Mathematics and Statistics 12(1): 63-68, 2024
DOI: 10.13189/ms.2024.120109 http://www.hrpub.org

On The Existence of MDS Matrices over $\mathcal{B}_{k,q}$

Defita[1,2,*], **Intan Muchtadi-Alamsyah**[2], **Aleams Barra**[2]

[1] Doctoral Program in Mathematics, Faculty of Mathematics and Natural Sciences, Bandung Institute of Technology, Indonesia

[2] Algebra Research Group, Faculty of Mathematics and Natural Sciences, Bandung Institute of Technology, Indonesia

Received July 24, 2023; Revised November 10, 2023; Accepted November 20, 2023

Cite This Paper in the following Citation Styles

***(a)**: [1] Defita, Intan Muchtadi-Alamsyah, Aleams Barra, "On The Existence of MDS Matrices over," Mathematics and Statistics, Vol.12, No.1, pp. 63-68, 2024. DOI: 10.13189/ms.2024.120109*

***(b)**: Defita, Intan Muchtadi-Alamsyah, Aleams Barra (2024). On The Existence of MDS Matrices over. Mathematics and Statistics, 12(1), 63-68. DOI: 10.13189/ms.2024.120109*

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 matrix used in the process of decryption is the inverse matrix used in the encryption. Therefore, choosing a matrix which inverse is easy to find, is more efficient. Orthogonal and involutory matrices are two kinds of matrices in which inverses are easy to find. On the other hand, in terms of storage memory, a circulant matrix is more advantageous than any square matrix. In 2019, Cauchois and Loidreau proved that there is no involutory circulant MDS matrices of order $2m$ for $m \geq 2$ over a field of characteristics prime number $p \geq 2$. In 2022, Adhiguna et al. stated that there is no orthogonal circulant MDS matrix of even order and of order divisible by $p > 2$ over a field with characteristic p. This research concerns about observing the existence of MDS matrices over ring $\mathcal{B}_{1,q}$, that is, the ring $\mathbb{F}_q + v\mathbb{F}_q$ where $v^2 = v$ and q is the power of p. This paper shows that there is no involutory circulant MDS and no orthogonal circulant MDS matrices of certain order over $\mathcal{B}_{1,q}$. Furthermore, we can generalize these results for ring $\mathcal{B}_{k,q}$.

Keywords Finite Ring, Circulant Matrix, Orthogonal Matrix, Involutory Matrix, MDS Matrix

1 Introduction

In this digital era, technological developments multiply and make human life more managable. Especially in the development of information and communication technology, many human activities can be carried out through digital media, such as mobile phones, electronic mail, etc. In the process, we need a system that can guarantee security so that a message cannot be read by anyone other than the recipient. The cryptographic system is one of the solutions used to ensure the confidentiality and integrity of digital data.

One of the widely used cryptography in digital data communication is the block cipher. The block cipher has two algorithms: the encryption and the decryption. The encryption algorithm converts the original messages (plaintext) into codes (ciphertext) before the messages are sent. Instead, the decryption algorithm converts ciphertext to the plaintext before the messages are received. In general, block ciphers are vulnerable to two kinds of attacks: differential cryptanalysis and linear cryptanalysis [1].

One can apply the concepts of confusion and diffusion to avoid these attacks. Shannon first introduced these concepts in 1994 [2]. The algorithm component that performs the diffusion process is called the diffusion layer. A matrix can represent linear mapping in the diffusion layer.

An MDS (Maximum Distance Separable) 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 [3].

The decryption process uses the inverse of the MDS matrix used in the encryption process. Choosing an MDS in which the inverse is easy to find is more efficient; for example, an involutory or orthogonal MDS matrix. An involutory matrix is a matrix in which the inverse is itself. Meanwhile, an orthogonal matrix is a matrix where the inverse is its transpose. As a result, if a cryptosystem uses an orthogonal MDS matrix or an

involutory MDS matrix, then the decryption process uses the matrix itself or its transpose. Thus, it provides low memory complexity as well.

