Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 4, pp. 1595–1608
DOI : 10.47974/JDMSC-2315

A note on MDS property of circulant matrices

Tapas Chatterjee *
Department of Mathematics
Indian Institute of Technology Ropar
Ropar
Punjab
India

Ayantika Laha †
Department of Computer Science and Engineering
Indian Institute of Technology Palakkad
Palakkad
Kerala
India

Abstract

In 2014, Gupta and Ray proved that the circulant involutory matrices over the finite field $\mathbb{F}_{2^m}$ can not be maximum distance separable (MDS). This non-existence also extends to circulant orthogonal matrices of order $2^d \times 2^d$ over finite fields of characteristic 2. These findings inspired many authors to generalize the circulant property for constructing lightweight MDS matrices with practical applications in mind. Recently, in 2022, Chatterjee and Laha initiated a study of circulant matrices by considering semi-involutory and semi-orthogonal properties. Expanding on their work, this paper establishes a link between the trace of associated diagonal matrices and the MDS property of matrices over the finite field $\mathbb{F}_{2^m}$. Given that existing constructions of circulant MDS matrices rely on exhaustive search methods, our result introduces a necessary condition for a circulant semi-orthogonal (or semi-involutory) matrix to be MDS. Specifically, we prove that for circulant semi-orthogonal matrices of even order and circulant semi-involutory matrices, if the trace of the associated diagonal matrices is non-zero, the matrix cannot be MDS.

Subject Classification (2020): *Primary 15B10, 12E20, 94A60, Secondary 15B05.*
Keywords: *Circulant matrices, MDS matrices, Semi-involutory matrices, Semi-orthogonal matrices.*

This paper was posted on arXiv before being submitted to this journal (arxiv.org/pdf/2406.16973).

* *ORCID-ID:* 0000-0002-6956-2322
† *ORCID-ID:* 0000-0001-8406-3006

* *E-mail:* tapasc@iitrpr.ac.in (Corresponding Author)
† *E-mail:* ayantikalaha@iitpkd.ac.in

1. Introduction

Maximum Distance Separable (MDS) matrices have gained significant attention since their implementation in the block cipher SHARK [24] in 1996. These matrices play a vital role in ensuring optimal diffusion in the diffusion layer of the cipher, thereby enhancing the cipher's resilience against both differential and linear cryptanalysis. As a consequence, many block ciphers such as SQUARE [9], AES [10], Twofish [28], and hash functions like PHOTON [13], Whirlpool [1] incorporate MDS matrices for enhancing the overall security of these cryptographic systems.

Two primary approaches for constructing MDS matrices are recursive and non-recursive. In recursive construction, we mainly start with a sparse matrix A of order $n \times n$ with entries from a finite field such that A^n is an MDS matrix. Notably, the block cipher LED [14] and the hash function PHOTON use recursive MDS matrices, which are constructed from companion matrices. On the other hand, in non-recursive constructions, various types of matrices are employed to directly construct MDS matrices. This involves leveraging the algebraic properties of the matrix and making appropriate choices for the entries from the finite fields.

In 1996, Youssef, Mister and Tavares [30] used a Cauchy matrix to construct an involutory MDS matrix. The involutory property is crucial in block cipher implementations, as it ensures that the same MDS matrix M can be used for both encryption and decryption. Therefore, finding efficient MDS matrices that are also involutory or orthogonal is of particular interest. In 2004, Lacan and Fimes [20] introduced a method for constructing MDS matrices using two Vandermonde matrices with entries selected from a finite field. Later, in 2012, Sajadieh *et al.* [27] demonstrated that the Vandermonde-based MDS matrix construction proposed by Lacan and Fimes [20] could be transformed into an involutory matrix. Additionally, in [15], the authors presented a direct construction of MDS matrices using a Cauchy matrix. Since then, several direct constructions of MDS matrices have been proposed, leveraging the distinct properties of Cauchy and Vandermonde matrices. Recursive constructions offer another approach to constructing MDS matrices. In [19], the authors employ shortened BCH codes for recursive construction, while in [22], Reed-Solomon codes are used for the construction of 8×8 self-reciprocal recursive MDS matrices over the field $\mathbb{F}_{p^r}$.

