)$ using Theorem 6.2.1 :

$$\begin{aligned} A^2(0,g+1) &= \sum_{\substack{i,j=0,\\ gi+j=g+1 \pmod{k}}}^{k-1} c_i c_j \\ &= \sum_{\substack{i=0,\\ gi+i=g+1 \pmod{k}}}^{k-1} c_i^2 + \sum_{\substack{i\neq j,\ i,j=0,\\ gi+j=g+1 \pmod{k}}}^{k-1} c_i c_j \end{aligned}$$

Let (i,j) satisfy the equation $gi + j = g + 1 \pmod{k}$. Then (j,i) also satisfy the same because g is self-invertible . This implies $i + gj = 1 + g^{-1} = 1 + g \pmod{k}$. Therefore we can write $A^2(0, g+1)$ as the following:

$$\begin{aligned} A^2(0,g+1) &= \sum_{\substack{i=0,\\ gi+i=g+1 \pmod{k}}}^{k-1} c_i^2 + \sum_{\substack{i<j,\ i,j=0,\\ gi+j=g+1 \pmod{k}}}^{k-1} 2c_i c_j \\ &= \sum_{\substack{i=0,\\ (g+1)i=g+1 \pmod{k}}}^{k-1} c_i^2 \end{aligned}$$

Consider the set $S = \{i : gi + i = g + 1 \pmod{k}\}$. This set is non-empty because $1 \in S$. Note that, there always exists a smallest non-zero integer $\alpha < k$ such that $(1+g)\alpha = 0 \pmod{k}$. This holds because, the conditions $k|(g+1)(g-1)$ and $1 \leq (g+1), (g-1) < k$ implies $\gcd(k, g+1) > 1$. Therefore, such α exists.

Then $1 + \beta\alpha \in S$ for $\beta = \{1, 2, \ldots, \lfloor \frac{k-1}{\alpha} \rfloor\}$, because $(1+g)(1+\beta\alpha) = (1+g) + \beta\alpha(1+g) =$

$1+g \pmod k$. Therefore $A^2(0, g+1)$ can be written as:

$$\begin{aligned} A^2(0,g+1) &= \sum_{\substack{i=0,\\ (g+1)i=g+1 \pmod k}}^{k-1} c_i^2 \\ &= c_1^2 + c_{1+\alpha}^2 + c_{1+2\alpha}^2 + \cdots + c_{1+\lfloor \frac{k-1}{\alpha} \rfloor \alpha}^2 \\ &= (c_1 + c_{1+\alpha} + c_{1+2\alpha} + \cdots + c_{1+\lfloor \frac{k-1}{\alpha} \rfloor \alpha})^2 \end{aligned}$$

Since A is involutory, we get $c_1 + c_{1+\alpha} + c_{1+2\alpha} + \cdots + c_{1+\lfloor \frac{k-1}{\alpha} \rfloor \alpha} = 0$. This equation has $\lfloor \frac{k-1}{\alpha} \rfloor \alpha + 1 = \frac{k}{\alpha}$ number of entries.
Construct the submatrix B of A with order $\frac{k}{\alpha} \times \frac{k}{\alpha}$ as follows: The entries of B are drawn from the rows $R_0, R_\alpha, R_{2\alpha}, \ldots, R_{\lfloor \frac{k-1}{\alpha} \rfloor \alpha}$ and columns $C_1, C_{1+\alpha}, C_{1+2\alpha}, \ldots, C_{1+\lfloor \frac{k-1}{\alpha} \rfloor \alpha}$ of A. The entries of the first row of B are $(c_1, c_{1+\alpha}, c_{1+2\alpha}, \ldots, c_{1+\lfloor \frac{k-1}{\alpha} \rfloor \alpha})$.
To generate the entries of the second row of B, consider the sequence :

$$A(\alpha, 1) = A(\alpha - 1, 1 - g) = A(\alpha - 2, 1 - 2g) = \cdots = A(\alpha - p, 1 - pg) = \cdots .$$

Given that the matrix A is g-circulant, we have $A(\alpha, 1) = A(0, j)$ for some $0 \leq j \leq k-1$. Thus $\alpha - p = 0 \pmod k$ implies $1 - \alpha g = 0 \pmod k$. As $\alpha(1+g) = 0 \pmod k$, this implies $j = 1 + \alpha$. Continuing this process we obtain

$$A(\alpha, 1 + \beta\alpha) = A(\alpha - 1, 1 + \beta\alpha - g) = \cdots = A(0, 1 - \beta\alpha - \alpha g) = A(0, 1 + \alpha(\beta + 1)).$$

Also $A(\alpha, 1 + (\lfloor \frac{k-1}{\alpha} \rfloor + 1)\alpha) = A(0, 1)$ and second row of B is one left-shift of the first row. By calculating in similar manner, we get

$$A(2\alpha, 1 + \beta\alpha) = A(\alpha, 1 + \alpha(\beta + 1)),$$

with the entries calculated modulo k. This implies that the rows of B are left shifts of the previous row, making B a left-circulant matrix of order $\frac{k}{\alpha} \times \frac{k}{\alpha}$. Also determinant of B is zero. Therefore A is not MDS. □

In next case, we prove that it is possible to construct left-circulant involutory MDS under certain conditions. This result is similar of Proposition 6 of [25].

Theorem 6.2.10. *Let A be a left-circulant matrix of order $k \times k$ over a finite field of characteristic 2 with $k = 2^m \prod_{i=1}^{l} p_i^{m_i}, m \geq 0, m_i \geq 1$ and p_i's are primes. Let $(c_0, c_1, c_2, \ldots, c_{k-1})$ be the first row of A. Then A is involutory and MDS if and only if the following conditions holds:*

1. $\sum_{i=0}^{k-1} c_i = 1,$
2. $\sum_{\substack{i,j=0,\\ gi+j=l \pmod k}}^{k-1} c_i c_j = 0, \ 1 \leq l \leq \lfloor \frac{k-1}{2} \rfloor,$

3. *All submatrices of A have non-zero determinant.*

Proof. Consider a left-circulant matrix A of order $k \times k$ over the finite field of characteristic 2 with $k = 2^m \prod_{i=1}^{l} p_i^{m_i}$ and p_i's are primes. Since $g \equiv -1 \pmod{k}$, then from Theorem 2.2.10, A^2 is circulant. Let A be involutory. Then $A^2(0,0) = 1$ and $A^2(0,l) = 0, 1 \leq l \leq k-1$. Therefore using Theorem 6.2.1, $A^2(0,0)$ can be written as:

$$A^2(0,0) = \sum_{\substack{i,j=0,\\ gi+j=0 \pmod{k}}}^{k-1} c_i c_j = \sum_{\substack{i=0,\\ gi+i=0 \pmod{k}}}^{k-1} c_i^2 = (\sum_{i=0}^{k-1} c_i)^2.$$

This holds because $gi+j = 0 \pmod{k}$ and $g \equiv -1 \pmod{k}$ implies $j = i$. Thus $\sum_{i=0}^{k-1} c_i = 1$.

The coefficient of P^l is $\sum_{\substack{i,j=0,\\ gi+j=l \pmod{k}, l\neq 0}}^{k-1} c_i c_j$ for $1 \leq l \leq k-1$. Therefore

$$A^2(0,l) = \sum_{\substack{i,j=0,\\ gi+j=l \pmod{k}, l\neq 0}}^{k-1} c_i c_j$$

Since $g^2 \equiv 1 \pmod{k}$, the equation $gi+j = l \pmod{k}$ can be written as $i+gj = gl = k-l \pmod{k}$. Hence the set $\{(i,j) : gi+j = l \pmod{k}\}$ same as the set $\{(i,j) : i+gj = k-l \pmod{k}\}$.

Therefore, it is enough to consider first $\lfloor \frac{k-1}{2} \rfloor$ entries of first row of A^2, i.e., coefficients of P^l with $1 \leq l \leq \lfloor \frac{k-1}{2} \rfloor$. Note that, when k is even,

$$A^2\left(0, \frac{k}{2}\right) = \sum_{\substack{i,j=0,\\ gi+j=\frac{k}{2} \pmod{k}}}^{k-1} c_i c_j = \sum_{\substack{i,j=0,\\ gi+j=\frac{k}{2} \pmod{k}, i<j}}^{k-1} 2c_i c_j = 0.$$

This holds because the set $\{(i,j) : gi+j = \frac{k}{2} \pmod{k}\}$ equals to $\{(i,j) : i+gj = g^{-1}\frac{k}{2} = g\frac{k}{2} = \frac{k}{2} \pmod{k}\}$. This implies for even k, $A^2(0, \frac{k}{2})$ always 0. Therefore the conditions hold.

Conversely, if the conditions hold, then $A^2(0,0) = 1$ and $A^2(0,l) = 0$ for $1 \leq l \leq k-1$. Since A^2 is circulant, this implies A is involutory. From the third condition it is evident that A is MDS. Hence proved. □

Consider the following example of left-circulant involutory MDS matrix from [25].

Example 6.2.11. *Consider the finite field $\mathbb{F}_{2^8}$ defined by the irreducible polynomial $1+x^2+x^5+x^6+x^8$. Let a be a primitive element. Construct the left-circulant matrix of order 5×5 with the*

first row $(1, a, 1+a+a^4+a^5+a^7, 1+a+a^3+a^4+a^5+a^7, a+a^3)$. *Then*

$$\sum_{i=0}^{k-1} c_i = 1+a+1+a+a^4+a^5+a^7+1+a+a^3+a^4+a^5+a^7+a+a^3 = 1,$$

$$\begin{aligned}
\sum_{\substack{i,j=0,\\ 4i+j=1 \pmod k}}^{k-1} c_i c_j &= c_0c_1 + c_1c_2 + c_2c_3 + c_3c_4 + c_4c_0 \\
&= (1\cdot a) + (a\cdot(1+a+a^4+a^5+a^7)) + ((1+a+a^4+a^5+a^7) \\
&\cdot (1+a+a^3+a^4+a^5+a^7)) + ((1+a+a^3+a^4+a^5+a^7) \\
&\cdot (a^3+a)) + ((a^3+a)) \\
&= 0,
\end{aligned}$$

$$\begin{aligned}
\sum_{\substack{i,j=0,\\ 4i+j=2 \pmod k}}^{k-1} c_i c_j &= c_0c_2 + c_1c_3 + c_2c_4 + c_3c_0 + c_4c_1 \\
&= (1\cdot(1+a+a^4+a^5+a^7)) + (a\cdot(1+a+a^3+a^4+a^5+a^7)) + \\
&((1+a+a^4+a^5+a^7)\cdot(a^3+a)) + ((1+a+a^3+a^4+a^5+a^7)) \\
&+ ((a^3+a)\cdot a) \\
&= 0.
\end{aligned}$$

Therefore, $A^2 = I$ *from Theorem 6.2.10. Additionally, all submatrices of* A *are non-singular, affirming that* A *is an MDS matrix as well.*

6.3 g-Circulant matrices with semi-involutory and semi-orthogonal properties

In this section, we focus on g-circulant matrices endowed with semi-involutory and semi-orthogonal properties. As discussed in Section 3.4, Chatterjee and Laha [63] demonstrated that for a circulant matrix of order $k \times k$, possessing the semi-orthogonal property leads to the intriguing result that the k-th power of the associated diagonal matrices yields a scalar matrix. This finding prompts a natural question: does this distinctive characteristic also hold true for g-circulant semi-orthogonal matrices? Our investigation extends to this inquiry, considering the case where $\gcd(g, k) = 1$, as this condition proves to be essential for the non-singularity of the matrix in Theorem 5.2.1 in Chapter 5. We also need the following characteristic of semi-orthogonal matrices described in Theorem 2.5 of [64].

Theorem 6.3.1. *Let* A *be a semi-orthogonal matrix of order* $k \times k$ *and* P *be an* $k \times k$ *permutation matrix. Then both* AP *and* PA *are semi-orthogonal matrices.*

Proof. Since A is semi-orthogonal, there exists diagonal matrices D_1 and D_2 such

that $A^{-T} = D_1AD_2$. Let $D_1 = \text{diagonal}(d_1, \ldots, d_k)$ and $D_2 = \text{diagonal}(e_1, \ldots, e_k)$. Additionally the permutation matrix P satisfy $PP^T = I$. Now $(AP)^{-T} = A^{-T}P^{-T} = D_1APP^{-1}D_2P^T = D_1APD_3$, where $D_3 = PD_2P^T$. Then $D_3 = \text{diagonal}(e_{\sigma^{-1}(1)}, e_{\sigma^{-1}(2)}, e_{\sigma^{-1}(3)}, \ldots, e_{\sigma^{-1}(k)})$, where σ is the permutation associated with P. Similarly, PA also semi-orthogonal. □

Theorem 6.3.2. *Let A be a g-circulant matrix of order $k \times k$ over a finite field $\mathbb{F}$ with $\gcd(g, k) = 1$. Then A is semi-orthogonal if and only if there exist non-singular diagonal matrices D_1, D_2 such that $D_1^k = k_1 I$ and $D_2^k = k_2 I$ for non-zero scalars k_1, k_2 in the finite field and $A^{-T} = D_1AD_2$.*

Proof. Let A be a g-circulant matrix with semi-orthogonal property. Then there exists non-singular diagonal matrices D_1 and D_2 such that $A^{-T} = D_1AD_2$. Since A is g-circulant and $\gcd(g, k) = 1$, by Theorem 5.2.3, there exists a unique permutation matrix Q such that $AQ = C$, where C is a circulant matrix. Lemma 6.3.1 implies that C is also semi-orthogonal. According to Theorem 3.4.3, the associated diagonal matrices E_1, E_2 of C satisfy $E_1^n = k_1 I$ and $E_2^n = k_2 I$ for some non-zero scalars k_1, k_2 in the finite field and $C^{-T} = E_1CE_2$. This implies $(AQ)^{-T} = E_1AQE_2$. Thus $A^{-T} = E_1AQE_2Q^T$. Consider $D_1 = E_1$, which implies $D_1^n = E_1^n = k_1 I$. Let $D_2 = QE_2Q^T$. If $E_2 = \text{diagonal}(e_0, e_1, \ldots, e_{k-1})$ and $\sigma \in S_k$ be the permutation associated to Q, then D_2 is also a diagonal matrix with diagonal entries $(e_{\sigma^{-1}(0)}, e_{\sigma^{-1}(1)}, e_{\sigma^{-1}(2)}, \ldots, e_{\sigma^{-1}(k-1)})$. Since $e_{\sigma^{-1}(i)} = e_j$ for $0 \leq i, j \leq k-1$ and $QQ^T = I$, then $D_2^n = (QE_2Q^T)^n = k_2 I$. Hence proved.
Conversely, if there exists non-singular diagonal matrices D_1, D_2 such that $D_1^n = k_1 I$ and $D_2^n = k_2 I$ for non zero scalars k_1, k_2 in the finite field and $A^{-T} = D_1AD_2$, then by the definition A is semi-orthogonal. □

Example 6.3.3. *Consider the 5×5 matrix $A = \text{circulant}(1, 1+\alpha+\alpha^3, 1+\alpha+\alpha^3, \alpha+\alpha^3, 1+\alpha^3+\alpha^4+\alpha^7)$, where α is a primitive element of the finite field $\mathbb{F}_{2^8}$ with the generating polynomial $x^8+x^4+x^3+x^2+1$. Note that, A is semi-orthogonal since $A^{-T} = D_1AD_2$, where $D_1 = \text{diagonal}(\alpha^2+\alpha, \alpha^7+\alpha^2+1, \alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2, \alpha^5+\alpha^4+\alpha^3+\alpha^2, \alpha^6+\alpha^3+\alpha+1)$ and $D_2 = \text{diagonal}(\alpha^7+\alpha^6+\alpha^3+\alpha^2+\alpha+1, \alpha^7+\alpha^5+\alpha^3, \alpha^7+\alpha^5+\alpha^4+\alpha^2+1, \alpha^6+\alpha^5+\alpha^2, \alpha^7+\alpha^5+\alpha^4+\alpha^2+\alpha)$. Here $k_1 = \alpha^5+\alpha^3+\alpha^2+\alpha$ and $k_2 = \alpha^6+\alpha^4+\alpha^3+1$. A is also an MDS matrix.*

The generalization of Theorem 3.4.1 to the case of g-circulant matrices is noted in the subsequent theorem.