An alternative to obtaining low complexity is to use an involutory circulant MDS matrix or an orthogonal circulant MDS matrix. Several previous studies have proven the existence of a circulant MDS matrix, either involutory or orthogonal, in a field with specific characteristics and at a certain matrix size. Gupta and Ray in 2015 [4] proved that there is no a $2n \times 2n$ orthogonal circulant MDS matrix for fields with characteristics 2. In addition, they also proved that there is no an $n \times n$ involutory circulant MDS matrix with $n \geq 3$ for fields with characteristics 2. Then in 2019, Cauchois and Loidreau [5] proved that for a field with characteristics prime number $p \geq 2$, there is no $2n \times 2n$ involutory circulant MDS matrix with $n \geq 2$. Moreover, in 2022, Adhiguna et al. [6] proved that there is no orthogonal circulant MDS matrix with even order and of order multiple p for fields with characteristics prime number $p > 2$. In this research, we will examine the existence of an orthogonal circulant MDS matrix and an involutory circulant MDS matrix over the finite ring $\mathcal{B}_{k,q} = \dfrac{\mathbb{F}_q[v_1, \cdots, v_k]}{\langle v_i^2 = v_i, v_i v_j = v_j v_i \rangle}, 1 \leq i, j \leq k$ where q is the power of prime number p. This ring was introduced by Irwansyah et al. in 2017 [8].

2 MDS Matrices over Ring

Let R denotes a commutative ring with identity, R^n denotes the set of n-tuples of elements of R. It is an R-module. A set $\mathcal{C}$, subset of R^n, is a linear code over R with 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 parameters $[n, k]$. The elements in the linear code $\mathcal{C}$ are called codewords.

Let $\bar{c} = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$ be a codeword. The Hamming weight is the number of non-zero components of the code $\bar{c}$, denoted as $wt(\bar{c})$.

Definition 2.1. *The Hamming weight wt of an element $a \in R$ is defined as*

$$wt(a) = \begin{cases} 1 & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases}$$

for each $a \in R$.

The Hamming distance of $\bar{a} = (a_1, a_2, \ldots, a_n)$ and $\bar{b} = (b_1, b_2, \ldots, b_n)$ in $\mathcal{C}$, denoted as $d(\bar{a}, \bar{b})$ is the number of distinct components in codeword $\bar{a}$ and codeword $\bar{b}$. The Hamming distance can be viewed as a mapping

$$R^n \times R^n \longrightarrow \mathbb{C}$$
$$(\bar{a}, \bar{b}) \longrightarrow d(\bar{a}, \bar{b}) := |\{i \in 1, 2, \ldots, n | a_i \neq b_i\}|$$

In other words, the Hamming distance $d(\bar{a}, \bar{b})$ is the Hamming weight of $(\bar{a} - \bar{b})$,

$$d(\bar{a}, \bar{b}) = wt(\bar{a} - \bar{b}).$$

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

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

For an arbitrary linear code $\mathcal{C}$, the Hamming distance of $\mathcal{C}$ is the smallest Hamming distance of all possible non-zero codewords in $\mathcal{C}$.

Definition 2.2. *Let R denote a ring and $\mathcal{C} \subseteq R^n$ is a linear code over R. The Hamming distance of $\mathcal{C}$, $d(\mathcal{C})$ or d, is defined as*

$$d = \min\{d(\bar{a}, \bar{b}) | \text{ for every } \bar{a}, \bar{b} \in R^n\}$$

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

$$d = \min\{wt(\bar{c}) | \text{ for every } \bar{c} \neq 0 \in \mathcal{C}\}.$$

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

Theorem 2.3. *[7] If $\mathcal{C}$ is an $[n, k, d]$ linear code then $d \leq n - k + 1$.*

Definition 2.4. *An $[n, k, d]$ linear code is called an MDS code (maximum distance separable) if it satisfies $d = n - k + 1$.*

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

$$M = \begin{bmatrix} I_k & | & B_{k \times n-k}. \end{bmatrix}$$

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

Theorem 2.5. *[7] An $[n, k, d]$ linear code $\mathcal{C}$ with generator matrix $M = [I_k | B]$ is an MDS code if and only if every square submatrix of B is non-singular.*

In other words, Theorem 2.5 gives information that the matrix B is an MDS matrix if and only if the code $\mathcal{C}$ is an MDS code.