Another class of matrices that gained a significant attention in the construction of MDS matrices is the circulant matrix. The block cipher AES uses a 4×4 circulant MDS matrix in its diffusion layer, chosen for its lightweight characteristics. The matrix is circulant$(\alpha, \alpha + 1,1,1)$ with entries from the finite field $\mathbb{F}_{2^8}$, where α is a root of the polynomial $x^8 + x^4 + x^3 + x + 1$. Its lightweight nature is due to the two ones in the first row and the fact that a circulant matrix of order $n \times n$ can have at most n distinct entries. However, this matrix is neither involutory nor orthogonal. In 2014, Gupta and Ray [16, 17] showed that the circulant orthogonal matrix of order $2^d \times 2^d$ can not be MDS when their entries are from a finite field of characteristic 2. They also demonstrated that circulant matrices of order $n \geq 3$ can not simultaneously be involutory and MDS over the finite field $\mathbb{F}_{2^m}$. However, circulant MDS and circulant orthogonal MDS matrices of odd orders do exist, though they have been constructed through exhaustive search.

These two non-existence results motivated further exploration of circulant-like matrices with MDS properties. In [25, 26], Sarkar and Syed explored Toeplitz matrices, examining their involutory, orthogonal, and MDS properties. Similarly, Hankel matrices with these characteristics were studied in [18]. In [21], Liu and Sim generalized circulant matrices to cyclic matrices by changing the permutations and demonstrated the potential for left-circulant matrices to be MDS and involutory. In 2022, Chatterjee and Laha initiated a study of circulant matrices with semi-involutory and semi-orthogonal properties with entries from a finite field in [3, 5]. Subsequently, in [4, 6], Chatterjee and Laha studied cyclic matrices and g-circulant matrices, meticulously analyzing their involutory, orthogonal, semi-involutory, semi-orthogonal and MDS characteristics. In all these cases, verifying the MDS property for circulant and generalized circulant matrices requires checking the determinants of all square submatrices.

Many authors have continued the search for MDS matrices from finite fields to rings and modules. In 1995, Zain and Rajan defined MDS codes over cyclic groups [31] and Dong, Cheong, and Gunawan characterized MDS codes over elementary Abelian groups [11]. By considering a finite Abelian group as a torsion module over a PID, Chatterjee, Laha and Sanadhya proved some non-existent results of MDS matrices in 2022 [7]. In [2], Cauchois and Loidreau introduced θ-circulant matrices over the quasi-polynomial ring. They proposed a construction for θ-circulant almost-involutory MDS matrix over the quasi-polynomial ring. Furthermore, in [29], the authors study the construction of non-linear MDS diffusion layers over finite fields of characteristic 2.

2. Contribution

In Section 4 of this article, we explore circulant semi-orthogonal matrices over the finite field $\mathbb{F}_{2^m}$. We establish that, for an order of $2^d \times 2^d$, the associated diagonal matrices of a circulant semi-orthogonal matrix have trace zero. For other even orders, matrices are classified based on whether the order k is congruent to 0 or 2 modulo 4. Specifically, for $k \equiv 0 \pmod 4$, we demonstrate that if the circulant semi-orthogonal matrix possesses the MDS property, the trace of the associated diagonal matrices is guaranteed to be zero. For other even orders, an additional condition on the diagonal matrices is necessary for the trace to be zero. Similarly, in Section 5, we present analogous results for circulant semi-involutory matrices of order $n \geq 3$.

3. Preliminaries

In this section, we describe the notations and important definitions we use throughout the paper.

We begin with some notations and definitions from [23]. Let $\mathbb{F}_q$ denote a finite field with q elements where q is power of a prime p. Let $\mathcal{C}$ be an

$[n,k,d]$ linear error correcting code over the finite field $\mathbb{F}_q$ with length n, dimension k, and minimum Hamming distance d. The code $\mathcal{C}$ is a k dimensional subspace of $\mathbb{F}_q^n$. The generator matrix G of $\mathcal{C}$ is a $k \times n$ matrix with the standard form $[I|A]$, where I is a $k \times k$ identity matrix and A is $k \times n - k$ matrix. The Singleton bound states that, for a $[n,k,d]$ code, $n - k \geq d - 1$. An $[n,k,n-k+1]$ code is called a maximum distance separable (MDS) code. Another definition of an MDS code in terms of a generator matrix is the following.