Theorem 6.3.4. *Let A be a g-circulant matrix of order $k \times k$ over a finite field $\mathbb{F}$ with $\gcd(g, k) = 1$. Then A is semi-involutory if and only if there exist non-singular diagonal matrices D_1, D_2 such that $D_1^k = k_1 I$ and $D_2^k = k_2 I$ for non-zero scalars k_1, k_2 in the finite field and $A^{-1} = D_1AD_2$.*

Proof. Let $A = g\text{-circulant}(a_0, a_1, \ldots, a_{k-1})$ and $\rho \in S_k$ be the k-cycle associated to A. Assume that A is semi-involutory. This implies the existence of non-singular diagonal

matrices D_1 and D_2 such that $A^{-1} = D_1AD_2$. Let D_1 =diagonal$(d_0, d_1, \ldots, d_{k-1})$ and D_2 =diagonal$(d'_0, d'_1, \ldots, d'_{k-1})$. Then the matrix A^{-1} takes the form

$$A^{-1} = \begin{bmatrix} d_0a_0d'_0 & d_0a_1d'_1 & \cdots & d_0a_{k-1}d'_{k-1} \\ d_1a_{k-g}d'_0 & d_1a_{k-g+1}d'_2 & \cdots & d_1a_{k-1-g}d'_{k-1} \\ \vdots & \vdots & \cdots & \vdots \\ d_{k-1}a_gd'_0 & d_{k-1}a_{g+1}d'_1 & \cdots & d_{k-1}a_{g-1}d'_{k-1} \end{bmatrix}.$$

Here the suffixes of a_i's are calculated modulo k. Since inverse of a g-circulant matrix is h-circulant with $gh \equiv 1 \pmod{k}$, the entries of the second row of A^{-1} are the same as the entries of the first row shifted right by h positions. Since $h < k$, there exists l such that $0 \leq l \leq k-1$ and $\rho(l) = h$. Therefore,

$$\begin{aligned} d_0a_0d'_0 &= d_1a_ld'_h \\ d_0a_1d'_1 &= d_1a_{l+1}d'_{h+1} \\ &\vdots \\ d_0a_{k-1}d'_{k-1} &= d_1a_{l-1}d'_{h-1}. \end{aligned}$$

Here all the suffixes of d_i, a_i and d'_i are calculated modulo k. Note that, the sets $\{l, l+1, \ldots, l-1\}$ and $\{h, h+1, \ldots, h-1\}$ form a complete set of residues modulo k. Then multiplying all these equalities, we get $d_0^k = d_1^k$. Similarly, entries of the third row are the same as entries of the second row right shifted by h positions, and that implies $d_1a_{\rho^{-1}(i)}d'_i = d_2a_{\rho^{-1}(h+i)}d'_{h+i}$ for $i = 0, \ldots, k-1$, and the indices are reduced modulo k, which leads to $d_2^k = d_3^k$. Continuing this process, we get $d_1^k = d_2^k = d_3^k = d_4^k = \cdots = d_k^k$. Moreover, in A^{-1}, the second column is g-shift of the first column by Lemma 6.1. Therefore $d_0a_0d'_0 = d_ha_{k-hg+1}d'_1$, $d_1a_{k-g}d'_0 = d_{h+1}a_{k-(h+1)g+1}d'_1, \ldots, d_{k-1}a_gd'_0 = d_{h+(k-1)}a_{k-(h-1)g-1}d'_1$. Multiplying these equations we get $d_0'^n = d_1'^n$. Applying the same reasoning for the second and the third columns, we get $d_1'^n = d_2'^n$. Continuing in a similar manner, we conclude that $d_0'^n = d_1^n = d_2'^n = d_3'^n = \cdots = d_{k-1}'^n$.
Conversely, if there exists non-singular diagonal matrices D_1, D_2 such that $D_1^n = k_1I$ and $D_2^n = k_2I$ for non zero scalars k_1, k_2 in the finite field and $A^{-1} = D_1AD_2$, then by the definition A is semi-involutory. □

Example 6.3.5. *Consider the 2×2 matrix $A = circulant(1, a^2)$, where a is a primitive element of the finite field $\mathbb{F}_{2^2}$ with the generating polynomial $x^2 + x + 1$. Note that, A is semi-involutory since $A^{-1} = D_1AD_2$, where $D_1 = diagonal(a, a)$ and $D_2 = I_{2\times2}$. Here $k_1 = a + 1$ and $k_2 = 1$. A is also an MDS matrix.*

Example 6.3.6. *Consider the 4×4 matrix $A = circulant(a, a^3, a^2 + a + 1, a^3)$, where a is a primitive element of the finite field $\mathbb{F}_{2^4}$ with the generating polynomial $x^4 + x + 1$. Note that, A is semi-involutory since $A^{-1} = D_1AD_2$, where $D_1 = diagonal(a^3 + 1, a^3 + 1, a^3 + 1, a^3 + 1)$ and $D_2 = I_{4\times4}$. Here $k_1 = a^3 + a^2 + a$ and $k_2 = 1$.*

6.4 Conclusion

This chapter offers a comprehensive exploration of g-circulant involutory MDS matrices and g-circulant semi-orthogonal and semi-involutory matrices. However, the study of g-circulant MDS matrices with either semi-orthogonal or semi-involutory properties remains an unexplored area in current research.

Chapter 7

Circulant MDS matrices with semi-involutory and semi-orthogonal properties

Circulant matrices and their extensions have gained considerable attention in recent years, as discussed in previous chapters. The absence of the MDS property in circulant orthogonal and involutory matrices for different orders over the finite field $\mathbb{F}_{2^m}$ has prompted numerous researchers [17, 25, 30, 31, 32, 33] to investigate Toeplitz matrices, Hankel matrices, and Cyclic matrices etc. with the MDS property. In 2023, Chatterjee and Laha initiated a study of circulant matrices, focusing on semi-involutory and semi-orthogonal properties as discussed in Chapter 3. Building upon their results, this chapter establishes a relationship between the trace of the associated diagonal matrices of a semi-orthogonal (semi-involutory) circulant matrix and the MDS property for various orders over the finite field $\mathbb{F}_{2^m}$. Additionally, we present examples of circulant, semi-orthogonal matrices with odd orders over a finite field of characteristic 2. The work presented in this chapter can be found in [71].

7.1 Introduction

In [30, 31], Gupta *et al.* proved that circulant orthogonal matrices of order $2^d \times 2^d$ cannot be MDS over a finite field of characteristic 2. Furthermore, they provided examples of circulant orthogonal MDS matrices for orders $3, 5, 6, 7$ over the finite field $\mathbb{F}_{2^8}$. Subsequently, in 2023, Chatterjee *et al.* [63] delved into the semi-involutory and semi-orthogonal properties of circulant matrices. Their study showed that in a circulant semi-orthogonal (semi-involutory) matrix of order $n \times n$, the n-th power of the associated diagonal matrices are scalar matrices. The summarized results are as follows:

Theorem 7.1.1. *A be an $n \times n$ circulant matrix over a finite field $\mathbb{F}$. Then A is semi-orthogonal if and only if there exist non-singular diagonal matrices D_1 and D_2 such that $D_1^n = k_1 I$ and $D_2^n = k_2 I$ for non-zero scalars $k_1, k_2 \in \mathbb{F}$, and $A^{-T} = D_1 A D_2$.*

Theorem 7.1.2. *A be an $n \times n$ circulant matrix over a finite field $\mathbb{F}$. Then A is semi-involutory if and only if there exist non-singular diagonal matrices D_1 and D_2 such that $D_1^n = k_1 I$ and $D_2^n = k_2 I$ for non-zero scalars $k_1, k_2 \in \mathbb{F}$, and $A^{-1} = D_1 A D_2$.*

In [63], the absence of the MDS property for circulant sesqui-semi-orthogonal matrices of order $2p \times 2p$ over the finite field $\mathbb{F}_{p^n}$ was established. However, a comprehensive study of circulant semi-orthogonal matrices for other orders was not conducted. In the following section, our attention is directed towards diverse orders of circulant semi-orthogonal MDS matrices over the finite fields of characteristic 2.

7.2 Circulant matrices with MDS and semi-orthogonal properties

Leveraging Theorem 7.1.1, we establish that for circulant semi-orthogonal matrices of order $2^d \times 2^d$, the trace of the associated diagonal matrices are zero over a finite field of characteristic 2.

Proposition 7.2.1. *Let A be a circulant, semi-orthogonal matrix of order $2^d \times 2^d$ over the finite field $\mathbb{F}_{2^m}$ with associated diagonal matrices D_1 and D_2. Then trace of D_1 and D_2 are zero.*

Proof. Let A be a circulant semi-orthogonal matrix with associated diagonal matrices D_1 and D_2. Then $A^{-T} = D_1 A D_2$, where D_1 and D_2 are non-singular diagonal matrices. Let $D_1 = \text{diagonal}(d_0, d_1, d_2, \ldots, d_{2^d-1})$ and $D_2 = \text{diagonal}(e_0, e_1, e_2, \ldots, e_{2^d-1})$. These two diagonal matrices also satisfy $D_1^{2^d} = k_1 I$ and $D_2^{2^d} = k_2 I$ for some non-zero scalers k_1, k_2 of the finite field by Theorem 7.1.1. This implies $\text{trace}(D_1^{2^d}) = 2^d k_1 = 0$ and $\text{trace}(D_2^{2^d}) = 2^d k_2 = 0$. This leads to the expressions:

$$d_0^{2^d} + d_1^{2^d} + d_2^{2^d} + \cdots + d_{2^d-1}^{2^d} = (d_0 + d_1 + d_2 + \cdots + d_{2^d-1})^{2^d} = 0$$

and

$$e_0^{2^d} + e_1^{2^d} + e_2^{2^d} + \cdots + e_{2^d-1}^{2^d} = (e_0 + e_1 + e_2 + \cdots + e_{2^d-1})^{2^d} = 0.$$

Thus $\text{trace}(D_1)$ and $\text{trace}(D_2)$ are zero. □

Next we prove Theorem 1.4.37 which establish a significant relationship between the MDS property and the trace of the associated diagonal matrices for circulant, semi-orthogonal matrices of even orders other than powers of 2.

Theorem 7.2.2. *Let A be a circulant, semi-orthogonal matrix of order $k \times k$ over the finite field $\mathbb{F}_{2^m}$ with associated diagonal matrices D_1 and D_2, where $k = 2^i n, i > 1$ and $n \geq 3$, an odd integer. Then A is MDS implies both the matrices D_1 and D_2 have trace zero.*

Proof. Let $A = \text{circulant}(a_0, a_1, a_2, \ldots, a_{k-1})$. Since A is semi-orthogonal, we have $A^{-T} = D_1 A D_2$, where D_1 and D_2 are non-singular diagonal matrices given by $D_1 = \text{diagonal}(d_0, d_1, d_2, \ldots, d_{k-1})$ and $D_2 = \text{diagonal}(e_0, e_1, e_2, \ldots, e_{k-1})$. Let A be an MDS matrix, then all the submatrices of A have determinant non-zero. Using the identity $AA^{-1} = I$, we have $AD_2A^TD_1 = I$. Let $M = AD_2A^TD_1$. Since all non-diagonal entries of M are zero, we can derive the following set of equations from the entries

$M(0,1), M(1,2), M(2,3), \ldots, M(k-2,k-1), M(k-1,0)$:

$$\begin{aligned}
&(\sum_{i=0}^{k-1} a_i a_{i+1} e_{i+1}) d_1 = 0 \\
&(\sum_{i=0}^{k-1} a_i a_{i+1} e_{i+2}) d_2 = 0 \\
&\qquad\qquad \vdots \\
&(\sum_{i=0}^{k-1} a_i a_{i+1} e_{i+(k-1)}) d_{k-1} = 0 \\
&(\sum_{i=0}^{k-1} a_i a_{i+1} e_{i+k}) d_0 = 0.
\end{aligned}$$

Here all the suffixes are calculated modulo k. Since d_i's are non-zero, these equations reduce to the following:

$$(\sum_{i=0}^{k-1} a_i a_{i+1} e_{i+1}) = 0, (\sum_{i=0}^{k-1} a_i a_{i+1} e_{i+2}) = 0, \ldots, (\sum_{i=0}^{k-1} a_i a_{i+1} e_{i+k}) = 0$$

Adding these equations we get

$$(\sum_{i=0}^{k-1} a_i a_{i+1})(e_0 + e_1 + \cdots + e_{k-1}) = 0. \tag{7.1}$$

Next, consider the following set of entries of the matrix M: $M(0,3)$, $M(1,4)$, $M(2,5)$, $\ldots, M(k-3,0), M(k-2,1), M(k-1,2)$. From these entries, we get the following set of equations:

$$\begin{aligned}
&(\sum_{i=0}^{k-1} a_i a_{i+3} e_{i+3}) d_3 = 0 \\
&(\sum_{i=0}^{k-1} a_i a_{i+3} e_{i+4}) d_4 = 0 \\
&(\sum_{i=0}^{k-1} a_i a_{i+3} e_{i+5}) d_5 = 0 \\
&\qquad\qquad \vdots \\
&(\sum_{i=0}^{k-1} a_i a_{i+3} e_{i+k+1}) d_1 = 0 \\
&(\sum_{i=0}^{k-1} a_i a_{i+3} e_{i+k+2}) d_2 = 0.
\end{aligned}$$

Here all the suffixes are calculated modulo k. Similarly as before, using that d_i's are

non-zero and adding these equations, we get

$$(\sum_{i=0}^{k-1} a_i a_{i+3})(e_0 + e_1 + \cdots + e_{k-1}) = 0. \tag{7.2}$$

Continuing this process to cover all the odd positions of the first row till the position $M(0, \frac{k}{2})$.
Consider the entries at positions $M(0, \frac{k}{2}-1), M(1, \frac{k}{2}), M(2, \frac{k}{2}+1), \ldots, M(\frac{k}{2}+1, 0), M(\frac{k}{2}+2, 1), \cdots, M(k-1, \frac{k}{2}-2)$. From these entries, we get the equation

$$(\sum_{i=0}^{k-1} a_i a_{i+\frac{k}{2}-1})(\sum_{i=0}^{k-1} e_i) = 0, \tag{7.3}$$

where the suffixes are calculated modulo k.
Adding the following $\frac{k}{4}$ equations

$$(\sum_{i=0}^{k-1} a_i a_{i+1})(\sum_{i=0}^{k-1} e_i) = 0, (\sum_{i=0}^{k-1} a_i a_{i+3})(\sum_{i=0}^{k-1} e_i) = 0, \ldots, (\sum_{i=0}^{k-1} a_i a_{i+\frac{k}{2}-1})(\sum_{i=0}^{k-1} e_i) = 0,$$

we get

$$(a_0 + a_2 + \cdots + a_{k-2})(a_1 + a_3 + \cdots + a_{k-1})(e_0 + e_1 + \cdots + e_{k-1}) = 0. \tag{7.4}$$

Given that A is a circulant matrix of order $k \times k$, it has two circulant submatrices of order $\frac{k}{2}$ with the first row $(a_0, a_2, \ldots, a_{k-2})$ and $(a_1, a_3, \ldots, a_{k-1})$ respectively. According to Equation (2.3), both $(a_0 + a_2 + \cdots + a_{k-2})$ and $(a_1 + a_3 + \cdots + a_{k-1})$ must be non-zero since A is an MDS matrix. Therefore from Equation 7.4, we have $(e_0 + e_1 + \cdots + e_{k-1}) = 0$ and this implies trace$(D_2) = 0$.
Similarly using the identity $A^{-1}A = I$ and following the same process, we will get trace$(D_1) = 0$. □

In the next result, we explore the case where the order of the matrix is an even number of the form $2n, n$ is an odd number. In this case, we need one additional condition on the entries of at least one of the associated diagonal matrix. Any diagonal matrix of even order meeting this criterion is termed as non-periodic diagonal matrix. Specifically, we define a diagonal matrix $D =$ diagonal$(d_0, d_1, d_2, \ldots, d_{2n-1})$ as a non-periodic diagonal matrix, if the entries satisfy $d_i \neq d_{i+n}, i = 0, 1, 2, \ldots, n-1$.

Theorem 7.2.3. *Let A be a circulant, semi-orthogonal matrix of order $2n \times 2n, n \geq 3$ be an odd number, over $\mathbb{F}_{2^m}$ with associated diagonal matrices D_1 and D_2. If A is an MDS matrix and at least one of the associated diagonal matrix is non-periodic, then trace of that non-periodic diagonal matrix is zero.*

Proof. Let $A =$ circulant$(a_0, a_1, a_2, \ldots, a_{2n-1})$. Since A is semi-orthogonal, it satisfy $A^{-T} = D_1 A D_2$, where D_1 and D_2 are non-singular diagonal matrices given by $D_1 =$

diagonal$(d_0, d_1, d_2, \ldots, d_{2n-1})$ and D_2 = diagonal$(e_0, e_1, e_2, \ldots, e_{2n-1})$. Without loss of generality, we assume that D_2 is non-periodic diagonal matrix. Then $e_i \neq e_{i+n}, i = 0, 1, 2, \ldots, n-1$. Let A be an MDS matrix.

Since $AA^{-1} = I$, we have $AD_2A^TD_1 = I$. Let $AD_2A^TD_1 = M$. All non-diagonal entries of M are zero. Form the entries $M(0,1), M(1,2), M(2,3), \ldots, M(2n-2, 2n-1), M(2n-1, 0)$ we get the following equations:

$$
\begin{aligned}
(\sum_{i=0}^{2n-1} a_i a_{i+1} e_{i+1}) d_1 &= 0 \\
(\sum_{i=0}^{2n-1} a_i a_{i+1} e_{i+2}) d_2 &= 0 \\
&\vdots \\
(\sum_{i=0}^{2n-1} a_i a_{i+1} e_{i+(2n-1)}) d_{2n-1} &= 0 \\
(\sum_{i=0}^{2n-1} a_i a_{i+1} e_{i+2n}) d_0 &= 0.
\end{aligned}
$$

Here all the suffixes are calculated modulo $2n$. Since d_i's are non zero, we can add these equations and get

$$
(\sum_{i=0}^{2n-1} a_i a_{i+1})(e_0 + e_1 + \cdots + e_{2n-1}) = 0.
$$

Continuing the similar process for the entries at positions $M(0,3)$, $M(1,4)$, $M(2,5)$, $\ldots$, $M(2n-3, 0)$ we get:

$$
\begin{aligned}
(\sum_{i=0}^{2n-1} a_i a_{i+3} e_{i+3}) d_3 &= 0 \\
(\sum_{i=0}^{2n-1} a_i a_{i+3} e_{i+4}) d_4 &= 0 \\
&\vdots \\
(\sum_{i=0}^{2n-1} a_i a_{i+3} e_{i+(2n)}) d_0 &= 0 \\
(\sum_{i=0}^{2n-1} a_i a_{i+3} e_{i+2n+1}) d_1 &= 0 \\
(\sum_{i=0}^{2n-1} a_i a_{i+3} e_{i+2n+2}) d_2 &= 0.
\end{aligned}
$$

Here all the suffixes are calculated modulo $2n$. Adding these equations we get

$$(\sum_{i=0}^{2n-1} a_i a_{i+3})(\sum_{i=0}^{2n-1} e_i) = 0.$$

Continue this process to cover all the odd positions of the first row, upto the position $M(0,n)$. From the entries $M(0,n), M(1,n+1), M(2,n+2), \ldots, M(n-1,2n-1)$ we get:

$$\begin{aligned}
&(\sum_{i=0}^{n-1} a_i a_{i+n}(e_i + e_{i+n}))d_n = 0 \\
&(\sum_{i=0}^{n-1} a_i a_{i+n}(e_{i+1} + e_{i+(n+1)}))d_{n+1} = 0 \\
&\qquad\qquad \vdots \\
&(\sum_{i=0}^{n-1} a_i a_{i+n}(e_{i+(n-1)} + e_{(i+n)+(n-1)}))d_{2n-1} = 0.
\end{aligned} \tag{7.5}$$

Here all the suffixes are calculated modulo $2n$. Using the given conditions on e_i's and d_i's non-zero, we get $(\sum_{i=0}^{2n-1} a_i a_{i+n})(\sum_{i=0}^{2n-1} e_i) = 0$.
Note that, in Equation (7.5), we have n number of equations, where the other sets of involve $2n$ equations each. Finally, adding the following $\lceil \frac{n}{2} \rceil$ equations:

$$(\sum_{i=0}^{2n-1} a_i a_{i+1})(\sum_{i=0}^{2n-1} e_i) = 0, (\sum_{i=0}^{2n-1} a_i a_{i+3})(\sum_{i=0}^{2n-1} e_i) = 0, \ldots, (\sum_{i=0}^{n-1} a_i a_{i+n})(\sum_{i=0}^{2n-1} e_i) = 0,$$

we obtain

$$(a_0 + a_2 + \cdots + a_{2n-2})(a_1 + a_3 + \cdots + a_{2n-1})(e_0 + e_1 + \cdots + e_{2n-1}) = 0.$$

Since A is MDS, using the same argument as previous theorem, we get $(\sum_{i=0}^{2n-1} e_i) = 0$. This implies trace$(D_2) = 0$.
Similarly using the identity $A^{-1}A = I$, D_1 is non-cyclic diagonal matrix, and following the same process, we will get trace$(D_1) = 0$. □

For circulant, semi-orthogonal matrices of odd order, the following examples demonstrate the possibility of achieving the MDS property.