Next, the definitions of the matrices that will be used in this study will be given; these are the circulant matrix, orthogonal matrix, and involutory matrix.

Definition 2.6. *Let R denotes a commutative ring and A an $n \times n$ matrix over R.*

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

$$\begin{aligned} A &= circ\,(\bar{z}) \\ &= circ(z_0, z_1, \cdots, z_{n-1}) \\ &= \begin{bmatrix} z_0 & z_1 & \cdots & z_{n-1} \\ z_{n-1} & z_0 & \cdots & z_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ z_1 & z_2 & \cdots & z_0 \end{bmatrix} \end{aligned}$$

where $z_0, z_1, \cdots, z_{n-1} \in R$.

2. *Matrix A is called an orthogonal if $AA^T = I_n$.*
3. *Matrix A is called an involutory matrix if $A^2 = I_n$.*

3 The ring $\mathcal{B}_{k,q}$

Let $p > 2$ 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 $\mathcal{B}_{1,q}$ is defined by

$$\mathbb{F}_q + v\mathbb{F}_q := \{a + vb \mid a, b \in \mathbb{F}_q\}$$

with $v^2 = v$. It is isomorphic to the polynomial ring $\frac{\mathbb{F}_q[v]}{\langle v^2 - v\rangle}$.

If we have k variabel: $v_1, v_2, \ldots, v_k$, we can define ring $\mathcal{B}_{k,q}$ as a generalization of ring $\mathcal{B}_{1,q}$, and it is isomorphic to the polinomial ring

$$\frac{\mathbb{F}_q[v_1, \cdots, v_k]}{\langle v_i^2 - v_i, v_i v_j - v_j v_i\rangle}, 1 \le i, j \le k.$$

The following lemma gives another way of writing the elements in the ring $\mathcal{B}_{k,q}$ and it will be very useful in this research.

Lemma 3.1. *[8] Every element in the ring $\mathcal{B}_{k,q}$ can be written as $\alpha + v_k\beta$, where α, β in $\mathcal{B}_{k-1,q}$.*

For $k = 1$, we have $\mathcal{B}_{k-1,q} = \mathcal{B}_{0,q}$ and we can view $\mathcal{B}_{0,q}$ as the finite field $\mathbb{F}_q$. The unit elements in ring $\mathcal{B}_{k,q}$ are described in the following lemma.

Lemma 3.2. *[8] Any element $a + v_k b \in \mathcal{B}_{k,q}$ is a unit if and only if both a and $a + b$ are units in $\mathcal{B}_{k-1,q}$.*

Proof. ($\Longrightarrow$) Let $a + v_k b \in \mathcal{B}_{k,q}$ be a unit. Then there is an element $c + v_k d \in \mathcal{B}_{k,q}$ such that $(a + v_k b)(c + v_k d) = 1$. Note that

$$\begin{aligned}(a + v_k b)(c + v_k d) = 1 &\iff ac = 1 \text{ and } ad + bc + bd = 0\\ &\iff ac = 1 \text{ and } (a + b)(c + d) = 1\\ &\Longrightarrow a \text{ and } (a + b) \text{ are units}\end{aligned}$$

So we have both a and $a + b$ are units in $\mathcal{B}_{k-1,q}$.

($\Longleftarrow$) Let $a + v_k b \in \mathcal{B}_{k,q}$ such that a and $a + b$ are units in $\mathcal{B}_{k-1,q}$. Then there are $c, x \in \mathcal{B}_{k-1,q}$ such that

$$ac = 1 \text{ and } (a + b)x = 1.$$

Write $x = c + d$, then $d = x - c$. Note that

$$\begin{aligned}(a + v_k b)(c + v_k d) &= ac + v_k[(a + b)d + bc]\\ &= ac + v_k[(a + b)(x - c) + bc]\\ &= ac + v_k[(a + b)(-xbc) + bc]\\ &= ac + v_k[(a + b)(x)(-bc) + bc]\\ &= ac + v_k[(-bc) + bc]\\ &= ac\\ &= 1\end{aligned}$$

So we have $a + v_k b \in \mathcal{B}_{k,q}$ is a unit. □

4 Matrices over $\mathcal{B}_{k,q}$

In this section, we will give some results about the properties of matrices over ring $\mathcal{B}_{k,q}$.