Definition 3.1: An $[n,k,d]$ code $\mathcal{C}$ with the generator matrix $G = [I|A]$, where A is a $k \times (n-k)$ matrix, is *MDS* if and only if every $i \times i$ submatrix of A is non-singular, $i = 1,2,,min(k, n-k)$.

This definition of MDS code gives the following characterization of an MDS matrix.

Definition 3.2: A square matrix A is said to be MDS if every square submatrix of A is non-singular.

MDS matrices with easily implementable inverses play a crucial role in the decryption layer of an SPN based block cipher. Therefore, either the involutory or orthogonal property of MDS matrices is essential. Here A^{-1} denotes the inverse of A, A^T denotes the transpose of A and I is the identity matrix.

Definition 3.3: A square matrix A is said to be involutory if $A^2 = I$ and orthogonal if $AA^T = A^TA = I$. Also the trace of a square matrix is the sum of the elements in the main diagonal.

In 2012, Fielder *et al.* generalized the orthogonal property of matrices to semi-orthogonal in [12]. The definition of a semi-orthogonal matrix is as follows.

Definition 3.4: A non-singular matrix M is semi-orthogonal if there exist non-singular diagonal matrices D_1 and D_2 such that $M^{-T} = D_1MD_2$, where M^{-T} denotes the transpose of the matrix M^{-1}.

We refer to the matrices D_1 and D_2 in Definition 3.3 as associated diagonal matrices for the semi-orthogonal matrix A.

Following that, in 2021, Cheon, Curtis and Kim [8] defined semi-involutory matrices as a generalization of the involutory matrices. The definition of a semi-involutory matrix is as follows.

Definition 3.5: 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 $M^{-1} = D_1MD_2$.

We refer to the matrices D_1 and D_2 in Definition 3.5 as associated diagonal matrices for the semi-involutory matrix A.

As previously mentioned, circulant matrices find application in the diffusion layer. In this context, we now provide definitions for circulant matrices and their generalizations. Let A be an $n \times n$ matrix. The i-th row of A is denoted by R_i

for $0 \leq i \leq n-1$ and the j-th column as C_j for $0 \leq j \leq n-1$. Furthermore, $A[i, j]$ denotes the entry at the intersection of the i-th row and j-th column. The definition of a circulant matrix is the following.

Definition 3.6: The square matrix of the form $\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{k-1} & c_0 & c_1 & \cdots & c_{n-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}$ is said to be circulant matrix and denoted by $\mathcal{C} =$ circulant$(c_0, c_1, c_2, , c_{n-1})$.

The entries of the circulant matrix $\mathcal{C}$ can be expressed as $\mathcal{C}[i, j] = c_{j-i}$, where subscripts are calculated modulo n.

The determinant of a circulant matrix of order $n \times n$ is

$$\det(\mathcal{C}) = \prod_{j=0}^{n-1} \left(\sum_{l=0}^{n-1} c_l \omega_n^{jl}\right), \tag{1}$$

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

In [3], Chatterjee and Laha proved the following result for circulant semi-involutory matrices over a finite field.

Theorem 3.7: *Let A be an $n \times n$ circulant matrix over a finite field. 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 $A^{-1} = D_1 A D_2$.*

The analogous result for circulant semi-orthogonal matrices over a finite field is as follows.

Theorem 3.8: *A be an $n \times n$ circulant matrix over a finite field. 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 $A^{-T} = D_1 A D_2$.*

4. Circulant matrices with MDS and semi-orthogonal properties

In [16, 17], Gupta and Ray proved that circulant orthogonal matrices of order $2^d \times 2^d$ can not be MDS over a finite field of characteristic 2. After that, in 2023, Chatterjee and Laha [3] studied semi-involutory and semi-orthogonal properties of circulant matrices. They showed that in a circulant semi-orthogonal matrix of order $n \times n$, the n-th power of the associated diagonal matrices are scalar matrices.