Example 7.2.4. *Consider the* 3×3 *matrix* $A = circulant(\alpha, \alpha+1, \alpha^2+\alpha)$, *where* α *is a primitive element of the finite field* $\mathbb{F}_{2^8}$ *with the generating polynomial* $x^8 + x^4 + x^3 + x^2 + 1$. *Note that,* A *is semi-orthogonal since* $A^{-T} = D_1 A D_2$, *where* $D_1 = diagonal(\alpha^7+\alpha^6+\alpha^5+\alpha, \alpha^7+\alpha^6+\alpha^5+\alpha, \alpha^7+\alpha^6+\alpha^5+\alpha)$ *and* $D_2 = diagonal(\alpha^6+\alpha^4+\alpha^3+\alpha, \alpha^6+\alpha^4+\alpha^3+\alpha, \alpha^6+\alpha^4+\alpha^3+\alpha)$. A *is also an MDS matrix.*

Example 7.2.5. *Consider the* 5×5 *matrix* $A = circulant(1, 1+\alpha+\alpha^3, 1+\alpha+\alpha^3, \alpha+\alpha^3, 1+\alpha^3+\alpha^4+\alpha^7)$, *where* α *is a primitive element of the finite field* $\mathbb{F}_{2^8}$ *with the generating polynomial*

$x^8 + x^4 + x^3 + x^2 + 1$. *Note that, A is semi-orthogonal since $A^{-T} = D_1AD_2$, where $D_1 = diagonal(\alpha^2 + \alpha, \alpha^7 + \alpha^2 + 1, \alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2, \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2, \alpha^6 + \alpha^3 + \alpha + 1)$ and $D_2 = diagonal(\alpha^7 + \alpha^6 + \alpha^3 + \alpha^2 + \alpha + 1, \alpha^7 + \alpha^5 + \alpha^3, \alpha^7 + \alpha^5 + \alpha^4 + \alpha^2 + 1, \alpha^6 + \alpha^5 + \alpha^2, \alpha^7 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha)$. A is also an MDS matrix.*

Remark 7.2.6. *We have classified circulant semi-orthogonal matrices over the finite field $\mathbb{F}_{2^m}$ into four distinct categories. Specifically, for odd orders, we provide examples of circulant semi-orthogonal matrices of orders 3×3 and 5×5 with the MDS property. For matrices of order $2^d \times 2^d$, the trace of the associated diagonal matrices is zero. Additionally, for matrices of even order, where the order $k \equiv 0 \pmod 4$, the MDS property ensures that the trace of the associated diagonal matrices remains zero. Furthermore, when the order is even and congruent to $2 \pmod 4$, the MDS property together with non-periodic diagonal matrices results in a trace value of zero for the associated diagonal matrices.*

In the subsequent section, we explore circulant matrices with the semi-involutory property. Our objective is to determine whether similar outcomes persist under semi-involutory property or not.

7.3 Circulant matrices with MDS and semi-involutory properties

In [30], Gupta *et al.* proved that circulant involutory matrices of order $n \geq 3$ cannot be MDS over the finite field of characteristic 2. In the subsequent results, we extend this characteristic to circulant semi-involutory matrices. In this direction, our first result demonstrate that, the trace of the associate diagonal matrices of a circulant, semi-involutory matrix of order $2^d \times 2^d$ is zero. This mirrors a similar outcome as presented in Theorem 7.2.1, and for the sake of completeness, we acknowledge this result.

Proposition 7.3.1. *Let A be a $2^d \times 2^d$ circulant, semi-involutory matrix over the finite field $\mathbb{F}_{2^m}$ with associated diagonal matrices D_1 and D_2. Then trace of D_1 and D_2 are zero.*

Proof. Let A be a circulant semi-involutory matrix with associated diagonal matrices D_1 and D_2. Then $A^{-1} = D_1AD_2$, where D_1 and D_2 are non-singular diagonal matrices. Let $D_1 = \text{diagonal}(d_0, d_1, d_2, \ldots, d_{2^d-1})$ and $D_2 = \text{diagonal}(e_0, e_1, e_2, \ldots, e_{2^d-1})$. These two diagonal matrices also satisfy $D_1^{2^d} = k_1 I$ and $D_2^{2^d} = k_2 I$ for some non-zero scalers k_1, k_2 of the finite field by Theorem 7.1.2. This implies $\text{trace}(D_1^{2^d}) = 2^d k_1 = 0$ and $\text{trace}(D_2^{2^d}) = 2^d k_2 = 0$. This leads to the expressions:

$$d_0^{2^d} + d_1^{2^d} + d_2^{2^d} + \cdots + d_{2^d-1}^{2^d} = (d_0 + d_1 + d_2 + \cdots + d_{2^d-1})^{2^d} = 0$$

and

$$e_0^{2^d} + e_1^{2^d} + e_2^{2^d} + \cdots + e_{2^d-1}^{2^d} = (e_0 + e_1 + e_2 + \cdots + e_{2^d-1})^{2^d} = 0.$$

Thus $\text{trace}(D_1)$ and $\text{trace}(D_2)$ are zero. □

For circulant semi-involutory matrices with orders other than $2^d \times 2^d$, our result establishes that the trace value of the associated diagonal matrices is zero when the matrix exhibits the MDS property which is noted in Theorem 1.4.39.

Theorem 7.3.2. *Let A be an $n \times n, n \geq 3, n \neq 2^i$ circulant, semi-involutory matrix over the finite field $\mathbb{F}_{2^m}$ with associated diagonal matrices D_1 and D_2. Then A is MDS implies both the matrices D_1 and D_2 have trace zero.*

Proof. Let A = circulant$(a_0, a_1, a_2, \ldots, a_{n-1})$. Since A is semi-involutory, we have $A^{-1} = D_1AD_2$, where D_1 and D_2 are non-singular diagonal matrices given by $D_1 =$ diagonal$(d_0, d_1, d_2, \ldots, d_{n-1})$ and $D_2 =$ diagonal$(e_0, e_1, e_2, \ldots, e_{n-1})$. Let A be an MDS matrix. Since $AA^{-1} = I$, we have $AD_1AD_2 = I$. Let $M = AD_1AD_2$. This implies that all non diagonal entries of M are 0.

Case I: Consider the case n is even, $n = 2k$.

From the entries $M(0,2), M(1,3), M(2,4), M(3,5), \ldots, M(2k-3, 2k-1), M(2k-2, 0), M(2k-1, 1)$ we get the following equations:

$$
\begin{aligned}
&(a_1^2 d_1 + a_{k+1}^2 d_{k+1} + a_0a_2(d_0 + d_2) + a_3a_{2k-1}(d_3 + d_{2k-1}) + \cdots + a_ka_{k+2}(d_k + d_{k+2}))e_2 = 0\\
&(a_1^2 d_2 + a_{k+1}^2 d_{k+2} + a_0a_2(d_1 + d_3) + a_3a_{2k-1}(d_4 + d_{2k}) + \cdots + a_ka_{k+2}(d_{k+1} + d_{k+3}))e_3 = 0\\
&\qquad\vdots\\
&(a_1^2 d_{2k-2} + a_{k+1}^2 d_{k-2} + a_0a_2(d_{2k-1} + d_{2k-3}) + +a_3a_{2k-1}(d_{3+(2k-3)} + d_{2k-4}) + \cdots + a_ka_{k+2}\\
&\qquad (d_{k-1} + d_{k-3}))e_{2k-1} = 0\\
&(a_1^2 d_{2k-1} + a_{k+1}^2 d_{k-1} + a_0a_2(d_{2k} + d_{2k-2}) + a_3a_{2k-1}(d_1 + d_{2k-3}) + \cdots + a_ka_{k+2}\\
&\qquad (d_{k-2} + d_k))e_0 = 0\\
&(a_1^2 d_{2k} + a_{k+1}^2 d_k + a_0a_2(d_1 + d_{2k-1}) + a_3a_{2k-1}(d_2 + d_{2k-2}) + \cdots + a_ka_{k+2}\\
&\qquad (d_{k-1} + d_{k+1}))e_1 = 0.
\end{aligned}
$$

All the suffixes are calculated modulo $2k$. Since e_i's are non-zero, adding all these equations, we get

$$(a_1^2 + a_{k+1}^2)(d_1 + d_2 + \cdots + d_{2k-1}) = 0 \tag{7.6}$$

Since A is an MDS matrix, all its submatrices have determinant non-zero. Consider the 2×2 submatrix of A with the positions $A[0,1], A[0,k+1], A[k,1], A[k,k+1]$. The determinant of this submatrix is $(a_1^2 + a_{k+1}^2)$ and thus it is non-zero. Consequently Equation (7.6) implies $(d_1 + d_2 + \cdots + d_{2k-1}) = 0$. Therefore trace of D_1 is zero.

Considering the identity $A^{-1}A = I$ and proceed similarly, we will get trace of D_2 is zero.

Case II: Consider the case n is odd, $n = 2k + 1$.

The entries at the positions $M(0,2), M(1,3), M(2,4), M(3,5), \ldots, M(2k-2, 2k), M(2k-$

$1,0), M(2k,1)$ give the following equations:

$$\begin{aligned}
&(a_1^2 d_1 + a_0 a_2(d_0 + d_2) + a_3 a_{2k}(d_3 + d_{2k}) + \cdots + a_{k+1} a_{k+2}(d_{k+1} + d_{k+2}))e_2 = 0\\
&(a_1^2 d_2 + a_0 a_2(d_1 + d_3) + a_3 a_{2k}(d_4 + d_{2k+1}) + \cdots + a_{k+1} a_{k+2}(d_{k+2} + d_{k+3}))e_3 = 0\\
&\qquad\vdots\\
&(a_1^2 d_{2k-1} + a_0 a_2(d_{0+2k-2} + d_{1+2k-2}) + a_3 a_{2k}(d_{3+2k-2} + d_{2k+2k-2}) + \cdots + a_{k+1} a_{k+2}\\
&\qquad (d_{k+1+2k-2} + d_{k+2++2k-2}))e_{2k-1} = 0\\
&(a_1^2 d_{2k} + a_0 a_2(d_{0+2k-1} + d_{2+2k-1}) + a_3 a_{2k}(d_{3+2k-1} + d_{2k+2k-1}) + \cdots + a_{k+1} a_{k+2}\\
&\qquad (d_{k+1+2k-1} + d_{k+2+2k-1}))e_0 = 0\\
&(a_1^2 d_0 + a_0 a_2(d_1 + d_{2k}) + a_3 a_{2k}(d_2 + d_{2k-1}) + \cdots + a_{k+1} a_{k+2}(d_k + d_{k+1}))e_1 = 0.
\end{aligned}$$

All the suffixes are calculated modulo $2k+1$. Since e_i's are non-zero, adding all these equations, we get

$$(a_1^2)(d_1 + d_2 + \cdots + d_{2k}) = 0 \tag{7.7}$$

Since A is an MDS matrix, all entries of A are non-zero. This implies $(d_1 + d_2 + \cdots + d_{2k}) = 0$. Therefore trace of D_1 is zero.
Considering the identity $A^{-1}A = I$ and proceed similarly, we will get trace of D_2 is zero. □

Remark 7.3.3. *For circulant semi-involutory matrices over the finite field $\mathbb{F}_{2^m}$, we have proven that matrices of order $2^d \times 2^d$ exhibit a zero trace for their associated diagonal matrices. Furthermore, for orders not represented as powers of 2, the trace remains zero if the matrix possesses the MDS property.*

7.4 Conclusion

In conclusion, this chapter has explored circulant matrices with both semi-orthogonal and MDS properties, as well as circulant matrices characterized by semi-involutory and MDS attributes. Exploring similar properties in the generalization of circulant matrices invites further inquiry, promising valuable insights for future research in this domain.

Chapter 8

Format preserving sets

In this chapter, we study format preserving sets (FPS), which play a crucial role in determining the cardinality of message space within format preserving encryption (FPE) schemes. We first explore certain constructions of FPS over finite commutative rings with identity. We show that it is possible to construct format preserving sets over a finite commutative ring that are not closed under addition. We also provide examples of format preserving sets of cardinalities 26 and 52 over torsion modules and rings. These cardinalities are interesting because they correspond to the set of English alphabets, without and with capitalization. The work presented in this chapter is published and can be found in [75], Section 3 and 4.

8.1 Introduction

Format preserving encryption is an encryption algorithm that preserves the length as well as the format of the plain text. The first formal study of format preserving encryption (FPE) schemes were initiated by Bellare *et al.* in 2009 [52]. In 2016, Chang *et al.* [59] proposed a new FPE algorithm SPF, based on a substitution permutation network (SPN) strategy. In the same year Gupta, Pandey and Ray [60] introduced the concept of format preserving set (FPS) in the diffusion layer of a format preserving encryption scheme as follows: Let M be the matrix corresponding to the diffusion layer with entries from some algebraic structure $\mathbb{A}$. Let X be any set with the desired input size and $\phi : X \to \mathbb{A}$ be an injective map. Then $\phi(X)$ is a format preserving set with respect to M if $M\mathbf{v} \in \phi(X)^n$ for all $\mathbf{v} \in \phi(X)^n$. The formal definition of an FPS over an algebraic structure $\mathcal{A}$ is the following:

Definition 8.1.1. *A non-empty set $S \subseteq \mathcal{A}$ is said to be a format preserving set with respect to an $n \times n$ matrix $M(\mathcal{A})$ if $M\boldsymbol{v} \in \mathcal{A}^n$ for all $\boldsymbol{v} \in \mathcal{A}^n$.*

It is evident from our discussion in Chapter 1, Section 1.3 that the cardinality of an FPS plays an important role in the diffusion layer of an FPE scheme.
In [60], Gupta *et al.* and in [62] Barua *et al.* established that format preserving sets are vector space over some subfield of the finite field $\mathbb{F}_{p^n}$. Therefore the possible cardinalities of an FPS must be prime powers. However, in practical scenarios, the goal of an FPE scheme is to encrypt messages of arbitrary length, not only restricted to prime powers. Additionally, message spaces with cardinalities such as $10, 26$ and 52 carry substantial

significance as they correspond respectively to the set of decimal digits, the set of English alphabets, without and with capitalization.

To address this gap, in 2018, Baura *et al.* [62] investigated the existence of an FPS over a finite commutative ring with identity under the restriction that the set is closed under addition. In this chapter, we present a detailed study of the construction of format preserving sets over rings and finitely generated modules. Our results show the feasibility of attending various cardinalities, which were not attained over finite fields previously.

8.2 Structure of format preserving sets over rings

We explore the structure of FPS over various rings. Initially, we study the structure of FPS over the ring $\mathbb{Z}_n$. Subsequently, we extend and generalize the findings to Galois rings. Finally, we provide few results applicable to arbitrary rings.

8.2.1 Structure of FPS over $\mathbb{Z}_n$

In 2018, Barua *et al.* [62] described the structure of a format preserving set S over a finite commutative unital ring $\mathcal{R}$ by assuming the condition that the set S is closed under addition. Curiously, they observed the following example of a format preserving set which does not satisfy their condition.

Example 8.2.1. *Consider the ring $\mathcal{R} = \mathbb{Z}_{10}$, and a 3×3 matrix M with entries from the set $\{1, 3, 5, 7, 9\} \subset \mathbb{Z}_{10}$. Consider the set $S = \{1, 3, 5, 7, 9\}$. S is not closed under addition, since $3 + 5 = 8 \notin S$. However, S is an FPS with respect to M over the ring $\mathbb{Z}_{10}$.*

Although the set is not closed under addition, it is still an FPS. The general theory behind this phenomenon is proved in the Theorem 8.2.3. Prior to that, we establish a lemma which is useful to prove the theorem.

