IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Construction Of MDS Rhotrices From Cauchy Rhotrices And Block Cauchy-Like Rhotrices Over Finite Fields

[1]Shalini Gupta , [2]Ruchi Narang, [3]Mansi Harish

[1]Associate Professor, [2]Research Scholar, [3] Assistant Professor

[1,2,3]Department of Mathematics and Statistics

[1,2,3] Himachal Pradesh University, Shimla, India

Abstract: Maximum Distance Separable (MDS) matrices have numerous applications in cryptography and coding theory and their properties make them a valuable tool for ensuring the confidentiality, integrity and reliability of data transmission and storage. Cauchy matrices have a variety of applications in different areas of mathematics and computer science including coding theory, cryptography and signal processing. Rhotrices are represented as coupled matrices of consecutive orders. A rhotrix provides double security when it is used in place of a matrix in a cryptographic algorithm. Conjugate elements have several applications in cryptography, particularly in the design and analysis of public key cryptosystem based on finite fields. In the present paper, we construct Maximum Distance Separable (MDS) rhotrices from Cauchy rhotrices using the conjugate elements of finite fields. Further, we define Block Cauchy- like Rhotrix. MDS Rhotrices are also constructed using Block Cauchy- like Rhotrices.

Index Terms **- Cauchy matrix; Maximum Distance Separable rhotrix; Conjugates; Finite fields; Block Cauchy-like Rhotrices.**

I. INTRODUCTION

Ajibade (2003) introduced a mathematical structure 'Rhotrix', as an extension of matrix, which is defined as follows

$$R_3 = \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle$$

where a, b, c, d, e are real numbers and c is the heart of rhotrix. He introduced the operation of addition and scalar multiplication. In the rhotrix theory literature, two methods of multiplication of rhotrices are defined. First method of multiplication of rhotrices is known as heart-oriented multiplication of rhotrices, which was discussed by Ajibade (2003) and further its generalisation was given by Mohammed et al. (2011) and second method of multiplication is row column multiplication of rhotrices which was discussed by Sani (2004). These two types of methods of multiplication characterised the rhotrices into commutative and non-commutative rhotrices. Ajibade's heart-based method for rhotrix multiplication corresponds to commutative rhotrix and row column multiplication method corresponds to non-commutative rhotrix. Tudunkaya and Makanjuola (2010) discussed the rhotrices over finite fields. Aminu (2009, 2012) discussed the rhotrix system of equations. Several authors have contributed for the development of rhotrices such as Absalom et al. (2011), Mohammed (2011), Sani (2007, 2008), Sharma et al. (2011-2014, 2018-2020) and Tudunkaya (2013).

Maximum Distance Separable (MDS) matrices have wide range of applications in cryptographic hash functions due to their diffusion properties, see Alfred et al. (1996), Gupta and Ray (2013, 2014) and Junod and Vaudenay (2004). MDS matrices play a vital role in various branches of mathematics such as combinatorics, cryptography and coding theory. Sajadieh et al. (2012), Lacan and Fimes (2004) and Qiuping et al. (2018) have constructed MDS matrices from Vandermonde matrices. Cauchy matrices have wide range of applications in coding theory, see Tzeng and Zimmermann (1975). Nakahara and Abrahao (2009) and Qiuping et al. (2018) used the Cauchy matrices for the construction of involutory MDS matrix of 16-order. As rhotrix is a structure like coupled matrices of consecutive order, therefore, the MDS rhotrices constructed using rhotrices enhance the security of the data and so it becomes more difficult to decrypt the data. Sharma et al. (2013) have introduced MDS rhotrices and Gupta et al. (2022) have introduced block rhotrices in the literature. Sharma et al. (2013, 2015, 2018, 2019) have used companion rhotrices, circulant rhotrices and Hankel rhotrices for the construction of MDS rhotrices. Cauchy rhotrix is defined by Sharma et al. (2017) and they have used it for the construction of MDS rhotrices over finite fields.

Conjugate elements of a finite field play an important role in the security analysis of finite field based cryptosystem, see Koushesh and Zamani (2010). Concept of conjugate element is an important tool in the design and analysis of cryptosystem based on finite fields and their properties are often analysed in the various cryptographic protocols and algorithms.

In present paper, we construct MDS Cauchy rhotrices using conjugates of the elements of prime finite fields. The paper is organized in five sections. The following section reviews the basic results required for the understanding of the paper. Section 3 gives interesting results for the construction of MDS rhotrix from Cauchy rhotrix and the results are demonstrated with the help of illustrations. In Section 4, we define block rhotrix and construct block Cauchy- like MDS rhotrix. This construction is explained with the help of some illustrations. Finally, we conclude in the Section 5.

II. Preliminaries

Definition 2.1 Cauchy Matrix: Qiuping et al. (2018)

The matrix of the form $A = (a_{ij})_{m\times n}$, where

$$a_{ij} = \frac{1}{u_i - v_j},\ u_i - v_j \neq 0, 1 \leq i \leq m, 1 \leq j \leq n,$$

is called a Cauchy matrix and u_i, v_j are the elements from finite field.

Definition 2.2 Cauchy Rhotrix: Sharma et al. (2017)

A 5- dimensional Cauchy rhotrix C_5 is defined as

$$C_5 = \left\langle \begin{matrix} & & & \frac{1}{u_1 - v_1} & \\ & & \frac{1}{u_2 - v_1} & \frac{1}{l_1 - m_1} & \frac{1}{u_1 - v_2} \\ & \frac{1}{u_3 - v_1} & \frac{1}{l_2 - m_1} & \frac{1}{u_2 - v_2} & \frac{1}{l_1 - m_2} & \frac{1}{u_1 - v_3} \\ & & \frac{1}{u_3 - v_2} & \frac{1}{l_2 - m_2} & \frac{1}{u_2 - v_3} & \\ & & & \frac{1}{u_3 - v_3} & \end{matrix} \right\rangle,$$

where $u_i, v_j (i, j = 1,2,3)$ and $l_r, m_s (r, s = 1,2)$ are elements from a finite field. Two coupled matrices of C_5 are

$$U = \begin{bmatrix} \frac{1}{u_1 - v_1} & \frac{1}{u_1 - v_2} & \frac{1}{u_1 - v_3} \\ \frac{1}{u_2 - v_1} & \frac{1}{u_2 - v_2} & \frac{1}{u_2 - v_3} \\ \frac{1}{u_3 - v_1} & \frac{1}{u_3 - v_2} & \frac{1}{u_3 - v_3} \end{bmatrix} \text{ and } V = \begin{bmatrix} \frac{1}{l_1 - m_1} & \frac{1}{l_1 - m_2} \\ \frac{1}{l_2 - m_1} & \frac{1}{l_2 - m_2} \end{bmatrix}$$

Definition 2.3 Conjugates: Koushesh and Zamani (2010)

Let F_{q^n} be an extension of F_q and $\alpha \in F_{q^n}$. Then, the conjugate elements of α in extension field F_{q^n} are the roots of the minimal polynomial of α over F_q and the elements $\{\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots\ldots, \alpha^{q^{n-1}}\}$ are called the conjugates of α with respect to F_q.