Leveraging this property, 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 4.1: 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 $A^{-T} = D_1AD_2$, where D_1 and D_2 are non-singular diagonal matrices. Let $D_1 = \text{diagonal}(d_0, d_1, d_2, \dots, d_{2^d-1})$ and $D_2 = \text{diagonal}$ $(e_0, e_1, e_2, \dots, e_{2^d-1})$. 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 scalars k_1, k_2 of the finite field by Theorem 3.8. 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-orthogonal matrices of even orders other than powers of 2, the following two theorems establish a significant relationship between the MDS property and the trace of the associated diagonal matrices.

Theorem 4.2: *Let A be a circulant, semi-orthogonal matrix of order $2^i n \times 2^i n$ over the finite field $\mathbb{F}_{2^m}$ with associated diagonal matrices D_1 and D_2, where $i > 1$ 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 $2^i n = k$ and $A =$ circulant $(a_0, a_1, a_2, \dots, a_{k-1})$. Since A is semi-orthogonal, we have $A^{-T} = D_1AD_2$, where D_1 and D_2 are non-singular diagonal matrices given by $D_1 =$ diagonal $(d_0, d_1, d_2, \dots, d_{k-1})$ and $D_2 = \text{diagonal}(e_0, e_1, e_2 \dots, e_{k-1})$. 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 $M[0,1], M[1,2], M[2,3], \dots, M[k-2, k-1], M[k-1, 0]$:

$$\begin{gathered}
(\textstyle\sum_{i=0}^{k-1} a_i a_{i+1}\, e_{i+1}) d_1 = 0 \\
(\textstyle\sum_{i=0}^{k-1} a_i a_{i+1}\, e_{i+2}) d_2 = 0 \\
\vdots \\
(\textstyle\sum_{i=0}^{k-1} a_i a_{i+1}\, e_{i+(k-1)}) d_{k-1} = 0 \\
(\textstyle\sum_{i=0}^{k-1} a_i a_{i+1}\, e_{i+k}) d_0 = 0.
\end{gathered}$$

Here all the suffixes are calculated modulo k. Since d_i's are non-zero, these equations reduce to the following:

$$(\textstyle\sum_{i=0}^{k-1} a_i a_{i+1} e_{i+1}) = 0, (\sum_{i=0}^{k-1} a_i a_{i+1} e_{i+2}) = 0, , (\sum_{i=0}^{k-1} a_i a_{i+1} e_{i+k}) = 0$$

Adding these equations we get

$$(\sum_{i=0}^{k-1} a_i a_{i+1})(e_0 + e_1 + \cdots + e_{k-1}) = 0. \tag{2}$$

Next, consider the following set of entries of the matrix M : $M[0,3], M[1,4], M[2,5]$, ..., $M[k-3,0]$, $M[k-2,1]$, $M[k-1,2]$. From these entries, we get the following set of equations:

$$\begin{gathered}(\sum_{i=0}^{k-1} a_i a_{i+3}\, e_{i+3})d_3 = 0\\ (\sum_{i=0}^{k-1} a_i a_{i+3}\, e_{i+4})d_4 = 0\\ (\sum_{i=0}^{k-1} a_i a_{i+3}\, e_{i+5})d_5 = 0\\ \vdots\\ (\sum_{i=0}^{k-1} a_i a_{i+3}\, e_{i+k+1})d_1 = 0\\ (\sum_{i=0}^{k-1} a_i a_{i+3}\, e_{i+k+2})d_2 = 0.\end{gathered}$$

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

$$(\sum_{i=0}^{k-1} a_i a_{i+3})(e_0 + e_1 + \cdots + e_{k-1}) = 0. \tag{3}$$

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 $M\left[0, \frac{k}{2} - 1\right]$, $M\left[1, \frac{k}{2}\right]$, $M\left[2, \frac{k}{2} + 1\right]$, ..., $M[\frac{k}{2} + 1, 0], M[\frac{k}{2} + 2, 1], \cdots, M[k-1, \frac{k}{2} - 2]$. From these entries, we get the equation

$$(\sum_{i=0}^{k-1} a_i a_{i+\frac{k}{2}-1})(\sum_{i=0}^{k-1} e_i) = 0, \tag{4}$$

where the suffixes are calculated modulo k.

