Proceedings of Science and Mathematics
Faculty of science, universiti teknologi malaysia
https://science.utm.my/procscimath/
Volume 26 (2024) 71-78

On The Existence of MDS Matrices over $\mathcal{R}_{2,q}$

Defita[a,b], Intan Muchtadi-Alamsyah[b], Aleams Barra[b]
[a]Doctoral Program in Mathematics, Faculty of Mathematics and Natural Sciences, Bandung Institute of Technology, Bandung, Indonesia
[b]Algebra Research Group, Faculty of Mathematics and Natural Sciences, Bandung Institute of Technology, Bandung, Indonesia
*Corresponding author: defita9@gmail.com

Abstract
An MDS (maximum distance separable) matrix is a square matrix where all its submatrices are non-singular. The MDS matrices are used in some cryptographic systems' encryption and decryption processes. The decryption process involves using the inverse matrix from encryption, so choosing matrices with easily computable inverses is efficient. Orthogonal and involutory matrices are particularly advantageous in this regard. On the other hand, circulant matrices are more storage-efficient compared to general square matrices. Recent research highlights include Cauchois and Loidreau's 2019 proof that there is no involutory circulant MDS matrix of order $2m$ for $m \geq 2$ over a field with characteristics $p \geq 2$, and Adhiguna et al.'s 2022 finding that there is no orthogonal circulant MDS matrix of even order and order divisible by $p > 2$ over fields with characteristic p. Current research explores the existence of MDS matrices over the ring $\mathcal{R}_{2,q}$, defined as $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ where $v^3 = v$ and q is a power of a prime p. This paper shows that there is no involutory circulant MDS matrix and no orthogonal circulant MDS matrix of certain order over $\mathcal{R}_{2,q}$.
Keywords: finite ring; circulant matrix; orthogonal matrix; involutory matrix

Introduction

In today's digital age, advancements in technology continue to grow, greatly enhancing human convenience. Specifically within information and communication technology, numerous activities are now conducted through digital platforms like mobile phones and email. As these technologies evolve, ensuring secure communication is paramount to safeguarding messages from unauthorized access. Cryptographic systems serve as a crucial solution in ensuring the confidentiality and integrity of digital data.

Block ciphers, a form of cryptography widely used in digital data communication, consist of two main algorithms: encryption and decryption. The encryption algorithm converts the original messages (plaintext) into codes (ciphertext) before they are transmitted, while the decryption algorithm converts ciphertext to the plaintext before the messages are received.

In the design of block ciphers, Shannon introduced the concepts of confusion and diffusion [8]. Diffusion is achieved by a component of the algorithm known as the diffusion layer, while the confusion layer handles the algorithm's confusion process. The diffusion layer's role is to obscure the relationship between ciphertext and plaintext through linear mappings represented by matrices, which significantly influence its diffusion capability. The effectiveness of a matrix in the diffusion layer is measured by its branch number, with matrices possessing a large branch number being highly desirable. MDS (maximum distance separable) matrices, known for their maximum branch number, are commonly used in diffusion layers of many ciphers.

An MDS matrix is needed for more efficient computation, as it provides low complexity or minimizes memory in the encryption and decryption processes. On the other hand, an $n \times n$ circulant matrix has at most n different components. A circulant matrix is a matrix whose rows can be obtained from cyclic permutations of the first row. Thus, a circulant matrix is very profitable in terms of storage memory. In 1997, Daemen et al. found that the probability of finding a circulant MDS matrix is greater than a random square matrix [4]. The decryption process involves using the inverse of the MDS matrix used in the encryption process. Choosing an MDS matrix for which finding the inverse is straightforward is more efficient; examples include involutory MDS or orthogonal MDS matrices. An involutory matrix is one where its inverse is the matrix itself, while an orthogonal matrix has an inverse that is its transpose. Therefore, if a cryptosystem utilizes an orthogonal MDS or involutory MDS matrix, the decryption process uses either the matrix itself or its transpose, resulting in reduced memory complexity. An alternative for achieving low complexity is to utilize an involutory circulant MDS matrix or an orthogonal circulant MDS matrix.