Definition 2.4 MDS Matrix: Sharma et al. (2017)

Let F be a finite field, and p, q be two positive integers. Let $x \to M \times x$ be a mapping from F^p to F^q defined by the $q \times p$ matrix M. We say that it is an MDS matrix if the set of all pairs $(x, M \times x)$ is an MDS code, which is a linear code of dimension p length $p + q$ and minimum distance $q + 1$. In other form we can say that a square matrix A is an MDS matrix if and only if every square sub-matrices of A are non-singular. This implies that all the entries of an MDS matrix must be non-zero.

Definition 2.5 Block Rhotrix: Gupta et al. (2022)

Let $R = < C, D >$ be a rhotrix of $2n - 1$ dimension, where C and D are coupled matrices of dimension $n \times n$ and $(n - 1) \times (n - 1)$ respectively. Then $R = < C, D >$ is a block rhotrix if coupled matrix C of even order is block matrix.

Definition 2.6 Block Cauchy - like Matrix: Qiuping et al. (2018)

Let $A_1, A_2, \ldots\ldots A_n$ and $B_1, B_2, \ldots\ldots, B_n$ be $m \times m$ matrices over F_2 satisfying that $A_i + B_j$ is non- singular for any $0 \leq i, j \leq n$. Then the matrix $C = \left[\frac{1}{A_i + B_j}\right]$ is called a block Cauchy - like matrix over F_2.

Lemma 2.7 Sharma et al. (2013)

Any rhotrix R_5 over GF(2^n) with all non zero entries is an MDS rhotrix iff its coupled matrices $M_1 = 3 \times 3$ and $M_2 = 2 \times 2$ are non-singular and all their entries are non- zero.

Theorem 2.8 Qiuping et al. (2018)

Assume $\{A_1, A_2, \dots\dots, A_n, B_1, B_2, \dots\dots, B_n\}$ is a set of $m \times m$ matrices over F_2 which are pairwise commutative and $A_i - B_j \neq 0$. Then block Cauchy -like matrix $C = \left[\frac{1}{A_i - B_j}\right]$ is an MDS matrix.

III. MDS Cauchy Rhotrices over F_{q^n}

In this section conjugates of the elements of finite field are used to construct maximum distance separable Cauchy rhotrices.

In the following Theorem, we shall show that if we take two elements a^r and a^s, where $\gcd(r, s) = 1$, then MDS rhotrix can be constructed using the conjugates of a^r and a^s.

Theorem 3.1

Let $R_t =< A, B >$ be a $t-$dimensional rhotrix with coupled matrices

$$A = (a_{ij})_{n\times n} = \frac{1}{u_i - v_j},$$

and

$$B = (b_{ij})_{(n-1)\times(n-1)} = \frac{1}{l_c - m_d} \text{ for } n = \frac{t+1}{2}.$$

If

$$u_i, l_c \in X = \{\alpha^r, (\alpha^r)^q, (\alpha^r)^{q^2}, (\alpha^r)^{q^3}, \dots\dots, (\alpha^r)^{q^{n-1}}\},$$

and

$$v_j, m_d \in Y = \{\alpha^s, (\alpha^s)^q, (\alpha^s)^{q^2}, (\alpha^s)^{q^3}, \dots\dots, (\alpha^s)^{q^{n-1}}\},$$
$$[(i, j = 1,2, \ , n), (c, d = 1,2, \dots., n-1)].$$

where $\gcd(r, s) = 1$ and α is the root of irreducible polynomial of F_{q^n} over F_q, then

$$u_i - v_j \neq 0,$$

and

$$l_c - m_d \neq 0,$$

implies A and B are Cauchy matrices and R_t is an MDS Cauchy rhotrix over F_{q^n}.

Proof:

It is given that F_{q^n} is an extension of F_q and let $\alpha \in F_{q^n}$ be the root of primitive polynomial of F_{q^n} over F_q. We have to show that

if

$$u_i, l_c \in X = \{\alpha^r, (\alpha^r)^q, (\alpha^r)^{q^2}, (\alpha^r)^{q^3}, \dots\dots, (\alpha^r)^{q^{n-1}}\},$$

and

$$v_j, m_d \in Y = \{\alpha^s, (\alpha^s)^q, (\alpha^s)^{q^2}, (\alpha^s)^{q^3}, \dots\dots, (\alpha^s)^{q^{n-1}}\},$$

then

$$u_i - v_j \neq 0,$$

and

$$l_c - m_d \neq 0.$$

If possible, let

$$\begin{aligned} u_i - v_j &= 0, \\ \Rightarrow \alpha^{rq^i} - \alpha^{sq^j} &= 0, \\ \Rightarrow \alpha^{rq^i} &= \alpha^{sq^j}, \\ \Rightarrow rq^i &= sq^j. \end{aligned} \tag{3.1}$$

This gives rise to two cases which are as follows:

Case 1:

When $r \neq s$ and $\gcd(r,s) = 1$. Also if

$$r = 1 \quad \text{or} \quad s = 1$$

equation (3.1) becomes,

$$\begin{aligned} q^i &= sq^j \quad \text{or} \quad rq^i = q^j, \\ \Longrightarrow \alpha^{q^i} &= \alpha^{sq^j} \quad \text{or} \quad \alpha^{rq^i} = \alpha^{q^j}, \\ \Longrightarrow \alpha^{q^i} &\in Y \quad \text{or} \quad \alpha^{q^j} \in X. \end{aligned}$$

which is a contradiction.

Case 2:

When $r \neq 1$ and $s \neq 1$ and $\gcd(r,s) = 1$, then

$$\begin{aligned} rq^i &= sq^j, \\ \Longrightarrow r &= s\, q^{j-i}, \\ \Longrightarrow r &= s\, q^k; \text{ for some } k \\ \Longrightarrow \alpha^r &= \alpha^{s\,(q^k)}, \\ \Longrightarrow \alpha^r &\in Y, \end{aligned}$$

which is a contradiction.
Hence, in both the cases $u_i - v_j \neq 0 \ \forall\, u_i \in X$ and $\forall\, v_j \in Y$.
Similarly, it can be shown that $l_c - m_d \neq 0 \ \forall\, l_c \in X$ and $\forall\, m_d \in Y$.
Therefore,

$$A = \frac{1}{u_i - v_j},$$

and

$$B = \frac{1}{l_c - m_d},$$

form Cauchy rhotrices of consecutive orders. We know that Cauchy rhotrices have non-zero determinant. Therefore, $R_t = < A, B >$ is a maximum distance separable Cauchy rhotrix.