Adding the following $\frac{k}{4}$ equations

$$\left(\sum_{i=0}^{k-1} a_i a_{i+1}\right)\left(\sum_{i=0}^{k-1} e_i\right) = 0, \left(\sum_{i=0}^{k-1} a_i a_{i+3}\right)\left(\sum_{i=0}^{k-1} e_i\right) = 0,$$
$$\ldots, (\sum_{i=0}^{k-1} a_i a_{i+\frac{k}{2}-1})(\sum_{i=0}^{k-1} e_i) = 0,$$

we get

$$(a_0 + a_2 + \cdots + a_{k-2})(a_1 + a_3 + \cdots + a_{k-1})(e_0 + e_1 + \cdots + e_{k-1}) = 0. \tag{5}$$

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 (1), 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 5, we have $(e_0 + e_1 + \cdots + e_{k-1}) = 0$ and this implies $\mathrm{trace}(D_2) = 0$.

Similarly using the identity $A^{-1}A = I$ and following the same process, we will get $\mathrm{trace}(D_1) = 0$.

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 $(d_0, d_1, d_2, \dots, d_{2n-1})$ as a non-periodic diagonal matrix, if the entries satisfy $d_i \neq d_{i+n}, i = 0,1,2, \dots, n-1$.

Theorem 4.3: *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$(a_0, a_1, a_2, \dots, a_{2n-1})$. 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 $(d_0, d_1, d_2, \dots, d_{2n-1})$ and $D_2 =$ diagonal $(e_0, e_1, e_2, \dots, e_{2n-1})$. Without loss of generality, we assume that D_2 is non-periodic diagonal matrix. Then $e_i \neq e_{i+n}, i = 0,1,2,, n-1$. 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 $M[0,1], M[1,2], M[2,3], \dots, M[2n-2, 2n-1], M[2n-1, 0]$ we get the following equations:

$$\begin{gathered}
(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+1}\, e_{i+1}) d_1 = 0 \\
(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+1}\, e_{i+2}) d_2 = 0 \\
\vdots \\
(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+1}\, e_{i+(2n-1)}) d_{2n-1} = 0 \\
(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+1}\, e_{i+2n}) d_0 = 0.
\end{gathered}$$

Here all the suffixes are calculated modulo $2n$. Since d_i's are non-zero, we can add these equations and get

$$(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+1})(e_0 + e_1 + \cdots + e_{2n-1}) = 0.$$

Continuing the similar process for the entries at positions $M[0,3]$, $M[1,4]$, $M[2,5]$, …, $M[2n-3, 0]$ we get:

$$\begin{gathered}
(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+3}\, e_{i+3}) d_3 = 0 \\
(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+3}\, e_{i+4}) d_4 = 0 \\
\vdots \\
(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+3}\, e_{i+(2n)}) d_0 = 0 \\
(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+3}\, e_{i+2n+1}) d_1 = 0 \\
(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+3}\, e_{i+2n+2}) d_2 = 0.
\end{gathered}$$

Here all the suffixes are calculated modulo $2n$. Adding these equations we get

$$(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+3})(\textstyle\sum_{i=0}^{2n-1} e_i) = 0.$$

Continue this process to cover all the odd positions of the first row, upto the position $M[0, n]$. From the entries $M[0, n], M[1, n+1], M[2, n+2], \dots, M[n -$

$1,2n-1]$ we get:

$$\begin{aligned}
&(\textstyle\sum_{i=0}^{n-1} a_i a_{i+n}(e_i + e_{i+n}))d_n = 0\\
&(\textstyle\sum_{i=0}^{n-1} a_i a_{i+n}(e_{i+1} + e_{i+(n+1)}))d_{n+1} = 0\\
&\qquad\vdots\\
&(\textstyle\sum_{i=0}^{n-1} a_i a_{i+n}(e_{i+(n-1)} + e_{(i+n)+(n-1)}))d_{2n-1} = 0.
\end{aligned} \tag{6}$$

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 (6), 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:

$$(\textstyle\sum_{i=0}^{2n-1} a_i a_{i+1})(\sum_{i=0}^{2n-1} e_i) = 0, (\sum_{i=0}^{2n-1} a_i a_{i+3})(\sum_{i=0}^{2n-1} e_i) = 0, \ldots, (\sum_{i=0}^{n-1} a_i a_{i+n})(\sum_{i=0}^{2n-1} e_i) = 0,$$

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 $\mathrm{trace}(D_2) = 0$.