Previous studies have demonstrated the existence of such circulant MDS matrices in fields with specific characteristics and at certain matrix sizes. Gupta and Ray (2015) [5] established that there is no $2n \times 2n$ orthogonal circulant MDS matrix over fields with characteristic 2, and they also proved the absence of $n \times n$ involutory circulant MDS matrix with $n \geq 3$ in such fields. Additionally, Cauchois and Loidreau (2019) [3] demonstrated that no $2n \times 2n$ involutory circulant MDS matrices exist over fields with prime characteristic $p \geq 3$ for $n \geq 2$. Furthermore, Adhiguna et al. (2022) [1] proved the non-existence of orthogonal circulant MDS matrices of even order and order divisible by a prime $p > 2$ over fields with characteristic p. This research investigates the presence of orthogonal and involutory circulant MDS matrices over the finite ring $\mathcal{R}_{2,q}$, defined as $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ where $v^3 = v$ and q is a power of prime number p.

MDS Matrices over Rings

Let R denotes a commutative ring with identity e, and R^n denotes the set of n-tuples of elements from R, which forms an R-module. A subset $\mathcal{C}$ of R^n is a linear code over R of length n if $\mathcal{C}$ is an R-submodule. If the code $\mathcal{C}$ is a linear code with length n and dimension k, then $\mathcal{C}$ is a linear code with parameter $[n, k]$. The elements in the linear code $\mathcal{C}$ are called codewords.

Let $\bar{c} = (c_1, c_2, \dots, c_n) \in \mathcal{C}$ be a codeword. The Hamming weight $wt(\bar{c})$ is the number of non-zero components of the code $\bar{c}$. For an element $x \in R$, the Hamming wight $wt(x)$ is defined as

$$wt(x) = \begin{cases} 1, & if\ x \neq 0 \\ 0, & if\ x = 0. \end{cases}$$

The Hamming distance of $\bar{x} = (x_1, x_2, \dots, x_n)$ and $\bar{y} = (y_1, y_2, \dots, y_n)$ in $\mathcal{C}$, denoted as $d(\bar{x}, \bar{y})$, is the number of distinct components between codewords $\bar{x}$ and $\bar{y}$. In other words, the Hamming distance $d(\bar{x}, \bar{y})$ is the Hamming weight of $(\bar{x} - \bar{y})$.

The Hamming distance function satisfies the properties of the metric space as follows.

1. $d(\bar{x}, \bar{y}) \geq 0$ for every $\bar{x}, \bar{y} \in R^n$.
2. $d(\bar{x}, \bar{y}) = 0$ if and only if $\bar{x} = \bar{y}$.
3. $d(\bar{x}, \bar{y}) = d(y, \bar{x}) \geq 0$ for each $\bar{x}, \bar{y} \in R^n$.
4. $d(\bar{x}, \bar{z}) \leq d(\bar{x}, \bar{y}) + d(\bar{y}, \bar{z})$ for each $\bar{x}, \bar{y}, \bar{z} \in R^n$.

For an arbitrary linear code $\mathcal{C}$, the Hamming distance of $\mathcal{C}$, denoted as $d(\mathcal{C})$ or d, is the smallest Hamming distance between any two non-zero codewords in $\mathcal{C}$:

$$d = \min\{d(\bar{x}, \bar{y}) | for\ every\ \bar{x}, \bar{y} \in \mathcal{C}\}.$$

The Hamming distance d can be considered as the smallest Hamming weight of the non-zero codewords in $\mathcal{C}$:

$$d = \min\{wt(\bar{c}) | for\ every\ \bar{c} \in \mathcal{C}\}.$$

Linear code $\mathcal{C}$ is called an $[n, k, d]$ linear code if it has length n, dimension k and a Hamming distance d. The relationship between n, k and d is given in the following theorem.

Theorem 1 [7]

If $\mathcal{C}$ is an $[n, k, d]$ linear code then $d \leq n - k + 1$.

Definition 1 [7]
An $[n, k, d]$ linear code is called an MDS (maximum distance separable) code if it satisfies

$$d = n - k + 1.$$

The generator matrix of an $[n, k, d]$ linear code $\mathcal{C}$ is a matrix G where its rows form a basis of $\mathcal{C}$. It has size $k \times n$. By performing elementary row operations, the matrix G can be written in standard form, that is

$$G = \left[I_k \middle| M_{k\times(n-k)}\right].$$

where I_k is the identity matrix of size $k \times k$ and M is a $k \times (n - k)$ matrix. An MDS code can be characterized by its generator matrix.