Remark:

The rhotrix of dimension $2n-1$ has coupled matrices of order $n \times n$ and $(n-1) \times (n-1)$. Therefore, to construct $n \times n$ matrix, we must use the field of order p^n, where the number of conjugates will be n.

Example 3.2

Let the 5-dimensional rhotrix R_5 has coupled matrices

$$A = (a_{ij})_{3\times 3} = \frac{1}{u_i - v_j},$$

and

$$B = (b_{ij})_{2\times 2} = \frac{1}{l_c - m_d},$$

where

$$u_i, l_c \in X = \{\alpha^5, (\alpha^5)^3, (\alpha^5)^{3^2}\},$$

and

$$v_j, m_d \in Y = \{\alpha^7, (\alpha^7)^3, (\alpha^7)^{3^2}\},$$
$$[(i,j = 1,2,3), (c,d = 1,2)].$$

where $\gcd(5,7) = 1$ and α is the root of the irreducible polynomial $p(x) = x^3 + 2x^2 + 1$, then $u_i - v_j \neq 0$, $l_c - m_d \neq 0$, A and B form maximum distance separable Cauchy rhotrix R_5 over F_{3^3}.

Proof:

Let the sets X and Y be the conjugates of α^5 and α^7, where $\gcd(5,7) = 1$.
Therefore,

$$X = \{\alpha^5, (\alpha^5)^3, (\alpha^5)^{3^2}\} = \{\alpha^5, \alpha^{15}, \alpha^{19}\},$$

and

$$Y = \{\alpha^7, (\alpha^7)^3, (\alpha^7)^{3^2}\} = \{\alpha^7, \alpha^{21}, \alpha^{11}\}.$$

So, matrix A is given by

$$A = \begin{bmatrix} \frac{1}{\alpha^5-\alpha^7} & \frac{1}{\alpha^5-\alpha^{21}} & \frac{1}{\alpha^5-\alpha^{11}} \\ \frac{1}{\alpha^{15}-\alpha^7} & \frac{1}{\alpha^{15}-\alpha^{21}} & \frac{1}{\alpha^{15}-\alpha^{11}} \\ \frac{1}{\alpha^{19}-\alpha^7} & \frac{1}{\alpha^{19}-\alpha^{21}} & \frac{1}{\alpha^{19}-\alpha^{11}} \end{bmatrix},$$

$$A = \begin{bmatrix} \frac{1}{\alpha^{21}} & \frac{1}{\alpha^7} & \frac{1}{\alpha} \\ \frac{1}{\alpha^3} & \frac{1}{\alpha^{11}} & \frac{1}{\alpha^{21}} \\ \frac{1}{\alpha^{11}} & \frac{1}{\alpha^9} & \frac{1}{\alpha^7} \end{bmatrix},$$

$$A = \begin{bmatrix} \alpha^5 & \alpha^{19} & \alpha^{25} \\ \alpha^{23} & \alpha^{15} & \alpha^5 \\ \alpha^{15} & \alpha^{17} & \alpha^{19} \end{bmatrix}.$$

Therefore,

$$det\ A = 2 \neq 0.$$

Hence, A is an MDS Cauchy matrix.
Similarly,

$$B = \begin{bmatrix} \frac{1}{\alpha^5-\alpha^7} & \frac{1}{\alpha^5-\alpha^{21}} \\ \frac{1}{\alpha^{15}-\alpha^7} & \frac{1}{\alpha^{15}-\alpha^{21}} \end{bmatrix}.$$

It can be easily verified that it is an MDS Cauchy matrix.
Hence, by Lemma 2.7, we can say that

$$R_5 = \left\langle \begin{matrix} \frac{1}{\alpha^{19}-\alpha^7} & \frac{1}{\alpha^{15}-\alpha^7} & \frac{1}{\alpha^{15}-\alpha^{21}} \\ \frac{1}{\alpha^{19}-\alpha^{21}} & \frac{1}{\alpha^{15}-\alpha^{21}} & \frac{1}{\alpha^{15}-\alpha^{11}} \end{matrix} \begin{matrix} \frac{1}{\alpha^5-\alpha^7} & \frac{1}{\alpha^5-\alpha^{21}} \\ \frac{1}{\alpha^5-\alpha^{21}} & \frac{1}{\alpha^5-\alpha^{11}} \\ \frac{1}{\alpha^{15}-\alpha^{11}} & \end{matrix} \right\rangle,$$

$$R_5 = \left\langle \begin{matrix} \frac{1}{\alpha^{11}} & \frac{1}{\alpha^3} & \frac{1}{\alpha^{11}} \\ \frac{1}{\alpha^9} & \frac{1}{\alpha^{11}} & \frac{1}{\alpha^{21}} \end{matrix} \begin{matrix} \frac{1}{\alpha^{21}} & \frac{1}{\alpha^7} \\ \frac{1}{\alpha^7} & \frac{1}{\alpha} \\ & \end{matrix} \right\rangle,$$

$$R_5 = \left\langle \begin{matrix} \alpha^{15} & \alpha^{23} & \alpha^5 \\ \alpha^{23} & \alpha^{15} & \alpha^{19} \\ \alpha^{17} & \alpha^{15} & \alpha^5 \end{matrix} \begin{matrix} \alpha^{19} & \alpha^{25} \\ \alpha^{19} & \\ \alpha^{19} & \end{matrix} \right\rangle.$$

is an MDS Cauchy rhotrix.

Example 3.3

Let the 5- dimensional rhotrix R_5 has coupled matrices

$$A = (a_{ij})_{3\times3} = \frac{1}{u_i - v_j},$$

and

$$B = (b_{ij})_{2\times2} = \frac{1}{l_c - m_d},$$

where

$$u_i, l_c \in X = \{\alpha^2, (\alpha^2)^5, (\alpha^2)^{5^2}\},$$

and

$$v_j, m_d \in Y = \{\alpha^3, (\alpha^3)^5, (\alpha^3)^{5^2}\},$$
$$[(i, j = 1,2,3\ ), (c, d = 1,2)].$$

where $\gcd(2,3) = 1$ and α is the root of irreducible polynomial $p(x) = x^3 + 3x + 2$ of F_{5^3} over F_5, then, $u_i - v_j \neq 0$, $l_c - m_d \neq 0$, A and B form MDS rhotrix R_5 over F_{5^3}.