Let $A \in [\mathcal{B}_{k,q}]^{n\times n}$ be a matrix over $\mathcal{B}_{k,q}$ of order n, that is

$$A = \begin{bmatrix} a_{1,1} + v_k b_{1,1} & a_{1,2} + v_k b_{1,2} & \cdots & a_{1,n} + v_k b_{1,n}\\ a_{2,1} + v_k b_{2,1} & a_{2,2} + v_k b_{2,2} & \cdots & a_{2,n} + v_k b_{2,n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{n,1} + v_k b_{n,1} & a_{n,2} + v_k b_{n,2} & \cdots & a_{n,n} + v_k b_{n,n}\end{bmatrix}$$

Then A can be uniquely written as

$$A = v_k A_1 + (1 - v_k)A_2 \tag{1}$$

where

$$A_1 = \begin{bmatrix} a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} & \cdots & a_{1,n} + b_{1,n}\\ a_{2,1} + b_{2,1} & a_{2,2} + b_{2,2} & \cdots & a_{2,n} + b_{2,n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{n,1} + b_{n,1} & a_{n,2} + b_{n,2} & \cdots & a_{n,n} + b_{n,n}\end{bmatrix}$$

and

$$A_2 = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n}\\ a_{2,1} & a_{2,2} & \cdots & a_{2,n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{n,1} & a_{n,2} & \cdots & a_{n,n}\end{bmatrix}$$

Thus the matrix set $[\mathcal{B}_{k,q}]^{n\times n}$ can be decomposed into a direct sum ($\oplus$) of two matrix sets as follows.

$$[\mathcal{B}_{k,q}]^{n\times n} = v_k[\mathcal{B}_{k-1,q}]^{n\times n} \oplus (1 - v_k)[\mathcal{B}_{k-1,q}]^{n\times n}.$$

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

$$\begin{aligned}A &= circ[(a_{1,1} + v_k b_{1,1}),\ \cdots,\ (a_{1,n} + v_k b_{1,n})]\\ &= circ[v_k(a_{1,1} + b_{1,1}) + (1 - v_k)a_{1,1},\ \cdots,\\ &\quad v_k(a_{1,n} + b_{1,n}) + (1 - v_k)a_{1,n}]\\ &= circ[v_k(a_{1,1} + b_{1,1}),\ \cdots,\ v_k(a_{1,n} + b_{1,n})]\\ &\quad + circ[(1 - v_k)a_{1,1},\ \cdots,\ (1 - v_k)a_{1,n}]\\ &= v\, circ[(a_{1,1} + b_{1,1}),\ \cdots,\ (a_{1,n} + b_{1,n})]\\ &\quad + (1 - v_k)circ[a_{1,1},\ \cdots,\ a_{1,n}]\\ &= v_k A_1 + (1 - v_k)A_2.\end{aligned}$$

Therefore, A is a circulant matrix if and only if A_1 and A_2 are circulant matrices.

The following theorems give some results about properties of matrix over ring $\mathcal{B}_{k,q}$.

Theorem 4.1. *Let $A \in [\mathcal{B}_{k,q}]^{n\times n}$ written as equation (1). Then A is an orthogonal matrix if and only if A_1 and A_2 are orthogonal matrices.*

Proof. We have

$$\begin{aligned}AA^T &= [v_k A_1 + (1 - v_k)A_2][v_k A_1 + (1 - v_k)A_2]^T\\ &= v_k A_1 A_1^T + (1 - v_k)A_2 A_2^T.\end{aligned}$$

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

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

$$\begin{aligned} & x_{i,j} = v_k y_{i,j} + (1 - v_k) z_{i,j} \\ \implies & 1 = z_{i,j} + v_k (y_{i,j} - z_{i,j}) \\ \implies & z_{i,j} = 1 \text{ and } y_{i,j} = 1. \end{aligned}$$

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

$$\begin{aligned} & x_{i,j} = v_k y_{i,j} + (1 - v_k) z_{i,j} \\ \implies & 0 = z_{i,j} + v_k (y_{i,j} - z_{i,j}) \\ \implies & z_{i,j} = 0 \text{ and } y_{i,j} = 0. \end{aligned}$$

Hence both A_1 and A_2 are orthogonal matrices.

