GANITA,Vol.73(2), 2023, 123-139

ON CONSTRUCTION OF INVOLUTORY MAXIMUM DISTANCE SEPARABLE RHOTRICES USING SELF DUAL BASES OVER GALOIS FIELD

S. GUPTA ✉, R. NARANG and M. HARISH

Abstract

Self-dual bases are useful in many applications like the construction of devices for the arithmetic in finite fields such as multiplication, exponentiation, discrete logarithms and in applications to coding theory, cryptography and the discrete Fourier transforms. The Maximum Distance Separable (MDS) matrices have important applications in cryptography as these offer diffusion properties. In order to simplify the implementation process, it is crucial to explore involutory MDS matrices. Rhotrices, depicted as coupled matrices, serve as an alternative representation. Consequently, substituting matrices with rhotrices effectively enhances security twofold. This paper presents construction of involutory MDS rhotrices within the $\mathbb{F}_{3^3}$, $\mathbb{F}_{5^3}$ and $\mathbb{F}_{2^4}$, employing self-dual basis and finite field elements.

2010 *Mathematics subject classification:* 15A09; 20H30; 11T71.
Keywords and phrases: Rhotrix, Galois field, Maximum distance separable rhotrix, Self-dual basis, Involutory rhotrices.

1. Introduction

As studied in [2], back in 2003, Ajibade has firstly introduced the concept of a 3-dimensional rhotrix. This structure lies between 2×2 dimensional and 3×3 matrices. A 3-dimensional rhotrix, denoted as R_3 of the form:

$$R_3 = \left\langle \begin{array}{ccc} & l & \\ m & n & o \\ & p & \end{array} \right\rangle .$$

In this representation, the variables l, m, n, o, p represent real numbers, and the parameter $h(R_3) = n$ is referred to as the heart of the rhotrix R_3. It is very much clear from the structure of rhotrix that, it is always of odd dimension. Its generalisation is given by Mohammad et al. [8] to include any finite dimensional $(2n + 1)$ rhotrix where $n = 1, 2, \dots$.

In literature of rhotrix, algebra and analysis of rhotrices is discussed by Ajibade [2]. Sani [15, 16] introduced an alternative approach to rhotrix multiplication, while Aminu [3] explored linear systems involving rhotrices. Tudunkaya and Makanjuola [25] presented the concept of rhotrix polynomials. Absalom et al. [1] introduced the idea of heart-oriented rhotrix multiplication. Authors in references [14, 15] discussed the relationship between invertible rhotrices and their associated invertible rhotrices. The adjoint of rhotrices and bilinear forms over rhotrices was detailed in reference [16]. Sharma et al. [22–24] explored Hadamard rhotrices over finite fields and constructed MDS rhotrices from companion rhotrices, one may refer to, [18]. Decompositions of a special type of Vandermonde rhotrices were elaborated in [26]. Circulant rhotrices were introduced by Sharma et al. [13] in the realm of rhotrices. Tudunkaya et al. [25] discussed rhotrices over finite fields.

A square matrix A is called an MDS matrix if and only if all its square sub-matrices are non-singular, as explained in [6]. This condition implies that all entries in an MDS matrix must be non-zero. MDS matrices find various applications in cryptographic hash functions and block ciphers, as discussed by Gupta and Ray [4, 5]. Several methods for constructing MDS rhotrices have been explored. Sharma et al. [13, 17, 19, 20] utilized various rhotrix types, such as Pascal rhotrices, Circulant rhotrices, and Hadamard rhotrices for MDS rhotrix construction. The use of Vandermonde matrices for the construction of involutory MDS rhotrices was discussed by Sajadieh et al. [10], and Lacan and Fimes [6]. Nakahara and Abraho [9] constructed a 16-order involutory MDS matrix using a Cauchy matrix, which was subsequently used in MDS-AES design. Usaini [26] discussed the construction of involutory rhotrices.

In present work, the construction of MDS involutory rhotrices, are demonstrated using a self-dual basis of the finite field of odd characteristics. In the following section, we discuss the preliminaries, algebra of rhotrices and previously obtained results. In section 3, we propose the construction of MDS involutory rhotrices, using a self-dual basis of the finite field of odd characteristics. We demonstrate our proposition with the help of supporting example over $\mathbb{F}_{3^2}$ and $\mathbb{F}_{5^2}$. We construct the MDS rhotrices, using elements of the finite field in section 4. In section 5, some illustrations are given to show that multiplication of an involutory rhotrix with a diagonal rhotrix is again an MDS rhotrix. Lastly, we conclude our paper.