Proof:

Let

$$X = \{\alpha^2, \alpha^{10}, \alpha^{50}\},$$

and

$$Y = \{\alpha^3, \alpha^{15}, \alpha^{75}\}.$$

So, matrix A is given by

$$A = \begin{bmatrix} \frac{1}{\alpha^2 - \alpha^3} & \frac{1}{\alpha^2 - \alpha^{15}} & \frac{1}{\alpha^2 - \alpha^{75}} \\ \frac{1}{\alpha^{10} - \alpha^3} & \frac{1}{\alpha^{10} - \alpha^{15}} & \frac{1}{\alpha^{10} - \alpha^{75}} \\ \frac{1}{\alpha^{50} - \alpha^3} & \frac{1}{\alpha^{50} - \alpha^{15}} & \frac{1}{\alpha^{50} - \alpha^{75}} \end{bmatrix},$$

$$A = \begin{bmatrix} \frac{1}{\alpha^{98}} & \frac{1}{\alpha^{94}} & \frac{1}{\alpha^{25}} \\ \frac{1}{\alpha} & \frac{1}{\alpha^{118}} & \frac{1}{\alpha^{98}} \\ \frac{1}{\alpha^{118}} & \frac{1}{\alpha^5} & \frac{1}{\alpha^{94}} \end{bmatrix},$$

$$A = \begin{bmatrix} \alpha^{26} & \alpha^{30} & \alpha^{99} \\ \alpha^{123} & \alpha^6 & \alpha^{26} \\ \alpha^6 & \alpha^{119} & \alpha^{30} \end{bmatrix}.$$

$$det\ A = 2 \neq 0.$$

Hence, A is an MDS Cauchy matrix.
Similarly, it can be easily verified that

$$B = \begin{bmatrix} \frac{1}{\alpha^2 - \alpha^3} & \frac{1}{\alpha^2 - \alpha^{15}} \\ \frac{1}{\alpha^{10} - \alpha^3} & \frac{1}{\alpha^{10} - \alpha^{15}} \end{bmatrix},$$

is an MDS Cauchy matrix.
Hence, by Lemma 2.7, we can say that

$$R_5 = \left\langle \frac{1}{\alpha^{50} - \alpha^3} \quad \begin{matrix} \frac{1}{\alpha^{10} - \alpha^3} \\ \frac{1}{\alpha^{10} - \alpha^3} \\ \frac{1}{\alpha^{50} - \alpha^{15}} \end{matrix} \quad \begin{matrix} \frac{1}{\alpha^2 - \alpha^3} \\ \frac{1}{\alpha^2 - \alpha^3} \\ \frac{1}{\alpha^{10} - \alpha^{15}} \\ \frac{1}{\alpha^{10} - \alpha^{15}} \\ \frac{1}{\alpha^{50} - \alpha^{75}} \end{matrix} \quad \begin{matrix} \frac{1}{\alpha^2 - \alpha^{15}} \\ \frac{1}{\alpha^2 - \alpha^{15}} \\ \frac{1}{\alpha^{10} - \alpha^{75}} \end{matrix} \quad \frac{1}{\alpha^2 - \alpha^{75}} \right\rangle,$$

$$R_5 = \left\langle \alpha^6 \quad \begin{matrix} \alpha^{123} \\ \alpha^{123} \\ \alpha^{119} \end{matrix} \quad \begin{matrix} \alpha^{26} \\ \alpha^{26} \\ \alpha^6 \\ \alpha^{30} \end{matrix} \quad \begin{matrix} \alpha^{30} \\ \alpha^{30} \\ \alpha^{26} \end{matrix} \quad \alpha^{99} \right\rangle.$$

is an MDS Cauchy rhotrix.

Example 3.4

Let the 7-dimensional rhotrix R_7 has coupled matrices

$$A = (a_{ij})_{4\times4} = \frac{1}{u_i - v_j},$$

and

$$B = (b_{ij})_{3\times3} = \frac{1}{l_c - m_d},$$

where

$$u_i, l_c \in X = \{\alpha^2, (\alpha^2)^2, (\alpha^2)^{2^2}, (\alpha^2)^{2^3}\},$$

and

$$v_j, m_d \in Y = \{\alpha^3, (\alpha^3)^2, (\alpha^3)^{2^2}(\alpha^3)^{2^3}\},$$

$$[(i, j = 1,2,3,4\ ), (c, d = 1,2,3)].$$

where $\gcd(2,3) = 1$ and α is the root of primitive polynomial $p(x) = x^4 + x + 1$ of F_{2^4} over F_2 then, $u_i - v_j \neq 0$ and $l_c - m_d \neq 0$, A and B are Cauchy matrices and form MDS rhotrix R_7 over F_{2^4} over F_2.

Proof:

Here, the sets X and Y are taken as the conjugates of α^2 and α^3, where $\gcd(2,3) = 1$.
Therefore,

$$X = \{\alpha^2, \alpha^4, \alpha^8, \alpha^{16}\},$$

and,

$$Y = \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}\}.$$

So, matrix A is given by

$$A = \begin{bmatrix} \frac{1}{\alpha^2-\alpha^3} & \frac{1}{\alpha^2-\alpha^6} & \frac{1}{\alpha^2-\alpha^{12}} & \frac{1}{\alpha^2-\alpha^{24}} \\ \frac{1}{\alpha^4-\alpha^3} & \frac{1}{\alpha^4-\alpha^6} & \frac{1}{\alpha^4-\alpha^{12}} & \frac{1}{\alpha^4-\alpha^{24}} \\ \frac{1}{\alpha^8-\alpha^3} & \frac{1}{\alpha^8-\alpha^6} & \frac{1}{\alpha^8-\alpha^{12}} & \frac{1}{\alpha^8-\alpha^{24}} \\ \frac{1}{\alpha^{16}-\alpha^3} & \frac{1}{\alpha^{16}-\alpha^6} & \frac{1}{\alpha^{16}-\alpha^{12}} & \frac{1}{\alpha^{16}-\alpha^{24}} \end{bmatrix},$$