Lemma 8.2.2. *Let $\mathcal{I} = \langle a \rangle$ be a proper ideal of $\mathcal{R} = \mathbb{Z}_n$ where n is a composite positive integer and $S = \mathcal{I} + 1$. Then $\sum_{t=1}^{r} a_t \pmod n \in S$ for all $a_t \in S,\ 1 \leq t \leq r$, where $r \equiv 1 \pmod a$.*

Proof. Since $S = \mathcal{I} + 1$, for every element $s \in S$ there exists $i \in \mathcal{I}$ such that $s = i + 1$. Also $i = an' \pmod n$, where $n' \in \mathbb{Z}_n$, so $s = an' + 1 \pmod n$. Now

$$\begin{aligned} \sum_{t=1}^{r} a_t \pmod n &= \sum_{t=1}^{r} (i_t + 1) \pmod n \\ &= \sum_{t=1}^{r} i_t + r \pmod n. \end{aligned}$$

Since $i_1, \ldots, i_r$ are elements of $\mathcal{I}$, there exist $n_1, n_2, \ldots, n_r \in \mathbb{Z}_n$ such that $i_j = an_j,\ 1 \leq$

$j \leq r$. Using the given condition $r \equiv 1 \pmod{a}$ (i.e. $r = an'' + 1$), we have the following.

$$\sum_{t=1}^{r} a_t \pmod{n} = \sum_{t=1}^{r} an_t + (an'' + 1) \pmod{n} \in \langle a \rangle + 1 = S.$$

□

Theorem 8.2.3. *Let $\mathcal{I} = \langle a \rangle$ be a proper ideal of $\mathcal{R} = \mathbb{Z}_n$, where n is a composite positive integer and $S = \mathcal{I} + 1 \subseteq \mathcal{R}$. Then S is an FPS with respect to a matrix $M_{r\times r}(S)$ if and only if the order of the matrix $r \equiv 1 \pmod{a}$.*

Proof. Let $s_1, s_2 \in S$. Then there exist $i_1, i_2 \in \mathcal{I}$ such that $s_1 = i_1 + 1$ and $s_2 = i_2 + 1$. Consider the product of s_1 and s_2 as follows:

$$\begin{aligned} s_1 \cdot s_2 &= (i_1 + 1) \cdot (i_2 + 1) \pmod{n} \\ &= i_1 \cdot i_2 + i_1 + i_2 + 1 \pmod{n} \\ &\in \mathcal{I} + 1 \text{ (since } \mathcal{I} \text{ is ideal)} \\ &= S, \end{aligned}$$

i.e., S is closed under multiplication.
For an arbitrary column vector $\mathbf{v} = [s_1, s_2, \ldots, s_r]^t \in S^r$, we show that $M\mathbf{v} \in S^r$. The i-th entry of the vector $M\mathbf{v}$ is $[M\mathbf{v}]_i = m_{i,1}s_1 + m_{i,2}s_2 + \cdots + m_{i,r}s_r$. Since $m_{i,j} \in S$ and S is closed under multiplication, therefore $m_{i,j}s_j \in S$ for all $j = 1, 2, \ldots, r$. Now $[M\mathbf{v}]_i$ is the sum of r elements with entries from S and by the given condition $r \equiv 1 \pmod{a}$. Hence, by Lemma 8.2.2, we have that $[M\mathbf{v}]_i \in S$. Since i is arbitrary, $M\mathbf{v} \in S^r$.
Conversely, let $\mathcal{I} = \langle a \rangle$ be an ideal of $\mathcal{R}$ and $S = \mathcal{I} + 1$ be an FPS with respect to $M_{r\times r}(S)$. Then $M\mathbf{v} \in S^r$ for all vectors $\mathbf{v} \in S^r$. Consider an arbitrary column vector $\mathbf{v} = [s_1, s_2, \ldots, s_r]^t \in S^r$. The i-th entry of the vector $M\mathbf{v}$ is $m_{i,1}s_1 + m_{i,2}s_2 + \cdots + m_{i,r}s_r \in S$. Since both $m_{i,j}$ and s_j are from S, there exist $n_{i,j}, n'_j$ such that $m_{i,j} = an_{i,j} + 1 \pmod{n}$ and $s_j = an'_j + 1 \pmod{n}$ for all $j = 1, 2, \ldots, r$. Therefore,

$$\begin{aligned} [M\mathbf{v}]_i &= m_{i,1}s_1 + m_{i,2}s_2 + \cdots + m_{i,r}s_r \\ &= (an_{i,1} + 1)(an'_1 + 1) + \cdots + (an_{i,r} + 1)(an'_r + 1) \pmod{n} \\ &= (a^2 n_{i,1}n'_1 + an_{i,1} + an'_1 + \cdots + a^2 n_{i,r}n'_r + an_{i,r} + an'_r) + r \pmod{n}. \end{aligned}$$

The first part belongs to $\mathcal{I}$ and is equal to an_1(say) for some $n_1 \in \mathbb{Z}_n$. Therefore, $[M\mathbf{v}]_i = an_1 + r \pmod{n} = s' \in S$. Since $S = \mathcal{I}+1$, we have $s' \equiv 1 \pmod{a}$. Therefore, $an_1 + r \equiv 1 \pmod{a}$ and thus $r \equiv 1 \pmod{a}$. This completes the proof. □

Note that, if the characteristic of $\mathbb{Z}_n$ is even then by considering $\mathcal{I} = \langle 2 \rangle$, we see that $S = \mathcal{I} + 1$ forms a set which is not closed under addition. However, if we take any odd number of elements from S, then by Lemma 8.2.2, the sum of those elements belongs to S. This implies that S is a format preserving set with respect to any odd order matrix

with entries from S by Theorem 8.2.3. This is precisely the example provided by Barua *et al.* at [62].

Next two examples are applications of Theorem 8.2.3 under different conditions. These examples illustrate that constructing an FPS becomes straightforward when an ideal is provided.

Example 8.2.4. *Consider the ring* $\mathbb{Z}_{16}$ *and* $\mathcal{I} = \langle 2 \rangle$. *Then* $S = \mathcal{I} + 1 = \{1, 3, 5, 7, 9, 11, 13, 15\}$. *Consider the* 3×3 *matrix* $M = \begin{bmatrix} 7 & 11 & 15 \\ 5 & 7 & 1 \\ 13 & 3 & 5 \end{bmatrix}$. *Then by Theorem 8.2.3,* S *is a format preserving set with respect to* M.

If $\mathcal{I} = \langle 4 \rangle$, *and* $S = \mathcal{I} + 1 = \{1, 5, 9, 13\}$. *Then* S *is a format preserving with respect to any* 5×5 *matrix with entries from* S.

Example 8.2.5. *Consider the ring* $\mathbb{Z}_{15}$ *and the ideal* $\mathcal{I} = \langle 3 \rangle = \{0, 3, 6, 9, 12\}$. *Then the set* $S = \mathcal{I} + 1 = \{1, 4, 7, 10, 13\}$. *Here,* S *is not closed under addition. Now by Lemma 8.2.2, sum of any four elements in* S *belongs to* S. *For example* $4 + 7 + 10 + 13 \ (mod\ 15) = 4 \in S,\ 4 + 4 + 7 + 13 \ (mod\ 15) = 13 \in S$. *Consider* $M = \begin{bmatrix} 7 & 4 & 1 & 7 \\ 10 & 1 & 4 & 10 \\ 13 & 4 & 13 & 7 \\ 4 & 4 & 7 & 7 \end{bmatrix}$ *and* $\mathbf{v} = [10, 7, 13, 10]^t \in S^4$. *By Theorem 8.2.3, we know that* $M\mathbf{v} \in S^4$.

We notice that the condition $r \equiv 1 \pmod{a}$ is an equivalent condition for the Theorem 8.2.3. Next, we provide a counterexample of the theorem.

Remark 8.2.6. *Consider the ring* $\mathbb{Z}_{15}$ *and* $\mathcal{I} = \langle 3 \rangle$. *Then* $S = \mathcal{I} + 1 = \{1, 4, 7, 10, 13\}$. *Set* $M = \begin{bmatrix} 1 & 4 & 13 \\ 7 & 1 & 7 \\ 10 & 4 & 1 \end{bmatrix}$ *is a* 3×3 *matrix with entries from* S *and* $\mathbf{v} = [1, 7, 1]^t \in S^3$. *But* $M\mathbf{v} = [12, 6, 9]^t \notin S^3$.

In the next section we provide similar results over Galois ring.

8.2.2 Structure of FPS over Galois rings

In this section we generalize the results of the previous section to Galois rings $GR(p^n, r)$, where p is a prime and n, r are positive integers. We commence with the following lemma which is crucial to prove Theorem 8.2.8.

Lemma 8.2.7. *Let* $\mathcal{R}$ *be the Galois ring* $GR(p^n, r)$ *and* $\mathcal{I}_i$ *(where* $0 \leq i \leq n$*) are the principal ideals of* $\mathcal{R}$. *Let* $S = \mathcal{I}_i + 1$. *Then* $\sum_{k=1}^{r} f_k \pmod{p^n} \in S$, *for all* $f_k \in S,\ 1 \leq k \leq r$, *if* $r \equiv 1 \pmod{p^i}$.

Proof. We know that $GR(p^n, r) \cong \mathbb{Z}_{p^n}[x]/(f(x))$, where $f(x) \in \mathbb{Z}_{p^n}[x]$ is a monic, basic, irreducible polynomial of degree r. Then $\mathcal{I}_i = \{a_0 + a_1x + \cdots + a_{r-1}x^{r-1} : a_j \in \langle p^i \rangle,\ 1 \leq j \leq r-1\}$ is a principal ideal of $\mathcal{R}$. Now

$$\begin{aligned}
\sum_{k=1}^{r} f_k \pmod{p^n} &= \sum_{k=1}^{r}(g_k + 1) \pmod{p^n} \\
&= \sum_{k=1}^{r}\sum_{j=0}^{r-1}(g_{k,j}x^j + 1) \pmod{p^n} \\
&= \sum_{k=1}^{r} g_{k,0} + \sum_{k=1}^{r}\sum_{j=1}^{r-1} g_{k,j}x^j + r \pmod{p^n} \\
&= \sum_{k=1}^{r} g_{k,0} + \sum_{k=1}^{r}\sum_{j=1}^{r-1} g_{k,j}x^j + p^i l + 1 \pmod{p^n}.
\end{aligned}$$

The last statement in the proof above follows from the given condition $r \equiv 1 \pmod{p^i}$. Since $\mathcal{I}_i$ is an ideal generated by p^i, $\sum_{k=1}^{r} g_{k,0} + p^i l \in \mathcal{I}_i$. Hence $\sum_{k=1}^{r} f_k \pmod{p^n} = \sum_{i=0}^{r-1} d_i x^i + 1 \in \mathcal{I}_i + 1 = S$. □

Lemma 8.2.7 allows us to prove the following theorem in a manner analogous to Theorem 8.2.3.

Theorem 8.2.8. *Let $\mathcal{R} = GR(p^n, r)$ and $\mathcal{I}_i$ be a principal ideal of $\mathcal{R}$. Consider $S = \mathcal{I}_i + 1 \subseteq \mathcal{R}$. Then S is an FPS with respect to a matrix $M_{r\times r}$ with entries from S if and only if $r \equiv 1 \pmod{p^i}$.*

Proof. Let $f_1, f_2 \in S$. Then there exist $g_1, g_2 \in \mathcal{I}_i$ such that $f_1 = g_1 + 1$ and $f_2 = g_2 + 1$. Considering $g_1 = \sum_{i=0}^{r-1} a_i x^i$ and $g_2 = \sum_{i=0}^{r-1} b_i x^i$, we have

$$f_1 = (a_0 + 1) + \sum_{i=1}^{r-1} a_i x^i \text{ and } f_2 = (b_0 + 1) + \sum_{i=1}^{r-1} b_i x^i.$$

Consider the product $f_1 \cdot f_2$ as follows.

$$\begin{aligned}
f_1 \cdot f_2 &= \left((a_0 + 1) + \sum_{i=1}^{r-1} a_i x^i\right) \cdot \left((b_0 + 1) + \sum_{i=1}^{r-1} b_i x^i\right) \pmod{p^n} \\
&= \sum_{i=0}^{r-1} c_i x^i + \sum_{i=0}^{r-1} a_i x^i + \sum_{i=0}^{r-1} b_i x^i + 1 \pmod{p^n} \text{ (where } c_i = \sum_{j=0}^{i} a_j b_{i-j}) \\
&\in \mathcal{I}_i + 1 \text{ (since } \mathcal{I}_i \text{ is an ideal)} = S.
\end{aligned}$$

This proves that S is closed under multiplication.
To show that S is an FPS with respect to the matrix $M(S)$, where the order of M is congruent to $1 \pmod{p^i}$, consider an arbitrary vector $\mathbf{v} = [f_1, f_2, \cdots, f_r]^t \in S^r$. The

i-th entry of $M\mathbf{v}$ is $m_{i,1}f_1 + m_{i,2}f_2 + \cdots + m_{i,r}f_r$. Since $m_{i,j} \in S$ and S is closed under multiplication, it is evident that each $m_{i,j}f_j \in S$ for $j = 1, 2, \cdots, r$. By Lemma 8.2.7, we get that $[M\mathbf{v}]_i \in S$.
Conversely, let $\mathcal{I}_i = \langle p^i \rangle = \langle a \rangle$ (say) be an ideal of $\mathcal{R}$ and $S = \mathcal{I}_i + 1$ be an FPS with respect to $M_{r\times r}(S)$. Then $M\mathbf{v} \in S^r$ for all vectors $\mathbf{v} \in S^r$. Consider an arbitrary column vector $\mathbf{v} = [s_1, s_2, \ldots, s_r]^t \in S^r$. The i-th entry of the vector $M\mathbf{v}$ is $m_{i,1}s_1 + m_{i,2}s_2 + \cdots + m_{i,r}s_r \in S$. Since both $m_{i,j}$ and s_j are from S, there exist $n_{i,j}, n'_j$ such that $m_{i,j} = an_{i,j} + 1 \pmod{p^n}$ and $s_j = an'_j + 1 \pmod{p^n}$ for all $j = 1, 2, \ldots, r$. Therefore,

$$\begin{aligned}
[M\mathbf{v}]_i &= m_{i,1}s_1 + m_{i,2}s_2 + \cdots + m_{i,r}s_r \\
&= (an_{i,1} + 1)(an'_1 + 1) + \cdots + (an_{i,r} + 1)(an'_r + 1) \pmod{p^n} \\
&= (a^2 n_{i,1}n'_1 + an_{i,1} + an'_1 + \cdots + a^2 n_{i,r}n'_r + an_{i,r} + an'_r) + r \pmod{p^n}.
\end{aligned}$$

The first part belongs to $\mathcal{I}$ and is equal to an_1(say) for some n_1. Therefore, $[M\mathbf{v}]_i = an_1 + r \pmod{p^n} = s' \in S$. Since $S = \mathcal{I} + 1$, we have $s' \equiv 1 \pmod{p^i}$. Therefore, $an_1 + r \equiv 1 \pmod{p^i}$ and thus $r \equiv 1 \pmod{p^i}$. This completes the proof. □

8.2.3 Structure of FPS over arbitrary rings

In the preceding two sections, we provided constructions of an FPS from the translation of an ideal by 1. In this section, we study the construction of a new FPS through the translation of another format preserving set using arbitrary elements from a ring. Under this assumption, we prove Theorem 8.2.9. Following that, we discuss some more properties of FPS over arbitrary rings in Theorem 8.2.11 and Theorem 8.2.17.

Theorem 8.2.9. *Let $\mathcal{R}$ be a finite commutative ring with unity, $S \subseteq \mathcal{R}$ and $S_\beta = S + \beta$, where $\beta \in \mathcal{R}$. Suppose $M = (m_{i,j})_{n\times n}$ is a matrix with entries from $\mathcal{R}$ and $\sum_{j=1}^{n} m_{i,j} = 1$ for all $i = 1, 2, \ldots, n$. Then S_β is an FPS with respect to M if and only if S is an FPS with respect to M.*

Proof. Let S be an FPS with respect to M. Then for any vector $\mathbf{v} \in S^n$, $M\mathbf{v} \in S^n$. Let $\mathbf{v}_1 = [s_1, s_2, \ldots, s_n]^t$ be an arbitrary vector from S_β^n. Since $s_i \in S_\beta$, there exists $\alpha_i \in S$ such that $s_i = \alpha_i + \beta$ for $i = 1, 2, \ldots, n$. The i-th entry of $M\mathbf{v}_1$ is given by the following:

$$\begin{aligned}
[M\mathbf{v}_1]_i &= m_{i,1}s_1 + \cdots + m_{i,n}s_n \\
&= m_{i,1}(\alpha_1 + \beta) + \cdots + m_{i,n}(\alpha_n + \beta) \\
&= m_{i,1}\alpha_1 + \cdots + m_{i,n}\alpha_n + \beta(m_{i,1} + \cdots + m_{i,n}) \\
&= m_{i,1}\alpha_1 + \cdots + m_{i,n}\alpha_n + \beta \cdot 1 \\
&= m_{i,1}\alpha_1 + \cdots + m_{i,n}\alpha_n + \beta.
\end{aligned}$$

Consider $\mathbf{v} = [\alpha_1, \alpha_2, \ldots, \alpha_n]^t \in S^n$. Then by the given condition the i-th entry of $M\mathbf{v}$ i.e. $[M\mathbf{v}]_i = m_{i,1}\alpha_1 + m_{i,2}\alpha_2 + \cdots + m_{i,n}\alpha_n = s \in S$. Hence $[M\mathbf{v}_1]_i = s + \beta \in S_\beta$. Since i is

arbitrary, $M\mathbf{v}_1 \in S_\beta^n$. This proves the "if" part of the theorem.
Conversely, assume S_β is an FPS with respect to M. Let $\mathbf{v}' = [x_1, x_2, \ldots, x_n]^t \in S^n$. Then $x_i = s_i - \beta$ for some $s_i \in S_\beta$ for all $i = 1, 2, \ldots, n$. The i-th entry of $M\mathbf{v}'$ is given by the following:

$$\begin{aligned}[M\mathbf{v}']_i &= m_{i,1}x_1 + m_{i,2}x_2 + \cdots + m_{i,n}x_n \\ &= m_{i,1}(s_1 - \beta) + \cdots + m_{i,n}(s_n - \beta) \\ &= m_{i,1}s_1 + \cdots + m_{i,n}s_n - \beta(m_{i,1} + \cdots + m_{i,n}) \\ &= m_{i,1}s_1 + \cdots + m_{i,n}s_n - \beta.\end{aligned}$$

Consider $\mathbf{w} = [s_1, s_2, \ldots, s_n]^t \in S_\beta^n$. By the given condition, the i-th entry of $M\mathbf{w}$, i.e. $[M\mathbf{w}]_i = m_{i,1}s_1 + m_{i,2}s_2 + \cdots + m_{i,n}s_n = s' \in S_\beta$. Hence $[M\mathbf{v}']_i = s' - \beta \in S$. Since i is arbitrary, $M\mathbf{v}' \in S^n$. □

The following example illustrates Theorem 8.2.9.

Example 8.2.10. *Consider the set* $S = \{1, 4, 7, 10, 13\}$ *in* $\mathbb{Z}_{15}$ *and the matrix* $M = \begin{bmatrix} 7 & 4 & 1 & 4 \\ 10 & 1 & 4 & 1 \\ 1 & 7 & 4 & 4 \\ 1 & 1 & 4 & 10 \end{bmatrix}$. *Then* M *satisfies the condition* $\sum_{j=1}^{n} m_{i,j} = 1 \pmod{15}$. *Let* $S_2 = S + 2 = \{0, 3, 6, 9, 12\}$. *Therefore* S_2 *is format preserving with respect to* M.

To construct format preserving sets of cardinality 10 and 26, Barua *et al.*[62] considered either the entire ring $\mathbb{Z}_{10}$ or $\mathbb{Z}_{26}$ or free module over subrings which are also isomorphic to $\mathbb{Z}_{10}$ or $\mathbb{Z}_{26}$. But in Example 8.2.10, S_2 is an ideal of $\mathbb{Z}_{15}$ and yet an FPS. In the next result, we show that ideals are a natural source of format preserving sets.

Theorem 8.2.11. *Let* S *be an ideal of the ring* $\mathcal{R}$, *then* S *is a format preserving set with respect to any matrix* $M_{n\times n}(\mathcal{R})$.

Proof. Consider any arbitrary column vector $\mathbf{v} = [x_1, x_2, \ldots, x_n]^t \in S^n$ and an arbitrary matrix $M = (m_{i,j})_{n\times n}$, where $m_{i,j} \in \mathcal{R},\ 1 \le i, j \le n$.
The i-th row of the vector $M\mathbf{v}$ is $[M\mathbf{v}]_i = m_{i,1}x_1 + m_{i,2}x_2 + \cdots + m_{i,n}x_n$. Since S is an ideal of $\mathcal{R}$, then $m_{i,j}x_j \in S$ and S also closed under addition. Hence, $M\mathbf{v} \in S^n$ and thus S is an FPS with respect to M. □

In the following examples we construct format preserving sets of cardinalities $3, 5$ and 10 derived from the ideals of a ring.