2. Preliminaries

In present section, we recall some basic fundamentals of rhotrices and previously obtained results which are required in of what follows.

2.1 Algebra of Rhotrices

Ajibade [2] defined a 3× 3–dimensional rhotrix, which is, in some way, between 2×2–dimensional and 3×3–dimensional matrices as

$$R_3 = \left\langle \begin{array}{ccc} & l & \\ m & n & o \\ & p & \end{array} \right\rangle,$$

where l, m, n, o, p are real numbers and $h(R_3) = n$ is called the heart of rhotrix R_3. He also defined the operations of addition and scalar multiplication of two rhotrices and also have shown that there are many similarities in the operations of rhotrices and matrices.

Let $Q_3 = \left\langle \begin{array}{ccc} & r & \\ s & t & u \\ & v & \end{array} \right\rangle$ be another 3-dimensional rhotrix, then the addition of two rhotrices is defined as

$$R_3 + Q_3 = \left\langle \begin{array}{ccc} & l & \\ m & n & o \\ & p & \end{array} \right\rangle + \left\langle \begin{array}{ccc} & r & \\ s & t & u \\ & v & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & l+r & \\ m+s & n+t & o+u \\ & p+v & \end{array} \right\rangle,$$

and for any real number α, the scalar multiplication of a rhotrix R_3 is defined as

$$\alpha R_3 = \alpha \left\langle \begin{array}{ccc} & l & \\ m & n & o \\ & p & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & \alpha l & \\ \alpha m & \alpha n & \alpha o \\ & \alpha p & \end{array} \right\rangle.$$

In the literature of rhotrix theory, two types of multiplications of rhotrices are discussed. First type of multiplication is heart oriented multiplication of rhotrices which is discussed by Ajibade and second type of multiplication is row-column multiplication of rhotrices which was given by Sani. Ajibade in [2], discussed the heart-oriented multiplication of 3-dimensional rhotrices as given below:

$$R_3\, o\ Q_3 = \left\langle \begin{array}{ccc} & lt+rn & \\ mt+sn & nt & ot+un \\ & pt+vn & \end{array} \right\rangle.$$

Further, the generalization of the heart-oriented multiplication of 3-dimensional rhotrices to n-dimensional rhotrices is given by Mohammed in [8]. In [1], Sani defined the row column multiplication of 3-dimensional rhotrices as follows:

$$\begin{aligned} R_3\, o\, Q_3 &= \left\langle \begin{array}{ccc} & l & \\ m & n & o \\ & p & \end{array} \right\rangle \left\langle \begin{array}{ccc} & r & \\ s & t & u \\ & v & \end{array} \right\rangle \\ &= \left\langle \begin{array}{ccc} & lr+os & \\ mr+ps & nt & lu+ov \\ & mu+pv & \end{array} \right\rangle. \end{aligned}$$

$$R_3\, o\, Q_3 = \left\langle \begin{array}{ccc} & l & \\ m & n & o \\ & p & \end{array} \right\rangle \left\langle \begin{array}{ccc} & r & \\ s & t & u \\ & v & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & lr+os & \\ mr+ps & nt & lu+ov \\ & mu+pv & \end{array} \right\rangle.$$

2.2 Finite Fields

Let $\mathbb{F}_{q^n}$ be an extension field over the field $\mathbb{F}_q$. There exists an isomorphism between the extension field $\mathbb{F}_{q^n}$ and the n -dimensional vector space $\mathbb{F}_q^n$. The special types of basis namely normal basis, self-dual basis and self-dual normal basis are of particular interest in studies regarding the finite fields and their applications. The following definitions provide the insight about the algebraic structure and properties of these basis.

2.3 Self-dual basis

Consider a basis $a = \{a_1, a_2, \ldots, a_n\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Any other basis $b = \{b_1, b_2, \ldots, b_n\}$ of $\mathbb{F}_{q^n}$ satisfying the relation $tr(a_i b_j) = \delta_{ij}$, where Tr is the trace, defined as $Tr(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$ of an element $\alpha \in \mathbb{F}_{q^n}$ and δ_{ij} is the Kronecker delta function. A basis $a = \{a_1, a_2, \ldots, a_n\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is called self-dual basis if $Tr(a_i a_j) = \delta_{ij}$. A self-dual basis exists in an extension field $\mathbb{F}_{q^n}$ of the field $\mathbb{F}_q$ if q is even or both q and n are odd.

A normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $N = \{a_1, a_2, \ldots, a_n\}$, where $\alpha_i = \alpha^{q^i}, 1 \leq i \leq n$. We say that α is a normal element of $\mathbb{F}_{q^n}$, or that α generates the normal basis N. It is a well-known fact that the normal bases exist in any finite field extension.

2.4 Maximum Distance Separable (MDS) matrices

Definition 2.1. [4] 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, that 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-matrix of A are non-singular. This implies that all the entries of an MDS matrix must be non-zero.

Definition 2.2. [18] An $m \times n$ rhotrix over a finite field K is an MDS rhotrix if it is the linear transformation $f(x) = Ax$ from K^n to K^m such that no two different $(m+n)$-tuples of the form $(x, f(x))$ coincide. The necessary and sufficient condition for a rhotrix to be an MDS rhotrix is that all its sub-rhotrices are non-singular.

Definition 2.3. [26] An involutory rhotrix is a rhotrix that is its own inverse, that is $R = R^{-1}$. It is also called self-invertible rhotrix.

Lemma 2.4. *[18] Any rhotrix R_7 over $GF(2^n)$ with all non-zero entries is known as an MDS rhotrix iff its coupled matrices $M_1 = 4 \times 4$ and $M_2 = 3 \times 3$ are non-singular and all their entries are non -zero.*

A rhotrix is said to be involutory rhotrix if its coupled matrices are involutory.

3. Construction Of Involutory MDS Rhotrices Over The Finite Fields Of Odd Charactristics

The construction of MDS involutory rhotrices from self- dual basis.

Consider a finite field $\mathbb{F}_q$ with q elements, where $q = p^n$ (p be an odd prime). Let $g = \{\alpha_1, \alpha_2,\ ...,\ \alpha_n\}$ be a self dual basis of $\mathbb{F}_q$. Let the matrix of the q cycles of g i.e.

$g^{[i]}$ for $1 \leq i \leq n$, where $[i]$ denotes the q^i (i an integer) be denoted by A, given as:

$$\mathrm{A} = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ {\alpha_1}^{[1]} & {\alpha_2}^{[1]} & \cdots & {\alpha_n}^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ {\alpha_1}^{[n]} & {\alpha_2}^{[n]} & \cdots & {\alpha_n}^{[n]} \end{bmatrix}.$$

Then, we know that $AA^T = I_n$ where I_n is the $n \times n$ identity matrix.
In order to construct an involutory MDS rhotrix $\mathrm{R_T} = \langle \mathrm{A}, \mathrm{B} \rangle$ of dimension $T = 2n - 1$ over $\mathbb{F}_q$, consider A an $n \times n$ matrix constructed using a self-dual basis $\mathrm{g} = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ of $\mathbb{F}_q$ and B an arbitrary $(n-1) \times (n-1)$ involutory matrix with entries in $\mathbb{F}_q$. Thus for, A and B are the coupled matrices of the rhotrix $\mathrm{R_T}$, as long as these are involutory matrices, the rhotrix $\mathrm{R_T}$ is an involutory MDS rhotrix over $\mathbb{F}_q$.
From above discussion, we propose the result in the form of following theorem.

Theorem 3.1. *Let $\mathbb{F}_q$ be the finite field with q elements, where $q = p^n$ (p an odd prime). Let $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ be a self-dual basis of $\mathbb{F}_q$. Let $R_T = \langle C, D \rangle$ be a $2n-1$ dimensional rhotrix whose coupled matrix $C = \left(c_{ij}\right)_{n \times n}$ is generated by $q -$ cycles of the self-dual bases $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ of $\mathbb{F}_q$ and $D = \left(d_{ij}\right)_{(n-1)\times(n-1)}$ be an arbitrary involutory matrix with entries in $\mathbb{F}_q$. Then, $R_T = \langle C, D \rangle$ is an involutory MDS rhotrix.*