$$A = \begin{bmatrix} \frac{1}{\alpha^6} & \frac{1}{\alpha^3} & \frac{1}{\alpha^7} & \frac{1}{\alpha^{11}} \\ \frac{1}{\alpha^7} & \frac{1}{\alpha^{12}} & \frac{1}{\alpha^6} & \frac{1}{\alpha^{14}} \\ \frac{1}{\alpha^{13}} & \frac{1}{\alpha^{14}} & \frac{1}{\alpha^9} & \frac{1}{\alpha^{12}} \\ \frac{1}{\alpha^9} & \frac{1}{\alpha^{11}} & \frac{1}{\alpha^{13}} & \frac{1}{\alpha^3} \end{bmatrix},$$

$$A = \begin{bmatrix} \alpha^9 & \alpha^{12} & \alpha^8 & \alpha^4 \\ \alpha^8 & \alpha^3 & \alpha^9 & \alpha \\ \alpha^2 & \alpha & \alpha^6 & \alpha^3 \\ \alpha^6 & \alpha^4 & \alpha^2 & \alpha^{12} \end{bmatrix}.$$

$$\det(A) = 1 \neq 0.$$

Therefore, A is an MDS Cauchy matrix.
Similarly,

$$B = \begin{bmatrix} \frac{1}{\alpha^2-\alpha^3} & \frac{1}{\alpha^2-\alpha^6} & \frac{1}{\alpha^2-\alpha^{12}} \\ \frac{1}{\alpha^4-\alpha^3} & \frac{1}{\alpha^4-\alpha^6} & \frac{1}{\alpha^4-\alpha^{12}} \\ \frac{1}{\alpha^8-\alpha^3} & \frac{1}{\alpha^8-\alpha^6} & \frac{1}{\alpha^8-\alpha^{12}} \end{bmatrix},$$

$$B = \begin{bmatrix} \frac{1}{\alpha^6} & \frac{1}{\alpha^3} & \frac{1}{\alpha^7} \\ \frac{1}{\alpha^7} & \frac{1}{\alpha^{12}} & \frac{1}{\alpha^6} \\ \frac{1}{\alpha^{13}} & \frac{1}{\alpha^{14}} & \frac{1}{\alpha^9} \end{bmatrix},$$

$$B = \begin{bmatrix} \alpha^9 & \alpha^{12} & \alpha^8 \\ \alpha^8 & \alpha^3 & \alpha^9 \\ \alpha^2 & \alpha & \alpha^6 \end{bmatrix}.$$

is an MDS Cauchy matrix.
Therefore,

$$R_7 = \left\langle \begin{matrix} & & & \alpha^9 & & & \\ & & \alpha^8 & \alpha^9 & \alpha^{12} & & \\ & \alpha^2 & \alpha^8 & \alpha^3 & \alpha^{12} & \alpha^8 & \\ \alpha^6 & \alpha^2 & \alpha & \alpha^3 & \alpha^9 & \alpha^8 & \alpha^4 \\ & \alpha^4 & \alpha & \alpha^6 & \alpha^9 & \alpha & \\ & & \alpha^2 & \alpha^6 & \alpha^3 & & \\ & & & \alpha^{12} & & & \end{matrix} \right\rangle.$$

is an MDS Cauchy rhotrix.

IV. Block Cauchy - like MDS Rhotrices over Prime Finite Fields

In this section, firstly we define block Cauchy - like rhotrix and then construct block Cauchy - like MDS rhotrices using conjugate elements of finite fields.

Definition 4.1 Block Cauchy - like Rhotrix:

Let $R = < C, D >$ be a rhotrix of dimension $2n - 1$, where C and D are coupled matrices of order $n \times n$ and $(n-1) \times (n-1)$ respectively. Then R is a block Cauchy - like rhotrix when the even ordered couple matrix is a block Cauchy – like matrix.

Theorem 4.2

Let $R = < C, D >$ be a rhotrix of dimension $2n - 1$, whose coupled matrix C is of even order and D is of odd order, satisfying that matrix $C = \left[\frac{1}{A_i - B_j}\right]$ is a block Cauchy - like matrix where $A_1, A_2, \ldots . A_n, B_1, B_2, \ldots \ldots B_n$ is a set of $m \times m$ matrices over F_{q^m} and $A_i - B_j \neq 0$ for any $0 \leq i, j \leq n$ and D is any Cauchy matrix having entries as conjugates. Then, $R = < C, D >$ is a block Cauchy – like MDS rhotrix.

Proof:

As matrix D is a Cauchy matrix, then by definition, matrix D is non-singular and therefore, it is an MDS matrix. Also, since C is a block Cauchy – like matrix therefore, all its submatrices also form block Cauchy – like matrices and are non – singular. This implies C is also MDS matrix. Hence, the rhotrix $R = < C, D >$ is a block Cauchy – like MDS rhotrix.

Example 4.3

Let $R = < C, D >$ be a rhotrix of dimension 7 where matrix $C = \left[\frac{1}{A_i - B_j}\right]$ is a block Cauchy - like matrix, where $\{A_1, A_2, \ldots . A_n, B_1, B_2, \ldots \ldots B_n\}$ is a set of $m \times m$ matrices over F_{2^3} which are pairwise commutative and $A_i - B_j \neq 0$ for any $0 \leq i, j \leq n$ of dimension 4 and D any Cauchy matrix of dimension 3 with entries as conjugate elements of F_{2^3}. Then, $R = < C, D >$ is a block Cauchy – like MDS rhotrix over F_{2^3}, where α is a root of irreducible polynomial $x^3 + x + 1 = 0$.

Proof:

Let F_{2^3} an extension field of F_2, and α be a root of the irreducible polynomial

$$x^3 + x + 1 = 0.$$

Consider

$$X = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8\},$$

and

$$Y = \{\alpha^2, \alpha^4, \alpha^6, \alpha^8, \alpha^{10}, \alpha^{12}, \alpha^{14}, \alpha^{16}\}.$$

where elements of set Y are conjugates of the respective elements of set X. Consider matrix

$$C = \begin{bmatrix} \frac{1}{A_1 - B_1} & \frac{1}{A_1 - B_2} \\ \frac{1}{A_2 - B_1} & \frac{1}{A_2 - B_2} \end{bmatrix},$$

where $A_i - B_j \neq 0$ and A_1, A_2, B_1, B_2 are 2×2 matrices such that elements of first row of each matrix are from set X and elements of second row of each matrix are from set Y as given below

$$A_1 = \begin{bmatrix} \alpha & \alpha^2 \\ \alpha^2 & \alpha^4 \end{bmatrix}, \quad B_1 = \begin{bmatrix} \alpha^3 & \alpha^4 \\ \alpha^6 & \alpha^8 \end{bmatrix}, \quad A_2 = \begin{bmatrix} \alpha^5 & \alpha^6 \\ \alpha^{10} & \alpha^{12} \end{bmatrix}, \quad B_2 = \begin{bmatrix} \alpha^7 & \alpha^8 \\ \alpha^{14} & \alpha^{16} \end{bmatrix}$$

$$A_1 - B_1 = \begin{bmatrix} \alpha - \alpha^3 & \alpha^2 - \alpha^4 \\ \alpha^2 - \alpha^6 & \alpha^4 - \alpha^8 \end{bmatrix},$$

which implies,

$$A_1 - B_1 = \begin{bmatrix} \alpha^7 & \alpha \\ \alpha^7 & \alpha^2 \end{bmatrix}.$$