Similarly using the identity $A^{-1}A = I, D_1$ is non-cyclic diagonal matrix, and following the same process, we will get $\mathrm{trace}(D_1) = 0$.

For circulant, semi-orthogonal matrices of odd order, the following examples demonstrate the possibility of achieving the MDS property and the trace of the associated diagonal matrices are non-zero.

Example 4.4: 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$(\alpha^6 + \alpha^4 + \alpha^3 + \alpha, \alpha^6 + \alpha^4 + \alpha^3 + \alpha, \alpha^6 + \alpha^4 + \alpha^3 + \alpha)$. Note that, $\mathrm{trace} D_1 = \alpha^7 + \alpha^6 + \alpha^5 + \alpha$ and $\mathrm{trace} D_2 = \alpha^6 + \alpha^4 + \alpha^3 + \alpha$. A is also an MDS matrix.

Example 4.5: Consider the 5×5 matrix $A =$ circulant$(\alpha, \alpha, \alpha^2, \alpha^3 + \alpha, \alpha^3 + \alpha^2 + 1)$, where α is a primitive element of the finite field $\mathbb{F}_{2^4}$ with the generating polynomial $x^4 + x + 1$. Note that, A is not orthogonal and it is semi-orthogonal since $A^{-T} = D_1 A D_2$, where $D_1 =$ diagonal$(\alpha^2, \alpha^2, \alpha^2, \alpha^2, \alpha^2)$ and $D_2 =$ diagonal$(\alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1)$. Note that, $\mathrm{trace} D_1 = \alpha^2$ and $\mathrm{trace} D_2 = \alpha^2 + \alpha + 1$. A is also an MDS matrix.

Remark 4.6: 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 $k \equiv 0(\mathrm{mod} 4)$, the MDS property ensures that the trace of the associated diagonal matrices remains zero. Furthermore, when the order is even and congruent to $2(\mathrm{mod} 4)$, 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.

5. Circulant matrices with MDS and semi-involutory properties

In [16], Gupta and Ray proved that circulant involutory matrices of order $n \geq 3$ can not be MDS. In the subsequent results, we extend this characteristic to circulant semi-involutory matrices. In this direction, our first result demonstrates that, the trace of these associate diagonal matrices is also zero under certain conditions.

Proposition 5.1: 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: The proof follows similarly as Theorem 4.1.

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.

Theorem 5.2: *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 $A = \text{circulant}(a_0, a_1, a_2, \dots, a_{n-1})$. Since A is semi-involutory, we have $A^{-1} = D_1 A D_2$, where D_1 and D_2 are non-singular diagonal matrices given by $D_1 = \text{diagonal}(d_0, d_1, d_2, \dots, d_{n-1})$ and $D_2 = \text{diagonal}(e_0, e_1, e_2, \dots, e_{n-1})$.

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 $M[0,2], M[1,3], M[2,4], M[3,5], , M[2k-3, 2k-1]$, $M[2k-2, 0], M[2k-1, 1]$ we get the following equations:

$$(a_1^2 d_1 + \ a_{k+1}^2 d_{k+1} + a_0 a_2(d_0 + d_2) + a_3 a_{2k-1}(d_3 + d_{2k-1}) + \cdots + \\ a_k a_{k+2}(d_k + d_{k+2}))e_2 = 0$$

$$(a_1^2 d_2 + \ a_{k+1}^2 d_{k+2} + a_0 a_2(d_1 + d_3) + a_3 a_{2k-1}(d_4 + d_{2k}) + \cdots + \\ a_k a_{k+2}(d_{k+1} + d_{k+3}))e_3 = 0$$

$$\vdots$$

$$(a_1^2 d_{2k-2} \ + a_{k+1}^2 d_{k-2} + a_0 a_2(d_{2k-1} + d_{2k-3}) + +a_3 a_{2k-1}(d_{3+(2k-3)} + d_{2k-4}) \\ + \cdots + a_k a_{k+2}(d_{k-1} + d_{k-3}))e_{2k-1} = 0$$

$$(a_1^2 d_{2k-1} \ + a_{k+1}^2 d_{k-1} + a_0 a_2(d_{2k} + d_{2k-2}) + a_3 a_{2k-1}(d_1 + d_{2k-3}) + \cdots + \\ a_k a_{k+2}(d_{k-2} + d_k))e_0 = 0$$

$$(a_1^2 d_{2k} \ + a_{k+1}^2 d_k + a_0 a_2(d_1 + d_{2k-1}) + a_3 a_{2k-1}(d_2 + d_{2k-2}) + \cdots + \\ a_k a_{k+2}(d_{k-1} + d_{k+1}))e_1 = 0.$$