In support of our proposition, we provide illustration over the finite fields with odd characteristics.
In this paper, we construct 5- dimensional MDS involutory rhotrices from self- dual basis over $\mathbb{F}_{3^3}$ using irreducible polynomial $p(x) = x^3 + 2x^2 + 1$.
Example 1 Let R_5 be a five dimensional rhotrix whose coupled matrices $C = \left(c_{ij}\right)_{3\times3}$ and $D = \left(d_{ij}\right)_{2\times2}$ are generated by $q-$ powers of self- dual bases $\{\alpha, \alpha^3, \alpha^9\}$ and $\{\alpha^4, \alpha^{23}\}$ respectively over $\mathbb{F}_{3^3}$, where α is the root of the irreducible polynomial $p(x) = x^3 + 2x^2 + 1$. Then, C and D are involutory matrices and hence $R_5 = \langle C,\ D \rangle$ is an involutory MDS rhotrix.

Proof. It is given that the coupled matrices C and D are generated by $q-$ powers of self- dual bases $\{\alpha, \alpha^3, \alpha^9\}$ and $\{\alpha^4, \alpha^{23}\}$ respectively, therefore, C and D are given by

$$C = \begin{bmatrix} \alpha & \alpha^3 & \alpha^9 \\ (\alpha)^3 & (\alpha^3)^3 & (\alpha^9)^3 \\ (\alpha)^{3^2} & (\alpha^3)^{3^2} & (\alpha^9)^{3^2} \end{bmatrix}$$

or

$$C = \begin{bmatrix} \alpha & \alpha^3 & \alpha^9 \\ \alpha^3 & \alpha^9 & \alpha^{27} \\ \alpha^9 & \alpha^{27} & \alpha^{81} \end{bmatrix}$$

and

$$D = \begin{bmatrix} \alpha^4 & \alpha^{23} \\ (\alpha^4)^3 & (\alpha^{23})^3 \end{bmatrix}$$

or

$$D = \begin{bmatrix} \alpha^4 & \alpha^{23} \\ \alpha^{12} & \alpha^{17} \end{bmatrix}.$$

To show that C is involutory matrix, we find CC^T

$$CC^T = \begin{bmatrix} \alpha & \alpha^3 & \alpha^9 \\ \alpha^3 & \alpha^9 & \alpha^{27} \\ \alpha^9 & \alpha^{27} & \alpha^{81} \end{bmatrix} \begin{bmatrix} \alpha & \alpha^3 & \alpha^9 \\ \alpha^3 & \alpha^9 & \alpha^{27} \\ \alpha^9 & \alpha^{27} & \alpha^{81} \end{bmatrix}$$

or

$$CC^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Hence, C is involutory matrix. Similarly, we can show that D is an involutory matrix. Therefore, $R_5 = \langle C,\ D \rangle$ is given by

$$R_5 = \left\langle \begin{array}{ccccc} & & \alpha & & \\ & \alpha^3 & \alpha^4 & \alpha^3 & \\ \alpha^9 & \alpha^{12} & \alpha^9 & \alpha^{23} & \alpha^9 \\ & \alpha^{27} & \alpha^{69} & \alpha^{27} & \\ & & \alpha^{81} & & \end{array} \right\rangle. \tag{3.1}$$

As α is the root of the irreducible polynomial $f(x) = x^3 + 2x^2 + 1$ in $\mathbb{F}_{3^3}$, therefore,

$$\alpha^{27} = \alpha, \alpha^{69} = \alpha^{17}$$

and

$$\alpha^{81} = \alpha^3.$$

Therefore, (3.1) reduces to

$$R_5 = \left\langle \begin{array}{ccccc} & & \alpha & & \\ & \alpha^3 & \alpha^4 & \alpha^3 & \\ \alpha^9 & \alpha^{12} & \alpha^9 & \alpha^{23} & \alpha^9 \\ & \alpha & \alpha^{17} & \alpha & \\ & & \alpha^3 & & \end{array} \right\rangle. \tag{3.2}$$

Since the coupled matrices of R_5 are involutory matrices, therefore, from Definition 2.2, R_5 is an involutory rhotrix. Also, coupled matrices of R_5 are non-singular and all the elements of R_5 are non-zero, therefore, from Lemma 2.4, it is clear that R_5 is MDS rhotrix. □

Example 2 Let R_5 be a five dimensional rhotrix whose coupled matrices $C = \left(c_{ij}\right)_{3\times3}$ and $D = \left(d_{ij}\right)_{2\times2}$ are generated by $q-$ powers of self- dual bases $\{\alpha^8, \alpha^{40}, \alpha^7\}$ and $\{\alpha^{17}, \alpha^{115}\}$ respectively over $\mathbb{F}_{5^3}$ where α is the root of the irreducible polynomial $p(x) = x^3 + 3x + 2$. Then, C and D are involutory matrices and hence $R_5 = \langle C,\ D \rangle$ is an involutory MDS rhotrix.