Therefore,

$$\det(A_1 - B_1) = \alpha^4 \neq 0.$$

also,

$$A_1 - B_2 = \begin{bmatrix} \alpha - \alpha^7 & \alpha^2 - \alpha^8 \\ \alpha^2 - \alpha^{14} & \alpha^4 - \alpha^{16} \end{bmatrix},$$

Thus,

$$A_1 - B_2 = \begin{bmatrix} \alpha^3 & \alpha^4 \\ \alpha^6 & \alpha \end{bmatrix}.$$

and

$$\det(A_1 - B_2) = \alpha^6 \neq 0.$$

Similarly,

$$A_2 - B_1 = \begin{bmatrix} \alpha^2 & \alpha^3 \\ \alpha^4 & \alpha^6 \end{bmatrix},$$

$$\det(A_2 - B_1) = \alpha^3 \neq 0.$$

and

$$A_2 - B_2 = \begin{bmatrix} \alpha^4 & \alpha^5 \\ \alpha & \alpha^3 \end{bmatrix},$$

$$\det(A_2 - B_2) = \alpha^2 \neq 0.$$

This gives,

$$\frac{1}{A_1 - B_1} = \begin{bmatrix} \alpha^5 & \alpha^4 \\ \alpha^3 & \alpha^3 \end{bmatrix},$$

$$\frac{1}{A_1 - B_2} = \begin{bmatrix} \alpha^2 & \alpha^5 \\ \alpha^7 & \alpha^4 \end{bmatrix},$$

$$\frac{1}{A_2 - B_1} = \begin{bmatrix} \alpha^3 & \alpha^7 \\ \alpha & \alpha^6 \end{bmatrix},$$

$$\frac{1}{A_2 - B_2} = \begin{bmatrix} \alpha & \alpha^3 \\ \alpha^6 & \alpha^2 \end{bmatrix}.$$

Hence,

$$C = \begin{bmatrix} \alpha^5 & \alpha^4 & \alpha^2 & \alpha^5 \\ \alpha^3 & \alpha^3 & \alpha^7 & \alpha^4 \\ \alpha^3 & \alpha^7 & \alpha & \alpha^3 \\ \alpha & \alpha^6 & \alpha^6 & \alpha^2 \end{bmatrix}.$$

Therefore, C is a block Cauchy-like MDS matrix. Now,

$$D = \begin{bmatrix} \frac{1}{\alpha-\alpha^3} & \frac{1}{\alpha-\alpha^6} & \frac{1}{\alpha-\alpha^{12}} \\ \frac{1}{\alpha^2-\alpha^3} & \frac{1}{\alpha^2-\alpha^6} & \frac{1}{\alpha^2-\alpha^{12}} \\ \frac{1}{\alpha^4-\alpha^3} & \frac{1}{\alpha^4-\alpha^6} & \frac{1}{\alpha^4-\alpha^{12}} \end{bmatrix},$$

$$D = \begin{bmatrix} \frac{1}{\alpha^7} & \frac{1}{\alpha^5} & \frac{1}{\alpha^6} \\ \frac{1}{\alpha^5} & \frac{1}{\alpha^7} & \frac{1}{\alpha^3} \\ \frac{1}{\alpha^6} & \frac{1}{\alpha^3} & \frac{1}{\alpha^7} \end{bmatrix}.$$

$$det\,(D) \;=\; 1 \neq 0.$$

Therefore, D is an MDS Cauchy matrix.
Hence,

$$R \;= \left\langle \alpha \quad \begin{matrix} \alpha^3 \\ \alpha \\ \alpha^6 \end{matrix} \quad \begin{matrix} \alpha^5 \\ \alpha^3 & \alpha^7 & \alpha^4 \\ \alpha^2 & \alpha^3 & \alpha^2 \\ \alpha^7 & \alpha^7 & \alpha^7 \\ \alpha^4 & \alpha & \alpha^4 \\ \alpha^6 & \alpha^7 & \alpha^3 \\ & \alpha^2 & \end{matrix} \quad \begin{matrix} \alpha^2 \\ \alpha \\ \alpha^4 \end{matrix} \quad \alpha^5 \right\rangle$$

is a block Cauchy-like MDS rhotrix.

Example 4.4

Let $R = < C, D >$ be a rhotrix of dimension 7, where matrix $C = \left[\frac{1}{A_i - B_j}\right]$ is a Block Cauchy - like matrix, where $\{A_1, A_2, \ldots . A_n, B_1, B_2, \ldots \ldots B_n\}$ is a set of $m \times m$ matrices over F_{3^3} which are pairwise commutative and $A_i - B_j \neq 0$ for any $0 \leq i, j \leq n$ of dimension 4 and D is any Cauchy matrix of dimension 3 with entries as conjugate elements of F_{3^3}. Then R is a block Cauchy – like MDS rhotrix over F_{3^3}, where α is a root of irreducible polynomial $x^3 + 2x^2 + 1 = 0$.

Proof:

Consider F_{3^3} be an extension field of F_3 and α be a root of irreducible polynomial

$$x^3 + 2x^2 + 1 \;=\; 0.$$

Let

$$X = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8\},$$

and

$$Y = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}, \alpha^{15}, \alpha^{18}, \alpha^{21}, \alpha^{24}\}.$$

where elements of set Y are conjugates of the respective elements of set X. Consider a matrix

$$C = \begin{bmatrix} \frac{1}{A_1-B_1} & \frac{1}{A_1-B_2} \\ \frac{1}{A_2-B_1} & \frac{1}{A_2-B_2} \end{bmatrix},$$

where $A_i - B_j \neq 0$ and A_1, A_2, B_1, B_2 are 2×2 matrices such that elements of first row of each matrix are from set X and elements of second row of each matrix are from set Y as

$$A_1 = \begin{bmatrix} \alpha & \alpha^2 \\ \alpha^3 & \alpha^6 \end{bmatrix} \quad , \quad B_1 = \begin{bmatrix} \alpha^3 & \alpha^4 \\ \alpha^9 & \alpha^{12} \end{bmatrix} \quad , \quad A_2 = \begin{bmatrix} \alpha^5 & \alpha^6 \\ \alpha^{15} & \alpha^{18} \end{bmatrix} \quad , \quad B_2 = \begin{bmatrix} \alpha^7 & \alpha^8 \\ \alpha^{21} & \alpha^{24} \end{bmatrix}.$$

Now,

$$A_1 - B_1 = \begin{bmatrix} \alpha & -\alpha^3 & \alpha^2 - \alpha^4 \\ \alpha^3 - \alpha^9 & \alpha^6 - \alpha^{12} \end{bmatrix},$$

and

$$\det(A_1 - B_1) = \alpha^{20} \neq 0.$$

.