Theorem 2 [7]
An $[n, k, d]$ linear code $\mathcal{C}$ with generator matrix $G = [I_k|M]$ is an MDS code if and only if every square submatrix of M is non-singular.

In other words, Theorem 2 gives information that the matrix M is an MDS matrix if and only if the code $\mathcal{C}$ is an MDS code.

Next, we will provide the definitions of the matrices central to this study: circulant matrix, orthogonal matrix and involutory matrix.

Definition 2 [3]
Let R denotes a commutative ring and A be an $n \times n$ matrix over R.

1. Matrix A is called a/an circulant matrix if it can be expressed as

$$A = circ(\bar{a}) = circ(a_0, a_1, \dots, a_{n-1}) = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix}$$

   where $a_0, a_1, \dots, a_{n-1} \in R$.
2. Matrix A is called a/an orthogonal matrix if $AA^T = I_n$.
3. Matrix A is called a/an involutory matrix if $A^2 = I_n$.

where I_n is the identity matrix of size $n \times n$.

The Ring $\mathcal{R}_{2,q}$
Let $p \geq 2$ be a prime number, $q = p^r$ for some positif integer r and $\mathbb{F}_q$ be the finite field with q elements. The ring $\mathcal{R}_{2,q}$ is defined by $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q := \{a + vb + v^2c | a, b, c \in \mathbb{F}_q \text{ with } v^2 = v\}$. It is isomorphic to the polynomial ring $\frac{\mathbb{F}_q[v]}{<v^3 - v>}$. The unit elements in the ring $\mathcal{R}_{2,q}$ are described in the following lemma.

Lemma 1
Any element $a + vb + v^2c \in \mathcal{R}_{2,q}$ is a unit if and only if a, $a + b + c$ and $a - b + c$ are units in $\mathbb{F}_q$.

Proof.
($\Longrightarrow$) Let $a + vb + v^2c \in \mathcal{R}_{2,q}$ be a unit. Then there is an element $x + vy + v^2z \in \mathcal{R}_{2,q}$ such that $(a + vb + v^2c)(x + vy + v^2z) = 1$. Note that

$$\begin{aligned} & (a + vb + v^2c)(x + vy + v^2z) = 1 \\ \Leftrightarrow\ & ax + v(bx + ay + cy + bz) + v^2(cx + by + az + cz) = 1 \\ \Leftrightarrow\ & ax = 1, bx + ay + cy + bz = 0, \text{and } cx + by + az + cz = 0 \\ \Leftrightarrow\ & ax = 1, ax + (bx + ay + cy + bz) + (cx + by + az + cz) = 1 \\ & \text{and } ax - (bx + ay + cy + bz) + (cx + by + az + cz) = 1 \end{aligned}$$

$\Leftrightarrow ax = 1, (a+b+c)(x+y+z) = 1, (a-b+c)(x-y+z) = 1$
$\Leftrightarrow a, (a+b+c)$ and $(a-b+c)$ are units in $\mathbb{F}_q$.

($\Longleftarrow$) Let $a + vb + v^2c \in \mathcal{R}_{2,q}$ such that $a, (a+b+c)$ and $(a-b+c)$ are units in $\mathbb{F}_q$. Then there are x, s and t in $\mathbb{F}_q$ such that $ax = 1, (a+b+c)(2s) = 1$ and $(a-b+c)(2t) = 1$. Write $y = s - t$ and $z = s + t - x$, then

$$\begin{aligned}(a+vb+v^2c)(x+vy+v^2z) &= ax + v[bx+ay+cy+bz] + v^2[cx+by+az+cz]\\ &= ax + v[(a+c)y + b(x+z)] + v^2[(a+c)(x+z) - ax + by]\\ &= ax + v[(a+c)(s-t) + b(s+t)] + v^2[(a+c)(s+t) - ax + b(s-t)]\\ &= ax + v[(a+b+c)s - (a-b+c)t] + v^2[-ax + (a+b+c)s\\ &\quad +(a-b+c)t]\\ &= ax\\ &= 1\end{aligned}$$

Hence, $a + vb + v^2c \in \mathcal{R}_{2,q}$ is a unit.