Example 8.2.12. *Let* $\mathcal{R} = \mathbb{Z}_{15}$ *and* $\mathcal{I}_1 = \{0, 3, 6, 9, 12\}$ *and* $\mathcal{I}_2 = \{0, 5, 10\}$. *Suppose* M *is any square matrix with entries from* $\mathbb{Z}_{15}$. *Then both* $\mathcal{I}_1$ *and* $\mathcal{I}_2$ *are format preserving sets with respect to* M.

Example 8.2.13. *Let* $\mathcal{R} = \mathbb{Z}_{20}$, *and suppose* $\mathcal{I}$ *is an ideal generated by* 2. *Cardinality of* $\mathcal{I}$ *is* 10 *and it is an FPS with respect to any matrix over* $\mathbb{Z}_{20}$.

Though ideals are format preserving sets with respect to any matrix with entries from the ring, union of two ideals is not necessarily a format preserving set. Therefore, union of two format preserving sets over a ring is not necessarily a format preserving set. We show an example of such a case below.

Example 8.2.14. *Consider $\mathcal{I}_1$ and $\mathcal{I}_2$ from Example 8.2.12. Then $\mathcal{I}_1 \bigcup \mathcal{I}_2 = \{0, 3, 5, 6, 9, 10, 12\}$. Consider a 3×3 matrix M with entries from $\mathbb{Z}_{15}$. Let $M = \begin{bmatrix} 1 & 5 & 1 \\ 4 & 3 & 9 \\ 2 & 2 & 1 \end{bmatrix}$ and $\mathbf{v} = [3, 0, 5]^t \in (\mathcal{I}_1 \bigcup \mathcal{I}_2)^3$. Then $M\mathbf{v} = [8, 12, 11]^t \notin (\mathcal{I}_1 \bigcup \mathcal{I}_2)^3$.*

Example 8.2.15. *Let the ring $\mathcal{R} = \mathbb{Z}_{21}$, $S = \langle 3 \rangle$, and $M = \begin{bmatrix} 2 & 20 \\ 6 & 16 \end{bmatrix}$. Suppose S is an FPS with respect to M. Consider $S' = S + 2 = \{2, 5, 8, 11, 14, 17, 20\}$. By Theorem 8.2.9, S' is also an FPS with respect to M. It can be observed that S' is not closed under addition.*

Remark 8.2.16. *In the ring $\mathbb{Z}_n$, consider $S = \langle a \rangle$. Suppose M is a matrix that satisfies the condition of Theorem 8.2.9. Then from S we can construct $(a-1)$ new format preserving sets which are $S + 1, S + 2, \ldots, S + (a-1)$.*

In the next result we show that we can construct an FPS containing all the units of a ring under certain conditions. Let $\mathcal{R}^*$ denote the group of units of ring $\mathcal{R}$. The following theorem allows us to construct an FPS.

Theorem 8.2.17. *Let $\mathcal{R}$ be a finite commutative ring with unity such that $\mathcal{R}^*$ is cyclic. Let S be a subset of $\mathcal{R}$ which contains at least one unit of $\mathcal{R}$. Suppose M is a square matrix with entries from $\mathcal{R}$ with $\mathcal{R}^*$ being generated by some entry of the matrix M. That is, $\mathcal{R}^* = \langle m_{i,j} \rangle$ for some $m_{ij} \in M$. If S is an FPS with respect to M, with $0 \in S$, then S contains all the units of $\mathcal{R}$.*

Proof. Since $\mathcal{R}^*$ is a finite cyclic group, there exist $k \in \mathbb{N}$ and $\beta \in \mathcal{R}$ such that $|\mathcal{R}^*| = k$ and $\beta^k = 1$. Let $\alpha \in S$ be a unit of $\mathcal{R}$, then $\alpha = \beta^i$ and $\alpha^{-1} = \beta^{k-i}$ for some $1 \leq i \leq k$. Assume that $M = (m_{i,j})_{n \times n}$ and $m_{11} = \beta$. Consider the vector $\mathbf{v} = [\alpha, 0, \ldots, 0]^t \in S^n$. Then $M\mathbf{v} = [\beta\alpha, m_{2,1}\alpha, \cdots, m_{n,1}\alpha]^t \in S^n$, i.e. $\beta\alpha = \beta^{i+1} \in S$. Clearly $\beta\alpha$ is a unit of $\mathcal{R}$. Now consider the vector $\mathbf{v_1} = [\beta\alpha, 0, 0, \ldots, 0]^t \in S^n$. Then $M\mathbf{v_1} \in S^n$ i.e. $\beta^2\alpha = \beta^{i+2} \in S$. Continuing this process $k - i$ times we get $\beta^{i+j} = 1 \in S$. For $\mathbf{v'} = [1, 0, \ldots, 0]^t$, we have $M\mathbf{v'} = [\beta, m_{2,1}, \ldots, m_{n,1}]^t$. Thus $\beta \in S$. Hence $\beta^i \in S$ for all $i = 1, 2, \cdots, k$. □

Example 8.2.18. *Consider $\mathcal{R} = \mathbb{Z}_{50}$, then $|\mathcal{R}^*| = 20$. If S is an FPS satisfying the conditions of Theorem 8.2.17, then cardinality of S is at least 21.*

Remark 8.2.19. *Note that for a format preserving set of arbitrary cardinality p satisfying the conditions of Theorem 8.2.17, one needs to find a ring of characteristic n such that cardinality of R^* is $\geq p$.*

The converse of Theorem 8.2.17 is not true. We prove this by the following example.

Example 8.2.20. *Let $\mathcal{R}$ be the ring $\mathbb{Z}_{10}$. Suppose S is the set containing all the units of $\mathcal{R}$ and 0. Let $M = \begin{bmatrix} 3 & 2 \\ 4 & 8 \end{bmatrix}$ and $\mathbf{v} = [3, 0]^t$. Then $M\mathbf{v} = [9, 2]^t \notin S^2$.*

In the next section we discuss the construction of format preserving sets with entries from modules.

8.3 Structure of format preserving sets over modules

So far we have considered the entries of a format preserving set S and the corresponding matrix M from the ring $\mathcal{R}$. In this section, we study the case where the entries of S and M are not necessarily from the same algebraic structure. We know that it is possible to generalize the concept of linear codes from a finite field to a module. This suggests us to study the construction FPS over modules. We provide some results for FPS over modules next.
While constructing FPS over modules, we need to put some restrictions because all the elements in the module and the ring are not necessarily units.

Lemma 8.3.1. *Let N be an $\mathcal{R}$-module and $S \subseteq N$. Suppose M is a square matrix with entries from the ring $\mathcal{R}$ and $a \in \mathcal{R}$ is a unit with $S' = aS$. Then S is an FPS with respect to M if and only if S' is an FPS with respect to M.*

Proof. Let S be an FPS with respect to $M = (m_{i,j})_{n\times n}$. Then for all $\mathbf{v} \in S^n,\ M\mathbf{v} \in S^n$. Let $\mathbf{v}' \in S'^n$. Then there exists a vector $\mathbf{v}_1 \in S^n$ such that $\mathbf{v}' = a \cdot \mathbf{v}_1$. Now $M\mathbf{v}' = M(a \cdot \mathbf{v}_1) = a(M\mathbf{v}_1) \in S'^n$.
Conversely, let S' be an FPS with respect to M. Then $M\mathbf{v} \in S'^n$ for all $\mathbf{v} \in S'^n$. Since a is unit, a^{-1} exists. Let $\mathbf{v}_2 \in S^n$, then there exists $\mathbf{v}_3 \in S'^n$ such that $\mathbf{v}_2 = a^{-1}\mathbf{v}_3$. Since S' is an FPS, we have $M\mathbf{v}_2 = M(a^{-1}\mathbf{v}_3) = a^{-1}(M\mathbf{v}_3) \in S^n$. □

We can see that under multiplication by a unit of the ring, the behaviour of a format preserving set remains unchanged. But there may exist some r in $\mathcal{R}$ such that $r \cdot n = 0$ for some $n \in N$, i.e., r is an annihilator of n. We consider this case in the next lemma.

Lemma 8.3.2. *Let N be an $\mathcal{R}$-module and $S \subseteq N$ be an FPS with respect to $M_{n\times n}(\mathcal{R})$. Suppose $r \in \mathcal{R}$ is an annihilator of some element of S and $S' = rS$. Then S' is an FPS with respect to $M_{n\times n}(\mathcal{R})$ if $0 \in S$.*

Proof. Let $r \in \mathcal{R}$ be an annihilator of $s \in S$. Consider an arbitrary vector $\mathbf{v}' \in S'^n$. Then there exists a column vector $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in S^n$ such that $\mathbf{v}' = r\mathbf{v}$.
First, suppose that $s \neq v_i$ for all $1 \leq i \leq n$. Then $\mathbf{v}' = [rv_1, rv_2, \ldots, rv_n]^t$ and none of the entries of $\mathbf{v}'$ is zero. Now, $M\mathbf{v}' = M[rv_1, rv_2, \ldots, rv_n]^t = rM[v_1, v_2, \ldots, v_n]^t$. But S is an FPS with respect to M, hence we have that $M[v_1, v_2, \ldots, v_n]^t \in S^n$. This implies that $M\mathbf{v}' \in rS^n = S'^n$.
Now assume that $v_i = s$ for some $1 \leq i \leq n$. Without loss of generality, let us assume that $v_1 = s$. Then $\mathbf{v}' = [0, rv_2, \ldots, rv_n]^t \in S'^n$. Now $M\mathbf{v}' = M[0, rv_2, \ldots, rv_n]^t =$

$rM[0, v_2, \cdots, v_n]^t$. Since $0 \in S$, $[0, v_2, \ldots, v_n]^t \in S^n$. Hence $M[0, v_2, \ldots, v_n]^t \in S^n$ and $rM[0, v_2, \ldots, v_n]^t \in S'^n$ i.e., $M\mathbf{v}' \in S'^n$. □

Note that the converse of Lemma 8.3.2 is not true. We illustrate this with the following example.

Example 8.3.3. *Consider $N = \mathbb{Z}_{10}$ and $\mathcal{R} = \mathbb{Z}_{20}$. Then N is an $\mathcal{R}$-module. Suppose $S = \{0, 2, 3\}$ and M is any square matrix with entries from $\mathcal{R}$. For $r = 10 \in Z_{20}$, we have $S' = \{0\}$ and hence S' is an FPS with respect to any matrix, but S is not.*
Consider $r = 5 \in Z_{20}$. Then we have $S' = \{0, 5\}$ and it is an FPS with respect to any matrix since it is a submodule of N. But S is not an FPS.

We have seen in Theorem 8.2.11 that ideals of a ring are format preserving sets. Similarly one can prove that submodules of a module are also format preserving with respect to any matrix with entries from the ring.

Theorem 8.3.4. *Let N be an $\mathcal{R}$-module and $\mathcal{I}$ be a submodule of N. Then $\mathcal{I}$ is a format preserving set with respect to any matrix $M_{n\times n}(\mathcal{R})$.*

Proof. Consider any arbitrary column vector $\mathbf{v} = [x_1, x_2, \ldots, x_n]^t \in \mathcal{I}^n$ and an arbitrary matrix $M = (m_{i,j})_{n\times n}$, where $m_{i,j} \in \mathcal{R},\ 1 \leq i, j \leq n$.
The i-th row of the vector $M\mathbf{v}$ is $[M\mathbf{v}]_i = m_{i,1}x_1 + m_{i,2}x_2 + \cdots + m_{i,n}x_n$. Since $\mathcal{I}$ is a submodule of N, then $m_{i,j}x_j \in \mathcal{I}$ and $\mathcal{I}$ also closed under addition. Hence, $M\mathbf{v} \in \mathcal{I}^n$ and thus $\mathcal{I}$ is an FPS with respect to M. □

In the next theorem we prove that translation of submodules are format preserving under some restriction on the matrix.

Theorem 8.3.5. *Let N be an $\mathcal{R}$-module and $\mathcal{I}$ be a submodule of N. Let $S = \mathcal{I} + 1$. Then S is a format preserving set with respect to $M_{r\times r}(\mathcal{R})$ if and only if $\sum_{j=1}^{r} m_{i,j} \in S$ for all $i = 1, 2, \ldots, r$.*

Proof. Let $s_1, s_2 \in S$. Then there exist $i_1, i_2 \in \mathcal{I}$ such that $s_1 = i_1 + 1$ and $s_2 = i_2 + 1$. Consider the product of s_1 and s_2 as follows.

$$\begin{aligned} s_1 \cdot s_2 &= (i_1 + 1) \cdot (i_2 + 1) \\ &= i_1 \cdot i_2 + i_1 + i_2 + 1 \\ &\in \mathcal{I} + 1 \text{ (since } \mathcal{I} \text{ is submodule)} \\ &= S. \end{aligned}$$

This shows that S is closed under multiplication.
Consider an arbitrary vector $\mathbf{v} = [s_1, s_2, \ldots, s_r]^t \in S^r$. We have to show that $M\mathbf{v} \in S^r$. The i-th entry of the vector $M\mathbf{v}$ is $[M\mathbf{v}]_i = m_{i,1}s_1 + m_{i,2}s_2 + \cdots + m_{i,r}s_r$. This entry can be written in the following form:

$$\begin{aligned} [M\mathbf{v}]_i &= m_{i,1}(i_1 + 1) + \cdots + m_{i,r}(i_r + 1) \\ &= m_{i,1}i_1 + \cdots + m_{i,r}i_r + (m_{i,1} + \cdots + m_{i,r}). \end{aligned}$$

Since $\mathcal{I}$ is a submodule, for some $i'' \in \mathcal{I}$, we have that $m_{i,1}i_1 + m_{i,2}i_2 + \cdots + m_{i,r}i_r = i''$. By the given condition $\sum_{j=1}^{r} m_{i,j} \in S$, there exists some $i' \in \mathcal{I}$ such that $\sum_{j=1}^{r} m_{i,j} = i' + 1$. Thus $[M\mathbf{v}]_i = i'' + i' + 1 \in \mathcal{I} + 1 = S$. Since i is arbitrary, $M\mathbf{v} \in S^r$.
Conversely, assume that S is an FPS with respect to M. Then for all $\mathbf{v} \in S^r$, $M\mathbf{v} \in S^r$. Let $\mathbf{v} = [s_1, s_2, \ldots, s_r]^t \in S^r$. Then $[M\mathbf{v}]_i = m_{i,1}s_1 + m_{i,2}s_2 + \cdots + m_{i,r}s_r = m_{i,1}i_1 + m_{i,2}i_2 + \cdots + m_{i,r}i_r + (m_{i,1} + m_{i,2} + \cdots + m_{i,r}) \in S$. Now $m_{i,1}i_1 + m_{i,2}i_2 + \cdots + m_{i,r}i_r + (m_{i,1} + m_{i,2} + \cdots + m_{i,r}) = i_1 + m' \in \mathcal{I} + m'$, where $(m_{i,1} + m_{i,2} + \cdots + m_{i,r}) = m'$. This implies that $i_1 + m' \in S$, hence $i_1 + m' = i_2 + 1$ for some $i_2 \in \mathcal{I}$. Therefore $m' - 1 \in \mathcal{I}$ i.e., $m' \in \mathcal{I} + 1 = S$. □

The following example illuminates Theorem 8.3.5.

Example 8.3.6. *Let $N = \mathcal{R} = \mathbb{Z}_{35}$ and suppose $\mathcal{I} = \langle 7 \rangle$ is a submodule of N. Then $S = \mathcal{I} + 1 = \{1, 8, 15, 22, 29\}$. Consider the matrix $M = \begin{bmatrix} 15 & 7 & 7 \\ 1 & 8 & 6 \\ 11 & 3 & 8 \end{bmatrix}$ with entries from the ring $\mathcal{R}$. Then by Theorem 8.3.5, S is an FPS with respect to M.*

8.3.1 Structure of FPS over torsion modules

Barua *et al.* provided sufficient conditions for an FPS to be an $\mathfrak{R}$-module in Theorem 4 of [62]. Moreover, if S is a free $\mathfrak{R}$-module, then $|S| = |\mathfrak{R}|^m$ for some $m \geq 0$. In this subsection, we explore other possible cardinalities that an FPS over a finite module can attain. Towards this goal, we now prove Theorem 8.3.7 using the Fundamental theorem of finitely generated modules over PID.

Theorem 8.3.7. *Let N be a finite module over a PID $\mathcal{R}$ with invariant factors $a_1, a_2, \ldots, a_m$. A subset S of N is an FPS with respect to $M_{n\times n}(\mathcal{R})$ if and only if there exists $S_i \subseteq \mathcal{R}/(a_i)$, such that each S_i is an FPS with respect to $M_{n\times n}(\mathcal{R})$ for all $i = 1, 2, \ldots, m$.*

Proof. Since N is a finite module over PID $\mathcal{R}$ with invariant factors $a_1, a_2, \ldots, a_m$, by Theorem 2.1.14, we have that $N \cong \mathcal{R}/(a_1) \bigoplus \mathcal{R}/(a_2) \bigoplus \cdots \bigoplus \mathcal{R}/(a_m)$ where $a_1 | a_2 | \cdots | a_m$.
For each $i \in \{1, 2, \ldots, m\}$, let S_i be an FPS with respect to M. In particular, there exists $S_1 \subseteq \mathcal{R}/(a_1)$ such that S_1 is format preserving with respect to M, where $M = (m_{i,j})_{n\times n}$.
For $\mathbf{v}' = [\bar{x}_{11}, \bar{x}_{21}, \ldots, \bar{x}_{n1}]^t \in S_1^n$, $M\mathbf{v}' = [m_{1,1}\bar{x}_{11} + m_{1,2}\bar{x}_{21} + \cdots + m_{1,n}\bar{x}_{n1}$, $m_{2,1}\bar{x}_{11} + m_{2,2}\bar{x}_{21} + \cdots + m_{2,n}\bar{x}_{n1}, \cdots, m_{n,1}\bar{x}_{11} + m_{n,2}\bar{x}_{21} + \ldots + m_{n,n}\bar{x}_{n1}]^t \in S_1^n$. This implies $m_{i,1}\bar{x}_{11} + m_{i,2}\bar{x}_{21} + \cdots + m_{i,n}\bar{x}_{n1} \in S_1$ for all $i = 1, 2, \ldots, m$.
Similarly, since each $S_j \subseteq \mathcal{R}/(a_j)$, $1 \leq j \leq m$, is an FPS with respect to M, for any vector $\mathbf{v}'' = [\bar{x}_{1j}, \bar{x}_{2j}, \ldots, \bar{x}_{nj}]^t \in S_j^n$, $M\mathbf{v}'' \in S_j^n$. This implies that $m_{i,1}\bar{x}_{1j} + m_{i,2}\bar{x}_{2j} + \cdots + m_{i,n}\bar{x}_{nj} \in S_j$ for $i = 1, 2, \ldots, n$.
We construct a set S from the sets $S_1, S_2, \ldots, S_m$, such that any element $s \in S$ is of the form $s = (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_m)$, where $\bar{x}_i \in S_i$, $1 \leq i \leq m$.