Similarly,

$$A_1 - B_2 = \begin{bmatrix} \alpha - \alpha^7 & \alpha^2 - \alpha^8 \\ \alpha^3 - \alpha^{21} & \alpha^6 - \alpha^{24} \end{bmatrix},$$

$$\det(A_1 - B_2) = \alpha^{18} \neq 0.$$

and

$$A_2 - B_1 = \begin{bmatrix} \alpha^5 - \alpha^3 & \alpha^6 - \alpha^4 \\ \alpha^{15} - \alpha^9 & \alpha^{18} - \alpha^{12} \end{bmatrix},$$

$$\det(A_2 - B_1) = \alpha^2 \neq 0.$$

also,

$$A_2 - B_2 = \begin{bmatrix} \alpha^5 - \alpha^7 & \alpha^6 - \alpha^8 \\ \alpha^{15} - \alpha^{21} & \alpha^{18} - \alpha^{24} \end{bmatrix},$$

$$\det(A_2 - B_2) = \alpha^{10} \neq 0.$$

Now,

$$\frac{1}{A_1 - B_1} = \frac{1}{\alpha^{20}} \begin{bmatrix} \alpha^2 & -\alpha^{18} \\ -\alpha^{25} & \alpha^{17} \end{bmatrix},$$

Therefore,

$$\frac{1}{A_1 - B_1} = \begin{bmatrix} \alpha^8 & 2\alpha^{24} \\ 2\alpha^5 & \alpha^{23} \end{bmatrix}.$$

In the same way,

$$\frac{1}{A_1 - B_2} = \begin{bmatrix} \alpha^2 & 2\alpha^6 \\ 2\alpha^{25} & \alpha^5 \end{bmatrix},$$

$$\frac{1}{A_2 - B_1} = \begin{bmatrix} \alpha^{19} & 2\alpha^5 \\ 2\alpha^{16} & \alpha^4 \end{bmatrix},$$

and

$$\frac{1}{A_2 - B_2} = \begin{bmatrix} \alpha^4 & 2\alpha^{12} \\ 2\alpha & \alpha^{11} \end{bmatrix}.$$

So,

$$C = \begin{bmatrix} \alpha^8 & \alpha^{11} & \alpha^2 & \alpha^{19} \\ \alpha^{18} & \alpha^{23} & \alpha^{12} & \alpha^5 \\ \alpha^{25} & \alpha^{18} & \alpha^4 & \alpha^{25} \\ \alpha^3 & \alpha^{10} & \alpha^{14} & \alpha^{11} \end{bmatrix}.$$

Therefore, C is a block Cauchy- like MDS Matrix.
also,

$$D = \begin{bmatrix} \frac{1}{\alpha - \alpha^2} & \frac{1}{\alpha - \alpha^6} & \frac{1}{\alpha - \alpha^{18}} \\ \frac{1}{\alpha^3 - \alpha^2} & \frac{1}{\alpha^3 - \alpha^6} & \frac{1}{\alpha^3 - \alpha^{18}} \\ \frac{1}{\alpha^9 - \alpha^2} & \frac{1}{\alpha^9 - \alpha^6} & \frac{1}{\alpha^9 - \alpha^{18}} \end{bmatrix},$$

$$det\ (D) = 2 \neq 0.$$

So, D is an MDS Cauchy matrix.
Therefore,

$$R = \left\langle \alpha^3 \quad \begin{matrix} \alpha^{25} \\ \alpha^{22} \\ \alpha^{10} \end{matrix} \quad \begin{matrix} \alpha^{18} \\ \alpha^{13} \\ \alpha^{18} \\ \alpha^{13} \end{matrix} \quad \begin{matrix} \alpha^8 \\ \alpha \\ \alpha^{23} \\ \alpha^3 \\ \alpha^4 \\ \alpha^9 \\ \alpha^{11} \end{matrix} \quad \begin{matrix} \alpha^{11} \\ \alpha^{14} \\ \alpha^{12} \\ \alpha^{16} \\ \alpha^{25} \end{matrix} \quad \begin{matrix} \alpha^2 \\ \alpha^{13} \\ \alpha^5 \end{matrix} \quad \alpha^{19} \right\rangle$$

is a block Cauchy-like MDS rhotrix.

V. Conclusion

In the present paper, the construction of MDS Cauchy rhotrices is generalised by taking the elements as conjugate elements of finite fields. This is an extension of the earlier work as the elements have been generalised here. Also, we defined Block Cauchy - like rhotrix which is an enrichment in the literature of rhotrix. Further, we constructed MDS rhotrices using block Cauchy-like rhotrices whose entries are the conjugates elements of finite fields. These constructions may have vast applications in the field of cryptography and coding theory.

REFERENCES

[1] Absalom, E. E., Sani, B. and Sahalu, J. B. (2011). The concept of heart-oriented rhotrix multiplication. Global J. Sci. Fro. Research, 11(2): 35-42.

[2] Ajibade, A. O. (2003). The concept of rhotrices in mathematical enrichment. Int. J. Math. Educ. Sci. Tech., 34(2):175-179.

[3] Alfred, J. M., Paul, C. V. O. and Scott, A. V. (1996). Hand book of Applied Cryptography. CRC Press (Third Edition).

[4] Aminu, A. (2009). On the linear system over rhotrices. Notes on Number Theory and Discrete Mathematics, 15: 7-12.

[5] Aminu, A. (2012). A note on the rhotrix system of equation. Journal of the Nigerian association of Mathematical Physics, 21: 289-296.

[6] Gupta, K. C. and Ray, I. G. (2013). On constructions of MDS matrices from companion matrices for lightweight cryptography: Cryptography Security Engineering and Intelligence Informatics. Lectures Notes in Computer Science, 8128: 29-43.