All the suffixes are calculated modulo $2k$. Since e_i's are non-zero, adding all these equations, we get

$$(a_1^2 + a_{k+1}^2)(d_1 + d_2 + \cdots + d_{2k-1}) = 0 \tag{7}$$

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) 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 $M[0,2], M[1,3], M[2,4], M[3,5], , M[2k-2,2k], M[2k-1,0], M[2k,2]$ give the following equations:

$$(a_1^2 d_1 + a_0 a_2(d_0 + d_2) + a_3 a_{2k}(d_3 + d_{2k}) + \cdots + a_{k+1} \\ a_{k+2}(d_{k+1} + d_{k+2}))e_2 = 0$$

$$(a_1^2 d_2 + a_0 a_2(d_1 + d_3) + a_3 a_{2k}(d_4 + d_{2k+1}) + \cdots + a_{k+1} \\ a_{k+2}(d_{k+2} + d_{k+3}))e_3 = 0$$

$$\vdots$$

$$(a_1^2 d_{2k-1} + a_0 a_2(d_{0+2k-2} + d_{1+2k-2}) + a_3 a_{2k}(d_{3+2k-2} + d_{2k+2k-2}) \ + \cdots + \\ a_{k+1} a_{k+2}(d_{k+1+2k-2} + d_{k+2++2k-2}))e_{2k-1} = 0$$

$$(a_1^2 d_{2k} + a_0 a_2(d_{0+2k-1} + d_{2+2k-1}) + a_3 a_{2k}(d_{3+2k-1} + d_{2k+2k-1}) + \cdots + \\ a_{k+1} a_{k+2}(d_{k+1+2k-1} + d_{k+2+2k-1}))e_0 = 0$$

$$(a_1^2 d_0 + a_0 a_2(d_1 + d_{2k}) + a_3 a_{2k}(d_2 + d_{2k-1}) + \cdots + a_{k+1} a_{k+2} \\ (d_k + d_{k+1}))e_1 = 0.$$

All the suffixes are calculated modulo $2k+1$. Since e_i's are non-zero, adding all these equations, we get

$$(a_1^2)(d_1 + d_2 + \cdots + d_{2k}) = 0 \tag{8}$$

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 5.3: 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.

6. Conclusion

In conclusion, this article has explored circulant matrices with both semi-orthogonal and MDS properties, as well as circulant matrices characterized by semi-involutory and MDS attributes. We have presented examples of circulant semi-orthogonal MDS matrices for certain odd orders. Moreover, our results open a new research direction to check the MDS property of circulant matrices with both semi-involutory and semi-orthogonal properties.

Acknowledgements

The authors would like to thank the referees for carefully reading of the manuscript and for their valuable suggestions.

References

[1] P. S. L. M. Barreto and V. Rijmen, The Whirlpool hashing function (2003).

[2] V. Cauchois and P. Loidreau, On circulant involutory MDS matrices, *Design, Codes and Cryptography*, vol. 87, pp. 249-260 (2019).

[3] T. Chatterjee and A. Laha, A note on Semi-Orthogonal (G-matrix) and Semi-Involutory MDS Matrices, *Finite Fields and Their Applications*, vol. 92, Paper No. 102279, 27 (2023).

[4] T. Chatterjee and A. Laha. A note on cyclic MDS and non-MDS matrices. *Cryptography and Communications*, vol. 17, pp. 1109–1124 (2025).

[5] T. Chatterjee and A. Laha, A Characterization of Semi-Involutory MDS Matrices, arxiv.org/pdf/2406.12842 (2024).

[6] T. Chatterjee and A. Laha, On MDS Property of g-Circulant Matrices, arxiv.org/pdf/2406.15872 (2024).

[7] 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*, vol. 68, no. 12, pp. 8268-8279 (2022).