For an arbitrary vector $\mathbf{v} = [s_1, s_2, \ldots, s_n]^t \in S^n$, we show that $M\mathbf{v} \in S^n$. For each $1 \leq j \leq n$, $s_j = (\bar{x}_{j1}, \bar{x}_{j2}, \ldots, \bar{x}_{jm})$, where $\bar{x}_{ji} \in S_i$ for all $i = 1, 2, \ldots, m$. The i-th entry of the vector $M\mathbf{v}$ is the following:

$$\begin{aligned}[M\mathbf{v}]_i &= m_{i,1}s_1 + \cdots + m_{i,n}s_n \\ &= m_{i,1}(\bar{x}_{11}, \ldots, \bar{x}_{1m}) + \cdots + m_{i,n}(\bar{x}_{n1}, \bar{x}_{n2}, \ldots, \bar{x}_{nm}) \\ &= (m_{i,1}\bar{x}_{11} + \cdots + m_{i,n}\bar{x}_{n1}, m_{i,1}\bar{x}_{12} + \cdots + m_{i,n}\bar{x}_{n2}, \ldots, m_{i,1}\bar{x}_{1m} + \cdots + m_{i,n}\bar{x}_{nm}).\end{aligned}$$

By our assumption $m_{i,1}\bar{x}_{11} + m_{i,2}\bar{x}_{21} + \cdots + m_{i,n}\bar{x}_{n1} \in S_1, \ldots, m_{i,1}\bar{x}_{1j} + m_{i,2}\bar{x}_{2j} + \cdots + m_{i,n}\bar{x}_{nj} \in S_j, \ldots, m_{i,1}\bar{x}_{1m} + m_{i,2}\bar{x}_{2m} + \cdots + m_{i,n}\bar{x}_{nm} \in S_m$. Hence $[M\mathbf{v}]_i \in S$ for all i. Conversely, let S be a format preserving set with respect to M. Construct S_i from the set S in the following way:

$$S_1 = \{s \pmod{a_1} : s \in S\}, S_2 = \{s \pmod{a_2} : s \in S\}, \ldots, S_m = \{s \pmod{a_m} : s \in S\}.$$

We show that each S_i is format preserving with respect to M for $i \in 1, 2, \ldots, m$. Consider an arbitrary column vector $\mathbf{v}' = [\bar{s}_{i1}, \bar{s}_{i2}, \ldots, \bar{s}_{in}]^t \in S_i^n$. Now

$$M\mathbf{v}' = \begin{bmatrix} m_{1,1}\bar{s}_{i1} + m_{1,2}\bar{s}_{i2} + \cdots + m_{1,n}\bar{s}_{in} \\ m_{2,1}\bar{s}_{i1} + m_{2,2}\bar{s}_{i2} + \cdots + m_{2,n}\bar{s}_{in} \\ \vdots \\ m_{n,1}\bar{s}_{i1} + m_{n,2}\bar{s}_{i2} + \cdots + m_{n,n}\bar{s}_{in} \end{bmatrix}.$$

Since $\bar{s}_{i1}, \bar{s}_{i2}, \ldots, \bar{s}_{in} \in S_i$, there exist $s_{i_1}, s_{i_2}, \ldots, s_{i_n} \in S$ such that $s_{i_j} \pmod{a_i} = \bar{s}_{ij}$ for all $j \in \{1, 2, \ldots, n\}$. Hence,

$$\begin{aligned}M\mathbf{v}' &= \begin{bmatrix} m_{1,1}s_{i_1} (\text{mod } a_i) + m_{1,2}s_{i_2} (\text{mod } a_i) + \cdots + m_{1,n}s_{i_n} (\text{mod } a_i) \\ m_{2,1}s_{i_1} (\text{mod } a_i) + m_{2,2}s_{i_2} (\text{mod } a_i) + \cdots + m_{2,n}s_{i_n} (\text{mod } a_i) \\ \vdots \\ m_{n,1}s_{i_1} (\text{mod } a_i) + m_{n,2}s_{i_2} (\text{mod } a_i) + \cdots + m_{n,n}s_{i_n} (\text{mod } a_i) \end{bmatrix} \\ &= \begin{bmatrix} (m_{1,1}s_{i_1} + \cdots + m_{1,n}s_{i_n}) (\text{mod } a_i) \\ (m_{2,1}s_{i_1} + \cdots + m_{2,n}s_{i_n}) (\text{mod } a_i) \\ \vdots \\ (m_{n,1}s_{i_1} + \cdots + m_{n,n}s_{i_n}) (\text{mod } a_i) \end{bmatrix}.\end{aligned}$$

By assumption S is an FPS with respect to M. Hence by considering $\mathbf{v} = [s_{i_1}, s_{i_2}, \ldots, s_{i_n}]^t \in S^n$, $M\mathbf{v} \in S^n$. This implies that $[M\mathbf{v}]_k = (m_{k,1}s_{i_1} + m_{k,2}s_{i_2} + \cdots + m_{k,n}s_{i_n}) \in S$. Therefore $[M\mathbf{v}]_k (\text{mod } a_i) \in S_i$ for $k \in \{1, 2, \ldots, n\}$, i.e., $(m_{k,1}s_{i_1} + m_{k,2}s_{i_2} + \cdots + m_{k,n}s_{i_n}) (\text{mod } a_i) \in S_i$. Hence $M\mathbf{v}' \in S_i^n$, i.e., S_i is an FPS with respect to M for $i \in \{1, 2, \ldots, n\}$. □

In the following example, we illustrate Theorem 8.3.7 and construct FPS of cardinalities

16 and 52.

Example 8.3.8. *Let N be an Abelian group of order 144. Clearly N is a module over $\mathbb{Z}$. By Theorem 2.1.14, $N \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_6 \bigoplus \mathbb{Z}_{12}$, where $\mathbb{Z}_{a_i} = \mathbb{Z}/a_i\mathbb{Z}, 1 \leq i \leq 3$ with $a_1 = 2, a_2 = 6$, and $a_3 = 12$. Let M be any square matrix with entries from $\mathbb{Z}$. Set $S_1 = \mathbb{Z}_2,\ S_2 = 3\mathbb{Z}_6,\ S_3 = 3\mathbb{Z}_{12}$ and $S = \{(x, y, z) : x \in S_1, y \in S_2, z \in S_3\}$. It is evident that $S_1,\ S_2$ and S_3 are format preserving with respect to M. Therefore $S \subseteq N$ is an FPS of cardinality 16 with respect to M.*

Remark 8.3.9. *We now use Theorem 8.3.7 to construct an FPS of cardinality 52. Consider an Abelian group N of order 416 as a $\mathbb{Z}$-module. Then by Theorem 2.1.14, $N \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_4 \bigoplus \mathbb{Z}_{52}$, where $\mathbb{Z}_{a_i} = \mathbb{Z}/a_i\mathbb{Z}, 1 \leq i \leq 3$ with $a_1 = 2, a_2 = 4$, and $a_3 = 52$. Let sets $S_1 = \mathbb{Z}_2, S_2 = 2\mathbb{Z}_4$, and $S_3 = 4\mathbb{Z}_{52}$. Consider $S = \{(x, y, z) : x \in S_1, y \in S_2, z \in S_3\}$. We see that S_1, S_2, S_3 are FPS with respect to any square matrix M with entries from $\mathbb{Z}$. Hence $S \subseteq N$ is an FPS of cardinality 52 with respect to M.*

We now make an observation about the direct product of two format preserving sets.

Proposition 8.3.10. *Direct product of two format preserving sets with respect to a matrix M is again format preserving.*

Proof. Suppose S_1 and S_2 are two format preserving sets with respect to matrix $M = (m_{i,j})_{n\times n}$. Let $(\mathbf{v_1}, \mathbf{v_2}) = [(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)]^t \in (S_1 \times S_2)^n$, where $\mathbf{v_1} = [x_1, x_2, \ldots, x_n]^t \in S_1^n$ and $\mathbf{v_2} = [y_1, y_2, \ldots, y_n]^t \in S_2^n$. The i-th entry of $[M(\mathbf{v_1}, \mathbf{v_2})]$ is $[M(\mathbf{v_1}, \mathbf{v_2})]_i = m_{i,1}(x_1, y_1) + m_{i,2}(x_2, y_2) + \cdots + m_{i,n}(x_n, y_n) = (m_{i,1}x_1 + m_{i,2}x_2 + \cdots + m_{i,n}x_n, m_{i,1}y_1 + m_{i,2}y_2 + \cdots + m_{i,n}y_n)$. Since S_1 and S_2 are format preserving with respect to M, we have $M\mathbf{v_1} \in S_1^n$ and $M\mathbf{v_2} \in S_2^n$. This implies that $[M\mathbf{v_1}]_i \in S_1$ and $[M\mathbf{v_2}]_i \in S_2$ for $1 \leq i \leq n$. Hence $[M(\mathbf{v_1}, \mathbf{v_2})]_i \in (S_1 \times S_2)$ for $1 \leq i \leq n$. This proves that $S_1 \times S_2$ is an FPS with respect to M. □

We illustrate this proposition with an example.

Example 8.3.11. *Consider $\mathbb{Z}_{26}$ as a $\mathbb{Z}$-module. Let $M = \begin{bmatrix} 3 & 15 & 7 \\ 7 & 21 & 19 \\ 11 & 17 & 21 \end{bmatrix}$ be a matrix over $\mathbb{Z}$ with entries from the set of odd integers. Let $S_1 = \langle 2 \rangle + 1$ and $S_2 = \{0, 13\}$. By Theorem 8.3.5, S_1 is an FPS with respect to M. Being a submodule of $\mathbb{Z}_{26},\ S_2$ is an FPS with respect to M. By Proposition 8.3.10, $S_1 \times S_2$ is an FPS with respect to M over $\mathbb{Z}_{26} \times \mathbb{Z}_{26}$. Observe that cardinality of $S_1 \times S_2$ is 26.*

Example 8.3.11 corresponds to the cardinality of the set of lowercase English alphabets, which is an interesting use-cases of FPS.

Note that M is not an MDS matrix over the $\mathbb{Z}$-module $\mathbb{Z}_{26}$ in the above example. A detailed study on the MDS matrices over rings modules is provided in next chapter.

8.4 Conclusion

In conclusion, we discussed the construction of format preserving sets that are not closed under addition over certain rings and modules. This research has unveiled intriguing avenues for future exploration in this domain. One such question arising is the possibility of constructing FPS independent of well-known subsets within algebraic structures. Additionally, beyond translation, the exploration of alternative methods for constructing FPS with diverse and interesting cardinalities from subclasses of rings and modules presents itself as a promising direction for further investigation.

Chapter 9

MDS matrices over modules

In this chapter we are primarily interested in the matrix characterization of maximum distance separable (MDS) codes over $\mathbb{Z}$-modules. Initially, we revisit the work of Zain and Rajan [72] on the construction of Maximum Distance Separable (MDS) group codes over cyclic groups. Following that, we generalize the results of Dong, Soh, and Gunawan [74] on the characterization of MDS group codes over the elementary Abelian group. The work presented in this chapter is published and can be found in [75], Section 6.

9.1 Introduction

An (n, k) group code over a group G is a subset of G^n which forms a group under componentwise group operations. This subset can be defined in terms of $(n-k)$ group homomorphism from G^k to G. The formal definition is the following:

Definition 9.1.1. *A (n, k) group code over an Abelian group G is a subgroup of G^n with order $|G|^k$ described by $n-k$ homomorphisms $\phi_j, j = 1, 2, \ldots, n-k$ of G^k onto G. Its codewords are $(x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_n)$, where*

$$x_{k+j} = \phi_j(x_1, \ldots, x_k) = \bigoplus_{l=1}^{k} \phi_j(e, \ldots, e, x_l, e, \ldots, e), j = 1, 2, \ldots, n-k. \tag{9.1}$$

Here e is the identity element and $\bigoplus$ is the group operation.

The term $\phi_j(e, \ldots, e, x_l, e, \ldots, e)$ can be replaced by an endomorphism of G say ψ_{lj}. Therefore the group code can be defined by the set of endomorphisms $\{\psi_{lj}, l = 1, 2, \ldots, k; j = 1, 2, \ldots, n-k\}$. Then the Equation 9.1 can be written as

$$x_{k+j} = \prod_{l=1}^{k} \phi_j(e, \ldots, c, x_j, e, \ldots, e) = \prod_{l=1}^{k} \psi_{lj}(x_j), j = 1, 2, \ldots, n-k. \tag{9.2}$$

In [72], Zain and Rajan established the necessary and sufficient the conditions for a $(k+s, k)$ group code over the cyclic group C_m of m to be MDS. The entries of associated matrix Λ of the generator matrix $G = [I_{k\times k}|\Lambda]$ play a crucial role in this characterization. Their result is as follows:

Theorem 9.1.2. *A $(k+s, k)$ group code L over the cyclic group C_m is MDS if and only if the determinant of every $h \times h$ submatrix, where $h = 1, 2, \ldots, min\{s, k\}$, of the associated matrix Λ is a unit in $\mathbb{Z}_m$.*

An immediate application of Theorem 9.1.2 is the following result.

Theorem 9.1.3. *Let C_m be a cyclic group with $m = p^d$ elements where p is prime. A $(k+s, k)$ MDS group code over C_m does not exists if max $\{s, k\} \geq p$ where d can take any value and $s, k \geq 2$.*

An immediate corollary of Theorem 9.1.3 is the following:

Corollary 9.1.4. *Let C_m be a cyclic group with $m = p^d$ elements where p is prime. Let $M_{k\times s}, s, k \geq 2$ be a matrix with entries from C_m. If max $\{s, k\} \geq p$, then M cannot be an MDS matrix.*

In [72], the authors also provided the following characterization of MDS codes for cyclic groups of order m, where m is an arbitrary integer.

Theorem 9.1.5. *Let C_m be a cyclic group with $m = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m}$ where $p_1, p_2, \ldots, p_m$ are distinct primes. A $(k+s, k)$ MDS group code for all $s, k \geq 2$ over C_m does not exists if max $\{s, k\} \geq p$, where $p = min\{p_1, p_2, \ldots, p_m\}$.*

9.2 Characterization of MDS Codes over Modules

In 1997, Dong *et al.*([74]) generalized the matrix characterizations of MDS codes over finite fields and MDS group codes over cyclic groups to linear codes with systematic parity check matrices over modules.
Let $\mathcal{R}$ be a commutative ring with identity and N be an $\mathcal{R}$-module. A linear code C of length n over a module N is defined to be a submodule of N^n. It is denoted by $C(k, r)$ where $n = k + r$ with generator matrix $[I_k|M_{k\times r}]$ and parity check matrix $[-M^t|I_r]$. In [74], Dong *et al.* provided a characterization for $C(k, r)$ to be an MDS code when N is a cyclic group with m elements and the ring $\mathcal{R} = \mathbb{Z}_m$. They proved the following theorem which can be seen as a generalization of Theorem 9.1.2.

Theorem 9.2.1. *Let $C(k, r)$ be a linear code of length $n = k + r$ with generator matrix $[I_k|M_{k\times r}]$. Then $C(k, r)$ is MDS if and only if the determinant of every $h \times h$ submatrix, $h = 1, 2, \ldots, min\{k, r\}$, of M is not an annihilator of any non zero element in N.*

If the group G is an elementary Abelian group of exponent p, where p is a prime number, then G is a $\mathbb{Z}_p$-module. In [74], Dong *et al.* established the following non-existence result of MDS group codes over an elementary Abelian group as module over $\mathbb{Z}_p$.

Corollary 9.2.2. *Let $\mathcal{R} = \mathbb{Z}_p$, N be an elementary Abelian group with exponent p, and $M = (a_{ij})_{k\times r}$ be any matrix over $\mathbb{Z}_p$. Then MDS group codes $C(k, r)$ with parity check matrix $[-M|I_r]$ do not exist if max$\{k, r\} \geq p$.*

For example, consider $N = \mathbb{Z}_5 \times \mathbb{Z}_5$ as $\mathcal{R} = \mathbb{Z}_5$ module. Using Corollary 9.2.2, we infer that there does not exist any MDS matrix of order n if $n \geq 5$.

9.3 Non-existence of MDS matrix over $\mathbb{Z}_m$ as $\mathbb{Z}$-module

In this section we shall consider the problem of constructing MDS matrices with entries from the Abelian group $\mathbb{Z}_m$ acting as $\mathbb{Z}$-module, where m is an integer. We begin with the case when the group $G = \mathbb{Z}_{p^i}, i \geq 1$, where p is prime and the ring is $\mathbb{Z}$. Recall that an element $x \in \mathbb{Z}$ is said to be an annihilator of $m \in \mathbb{Z}_{p^i}$ if $x \cdot m = 0$. For each $i \geq 1$, consider the map $\phi_i : \mathbb{Z} \to \mathbb{Z}_{p^i}$ defined by $\phi_i(a) = a \pmod{p^i} = \bar{a}\ (say)$. Note that ϕ_i is a surjective homomorphism for $i \geq 1$. Now we are ready to give a series of intermediate lemmas which we use to prove the main result of this chapter.

Lemma 9.3.1. *An element $x \in \mathbb{Z}$ is an annihilator of some element in $\mathbb{Z}_{p^i}$ for some $i \geq 1$ if and only if* $\gcd(\bar{x}, p) > 1$.

Proof. For $i = 1$, i.e, when we consider $\mathbb{Z}_p$ as a $\mathbb{Z}$-module for some prime p, the proof is obvious. Hence, we prove the lemma only for $i > 1$.
Fix an $i > 1$. Suppose $x \in \mathbb{Z}$ is annihilator of $m \in \mathbb{Z}_{p^i}$. Then $xm = 0 \pmod{p^i}$, i.e., $p^i | xm$. If $p^i | x$ then $\phi_i(x) = 0$ i.e., $\gcd(\bar{x}, p) = p$, and we are done. On the other hand, if a smaller power of p divides x, then we can show that the statement of the lemma is true as follows. Consider $p^m | x,\ p^n | m$, where $n + m = i, n, m \geq 1$. Then $x = p^m k'$ i.e. $\phi_i(x) = p^m k' \pmod{p^i} = p^m k_1$. Hence $\gcd(p^m k_1, p) > 1$. We had defined $\phi_i(x) = \bar{x}$, hence $\gcd(\bar{x}, p) > 1$.