($\Longleftarrow$) Suppose A_1 and A_2 are orthogonal matrices, such that

$$A_1 A_1^T = I_n \text{ and } A_2 A_2^T = I_n$$

We have

$$\begin{aligned} AA^T &= v_k A_1 A_1^T + (1 - v_k) A_2 A_2^T \\ &= v_k I_n + (1 - v_k) I_n \\ &= I_n \end{aligned}$$

Therefore, A is also an orthogonal matrix. □

Theorem 4.2. *Let $A \in [\mathcal{B}_{k,q}]^{n \times n}$ written as equation (1). Then A is involutory matrix if and only if A_1 and A_2 are involutory matrices.*

Proof. The proof is almost similar to the proof of the previous theorem. □

Theorem 4.3. *Let $A \in [\mathcal{B}_{k,q}]^{n \times n}$ written as equation (1). Then*

$$det(A) = v_k \det(A_1) + (1 - v_k) \det(A_2) \tag{2}$$

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

- For $n = 2$, we have

$$\begin{aligned} A &= \begin{bmatrix} a_{1,1} + v_k b_{1,1} & a_{1,2} + v_k b_{1,2} \\ a_{2,1} + v_k b_{2,1} & a_{2,2} + v_k b_{2,2} \end{bmatrix} \\ &= v_k \begin{bmatrix} a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} \\ a_{2,1} + b_{2,1} & a_{2,2} + b_{2,2} \end{bmatrix} \\ &\quad + (1 - v_k) \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \\ &= v_k A_1 + (1 - v_k) A_2 \end{aligned}$$

Notice that

$$\begin{aligned} & \det(A) \\ &= \begin{vmatrix} a_{1,1} + v_k b_{1,1} & a_{1,2} + v_k b_{1,2} \\ a_{2,1} + v_k b_{2,1} & a_{2,2} + v_k b_{2,2} \end{vmatrix} \\ &= \begin{vmatrix} v_k(a_{1,1} + b_{1,1}) + (1 - v_k) a_{1,1} & v_k(a_{1,2} + b_{1,2}) + (1 - v_k) a_{1,2} \\ v_k(a_{2,1} + b_{2,1}) + (1 - v_k) a_{2,1} & v_k(a_{2,2} + b_{2,2}) + (1 - v_k) a_{2,2} \end{vmatrix} \\ &= \left[v_k(a_{1,1} + b_{1,1}) + (1 - v_k) a_{1,1} \right] \left[v_k(a_{2,2} + b_{2,2}) + (1 - v_k) a_{2,2} \right] - \\ &\quad \left[v_k(a_{1,2} + b_{1,2}) + (1 - v_k) a_{1,2} \right] \left[v_k(a_{2,1} + b_{2,1}) + (1 - v_k) a_{2,1} \right] \\ &= v_k \left[(a_{1,1} + b_{1,1})(a_{2,2} + b_{2,2}) \right] + (1 - v_k) \left[(a_{1,1})(a_{2,2}) \right] - \\ &\quad v_k \left[(a_{1,2} + b_{1,2})(a_{2,1} + b_{2,1}) \right] + (1 - v_k) \left[(a_{1,2})(a_{2,1}) \right] \\ &= v_k \left[(a_{1,1} + b_{1,1})(a_{2,2} + b_{2,2}) - (a_{1,2} + b_{1,2})(a_{2,1} + b_{2,1}) \right] + \\ &\quad (1 - v_k) \left[(a_{1,1})(a_{2,2}) - (a_{1,2})(a_{2,1}) \right] \\ &= v_k \det(A_1) + (1 - v_k) \det(A_2). \end{aligned}$$

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

- Assume that for $n = k - 1$ the statement holds. We will prove for $n = k$.
Now let $A \in [\mathcal{B}_{k,q}]^{n \times n}$. We can write A as $A = v_k A_1 + (1 - v_k) A_2$ where

$$A = \left[a_{i,j} + v_k b_{i,j} \right], A_1 = \left[a_{i,j} + b_{i,j} \right], \text{ and } A_2 = \left[a_{i,j} \right].$$