By applying the Chinese Remainder Theorem, we can obtain orthogonal idempotent elements in $\mathcal{R}_{2,q}$. These elements are $(1-v^2)$, $\frac{p+1}{2}(v^2+v)$ and $\frac{p+1}{2}(v^2-v)$ that satisfy

$$(1-v^2) + \frac{p+1}{2}(v^2+v) + \frac{p+1}{2}(v^2-v) = 1.$$

Every element $a + vb + v^2c$ in the ring $\mathcal{R}_{2,q}$ can be uniquely written as

$$(1-v^2)a + \frac{p+1}{2}(v^2+v)(b+c) + \frac{p+1}{2}(v^2-v)(c-b)$$

For simplicity of the writing, we use the notation $\mu_1 = (1-v^2)$, $\mu_2 = \frac{p+1}{2}(v^2+v)$ and $\mu_3 = \frac{p+1}{2}(v^2-v)$. Therefore, we can write every element $a + vb + v^2c$ in the ring $\mathcal{R}_{2,q}$ as

$$a + vb + v^2c = \mu_1(a) + \mu_2(b+c) + \mu_3(c-b).$$

Matrices over $\mathcal{R}_{2,q}$

In this section, we will present some results regarding the properties of matrices over the ring $\mathcal{R}_{2,q}$. Let A be an $n \times n$ matrix over $\mathcal{R}_{2,q}$, written as follows

$$A = [a_{ij} + vb_{ij} + v^2c_{ij}] = \begin{bmatrix} a_{11}+vb_{11}+v^2c_{11} & a_{12}+vb_{12}+v^2c_{12} & \dots & a_{1n}+vb_{1n}+v^2c_{1n} \\ a_{21}+vb_{21}+v^2c_{21} & a_{22}+vb_{22}+v^2c_{22} & \dots & a_{2n}+vb_{2n}+v^2c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}+vb_{n1}+v^2c_{n1} & a_{n2}+vb_{n2}+v^2c_{n2} & \dots & a_{nn}+vb_{nn}+v^2c_{nn} \end{bmatrix}$$

Then A can be uniquely written as

$$A = \mu_1 A_1 + \mu_2 A_2 + \mu_3 A_3 \qquad (1)$$

where $A_1 = [a_{ij}]$, $A_2 = [b_{ij} + c_{ij}]$ and $A_3 = [c_{ij} - b_{ij}]$.

If A is an $n \times n$ circulant matrix over $\mathcal{R}_{2,q}$ and written as equation (1), note that

$$\begin{aligned}A &= circ(a_{11}+vb_{11}+v^2c_{11}, \dots, a_{1n}+vb_{1n}+v^2c_{1n})\\ &= circ(\mu_1[a_{11}] + \mu_2[b_{11}+c_{11}] + \mu_3[c_{11}-b_{11}], \dots, \mu_1[a_{1n}] + \mu_2[b_{1n}+c_{1n}] + \mu_3[c_{1n}-b_{1n}])\\ &= circ(\mu_1[a_{11}], \dots, \mu_1[a_{1n}]) + circ(\mu_2[b_{11}+c_{11}], \dots, \mu_2[b_{1n}+c_{1n}])\\ &\quad + circ(\mu_3[c_{11}-b_{11}], \dots, \mu_3[c_{1n}-b_{1n}])\\ &= \mu_1 circ([a_{11}], \dots, [a_{1n}]) + \mu_2([b_{11}+c_{11}], \dots, [b_{1n}+c_{1n}]) + \mu_3 circ([c_{11}-b_{11}], \dots, [c_{1n}-b_{1n}])\\ &= \mu_1 A_1 + \mu_2 A_2 + \mu_3 A_3\end{aligned}$$

Therefore, A is a circulant matrix if and only if A_1, A_2 and A_3 are circulant matrices. The following theorems present results concerning the properties of matrices over the ring $\mathcal{R}_{2,q}$.

Theorem 3

Let $A \in [\mathcal{R}_{2,q}]^{n\times n}$ written as equation (1). Then A is an orthogonal matrix if and only if A_1, A_2 and A_3 are orthogonal matrices.