Proof. It is given that the coupled matrices C and D are generated by $q-$ powers of self- dual bases $\{\alpha^8, \alpha^{40}, \alpha^{76}\}$ and $\{\alpha^{17}, \alpha^{115}\}$ respectively, therefore, C and D are given by

$$C = \begin{bmatrix} \alpha^8 & \alpha^{40} & \alpha^{76} \\ (\alpha^8)^5 & (\alpha^{40})^5 & (\alpha^{76})^5 \\ (\alpha^8)^{5^2} & (\alpha^{40})^{5^2} & (\alpha^{76})^{5^2} \end{bmatrix}$$

or

$$C = \begin{bmatrix} \alpha^8 & \alpha^{40} & \alpha^{76} \\ \alpha^{40} & \alpha^{200} & \alpha^{380} \\ \alpha^{200} & \alpha^{1000} & \alpha^{1900} \end{bmatrix}. \tag{3.3}$$

Since α is the root of the irreducible polynomial $p(x) = x^3 + 3x + 2$ in $\mathbb{F}_{5^3}$, therefore, $\alpha^{200} = \alpha^{76}$, $\alpha^{380} = \alpha^8$, $\alpha^{1000} = \alpha^8$ and $\alpha^{1900} = \alpha^{40}$.
Hence, C in (3.3) reduces to

$$C = \begin{bmatrix} \alpha^8 & \alpha^{40} & \alpha^{76} \\ \alpha^{40} & \alpha^{76} & \alpha^8 \\ \alpha^{76} & \alpha^8 & \alpha^{40} \end{bmatrix}.$$

Also,

$$D = \begin{bmatrix} \alpha^{17} & \alpha^{115} \\ (\alpha^{17})^5 & (\alpha^{115})^5 \end{bmatrix}$$

or

$$D = \begin{bmatrix} \alpha^{17} & \alpha^{115} \\ \alpha^{85} & \alpha^{79} \end{bmatrix}. \tag{3.4}$$

To show that C is involutory matrix, we find CC^T

$$CC^T = \begin{bmatrix} \alpha^{14} & \alpha^{16} & \alpha^{22} \\ \alpha^{16} & \alpha^{22} & \alpha^{14} \\ \alpha^{22} & \alpha^{14} & \alpha^{16} \end{bmatrix} \begin{bmatrix} \alpha^{14} & \alpha^{16} & \alpha^{22} \\ \alpha^{16} & \alpha^{22} & \alpha^{14} \\ \alpha^{22} & \alpha^{14} & \alpha^{16} \end{bmatrix}$$

which gives,

$$CC^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Hence, C is involutory matrix. Similarly, we can show that D is an involutory matrix. Therefore, $R_5 = \langle C,\ D \rangle$ is given by

$$R_5 = \left\langle \begin{array}{ccccc} & & \alpha^{14} & & \\ & \alpha^{16} & \alpha^{10} & \alpha^{16} & \\ \alpha^{22} & \alpha^4 & \alpha^{22} & \alpha^{25} & \alpha^{22} \\ & \alpha^{14} & \alpha^{23} & \alpha^{14} & \\ & & \alpha^{16} & & \end{array} \right\rangle.$$

Since the coupled matrices of R_5 are involutory matrices, therefore, from Definition 2.2, we conclude that R_5 is an involutory rhotrix. Also, all the elements of R_5 are non-zero, therefore, from Lemma 2.4, it is clear that R_5 is MDS rhotrix. □

4. Construction Of MDS Involutory Rhotrices Over The Finite Field Of Prime Characteristics

Theorem 4.1. *Let $\mathbb{F}_q$ be the finite field with q elements, where $q = p^n$. Let $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ be elements of $\mathbb{F}_q$. Let $R_T = \langle C, D\rangle$ be a $2n - 1$ dimensional Maximum Distance Separable rhotrix (but not involutory), whose coupled matrix $C = \left(c_{ij}\right)_{n\times n}$ and $D = \left(d_{ij}\right)_{(n-1)\times(n-1)}$ both are generated by elements $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ of $\mathbb{F}_q$ and if 's' is the sum of elements of any row then, $s^{-1}R_T$ is a MDS involutory rhotrix.*

In support of our proposition we provide illustrations over the finite field of prime characteristics.