Let M_{1i} be the minor of $(a_{1,i} + v_k b_{1,i})$ in A, $M_{1i}^{(1)}$ be the minor of $(a_{1,i} + b_{1,i})$ in A_1 and $M_{1i}^{(2)}$ be the minor of $(a_{1,i})$ in A_2. Notice that

$$\det(A_1) = \sum_{i=1}^{n} (-1)^{1+i} (a_{1,i} + b_{1,i}) M_{1,i}^{(1)} \tag{3}$$

$$\det(A_2) = \sum_{i=1}^{n} (-1)^{1+i} (a_{1,i}) M_{1,i}^{(2)}. \tag{4}$$

Now, suppose $D_{1,i}$ be a submatrix of A where the 1^{st} row and i^{th} column are deleted. Matrix $D_{1,i}$ for $i = 1, 2, \ldots, n$ can be uniquely written as

$$D_{1,i} = v_k D_{1,i}^{(1)} + (1 - v_k) D_{1,i}^{(2)}$$

Hence, $M_{1,i}$ is $\det(D_{1,i})$, $M_{1,i}^{(1)}$ is $\det(D_{1,i}^{(1)})$ and $M_{1,i}^{(2)}$ is $\det(D_{1,i}^{(2)})$. By the hypothesis, we have

$$M_{1,i} = v_k M_{1,i}^{(1)} + (1 - v_k) M_{1,i}^{(2)} \text{ for } i = 1, 2, \ldots, n.$$

Hence we have

$$\begin{aligned} \det(A) &= \sum_{i=1}^{n} (-1)^{1+i} (a_{1,i} + v_k b_{1,i}) M_{1,i} \\ &= \sum_{i=1}^{n} (-1)^{1+i} [v_k (a_{1,i} + b_{1,i}) + (1 - v_k) a_{1,i}] \\ &\quad [v_k M_{1,i}^{(1)} + (1 - v_k) M_{1,i}^{(2)}] \\ &= \sum_{i=1}^{n} (-1)^{1+i} [v_k (a_{1,i} + b_{1,i}) M_{1,i}^{(1)} \\ &\quad + (1 - v_k)(a_{1,i}) M_{1,i}^{(2)}] \\ &= v_k \left(\sum_{i=1}^{n} (-1)^{1+i} (a_{1,i} + b_{1,i}) M_{1,i}^{(1)} \right) \\ &\quad + (1 - v_k) \left(\sum_{i=1}^{n} (-1)^{1+i} (a_{1,i}) M_{1,i}^{(2)} \right) \\ &= v_k \det(A_1) + (1 - v_k) \det(A_2) \end{aligned}$$

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

□

Theorem 4.4. *Let $A \in [\mathcal{B}_{k,q}]^{n \times n}$ written as equation (1). Then $\det(A)$ is a unit in $\mathcal{B}_{k,q}$ if and only if both $\det(A_1)$ and $\det(A_2)$ are units in $\mathcal{B}_{k-1,q}$.*

Proof. Suppose A is an $n \times n$ matrix over $\mathcal{B}_{k,q}$ written as $A = v_k A_1 + (1 - v_k)A_2$ where

$$A = \left[a_{i,j} + v_k b_{i,j}\right], A_1 = \left[a_{i,j} + b_{i,j}\right], \text{ and } A_2 = \left[a_{i,j}\right].$$

Let M_{1i} be the minor of $(a_{1,i}+v_k b_{1,i})$ in A, $M_{1i}^{(1)}$ be the minor of $(a_{1,i} + b_{1,i})$ in A_1 and $M_{1i}^{(2)}$ be the minor of $(a_{1,i})$ in A_2. We also have equation (3) and equation (4). Note that