Proof.
We have

$$AA^T = \mu_1 A_1 A_1^T + \mu_2 A_2 A_2^T + \mu_3 A_3 A_3^T$$

($\Longrightarrow$) Suppose A is orthogonal and $AA^T = [w_{ij}], A_1 A_1^T = [x_{ij}], A_2 A_2^T = [y_{ij}], A_3 A_3^T = [z_{ij}]$.

- For the $(ij)^{th}$ entry where $i \neq j$, we have

$$w_{ij} = \mu_1 x_{ij} + \mu_2 y_{ij} + \mu_3 z_{ij}$$
$$\Longrightarrow w_{ij} = (1 - v^2)x_{ij} + \left(\frac{p+1}{2}\right)(v^2 + v)y_{ij} + \left(\frac{p+1}{2}\right)(v^2 - v)z_{ij}$$
$$\Longrightarrow 1 = x_{ij} + v\left(\frac{p+1}{2}\right)(y_{ij} - z_{ij}) + v^2\left[\left(\frac{p+1}{2}\right)(y_{ij} + z_{ij}) - x_{ij}\right]$$
$$\Longrightarrow x_{ij} = 1, y_{ij} - z_{ij} = 0, \left(\frac{p+1}{2}\right)y_{ij} + \left(\frac{p+1}{2}\right)z_{ij} - x_{ij} = 0$$
$$\Longrightarrow x_{ij} = 1, y_{ij} - z_{ij} = 0, \frac{1}{2}y_{ij} + \frac{1}{2}z_{ij} = 1$$
$$\Longrightarrow x_{ij} = y_{ij} = z_{ij} = 1$$

- For the $(ij)^{th}$ entry where $i = j$, we have

$$w_{ij} = \mu_1 x_{ij} + \mu_2 y_{ij} + \mu_3 z_{ij}$$
$$\Longrightarrow w_{ij} = (1 - v^2)x_{ij} + \left(\frac{p+1}{2}\right)(v^2 + v)y_{ij} + \left(\frac{p+1}{2}\right)(v^2 - v)z_{ij}$$
$$\Longrightarrow 0 = x_{ij} + v\left(\frac{p+1}{2}\right)(y_{ij} - z_{ij}) + v^2\left[\left(\frac{p+1}{2}\right)(y_{ij} + z_{ij}) - x_{ij}\right]$$
$$\Longrightarrow x_{ij} = 0, y_{ij} - z_{ij} = 0, \left(\frac{p+1}{2}\right)y_{ij} + \left(\frac{p+1}{2}\right)z_{ij} - x_{ij} = 0$$
$$\Longrightarrow x_{ij} = 0, y_{ij} - z_{ij} = 0, \frac{1}{2}y_{ij} + \frac{1}{2}z_{ij} = 1$$
$$\Longrightarrow x_{ij} = y_{ij} = z_{ij} = 0$$

Hence**,** A_1, A_2 and A_3 are orthogonal matrices.
($\Longleftarrow$) Suppose A_1, A_2 and A_3 are orthogonal matrices, such that $A_1 A_1^T = A_2 A_2^T = A_3 A_3^T = I_n$. We have

$$\begin{aligned} AA^T &= \mu_1 A_1 A_1^T + \mu_2 A_2 A_2^T + \mu_3 A_3 A_3^T \\ &= \mu_1 I_n + \mu_2 I_n + \mu_3 I_n \\ &= I_n \end{aligned}$$

Therefore, A is also an orthogonal matrix.

Theorem 4
Let $A \in [\mathcal{R}_{2,q}]^{n\times n}$ written as equation (1). Then A is an involutory matrix if and only if A_1, A_2 and A_3 are involutory matrices.

Proof.
The proof is almost similar to the proof of the Theorem 3.

Theorem 5
Let $A \in [\mathcal{R}_{2,q}]^{n\times n}$ written as equation (1). Then

$$det(A) = \mu_1 \det(A_1) + \mu_2 \det(A_2) + \mu_3 \det(A_3)$$

Proof.
We will prove this by mathematical induction on the matrix size.