[8] G. Cheon, B. Curtis and H. Kim, Semi-involutory matrices and signed self-inverse, *Linear Algebra and its Applications*, vol. 622, pp. 294-315 (2021).

[9] J. Daemen, L. R. Knudsen and V. Rijmen, The block cipher SQUARE, *Fast Software Encryption Workshop*, LNCS, vol. 1267, pp. 149-165 (1997).

[10] J. Daemen and V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, Springer-Verlag (2002).

[11] X. D. Dong, B. S. Cheong, and E. Gunawan, Matrix characterization of MDS linear codes over modules, *Linear Algebra and its Application*, vol. 277, pp. 57-61 (1998).

[12] M. Fiedler and F. J. Hall, G-matrices, *Linear Algebra and its Applications*, pp. 731-741 (2012).

[13] J. Guo, T. Peyrin and A. Poschmann, The PHOTON family of lightweight hash functions, CRYPTO 2011, *Lecture Notes in Computer Science,* vol. 6841, pp. 222-239 (2011).

[14] J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw, The LED Block Cipher, CHES 2011, LNCS, vol. 6917, pp. 326-341 (2011).

[15] K. C. Gupta and I. G. Ray, On Constructions of Involutory MDS Matrices, Progress in Cryptology -- AFRICACRYPT 2013, vol. 7918, pp. 43-60, 2013).

[16] K. C. Gupta and I. G. Ray, On constructions of circulant MDS matrices for lightweight cryptography, ISPEC 2014, Springer, pp. 564-576 (2014).

[17] K. C. Gupta and I. G. Ray, Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications, *Cryptography and Communications,* vol. 7, pp. 257-287 (2015).

[18] K. C. Gupta, S. K. Pandey, I. G. Ray and S. Samanta, Cryptographically significant mds matrices over finite fields: A brief survey and some generalized results, *Advances in Mathematics of Communications,* pp. 779-843 (2019).

[19] K. C. Gupta, S. K. Pandey and A. Venkateswarlu, On the direct construction of recursive MDS matrices, *Design Codes and Cryptography*, vol. 82, pp. 77-94 (2017).

[20] J. Lacan and J. Fimes, Systematic MDS erasure codes based on Vandermonde matrices, *IEEE Trans. Commun. Lett.*, vol. 8, pp. 570-572 (2004).

[21] M. Liu and S. M. Sim, Lightweight MDS generalized circulant matrices, Fast Software Encryption, LNCS, vol. 9783, pp. 101-120 (2016).

[22] T. Luong, On the direct building of 8×8 self-reciprocal recursive MDS Matrices effective for implementation over GF(q) using Reed-Solomon codes, *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 4, pp. 1237-1248 (2023).

[23] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland Publishing Co., Amsterdam-New York-Oxford (1977).

[24] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers and E.D. Win, The cipher SHARK, Fast Software Encryption Workshop, LNCS,vol. 1039, pp. 99-112 (1996).

[25] S. Sarkar and H. Syed, Lightweight diffusion layer: Importance of Toeplitz matrices, *IACR Trans. Symmetric Cryptol.,* 2016, 95-113 (2016).

[26] S. Sarkar and H. Syed, Analysis of Toeplitz MDS matrices, ACISP 2017, LNCS, vol. 10343, pp. 3-18 (2017).

[27] M. Sajadieh, M. Dakhilalian, H. Mala and B. Omoomi, On construction of involutory MDS matrices from Vandermonde Matrices in GF(2^q)., *Design, Codes Cryptography*, vol. 64, pp. 287-308 (2012).

[28] 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. National Institute for Standards and Technology (1998).

[29] M. R. M. Shamsabad and S. M. Dehnavi, Nonlinear 4×4 MDS diffusion layers, *Journal of Information and Optimization Sciences*, vol. 43, no. 4, pp. 663-676 (2022).

[30] A. M. Youssef, S. Mister and S. E. Tavares, On the Design of Linear Transformations for Substitution Permutation Encryption Networks, In Workshop On Selected Areas in Cryptography, SAC, vol. 97, pp. 40-48 (1997).

[31] A. A. Zain and B. S. Rajan, Algebraic characterization of MDS group codes over cyclic groups, *IEEE Transactions on Information Theory,* vol. 41, pp. 2052-2056 (1995).

Received October, 2024