[7] Gupta, K. C. and Ray, I. G. (2014). On constructions of MDS matrices from circulant-like matrices for lightweight cryptography. ASU/2014/1.

[8] Gupta, S., Narang, R., Harish, M. and Dhiman, N. (2022). MDS block Hankel-like rhotrices using conjugate elements and self-dual bases of finite fields. Bulletin of Pure and Applied Sciences, 41 E(2): 184-198.

[9] Junod, P. and Vaudenay, S. (2004). Perfect diffusion primitives for block ciphers building efficient MDS matrices. Lecture notes in computer science, 3357: 9-10.

[10] Koushesh, M. R. and Zamani, M. (2010). On the application of conjugate elements in finite fields. Finite Fields and Their Applications, 16 (4): 289-302.

[11] Lacan, J. and Fimes, J. (2004). Systematic MDS erasure codes based on Vandermonde matrices. IEEE Trans. Commun. Lett., 8(9): 570-572.

[12] Mohammed, A. (2011). Theoretical development and applications of rhotrices. Ph. D. Thesis. Ahmadu Bello University, Zaria.

[13] Mohammed, A., Ezugwu, E. A. and Sani, B. (2011). On generalization and algorithmatization of heart-based method for multiplication of rhotrices. International Journal of Computer Information Systems, 2: 46-49.

[14] Nakahara, J. and Abrahao, E. (2009). A new involutory MDS matrix for the AES. International Journal of Computer Security, 9: 109-116.

[15] Qiuping, Li., Baofeng, Wu. and Zhuojun, Liu. (2018). Direct construction of (involutory) MDS matrices from block Vandermonde and Cauchy matrices. 7th International Workshop, WAIFI, Bergen.

[16] Sajadieh, M., Dakhilian, M., Mala, H. and Omoomi, B. (2012). On construction of involutory MDS matrices from Vandermonde matrices. Des. Codes and Cry., 64: 287-308.

[17] Sani, B. (2004). An alternative method for multiplication of rhotrices. Int. J. Math. Educ. Sci. Tech., 35(5) : 777-781.

[18] Sani, B. (2007). The row-column multiplication for high dimensional rhotrices. Int. J. Math. Educ. Sci. Technology, 38: 657-662.

[19] Sani, B. (2008). Conversion of a rhotrix to a coupled matrix. Int. J. Math. Educ. Sci. Tech., 39: 244-249.

[20] Sharma, P. L., Gupta, S. and Rehan, M. (2015). Construction of MDS rhotrices using special type of circulant rhotrices over finite fields. Himachal Pradesh University Journal, 03(02): 25-43.

[21] Sharma, P. L., Gupta, S. and Dhiman, N. (2017). Construction of Maximum Distance Separable Rhotrices using Cauchy Rhotrices over Finite Fields. International Journal of Computer Application, 168 (9): 8-17.

[22] Sharma, P. L. and Kanwar, R. K. (2011). A note on relationship between invertible rhotrices and associated invertible matrices. Bulletin of Pure and Applied Sciences, 30 E (2): 333-339.

[23] Sharma, P. L. and Kanwar, R. K. (2012). Adjoint of a rhotrix and its basic properties. International J. Mathematical Sciences,11 (3-4): 337-343.

[24] Sharma, P. L. and Kanwar, R. K. (2012). On inner product space and bilinear forms over rhotrices. Bulletin of Pure and Applied Sciences, 31E(1): 109-118.

[25] Sharma, P. L. and Kanwar, R. K. (2012). The Cayley-Hamilton theorem for rhotrices. International Journal Mathematics and Analysis, 4(1): 171-178.

[26] Sharma, P. L. and Kanwar, R. K. (2013). On involutory and Pascal rhotrices. International J. of Math. Sci. & Engg. Appls. (IJMSEA), 7(4): 133-146.

[27] Sharma, P. L. and Kumar, S. (2013). On construction of MDS rhotrices from companion rhotrices over finite field. International Journal of Mathematical Sciences, 12(3-4): 271-286.

[28] Sharma, P. L. and Kumar, S. (2014). Some applications of Hadamard rhotrices to design balanced incomplete block. International J. of Math. Sci. & Engg. Appls. (IJMSEA), 8(2): 389-406.

[29] Sharma, P. L. and Kumar, S. (2014). Balanced incomplete block design (BIBD) using Hadamard rhotrices. International J. Technology, 4(1): 62-66.

[30] Sharma, P. L. and Kumar, S. (2014). On a special type of Vandermonde rhotrix and its decompositions: Recent Trends in Algebra and Mechanics. Indo-American Books Publisher New Delhi,: 33-40.

[31] Sharma, P. L., Kumar, S. and Rehan, M. (2014). On construction of Hadamard codes using Hadamard rhotrices. International Journal of Theoretical & Applied Sciences, 6(1): 102-111.

[32] Sharma, P. L., Kumar, S. and Rehan, M. (2013). On Hadamard rhotrix over finite field. Bulletin of Pure and Applied Sciences, 32 E (2): 181-190.

[33] Sharma, P. L., Kumar, S. and Rehan, M. (2013). On Vandermonde and MDS rhotrices over GF(2q). International Journal of Mathematics and Analysis, 5(2): 143-160.

[34] Sharma, P. L., Kumar, A. and Gupta, S. (2018). Maximum distance separable Hankel rhotrices over finite fields. J. of Combinatorics, Information & System Sciences, 43(1-4): 13-48.

[35] Sharma, P. L., Kumar, A. and Gupta, S. (2019). Hankel rhotrices and constructions of maximum distance separable rhotrices over finite fields. Applications and Applied Mathematics, 14(2): 1197-1214.

[36] Sharma, P. L., Kumar, A. and Gupta, S. (2020). Trace of the positive integral powers of three and five dimensional rhotrices. Bulletin of Pure and Applied Sciences Mathematics & Statistics, 39 E(1): 165–175.

[37] Sharma, P. L., Kumar, A. and Sharma K. A. (2020). On the characteristic roots and heart of a class of rhotrices over a finite field. Bulletin of Pure and Applied Sciences Mathematics & Statistics, 39 E(2): 277–288.

[38] Tudunkaya, S. M. (2013). Rhotrix polynomial and polynomial rhotrix. Pure and Applied mathematics Journal, 2: 38-41.

[39] Tudunkaya, S. M. and Makanjuola, S. O. (2010). Rhotrices and the construction of finite fields. Bulletin of Pure and Applied Sciences, 29 E(2): 225-229.

[40] Tzeng, K. K. and Zimmermann, K. (1975). On extending Goppa codes to cyclic codes. IEEE Transactions on Information Theory, 21: 721-716.