- For $n = 2$, we have

$$\begin{aligned} A &= \begin{pmatrix} a_{11} + vb_{11} + v^2 c_{11} & a_{12} + vb_{12} + v^2 c_{12} \\ a_{21} + vb_{21} + v^2 c_{21} & a_{22} + vb_{22} + v^2 c_{22} \end{pmatrix} \\ &= \mu_1 \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \mu_2 \begin{pmatrix} b_{11} + c_{11} & b_{12} + c_{12} \\ b_{21} + c_{21} & b_{22} + c_{22} \end{pmatrix} + \mu_3 \begin{pmatrix} c_{11} - b_{11} & c_{12} - b_{12} \\ c_{21} - b_{21} & c_{22} - b_{22} \end{pmatrix} \end{aligned}$$

$= \mu_1 A_1 + \mu_2 A_2 + \mu_3 A_3$

Note that

$$\begin{aligned}\det(A) &= \begin{vmatrix} a_{11} + vb_{11} + v^2c_{11} & a_{12} + vb_{12} + v^2c_{12} \\ a_{21} + vb_{21} + v^2c_{21} & a_{22} + vb_{22} + v^2c_{22} \end{vmatrix} \\ &= (a_{11} + vb_{11} + v^2c_{11})(a_{22} + vb_{22} + v^2c_{22}) - (a_{12} + vb_{12} + v^2c_{12})(a_{21} + vb_{21} + v^2c_{21}) \\ &= [\mu_1 a_{11} + \mu_2(b_{11} + c_{11}) + \mu_3(c_{11} - b_{11})][\mu_1 a_{22} + \mu_2(b_{22} + c_{22}) + \mu_3(c_{22} - b_{22})] - \\ &\quad [\mu_1 a_{12} + \mu_2(b_{12} + c_{12}) + \mu_3(c_{12} - b_{12})][\mu_1 a_{21} + \mu_2(b_{21} + c_{21}) + \mu_3(c_{21} - b_{21})] \\ &= [\mu_1 a_{11}a_{22} + \mu_2(b_{11} + c_{11})(b_{22} + c_{22}) + \mu_3(c_{11} - b_{11})(c_{22} - b_{22})] - \\ &\quad [\mu_1 a_{12}a_{21} + \mu_2(b_{12} + c_{12})(b_{21} + c_{21}) + \mu_3(c_{12} - b_{12})(c_{21} - b_{21})] \\ &= \mu_1[a_{11}a_{22} - a_{12}a_{21}] + \mu_2[(b_{11} + c_{11})(b_{22} + c_{22}) - (b_{12} + c_{12})(b_{21} + c_{21})] + \\ &\quad \mu_3[(c_{11} - b_{11})(c_{22} - b_{22}) - (c_{12} - b_{12})(c_{21} - b_{21})] \\ &= \mu_1 \det(A_1) + \mu_2 \det(A_2) + \mu_3 \det(A_3)\end{aligned}$$

Therefore, the statement holds for $n = 2$.

- Assume that for $n = m - 1$ the statement holds. We will prove for $n = m$.

  Now, let $A \in [\mathcal{R}_{2,q}]^{m\times m}$. We can write $A = [a_{ij} + vb_{ij} + v^2c_{ij}]$ as

  $$A = \mu_1 A_1 + \mu_2 A_2 + \mu_3 A_3$$

  where $A_1 = [a_{ij}], A_2 = [b_{ij} + c_{ij}]$ and $A_3 = [c_{ij} - b_{ij}]$.

  Let W_{1i} be the minor of $a_{1i} + vb_{1i} + v^2c_{1i}$ in A, X_{1i} be the minor of a_{1i} in A_1, Y_{1i} be the minor of $(b_{1i} + c_{1i})$ in A_2 and Z_{1i} be the minor of $(c_{1i} - b_{1i})$ in A_3. Notice that

  $$\det(A_1) = \sum_{i=1}^{m} (-1)^n \, a_{1i}X_{1i}$$

  $$\det(A_2) = \sum_{i=1}^{m} (-1)^n \, (b_{1i} + c_{1i})Y_{1i}$$

  $$\det(A_3) = \sum_{i=1}^{m} (-1)^n \, (c_{1i} - b_{1i})Z_{1i}$$

  Now, suppose D_{1i} be a submatrix of A where the 1^{st} row and i^{th} column are deleted. Matrix D_{1i} for $i = 1, \dots, m$ can be uniquely written as $D_{1i} = \mu_1 D_{1i}^1 + \mu_2 D_{1i}^2 + \mu_3 D_{1i}^3$. Hence, W_{1i} is $\det(D_{1i})$, X_{1i} is $\det(D_{1i}^1)$, Y_{1i} is $\det(D_{1i}^2)$ and Z_{1i} is $\det(D_{1i}^3)$. By the hypothesis, we have