$$\begin{aligned}
\det(A) &= \sum_{i=1}^{n}(-1)^{1+i}(a_{1,i} + v_k b_{1,i})M_{1i} \\
&= \sum_{i=1}^{n}(-1)^{1+i}\left[v_k(a_{1,i} + b_{1,i}) + (1 - v_k)(a_{1,i})\right] \\
&\quad \left[v_k M_{1i}^{(1)} + (1 - v_k)M_{1i}^{(2)}\right] \\
&= v_k \left(\sum_{i=1}^{n}(-1)^{1+i}\left[(a_{1,i} + b_{1,i})M_{1i}^{(1)} - (a_{1,i})M_{1i}^{(2)}\right]\right) \\
&\quad + \left(\sum_{i=1}^{n}(-1)^{1+i}(a_{1,i})M_{1i}^{(2)}\right) \\
&= v_k\left[\det(A_1) - \det(A_2)\right] + \det(A_2)
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
&\det(A) \text{ is a unit in } \mathcal{B}_{k,q} \\
&\iff v_k\left[\det(A_1) - \det(A_2)\right] + \det(A_2) \text{ is a unit in } \mathcal{B}_{k,q} \\
&\iff \det(A_2) \text{ and } \left[\det(A_1) - \det(A_2)\right] + \det(A_2) \\
&\quad \text{are units in } \mathcal{B}_{k-1,q} \\
&\iff \det(A_1) \text{ and } \det(A_2) \text{ are units in } \mathcal{B}_{k-1,q}
\end{aligned}$$

□

5 Orthogonal and Involutory Circulant MDS Matrices over $\mathcal{B}_{k,q}$

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

Theorem 5.1. *[5] Let $p \geq 2$ be a prime number, $m \geq 2$. Then there is no involutory circulant MDS matrices over a field of characteristic p of order $2m$. .*

In 2022, Adhiguna et al. proved this theorem.

Theorem 5.2. *[6] 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.*

Fisrt we will prove the non-existence of certain order involutory circulant MDS matrices and orthogonal circulant MDS matrices over $\mathcal{B}_{1,q}$.

Theorem 5.3. *Let $p \geq 2$ be a prime number and $q = p^r$. Then there is no involutory circulant MDS matrices over $\mathcal{B}_{1,q}$ of order $2m$ for $m \geq 2$.*

Proof. Assume that there is an involutory circulant MDS matrix over $\mathcal{B}_{1,q}$ of order $n = 2m$ for $m \geq 2$, namely matrix $M = [a_{i,j} + vb_{i,j}]_{n\times n}$. Matrix M can be uniquely written as

$$M = vM_1 + (1 - v)M_2$$

where $M_1 = [a_{i,j} + b_{i,j}]_{n\times n}$ and $M_2 = [a_{i,j}]_{n\times n}$ are matrices over $\mathbb{F}_q$. And by Theorem 4.2 and Theorem 4.3 we have

$$\det(M) = v\det(M_1) + (1 - v)\det(M_2)$$

where M_1, M_2 are also involutory circulant matrices. Let $M_1' = [a_{i_1,j_1} + b_{i_1,j_1}]_{k\times k}$ be any submatrix of M_1. Choose matrix $M_2' = [a_{i_1,j_1}]_{k\times k}$ such that

$$M' = [a_{i_1,j_1} + vb_{i_1,j_1}]_{k\times k} = vM_1' + (1 - v)M_2'.$$

It is clear that $\det(M') = v\det(M_1')+(1-v)\det(M_2')$ and M' is submatrix of M. Since matrix M is MDS, then $\det(M')$ is a unit. It implies both $\det(M_1')$ and $\det(M_2')$ are units by Theorem 4.4. Hence, matrix M_1 is an involutory circulant MDS matrix over $\mathbb{F}_q$ of order $2m$ for an $m \geq 2$. It contradicts Cauchois' result in Theorem 5.1. □

Theorem 5.4. *Let $p > 2$ be a prime number, $q = p^r$, $k \geq 2$ be an integer and $n = kp$. Then there is no orthogonal circulant MDS matrix over $\mathcal{B}_{1,q}$ of order n and of even order.*

Proof. The proof is almost similar as the proof of the previous theorem. □

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

Theorem 5.5. *Let $p \geq 2$ be a prime number and $q = p^r$. Then there is no involutory circulant MDS matrices over $\mathcal{B}_{k,q}$ of order $2m$ for $m \geq 2$.*

Proof. This theorem will be proved using mathematical induction on the numbers k in $\mathcal{B}_{k,q}$.