Conversely, assume that $\gcd(\bar{x}, p) > 1$. Since p is prime, this implies that $p | \bar{x}$ i.e. $\bar{x} = pk_1$. There exists an $m \in \mathbb{Z}$ such that $\phi_i(m) = \bar{x}$. Thus $m = \bar{x} + p^i k_2 = p(k_1 + p^{i-1} k_2) = pk_3$ where $k_1, k_2, k_3 \in \mathbb{Z}$. Hence $m \in \mathbb{Z}$ is an annihilator of $p^{i-1} \in \mathbb{Z}_{p^i}$. □

This lemma is also valid for the Abelian group $\mathbb{Z}_m$, where m is an integer. In this case, the map is $\phi : \mathbb{Z} \to \mathbb{Z}_m$ and $\phi(a) = a \pmod{m} = \bar{a}$. We state the generalized version of Lemma 9.3.1 below.

Lemma 9.3.2. *Consider the Abelian group $\mathbb{Z}_m$ as $\mathbb{Z}$-module where $m = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$. An element $x \in \mathbb{Z}$ is an annihilator of some element in $\mathbb{Z}_m$ if and only if there exists p_i for some $i \in \{1, 2, \ldots, l\}$ such that* $\gcd(\bar{x}, p_i) \neq 1$.

Proof. Suppose $x \in \mathbb{Z}$ is annihilator of $\alpha \in \mathbb{Z}_m$. Then $x\alpha = 0 \pmod{m}$ i.e., $m | x\alpha$. If $m | x$ then $p_i | x$ for all i. Since $\bar{x} = x \pmod{m}$ and $p_i | m$ then $p_i | \bar{x}$. Therefore $\gcd(\bar{x}, p_i) > 1$. On the other hand, since $\alpha < m$, there always exists p_i for $i \in \{1, 2, \ldots, l\}$ such that $p_i | x$. This implies there exists p_i such that $\gcd(\bar{x}, p_i) \neq 1$ for some $i \in \{1, 2, \ldots, l\}$.
Conversely, assume that $\gcd(\bar{x}, p_i) > 1$ for some $i \in \{1, 2, \ldots, l\}$. This implies $p_i | \bar{x}$ i.e. $\bar{x} = p_i k_1$. There exists an $\beta \in \mathbb{Z}$ such that $\phi(\beta) = \bar{x}$. Thus $\beta = \bar{x} + mk_2 = p_i k_1 + mk_2 = p_i k_3$ since $p_i | m$ and $k_1, k_2, k_3 \in \mathbb{Z}$. Therefore β is an annihilator of $\frac{n}{p_i} \in \mathbb{Z}_m$. □

The following example illuminates the general version of the lemma stated above.

Example 9.3.3. *Let $N = \mathbb{Z}_{2^2 3^2 5}$ be a $\mathbb{Z}$-module. Then $27 \in \mathbb{Z}$ is an annihilator of $\overline{20} \in N$. But $7 \in \mathbb{Z}$ is not an annihilator of any non zero element of N.*

In the next lemma we explore the condition for an arbitrary integer to be a unit of the Abelian group $\mathbb{Z}_{p^i}$ under the mapping ϕ_i.

Lemma 9.3.4. *Let $a \in \mathbb{Z}$ and $\phi_i(a)$ is image of a in $\mathbb{Z}_{p^i}$ under the surjective homomorphism ϕ_i described earlier. Then $\gcd(\phi_i(a), p) = 1$ if and only if $\gcd(a, p) = 1$.*

Proof. Suppose $\gcd(a, p) = 1$ and $\gcd(\phi_i(a), p) > 1$. This implies $p|\phi_i(a)$, i.e., $\phi_i(a) = pk_1$. Hence $a = pk_1 + p^i k_2 = p(k_1 + p^{i-1}k_2)$, where $k_1, k_2 \in \mathbb{Z}$. Thus $p|a$, contradicting our assumption.
Conversely, assume that $\gcd(\phi_i(a), p) = 1$ and $\phi_i(a) = \bar{a}$. For this, the following three cases may arise.

- If $a < p^i$ then $\bar{a} = a$ and $\gcd(a, p) = 1$.
- f $a > p^i$ and a is a multiple of p^i then $\bar{a} = 0$ and $\gcd(0, p) = p$. Hence $a \neq p^i k$.
- If $a = b + p^i k$ then $\phi_i(a) = b$, where $b, k \in \mathbb{Z}$. Hence $\gcd(b, p) = 1$ implies that p does not divide b. This implies that p does not divide a and $\gcd(a, p) = 1$.

In each of these cases, the statement of the lemma holds. Hence proved. □

Lemma 9.3.4 also holds for the mapping ϕ over the Abelian group $\mathbb{Z}_m$. For completeness we record the result here.

Lemma 9.3.5. *Let $a \in \mathbb{Z}$ and $\phi(a)$ is image of a in $\mathbb{Z}_m$ under the surjective homomorphism ϕ described earlier, where $m = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$. Then $\gcd(\phi(a), m) = 1$ if and only if $\gcd(a, p_i) = 1$ for all $i = 1, 2, \ldots, l$.*

Proof. Suppose $\gcd(a, p_i) = 1$ for all $i = 1, 2, \ldots, l$. Let us assume that $\gcd(\phi(a), m) > 1$. This implies, there exists at least one prime $p_i, i \in \{1, 2, \ldots, l\}$ such that $p_i|\phi(a)$. This implies $p_i|a$, a contradiction to the assumption.
Conversely, $\gcd(\phi(a), m) = 1$ and $\phi(a) = \bar{a}$. For this, the following three cases may arise.

- If $a < m$ then $\bar{a} = a$ and $\gcd(a, p_i) = 1$ for all $i = 1, 2, \ldots, l$.
- If $a > m$ and a is a multiple of m then $\bar{a} = 0$ and $\gcd(0, m) = m$. Hence this case will not appear.
- If $a = b + mk$ then $\phi(a) = b$, where $b, k \in \mathbb{Z}$. Hence $\gcd(b, m) = 1$ implies that p_i does not divide b for all $i = 1, 2, \ldots, l$. This implies that p_i does not divide a and $\gcd(a, p_i) = 1$ for all $i = 1, 2, \ldots, l$.

In each of these cases, the statement of the lemma holds. Hence proved. □

Given an $n \times n$ matrix $M = (m_{ij})$ with entries from $\mathbb{Z}$, the matrix $\overline{M} = (\overline{m_{i,j}})$ is construed by applying the map ϕ_i to all entries of the matrix M. Then the following relationship holds between the determinant value of both M and $\overline{M}$.

Lemma 9.3.6. *Let $M = (m_{ij})$ be an $n \times n$ matrix with entries from $\mathbb{Z}$. Suppose $\overline{M} = (\overline{m_{i,j}})$ is a matrix over $\mathbb{Z}_{p^i}$. Then $\phi_i(\det M) = \det \overline{M}$.*

Proof. By Leibniz formula for determinant of an $n \times n$ matrix, we have that $\det M = \sum_{\sigma \in S_n} sgn(\sigma) \prod_{i=1}^{n} m_{\sigma(i),i}$, where S_n is a permutation group with n elements and $a_{i,j}$ denotes the (i,j)-th entry of the matrix. Consider the following,

$$\begin{aligned}\phi_i(\det M) &= \phi_i\left(\sum_{\sigma \in S_n} sgn(\sigma) \cdot \prod_{i=1}^{n} m_{\sigma(i),i}\right) \\ &= \sum_{\sigma \in S_n} sgn(\sigma) \cdot \prod_{i=1}^{n} \phi_i(m_{\sigma(i),i}) \\ &= \det \overline{M}.\end{aligned}$$

In the last line above, we have used the fact that sgn(σ) is $+1$ or -1, depending on whether the permutation is even or odd, and hence it remains unchanged under ϕ_i. □

Theorem 9.3.7. *Let $N = \mathbb{Z}_{p^i}$, $i \geq 1$ be a $\mathbb{Z}$-module and $M = (m_{k,j})_{n \times n}$ be a matrix with entries from $\mathbb{Z}$. Then M is an MDS matrix if and only if $\overline{M}$ is an MDS matrix over $\mathbb{Z}_{p^i}$.*

Proof. Let M be an MDS matrix with entries from $\mathbb{Z}$. Then for all k and $j \in \{1, 2, \ldots, n\}$, $m_{k,j}$ is not an annihilator of any non zero element of $\mathbb{Z}_{p^i}$. Therefore Lemma 9.3.1 implies that $\gcd(m_{k,j}, p) = 1$. Then using Lemma 9.3.4, $\overline{m_{k,j}}$ is a unit in $\mathbb{Z}_{p^i}$ for all k, j.
Next, we show that determinant of every square submatrix of $\overline{M}$ is a unit in $\mathbb{Z}_{p^i}$. Suppose there exists an $r \times r$ sub-matrix $\overline{M}'$ of $\overline{M}$ whose determinant is not a unit. Then $\det \overline{M}' = \bar{d}$ must be a zero divisor in $\mathbb{Z}_{p^i}$, i.e., $\gcd(\bar{d}, p) > 1$. Let M' be the corresponding submatrix of $\overline{M}'$ in M. If $\det M' = d$ then $\bar{d} = \phi(d)$. Therefore, $\gcd(\bar{d}, p) > 1$ implies $\gcd(d, p) > 1$. Hence d is an annihilator of some non zero element in $\mathbb{Z}_{p^i}$ which is a contradiction to the assumption.
Conversely, let $\overline{M}$ be an MDS matrix. Then determinant of every $r \times r$ submatrix for $r \in \{1, 2, \ldots, n\}$ is a unit. Hence, by Lemma 9.3.1, 9.3.6 and 9.3.4, preimages of these determinants in $\mathbb{Z}$ are not annihilators of any non zero element in $\mathbb{Z}_{p^i}$. Hence M is also an MDS matrix. □

We provide an example MDS matrix constructed by using Theorem 9.3.7.

Example 9.3.8. *Consider $\mathbb{Z}_{7^2}$ as a $\mathbb{Z}$-module. Let $M = \begin{bmatrix} 58 & 32 \\ 3 & 9 \end{bmatrix}$ be a matrix with entries from $\mathbb{Z}$ such that $\gcd(m_{kj}, 7) = 1$ for all $1 \leq k, j \leq 2$ and $det(M) = 426$. Then by Theorem 9.2.1, M is an MDS matrix. Further, $\overline{M} = \begin{bmatrix} 9 & 32 \\ 3 & 9 \end{bmatrix}$ is the matrix over $\mathbb{Z}_{7^2}$. It is also an MDS matrix since entries of $\overline{M}$ are units in $\mathbb{Z}_{7^2}$ and determinant of $\overline{M}$ is 34, which is also a unit in $\mathbb{Z}_{7^2}$.*

An analogues result of Theorem 9.3.7 for Abelian group $\mathbb{Z}_m$ as $\mathbb{Z}$-module, where m is an arbitrary integer is the following:

Theorem 9.3.9. *Let $N = \mathbb{Z}_m$ be a $\mathbb{Z}$-module where $m = p_1^{a_1}p_2^{a_2}\cdots p_l^{a_l}$. Let $M = (m_{k,j})_{n\times n}$ be a matrix with entries from $\mathbb{Z}$. Then M is an MDS matrix if and only if $\overline{M}$ is an MDS matrix over $\mathbb{Z}_m$.*

Proof. Let M be an MDS matrix with entries from $\mathbb{Z}$. Then for all k and $j \in \{1, 2, \ldots, n\}$, $m_{k,j}$ is not an annihilator of any non zero element of $\mathbb{Z}_m$. Then Lemma 9.3.2 implies that $\gcd(m_{k,j}, p_i) = 1$ for all $i = 1, 2, \ldots, l$. Therefore from Lemma 9.3.5, $\gcd(\overline{m_{k,j}}, m) = 1$ and thus $\overline{m_{k,j}}$ is a unit in $\mathbb{Z}_m$ for all k, j.
Next, we show that determinant of every square submatrix of $\overline{M}$ is a unit in $\mathbb{Z}_m$. Suppose there exists an $r\times r$ sub-matrix $\overline{M}'$ of $\overline{M}$ whose determinant is not a unit. Then $\det \overline{M}' = \bar{d}$ must be a zero divisor in $\mathbb{Z}_m$, i.e., $\gcd(\bar{d}, p_i) > 1$ for some $i \in \{1, 2, \ldots, j\}$. Let M' be the corresponding submatrix of $\overline{M}'$ in M. If $\det M' = d$ then $\bar{d} = \phi(d)$. Therefore, $\gcd(\bar{d}, p_i) > 1$ implies $\gcd(d, p_i) > 1$. Hence d is an annihilator of some non zero element in $\mathbb{Z}_m$ which is a contradiction to the assumption that M is MDS.
Conversely, let $\overline{M}$ be an MDS matrix. Then determinant of every $r \times r$ submatrix for $r \in \{1, 2, \ldots, n\}$ is a unit. Hence, by Lemma 9.3.6 and 9.3.5, preimages of these determinants in $\mathbb{Z}$ are not annihilators of any non zero element in $\mathbb{Z}_{p^i}$. Hence M is also an MDS matrix. □

We are now in a position to state some non-existence results for MDS matrices when we consider an Abelian group as a $\mathbb{Z}$-module. Theorem 9.3.10 describes the case when order of the Abelian group is power of a prime, and Theorem 9.3.12 generalizes this to the case when the order is any composite integer.

Theorem 9.3.10. *Let $N = \mathbb{Z}_{p^i}$ be a $\mathbb{Z}$-module and $M = (a_{i,j})_{r\times k}$ be a matrix with entries from $\mathbb{Z}$. Then M cannot be MDS if max$\{r, k\} \geq p$.*

Proof. Let $M_{r\times k}$ be an MDS matrix and max$\{r, k\} \geq p$. By Theorem 9.3.7, $\overline{M}_{r\times k}$ is MDS. However, it contradicts the statement of Corollary 9.1.4, hence not possible. Therefore, M cannot be MDS. □

The next example shows an application of Theorem 9.3.10 by considering the ring $\mathbb{Z}_{3^2}$ as a $\mathbb{Z}$-module.

Example 9.3.11. *Consider $\mathbb{Z}_{3^2}$ as a $\mathbb{Z}$-module. Let $M = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 8 & 16 \\ 4 & 16 & 32 \end{bmatrix}$. Then $\overline{M} = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 8 & 7 \\ 4 & 7 & 5 \end{bmatrix}$ is a matrix over $\mathbb{Z}_{3^2}$. The determinant of the 2×2 sub-matrix $\begin{bmatrix} 1 & 1 \\ 4 & 7 \end{bmatrix}$ is 3 which is not a unit in $\mathbb{Z}_{3^2}$. Hence, M is not an MDS matrix over $\mathbb{Z}_{3^2}$ as $\mathbb{Z}$-module.*

Theorem 9.3.12. *Let $N = \mathbb{Z}_m$ be a $\mathbb{Z}$-module, where $m = p_1^{d_1}p_2^{d_2}\cdots p_l^{d_l}$, and p_i's are distinct primes, $1 \leq i \leq l$. Suppose $M = (a_{i,j})_{r\times k}$ is a matrix with entries from $\mathbb{Z}$. Then M cannot be MDS if max$\{r, k\} \geq p =$ min$\{p_1, p_2, \ldots, p_l\}$.*

Proof. Let $M_{r\times k}$ be an MDS matrix and $\max\{r,k\} \geq p = \min\{p_1, p_2, \ldots, p_l\}$. By Theorem 9.3.9, $\overline{M}_{r\times k}$ is MDS. However, it contradicts the statement of Theorem 9.1.5, hence not possible. Therefore, M cannot be MDS.

□

Example 9.3.13. *Consider $\mathbb{Z}_{20}$ as a $\mathbb{Z}$-module. Let $M = \begin{bmatrix} 3 & 7 & 1 \\ 11 & 1 & 9 \\ 3 & 13 & 7 \end{bmatrix}$ be a 3×3 matrix with entries from $\mathbb{Z}$. For this matrix, we have that $\overline{M} = M$. Consider the 2×2 sub-matrix $\begin{bmatrix} 7 & 1 \\ 1 & 9 \end{bmatrix}$ of $\overline{M}$. It's determinant is 62 which is an annihilator of 10 in $\mathbb{Z}_{20}$. Hence M is not MDS.*

Chapter 10

Conclusion

In conclusion, this thesis has delved into the intricate structures of MDS matrices over finite fields, particularly focusing on their semi-involutory and semi-orthogonal properties. Moreover, we have studied the construction of format preserving sets over finite commutative rings and modules and investigated the non-existence of MDS matrices over modules. The study commenced by establishing the MDS nature of 3×3 semi-orthogonal and semi-involutory matrices, extending to the analysis of well-known constructions such as Cauchy and Vandermonde based MDS matrices. A noteworthy contribution of this work is the formulation of a comprehensive method for constructing all 3×3 semi-involutory MDS matrices over the finite field $\mathbb{F}_{2^m}$. The proposed matrix form presented in Equation 4.16 offers practical benefits, particularly in the diffusion layer of SPN-based block ciphers. This is because of the simplicity of the inverse matrix, which involves a straightforward multiplication of two diagonal matrices with the original matrix. Furthermore, the thesis provides a quantitative assessment of the total number of 3×3 MDS semi-involutory matrices over the finite field $\mathbb{F}_{2^m}$.

However, despite these achievements, several intriguing avenues for future research emerge. The general structures of involutory and semi-involutory matrices, especially for even sizes or powers of 2, remain an open problem, prompting further exploration into their MDS properties. We have also studied various generalizations of circulant matrices with the MDS property and introduce a novel perspective by considering both semi-orthogonal and semi-involutory attributes. The exploration of cyclic matrices other than g-circulant matrices, with involutory property, remains an interesting and challenging problem for future investigation.

Also, the exploration of cyclic matrices with combined semi-involutory and semi-orthogonal properties is a further direction of research. Furthermore, our investigation of new construction method for FPS within finite modules over Principal Ideal Domains (PID), finite commutative rings and the existence of Maximum Distance Separable (MDS) matrices for modules over PID, shed light on the new constructions of FPS and MDS matrices within various algebraic structures. Our research open up several intriguing avenues for future exploration. The question of whether FPS can be constructed without relying on well-known subsets like ideals and submodules remains unresolved, challenging researchers to explore alternative methods for FPS generation. Additionally, the prospect of constructing rings or modules over which FPS can be generated with respect to an MDS matrix represents a promising direction for further investigation, offering insights into the diverse applicability of format preserving sets.

References

[1] National Institute of Standards and Technology. Fips-46: Data Encryption Standard (DES). 1979.