Example 1 Let R_7 be a seven dimensional rhotrix whose coupled matrices $A = \left(a_{ij}\right)_{4\times4}$ and $B = \left(b_{ij}\right)_{3\times3}$ are generated by elements $\{\alpha^2, \alpha^5, \alpha^{10}, \alpha^{14}\}$ and $\{\alpha^3, \alpha^9, \alpha^{11}\}$ respectively over $GF\left(2^4\right)$ where α is the root of the irreducible polynomial $p(x) = x^4 + x + 1$ and if sum of each row is α^6. Then, $\alpha^{-6}A$ and $\alpha^{-6}B$ are involutory matrices and hence $\alpha^{-6}R_7$ is an involutory MDS rhotrix.

Proof. Let α be a root of the irreducible polynomial $p(x) = x^4 + x + 1$ over $GF\left(2^4\right)$. As matrices $C = \left(c_{ij}\right)_{4\times4}$ and $D = \left(d_{ij}\right)_{3\times3}$ are generated by elements $\{\alpha^2, \alpha^5, \alpha^{10}, \alpha^{14}\}$ and $\{\alpha^3, \alpha^9, \alpha^{11}\}$. Therefore, matrices C and D are given by

$$C = \begin{bmatrix} \alpha^2 & \alpha^5 & \alpha^{10} & \alpha^{14} \\ \alpha^5 & \alpha^2 & \alpha^{14} & \alpha^{10} \\ \alpha^{10} & \alpha^{14} & \alpha^2 & \alpha^5 \\ \alpha^{14} & \alpha^{10} & \alpha^5 & \alpha^2 \end{bmatrix}$$

$$C^2 = \begin{bmatrix} \alpha^{12} & 0 & 0 & 0 \\ 0 & \alpha^{12} & 0 & 0 \\ 0 & 0 & \alpha^{12} & 0 \\ 0 & 0 & 0 & \alpha^{12} \end{bmatrix}$$

Matrix C is MDS but not involutory.
Sum of elements of each row is,

$$\alpha^2 + \alpha^5 + \alpha^{10} + \alpha^{14} = \alpha^6.$$

Also,

$$\frac{1}{(\alpha^6)^2}A^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

implies that,

$$\frac{1}{(\alpha^6)^2}A^2 = I$$

Hence, $\frac{1}{\alpha^6}C$ is an involutory matrix.
Now,

$$D = \begin{bmatrix} \alpha^3 & \alpha^9 & \alpha^{11} \\ \alpha^9 & \alpha^{11} & \alpha^3 \\ \alpha^{11} & \alpha^3 & \alpha^9 \end{bmatrix}$$

$$D^2 = \begin{bmatrix} \alpha^{12} & 0 & 0 \\ 0 & \alpha^{12} & 0 \\ 0 & 0 & \alpha^{12} \end{bmatrix}$$

Matrix D is MDS but not involutory.
Sum of elements of each row is,

$$\alpha^3 + \alpha^9 + \alpha^{11} = \alpha^6.$$

Also,

$$\frac{1}{(\alpha^6)^2}B^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

implies that,

$$\frac{1}{(\alpha^6)^2}B^2 = I$$

Hence, $\frac{1}{\alpha^6}D$ is an involutory MDS matrix.
Therefore,

$$\frac{1}{(\alpha^6)^2}{R_7}^2 = \left\langle \begin{array}{ccccccc} & & & 1 & & & \\ & & 0 & 1 & 0 & & \\ & 0 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ & 0 & 0 & 1 & 0 & 0 & \\ & & 0 & 1 & 0 & & \\ & & & 1 & & & \end{array} \right\rangle.$$