  $$W_{1i} = \mu_1 X_{1i} + \mu_2 Y_{1i} + \mu_3 Z_{1i}$$

  for $i = 1, \dots, m$. Hence, we have

  $$\begin{aligned}\det(A) &= \sum_{i=1}^{m} (-1)^n \, (a_{1i} + vb_{1i} + v^2c_{1i})W_{1i} \\ &= \sum_{i=1}^{m} (-1)^n \, [\mu_1 a_{1i} + \mu_2(b_{1i} + c_{1i}) + \mu_3(c_{1i} - b_{1i})][\mu_1 X_{1i} + \mu_2 Y_{1i} + \mu_3 Z_{1i}] \\ &= \sum_{i=1}^{m} (-1)^n \, [\mu_1 a_{1i}X_{1i} + \mu_2(b_{1i} + c_{1i})Y_{1i} + \mu_3(c_{1i} - b_{1i})Z_{1i}] \\ &= \mu_1 \sum_{i=1}^{m} (-1)^n \, a_{1i}X_{1i} + \mu_2 \sum_{i=1}^{m} (-1)^n \, (b_{1i} + c_{1i})Y_{1i} + \mu_3 \sum_{i=1}^{m} (-1)^n \, (c_{1i} - b_{1i})Z_{1i} \\ &= \mu_1 \det(A_1) + \mu_2 \det(A_2) + \mu_3 \det(A_3)\end{aligned}$$

  We conclude that the statement holds for $n = m$.

Theorem 6

Let $A \in [\mathcal{R}_{2,q}]^{n\times n}$ written as equation (1). Then $\det(A)$ is a unit in $\mathcal{R}_{2,q}$ if and only if $\det(A_1), \det(A_2)$ and $\det(A_3)$ are units in $\mathbb{F}_q$.

Proof.

From the previous theorem, we have

$$\begin{aligned}\det(A) &= \mu_1 \det(A_1) + \mu_2 \det(A_2) + \mu_3 \det(A_3) \\ &= (1-v^2)\det(A_1) + \left(\frac{p+1}{2}\right)(v^2+v)\det(A_2) + \left(\frac{p+1}{2}\right)(v^2-v)\det(A_3) \\ &= \det(A_1) + v\left(\frac{p+1}{2}\right)[\det(A_2) - \det(A_3)] + v^2\left[-\det(A_1) + \left(\frac{p+1}{2}\right)(\det(A_2) - \det(A_3))\right].\end{aligned}$$

Based on Lemma 1, we conclude that $\det(A)$ is a unit if and only if $\det(A_1)$, $\det(A_2)$ and $\det(A_3)$ are units in $\mathbb{F}_q$.

Orthogonal and Involutory Circulant MDS Matrices over $\mathcal{R}_{2,q}$

The following are previous results about circulant MDS matrices of a certain order, wheter involutory or orthogonal, in a field with a prime characteristic p.

Theorem 7 [3]

Let $p \geq 2$ be a prime number, $m \geq 2$.Then there is no involutory circulant MDS matrix over a field of characteristic p of order $2m$.

In 2022, Adhiguna et al. proved this theorem.

Theorem 8 [1]

Let $p > 2$ be a prime number, $k \geq 2$ be an integer and $n = kp$. Then there is no orthogonal circulant MDS matrix over a field of characteristic p of order n and of even order.

Based on previous results and properties of matrices over $\mathcal{R}_{2,q}$, we prove the non-existence of certain order involutory circulant MDS matrices and orthogonal circulant MDS matrices over $\mathcal{R}_{2,q}$.

Theorem 9

Let $p \geq 2$ is a prime number and $q = p^r$ for some positif integer r. Then there is no involutory circulant MDS matrix over $\mathcal{R}_{2,q}$ of order $2m$ for $m \geq 2$.

Proof.