- From Theorem 5.3, we have proved for ring $\mathcal{B}_{1,q}$. Hence, the statement holds for $k = 1$.
- Assume that the statement holds for $k - 1$. It means that there is no involutory circulant MDS matrix over $\mathcal{B}_{k-1,q}$ of order $n = 2m$ for $m \geq 2$. Suppose that there is an involutory circulant MDS matrix over $\mathcal{B}_{k,q}$ of order $n = 2m$ for $m \geq 2$, namely matrix $M = [a_{i,j} + v_k b_{i,j}]_{n\times n}$. Matrix M can be uniquely written as

  $$M = v_k M_1 + (1 - v_k)M_2.$$

  and from Theorem 4.2 and 4.3 we have

  $$\det(M) = v_k\det(M_1) + (1 - v_k)\det(M_2)$$

  where $M_1 = [a_{i,j} + b_{i,j}]_{n\times n}, M_2 = [a_{ij}]_{n\times n}$ are also involutory circulant. Let $M_1' = [a_{i_1,j_1} + b_{i_1,j_1}]_{t\times t}$ be any

submatrix of M_1. Choose matrix $M_2' = [a_{i_1,j_1}]_{t\times t}$ such that

$$M' = [a_{i_1,j_1} + v_k b_{i_1,j_1}]_{k\times k} = v_k M_1' + (1 - v_k)M_2'$$

and satisfy

$$\det(M') = v_k \det(M_1') + (1 - v_k) \det(M_2')$$

It is clear that M' is submatrix of M. Since matrix M is MDS, then $\det(M')$ is a unit. Based on Theorem 3.2, it implies both $\det(M_1')$ and $\det(M_2')$ are units. So that, matrix M_1 is involutory circulant MDS matrix over $\mathcal{B}_{k-1,q}$ of order $2m$ for an $m \geq 2$. It is contradiction with the hypothesis.

□

Theorem 5.6. *Let $p > 2$ be a prime number, $q = p^r$, $k \geq 2$ be an integer and $n = kp$. Then there is no orthogonal circulant MDS matrix over $\mathcal{B}_{k,q}$ of order n and of even order.*

Proof. The proof is almost similar as the proof of Theorem 5.5. □

6 Conclusions

We have proved that there is no involutory circulant MDS matrix over $\mathcal{B}_{k,q}$ of order $2m$ for $m \geq 2$ and there is no orthogonal circulant MDS matrix over $\mathcal{B}_{k,q}$ of even order and of order divisible by p. For further research we will look for a method to construct involutory or orthogonal cirulant MDS matrices over $\mathcal{B}_{k,q}$ of certain order, beside the orders mentioned in Theorem 5.5 and 5.6, if they exist. We will also try to investigate the existence of MDS Matrices over the Galois ring $GR(p^m, k)$.

Acknowledgements

This research is supported by Hibah PPMI ITB 2023.

REFERENCES

[1] Daemen, J. and Rijmen, V., "Preliminaries," in The Design of Rijndael: AES - The Advanced Encryption Standard, Springer-Verlag, 2002, pp. 20-21

[2] Shannon, C. E., "Communication Theory of Secrecy Systems," Bell Syst. Technical J., vol. 28, no. 4, pp. 656-715, 1949, https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

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

[4] Gupta, K. C. and Ray, I. G., "Cryptographically Significant MDS Matrices Based on Circulant and Circulant-like Matrices for Lightweight Applications,", Cryptography and Communications, vol. 7, no. 2, pp. 257-287, 2015, DOI: 10.1007/s12095-014-0116-3

[5] Cauchois, V. and Loidreau, P., "On Circulant Involutory MDS Matrices," Designs, Codes and Cryptography, vol. 87, no. 4, pp. 249-260, 2019, DOI: 10.1007/s10623-018-0520-3

[6] Adhiguna, I., Arifin, I.S.N, Yuliawan, F., I. Muchtadi-Alamsyah, "On Orthogonal Circulant MDS Matrices," International Journal of Mathematics and Computer Science, vol. 17, no. 4, pp. 1619-1637, 2022, http://ijmcs.future-in-tech.net/17.4/R-Muchtadi.pdf

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

[8] Irwansyah, A. Barra, I. Muchtadi-Alamsyah, A.Muchlis, and D. Suprijanto, "Skew-cyclic codes over B_k," Journal of Applied Mathematics and Computing, vol. 57, no. 4, 2018, DOI: 10.1007/s12190-017-1095-2