Hence, $\frac{1}{\alpha^6}R_7$ is an involutory MDS rhotrix. □

Example 2 Let R_5 be a five dimensional rhotrix whose coupled matrices $C = \left(c_{ij}\right)_{3\times3}$ and $D = \left(d_{ij}\right)_{2\times2}$ are generated by elements $\{\alpha^3, \alpha^9, \alpha^{11}\}$ and $\{\alpha^2, \alpha^3\}$ respectively over $GF\left(2^4\right)$ where α is the root of the irreducible polynomial $p(x) = x^4 + x + 1$ and if sum of each row is α^6. Then, $\alpha^{-6}C$ and $\alpha^{-6}D$ are involutory matrices and hence $\alpha^{-6}R_5$ is an involutory MDS rhotrix.

Proof. Let α be a root of the irreducible polynomial $p(x) = x^4 + x + 1$ over $GF\left(2^4\right)$. As matrices $C = \left(c_{ij}\right)_{3\times3}$and $D = \left(d_{ij}\right)_{2\times2}$ are generated by the elements $\{\alpha^3, \alpha^9, \alpha^{11}\}$

and $\{\alpha^2, \alpha^3\}$ respectively. Therefore matrices C and D are given by

$$C = \begin{bmatrix} \alpha^3 & \alpha^9 & \alpha^{11} \\ \alpha^9 & \alpha^{11} & \alpha^3 \\ \alpha^{11} & \alpha^3 & \alpha^9 \end{bmatrix}$$

$$C^2 = \begin{bmatrix} \alpha^{12} & 0 & 0 \\ 0 & \alpha^{12} & 0 \\ 0 & 0 & \alpha^{12} \end{bmatrix}.$$

Matrix C is MDS but not involutory.
Sum of elements of each row is,

$$\alpha^3 + \alpha^9 + \alpha^{11} = \alpha^6.$$

Also,

$$\frac{1}{(\alpha^6)^2} A^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

implies that,

$$\frac{1}{(\alpha^6)^2} A^2 = I$$

Hence, $\frac{1}{\alpha^6} C$ is an involutory MDS matrix.
Now, matrix D is given by

$$D = \begin{bmatrix} \alpha^2 & \alpha^3 \\ \alpha^3 & \alpha^2 \end{bmatrix}$$

implies,

$$D^2 = \begin{bmatrix} \alpha^{12} & 0 \\ 0 & \alpha^{12} \end{bmatrix}.$$

Therefore,
Matrix D is MDS but not involutory.
Sum of elements of each row is,

$$\alpha^2 + \alpha^3 = \alpha^6.$$

Also,

$$\frac{1}{(\alpha^6)^2} D^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

implies that,

$$\frac{1}{(\alpha^6)^2} D^2 = I$$

Hence, $\frac{1}{\alpha^6} D$ is involutory MDS matrix.

Therefore,

$$\frac{1}{(\alpha^6)^2} {R_5}^2 = \left\langle \begin{array}{ccccc} & & 1 & & \\ & 0 & 1 & 0 & \\ 0 & 0 & 1 & 0 & 0 \\ & 0 & 1 & 0 & \\ & & 1 & & \end{array} \right\rangle.$$

Hence, $\frac{1}{\alpha^6} R_5$ is involutory MDS rhotrix. □

5. Construction Of MDS Rhotrices By Multiplication Of Involutory Rhotrix With A Diagonal Rhotrix Using Self Dual Basis

Theorem 5.1. *Let $\mathbb{F}_q$ be the finite field with q elements, where $q = p^n$ (p an odd prime). Let $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ be a self-dual basis of $\mathbb{F}_q$. Let $R_T = \langle C,\ D\rangle$ be a $2n-1$ dimensional an involutory MDS rhotrix whose coupled matrix $C = \left(c_{ij}\right)_{n\times n}$ is generated by $q-$cycles of the self-dual basis $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ of F_q and $D = \left(d_{ij}\right)_{(n-1)\times(n-1)}$ be an arbitrary involutory matrix with entries in $\mathbb{F}_q$. Also $M = \langle E,\ F\rangle$ be any diagonal rhotrix, where $E = \left(e_{ij}\right)_{n\times n}$ is a diagonal matrix, whose diagonal entries are self dual basis $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ of $\mathbb{F}_q$ and $F = \left(f_{ij}\right)_{n-1\times n-1}$ is a diagonal matrix, whose diagonal entries are arbitrary basis which are same as are used to form arbitrary involutory matrix D. Then $R.M = \langle C,\ D\rangle . \langle E, F\rangle$ is again a MDS rhotrix.*