Assume that there is an involutory circulant MDS matrix over $\mathcal{R}_{2,q}$ of order $n = 2m$ for $m \geq 2$, namely matrix $A = \left[a_{ij} + vb_{ij} + v^2 c_{ij}\right]^{n\times n}$. Matrix A can be uniquely written as $A = \mu_1 A_1 + \mu_2 A_2 + \mu_3 A_3$ where $A_1 = \left[a_{ij}\right]^{n\times n}, A_2 = \left[b_{ij} + c_{ij}\right]^{n\times n}$ and $A_3 = \left[c_{ij} - b_{ij}\right]^{n\times n}$ are circulant matrices over $\mathbb{F}_q$. By Theorem 4 and Theorem 6, we have

$$\det(A) = \mu_1 \det(A_1) + \mu_2 \det(A_2) + \mu_3 \det(A_3).$$

where A_1, A_2 and A_3 are also involutory circulant matrices. Let matrix $A_1' = \left[a_{ij}\right]^{k\times k}$ be any submatrix of A_1. Choose $A_2' = \left[b_{ij} + c_{ij}\right]^{k\times k}$ and $A_3' = \left[c_{ij} - b_{ij}\right]^{k\times k}$ such that

$$A' = \left[a_{ij} + vb_{ij} + v^2 c_{ij}\right]^{k\times k} = \mu_1 A_1' + \mu_2 A_2' + \mu_3 A_3'.$$

It is clear that $\det(A') = \mu_1 \det(A_1') + \mu_2 \det(A_2') + \mu_3 \det(A_3')$ and A' is submatrix of A. Since matrix A is MDS, then $\det(A')$ is a unit. It implies $\det(A_1')$, $\det(A_2')$ and $\det(A_3')$ are units by Theorem 7. Hence, matrix A_1 is an involutory circulant MDS matrix over $\mathbb{F}_q$ of order $n = 2m$ for an $m \geq 2$. It contradicts Cauchois' result in Theorem 7.

Theorem 10

Let $p > 2$ be a prime number, $q = p^r$ for some positif integer r, and $k \geq 2$ be an integer and $n = kp$. Then there is no orthogonal circulant MDS matrix over $\mathcal{R}_{2,q}$ of order n and of even order.

Proof.

The proof is almost similar as the proof of Theorem 9.

Conclusion

There is no involutory circulant MDS matrix of order $2m$ for $m \geq 2$ over $\mathcal{R}_{2,q}$. For integer and $k \geq 2$, there is no orthogonal circulant MDS matrix over $\mathcal{R}_{2,q}$ of order kp and of even order.

Acknowledgement

This research is supported by Hibah P2MI ITB 2024.

References

[1] Adhiguna, I., Arifin, I.S.N, Yuliawan, F., I. and Muchtadi-Alamsyah. (2022). On Orthogonal Circulant MDS Matrices. International Journal of Mathematics and Computer Science, 17(4), 1619-1637.

[2] Ali, S., Khan, A.A. and Singh, B. (2024). On Circulant Involutory and Orthogonal MDS Matrices over Finite Commutative Rings. Applicable Algebra in Engineering, Communication and Computing, pp. 1-15, https://doi.org/10.1007/s00200-024-00656-4.

[3] Cauchois, V. and Loidreau, P. (2019). On Circulant Involutory MDS Matrices. Designs, Codes and Cryptography, 87(4), 249-260.

[4] Daemen, J., Knudsen, L. R., and Rijmen, V. (1997). The block cipher SQUARE. 4th International Workshop, Fast Software Encryption, Haifa, Israel, pp. 149-165.

[5] Gupta, K. C. and Ray, I. G. (2015). Cryptographically Significant MDS Matrices Based on Circulant and Circulant-like Matrices for Lightweight Applications. Cryptography and Communications, 7(2), 257-287.

[6] Kesarwani, A., Pandey, S., Sarkar, S., Venkateswarlu, A. (2021). Recursive MDS Matrices over Finite Commutative Rings. Discret. Appl. Math. 304, pp. 384-396.

[7] MacWilliams, F. J. and Sloane, N. J. A. (1977). MDS Code in The Theory of Error Correcting Codes. North-Holland Publishing Co., pp. 9-321.

[8] Shannon, C. E. (1949). Communication Theory of Secrecy Systems. Bell Syst. Technical J., 28(4), 656-715.