[2] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[3] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. Twofish: A 128-bit block cipher. *In the first AES Candidate Conference*, 1998.

[4] Ronald L. Rivest. The RC4 encryption algorithm. 1992.

[5] Daniel Bernstein. ChaCha, a variant of Salsa20. NIST Submission, 2008.

[6] Daniel Bernstein. The Salsa20 family of stream ciphers. NIST Submission, 2007.

[7] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Technical Journal*, pages 656–715, 1949.

[8] H. M. Heys and S. E. Tavares. The design of substitution-permutation networks resistant to differential and linear cryptanalysis. pages 148–155, 1994.

[9] H. M. Heys and S. E. Tavares. Avalanche characteristics of substitution-permutation encryption networks. *IEEE Trans. Comp.*, pages 1131–1139, 1995.

[10] H. M. Heys and S. E. Tavares. The design of product ciphers resistant to differential and linear cryptanalysis. *Journal of Cryptology*, pages 1–19, 1996.

[11] Serge Vaudenay. On the need for multipermutations: Cryptanalysis of MD4 and SAFER. In *Fast Software Encryption*, pages 286–297. Springer Berlin Heidelberg, 1995.

[12] Vincent Rijmen, Joan Daemen, Bart Preneel, Antoon Bosselaers, and Erik De Win. The cipher SHARK. pages 99–111, 1996.

[13] Joan Daemen, Lars Knudsen, and Vincent Rijmen. The block cipher SQUARE. In *Fast Software Encryption*, pages 149–165. Springer Berlin Heidelberg, 1997.

[14] Lars R. Knudsen and Gregor Leander. *PRESENT – Block Cipher*, pages 953–955. Springer US, Boston, MA, 2011.

[15] A. M. Youssef, S. Mister, and S.E .Tavares. On the design of linear transformations for substitution permutation encryption networks. *Workshop on Selected Areas in Cryptography (SAC)*, pages 40–48, 1997.

[16] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes*. North-Holland Publishing Co., 1977.

[17] Kishan Chand Gupta, Sumit Kumar Pandey, Indranil Ghosh Ray, and Susanta Samanta. Cryptographically significant MDS matrices over finite fields: A brief survey and some generalized results. *Adv. Math. Commun.*, 13:779–843, 2019.

[18] J. Lacan and J. Fimes. Systematic MDS erasure codes based on Vandermonde matrices. *IEEE Communications Letters*, 8(9):570–572, 2004.

[19] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Behnaz Omoomi. On construction of involutory MDS matrices from Vandermonde matrices in $GF(2^q)$. *Des. Codes Cryptogr.*, 64(3):287–308, 2012.

[20] Kishan Chand Gupta and Indranil Ghosh Ray. On constructions of involutory MDS matrices. *Progress in cryptology—AFRICACRYPT 2013*, 7918:43–60, 2013.

[21] Ting Cui, Chenhui Jin, and Zhiyin Kong. On compact Cauchy matrices for substitution-permutation networks. *IEEE Transactions on Computers*, 64(7): 2098–2102, 2015.

[22] R. M. Roth and G. Seroussi. On generator matrices of MDS codes (corresp.). *IEEE Transactions on Information Theory*, 31(6):826–830, 1985.

[23] M. K. Pehlivanoğlu, M. T. Sakalli, S. Akleylek, N. Duru, and V. Rijmen. Generalisation of Hadamard matrix to generate involutory MDS matrices for lightweight cryptography. *IET Information Security*, 121:348–355, 2018.

[24] Siang Meng Sim, Khoongming Khoo, Frédérique Oggier, and Thomas Peyrin. Lightweight MDS involution matrices. In *Fast Software Encryption*, pages 471–493. Springer Berlin Heidelberg, 2015.

[25] Meicheng Liu and Siang Meng Sim. Lightweight MDS generalized circulant matrices. pages 101–120, 2016.

[26] P. S. L. M. Barreto and M. A. Simplício Jr. CURUPIRA, a block cipher for constrained platforms. *Brazilian symposium on Computer Networks and Distributed Systems*, 2007.

[27] Gülsüm Gözde Güzel, Muharrem Tolga Sakalli, Sedat Akleylek, Vincent Rijmen, and Yasemin Çengellenmiş. A new matrix form to generate all involutory MDS matrices over F_{2^m}. *Information Processing Letters*, 147:61–68, 2019.

[28] Sun Y. Bai, J. and D. Wang. On the construction of involutory MDS matrices over $\mathbb{F}_{2^m}$. *J Syst Sci Complex*, 33:836—-848, 2020.

[29] Zeng X. Yang, Y. and S. Wang. Construction of lightweight involutory MDS matrices. *Des. Codes Cryptogr.*, 89:1453—-1483, 2021.

[30] Kishan Chand Gupta and Indranil Ghosh Ray. On Constructions of Circulant MDS Matrices for Lightweight Cryptography. *ISPEC 2014, Lecture Notes in Computer Science*, pages 564–576, 2014.

[31] Kishan Chand Gupta and Indranil Ghosh Ray. Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. *Cryptogr. Commun.*, 7(2):257–287, 2015.

[32] S. Sarkar and H. Syed. Lightweight diffusion layer: Importance of Toeplitz matrices. *Trans. Symmetric Cryptol.*, 95:95–113, 2016.

[33] S. Sarkar and H. Syed. Analysis of Toeplitz MDS matrices. *ACISP 2017, LNCS*, 10343: 3–18, 2017.

[34] Victor Cauchois and Pierre Loidreau. On circulant involutory MDS matrices. *Des. Codes Cryptogr.*, 87(2-3):249–260, 2019.

[35] I. Adhiguna, I. S. N. Arifin, F. Yuliawan, and I. M. Alamsyah. On orthogonal circulant MDS matrices. *International Journal of Mathematics and Computer Science*, pages 1619–1637, 2022.

[36] Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In *Advances in Cryptology – CRYPTO 2011*, pages 222–239. Springer Berlin Heidelberg, 2011.

[37] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matt Robshaw. The LED block cipher. In *Cryptographic Hardware and Embedded Systems – CHES 2011*, pages 326–341. Springer Berlin Heidelberg, 2011.

[38] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Pouyan Sepehrdad. Recursive diffusion layers for block ciphers and hash functions. In *Fast Software Encryption*, pages 385–401. Springer Berlin Heidelberg, 2012.

[39] Shengbao Wu, Mingsheng Wang, and Wenling Wu. Recursive diffusion layers for (lightweight) block ciphers and hash functions. In *Selected Areas in Cryptography*, pages 355–371. Springer Berlin Heidelberg, 2013.

[40] Thierry P. Berger. Construction of recursive MDS diffusion layers from Gabidulin codes. In *Progress in Cryptology – INDOCRYPT 2013*, pages 274–285. Springer International Publishing, 2013.

[41] Daniel Augot and Matthieu Finiasz. Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. In *2013 IEEE International Symposium on Information Theory*, pages 1551–1555, 2013.

[42] Pandey S. K. Gupta, K. C. and Venkateswarlu. A. On the direct construction of recursive MDS matrices. *Des. Codes Cryptogr.*, 82:77–94, 2017.

[43] Pandey S. K. Gupta, K. C. and Venkateswarlu. A. Towards a general construction of recursive MDS diffusion layers. *Des. Codes Cryptogr.*, 82:179–195, 2017.

[44] Dylan Toh, Jacob Teo, Khoongming Khoo, and Siang Meng Sim. Lightweight MDS serial-type matrices with minimal fixed XOR count. In *Progress in Cryptology – AFRICACRYPT 2018*, pages 51–71. Springer International Publishing, 2018.

[45] Kishan Chand Gupta, Sumit Kumar Pandey, and Susanta Samanta. A few negative results on constructions of MDS matrices using low XOR matrices. In *Security, Privacy, and Applied Cryptography Engineering*, pages 195–213. Springer International Publishing, 2019.

[46] Kishan Chand Gupta, Sumit Kumar Pandey, and Susanta Samanta. Construction of recursive MDS matrices using DLS matrices. In *Progress in Cryptology - AFRICACRYPT 2022*, pages 3–27. Springer Nature Switzerland, 2022.

[47] Abhishek Kesarwani, Sumit Kumar Pandey, Santanu Sarkar, and Ayineedi Venkateswarlu. Recursive MDS matrices over finite commutative rings. *Discrete Applied Mathematics*, 304:384–396, 2021.

[48] Khoongming Khoo, Thomas Peyrin, Axel Y. Poschmann, and Huihui Yap. FOAM: Searching for hardware-optimal SPN structures and components with a fair comparison. In *Cryptographic Hardware and Embedded Systems – CHES 2014*, pages 433–450. Springer Berlin Heidelberg, 2014.

[49] C. Beierle, T. Kranz, and G. Leander. Lightweight multiplication in $GF(2^n)$ with applications to MDS matrices. pages 625–653, 2016.

[50] Lukas Kölsch. XOR-counts and lightweight multiplication with fixed elements in binary finite fields. pages 285–312, 2019.

[51] Michael Brightwell and Harry E. Smith. Using datatype-preserving encryption to enhance data warehouse security. In *20-th National Information Systems Security Conference Proceedings (NISSC)*, pages 141–149, 1997.

[52] Mihir Bellare, Thomas Ristenpart, Phillip Rogaway, and Till Stegers. Format-preserving encryption. In *Selected Areas in Cryptography, 16th Annual International Workshop, SAC 2009*, volume 5867 of *Lecture Notes in Computer Science*, pages 295–312. Springer, 2009.

[53] Morris Dworkin. Recommendation for block cipher modes of operation: Methods for format-preserving encryption. 2016.

[54] John Black and Phillip Rogaway. Ciphers with arbitrary finite domains. In *Topics in Cryptology - CT-RSA 2002*, volume 2271 of *Lecture Notes in Computer Science*, pages 114–130. Springer, 2002.

[55] Terence Spies. Feistel finite set encryption. NIST submission, February 2008.

[56] Mihir Bellare, Phillip Rogaway, and Terence Spies. The FFX mode of operation for format-preserving encryption. NIST Submission, 2010.

[57] Eric Brier, Thomas Peyrin, and Jacques Stern. BPS : A format preserving encryption proposal. NIST Submission, 2010.

[58] Kim R. Wagner and John Sheets. Visa format preserving encryption. NIST submission, 2011.

[59] Donghoon Chang, Mohona Ghosh, Kishan Chand Gupta, Arpan Jati, Abhishek Kumar, Dukjae Moon, Indranil Ghosh Ray, and Somitra Kumar Sanadhya. SPF: A new family of efficient format-preserving encryption algorithms. In *Information Security and Cryptology - 12th International Conference, Inscrypt 2016*, volume 10143 of *Lecture Notes in Computer Science*, pages 64–83. Springer, 2016.

[60] Kishan Chand Gupta, Sumit Kumar Pandey, and Indranil Ghosh Ray. Format preserving sets: On diffusion layers of format preserving encryption schemes. *Lecture Notes in Computer Science*, 10095:411–428, 2016.

[61] Donghoon Chang, Mohona Ghosh, Arpan Jati, Abhishek Kumar, and Somitra Kumar Sanadhya. eSPF: A family of format-preserving encryption algorithms using MDS matrices. In *Security, Privacy, and Applied Cryptography Engineering - 7th International Conference, SPACE 2017*, volume 10662 of *Lecture Notes in Computer Science*, pages 133–150. Springer, 2017.

[62] Rana Barua, Kishan Chand Gupta, Sumit Kumar Pandey, and Indranil Ghosh Ray. On diffusion layers of SPN based format preserving encryption schemes: Format preserving sets revisited. In *Progress in Cryptology - INDOCRYPT 2018*, volume 11356 of *Lecture Notes in Computer Science*, pages 91–104. Springer, 2018.

[63] Tapas Chatterjee and Ayantika Laha. A note on semi-orthogonal (G-matrix) and semi-involutory MDS matrices. *Finite Fields Appl.*, 92:Paper No. 102279, 27, 2023.

[64] Miroslav Fiedler and Frank J. Hall. G-matrices. *Linear Algebra Appl.*, 436(3):731–741, 2012.

[65] Gi-Sang Cheon, Bryan Curtis, and Hana Kim. Semi-involutory matrices and signed self-inverse. *Linear Algebra Appl.*, 622:294–315, 2021.

[66] Tapas Chatterjee and Ayantika Laha. A characterization of semi-involutory MDS matrices. submitted.

[67] Bernard Friedman. Eigenvalues of composite matrices. *Mathematical Proceedings of the Cambridge Philosophical Society*, 57(1):37–49, 1961.

[68] P. J. Davis. *Circulant Matrices*. John Wiley and Sons, 1979.

[69] Tapas Chatterjee and Ayantika Laha. On cyclic non-MDS matrices. submitted.

[70] Tapas Chatterjee and Ayantika Laha. On MDS properties of g-circulant matrices. submitted.

[71] Tapas Chatterjee and Ayantika Laha. On MDS properties of circulant matrices. submitted.

[72] A. A. Zain and B. Sundar Rajan. Algebraic characterization of MDS group codes over cyclic groups. *IEEE Trans. Inf. Theory*, 41(6):2052–2056, 1995.

[73] G.D. Forney. On the Hamming distance properties of group codes. *IEEE Transactions on Information Theory*, 38(6):1797–1801, 1992.

[74] Xue-Dong Dong, Boon Soh Cheong, and Erry Gunawan. Matrix characterization of MDS linear codes over modules. In *Linear Algebra and its Applications*, pages 57–61, 1998.

[75] Tapas Chatterjee, Ayantika Laha, and Somitra Kumar Sanadhya. On the structure of format preserving sets in the diffusion layer of block ciphers. *IEEE Trans. Inform. Theory*, 68(12):8268–8279, 2022.

[76] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, 2004, 3 edition, 2003.

[77] C. M. Ablow and J. L. Brenner. Roots and canonical forms for circulant matrices. *Trans. Amer. Math. Soc.*, 107:360–376, 1963.

[78] Miroslav Fiedler and Thomas L. Markham. More on G-matrices. *Linear Algebra Appl.*, 438(1):231–241, 2013.

[79] Zhe xian Wan. *Lectures On Finite Fields And Galois Rings*. World Scientific Publishing Company, 2003.

[80] Xuting Zhou and Tianshuo Cong. Construction of generalized-involutory MDS matrices. Cryptology ePrint Archive, Paper 2022/577, 2022.

Curriculum Vitae

Name	Ayantika Laha
Email	2018maz0008@iitrpr.ac.in
Phone	+91-8910893367
Address	Dhaniakhali, Hooghly, West Bengal, India-712302

Present Currently I am a Research Scholar in the Department of Mathematics at Indian Institute of Technology Ropar working under the guidance of Dr. Tapas Chatterjee. My research area of interest is broadly mathematical aspects of symmetric cryptography and related areas.

Education

2021-20xx	*Senior Research Fellow* , Department of Mathematics, Indian Institute of Technology Ropar.
2019-2021	*Junior Research Fellow* , Department of Mathematics, Indian Institute of Technology Ropar.
2014-2016	Post Graduation (Mathematical Sciences), Ballygunge Science College, University of Calcutta.
2011-2014	Graduation (Mathematical Sciences), Bethune College, University of Calcutta.

Publications

1. T. Chatterjee and A. Laha, *A note on Semi-Orthogonal (G-matrix) and Semi-Involutory MDS Matrices*, Finite Fields and Their Applications, **92** (2023), Paper No. 102279, 27.
2. T. Chatterjee, A. Laha and S. K. Sanadhya, *On the Structure of Format Preserving Sets in the Diffusion Layer of Block Ciphers*, IEEE Transactions on Information Theory, **68** (2022), no. 12, pp. 8268–8279.
3. T. Chatterjee and A. Laha, *A Characterization of Semi-Involutory MDS Matrices* (submitted).
4. T. Chatterjee and A. Laha, *On Cyclic non- MDS Matrices* (submitted).
5. T. Chatterjee and A. Laha, *On MDS Property of g-Circulant Matrices* (submitted).
6. T. Chatterjee and A. Laha, *On MDS Property of Circulant Matrices* (submitted).

Conferences / Workshop / Schools

1. Participated in Annual Foundation Schools (AFS-III) from 1st July to 27th July, 2019 organized by National Centre for Mathematics (NCM) at NISER, Bhubaneswar, India.
2. Participated in Workshop on Algebraic Number Theory held online during 31 August-5 September, 2020.
3. Participated in International Workshop on Cryptography and Coding Theory (IWCC) 2021 a virtual event held online during March 08-12, 2021.
4. Participated in IACR-VIASM Summer School on Cryptography held at Vietnam Institute for Advanced Study in Mathematics in Hanoi, Vietnam during August 24-30, 2022.
5. Participated in INDOCRYPT 2022 held at TCG Crest, Kolkata during December 11-14, 2022.
6. Presented a poster in Indian Women and Mathematics (IWM) Annual Conference 2022-2023 held at IISER Pune during December 27-29, 2022.
7. Participated in SEAMS School on Number Theory and Applications held at The Industrial University of Ho Chi Minh City, Vietnam during June 12-22, 2023.
8. Participated in Advanced Instructional School(AIS) in Advanced topics in Finite Fields held in Institute of Mathematical Sciences, Chennai during July 10-30, 2023.
9. Teaching assistant of Algebra in Annual Foundation School-I (AFS) held in Indian Institute of Technology, Ropar during December 4-30, 2023.
10. Delivered a talk entitled *On Semi-orthogonal and Semi-involutory MDS Matrices* in Cynosure 2024 and National Symposium on Advances in Mathematics held at IIT Ropar, India on February 22, 2024.

Teaching Assistant at IIT Ropar

1. MA202 Probability and Statistics, 2023(Jan-July)
2. MA415 Algebra, 2022(Jul-Dec)
3. MA102 Linear Algebra, Integral Transforms and Special Functions, 2022(Jan-Jul).
4. MA101 Calculus, 2021(Jul-Dec).
5. MA426 Theory of Computation, 2021(Jan-Jul).
6. MA415 Algebra , 2020(Jul-Dec).
7. MA102 Linear Algebra, Integral Transforms and Special Functions , 2020(Jan-Jul).
8. MA101 Calculus, 2019(Jul-Dec).

Computer Skills

Languages	C
Software	LaTeX, Sage, Open Office, Microsoft Office Suite.

Fellowships and Awards

1. Received INSPIRE scholarship by Department of Science and Technology, Government of India [2011-2016].
2. Qualified GATE (Graduate Aptitude Test in Engineering) , 2018.
3. Received IACR-SEAMS travel grant to attend IACR-VIASM Summer School on Cryptography [2022].
4. Received CIMPA travel grant to attend SEAMS School on Number Theory and Applications [2023].
5. Received IACR travel grant to attend Real World Cryptography Symposium [2024].