Here are some illustrations

Example 1 Let R_5 be a five dimensional an involutory MDS rhotrix, whose coupled matrices $C = \left(c_{ij}\right)_{3\times3}$ and $D = \left(d_{ij}\right)_{2\times2}$ are generated by $q-$ powers of self- dual bases $\{\alpha^{14}, \alpha^{16}, \alpha^{22}\}$ and $\{\alpha^{10}, \alpha^{25}\}$ respectively over $\mathbb{F}_{3^3}$ where α is the root of the irreducible polynomial $p(x) = x^3 + 2x^2 + 1$, (C and D are involutory matrices). Let $M = \langle E,\ F\rangle$ be a five-dimensional diagonal rhotrix, where coupled matrices are $E = \left(e_{ij}\right)_{3\times3}$ and $F = \left(f_{ij}\right)_{2\times2}$ whose diagonal entries are basis $\{\alpha^{14}, \alpha^{16}, \alpha^{22}\}$ and $\{\alpha^{10}, \alpha^{25}\}$ respectively over $\mathbb{F}_{3^3}$. Then $R.M = \langle C,\ D\rangle . \langle E, F\rangle$ is again a MDS rhotrix.

Proof. Here coupled matrices $C = \left(c_{ij}\right)_{3\times3}$ and $D = \left(d_{ij}\right)_{2\times2}$ are generated by $q-$ powers of self- dual bases $\{\alpha^{14}, \alpha^{16}, \alpha^{22}\}$ and $\{\alpha^{10}, \alpha^{25}\}$ respectively.

Therefore, matrices A and B are given by

$$C = \begin{bmatrix} \alpha^{14} & \alpha^{16} & \alpha^{22} \\ (\alpha^{14})^3 & (\alpha^{16})^3 & (\alpha^{22})^3 \\ (\alpha^{14})^{3^2} & (\alpha^{16})^{3^2} & (\alpha^{22})^{3^2} \end{bmatrix}$$

$$C = \begin{bmatrix} \alpha^{14} & \alpha^{16} & \alpha^{22} \\ \alpha^{42} & \alpha^{48} & \alpha^{66} \\ \alpha^{126} & \alpha^{144} & \alpha^{198} \end{bmatrix}$$

$$C = \begin{bmatrix} \alpha^{14} & \alpha^{16} & \alpha^{22} \\ \alpha^{16} & \alpha^{22} & \alpha^{14} \\ \alpha^{22} & \alpha^{14} & \alpha^{16} \end{bmatrix}$$

and,

$$D = \begin{bmatrix} \alpha^{10} & \alpha^{25} \\ (\alpha^{10})^3 & (\alpha^{25})^3 \end{bmatrix}$$

or

$$D = \begin{bmatrix} \alpha^{10} & \alpha^{25} \\ \alpha^{4} & \alpha^{23} \end{bmatrix}.$$

To show that C is involutory matrix, we find CC^T

$$CC^T = \begin{bmatrix} \alpha^{14} & \alpha^{16} & \alpha^{22} \\ \alpha^{16} & \alpha^{22} & \alpha^{14} \\ \alpha^{22} & \alpha^{14} & \alpha^{16} \end{bmatrix} \begin{bmatrix} \alpha^{14} & \alpha^{16} & \alpha^{22} \\ \alpha^{16} & \alpha^{22} & \alpha^{14} \\ \alpha^{22} & \alpha^{14} & \alpha^{16} \end{bmatrix}$$

implies,

$$CC^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Hence, C is involutory matrix.
Similarly, we can show that D is an involutory matrix. Therefore, $R_5 = \langle C,\ D\rangle$ is given by

$$R_5 = \left\langle \begin{array}{ccccc} & & \alpha^{14} & & \\ & \alpha^{16} & \alpha^{10} & \alpha^{16} & \\ \alpha^{22} & \alpha^{4} & \alpha^{22} & \alpha^{25} & \alpha^{22} \\ & \alpha^{14} & \alpha^{23} & \alpha^{14} & \\ & & \alpha^{16} & & \end{array} \right\rangle.$$

As α is the root of the irreducible polynomial $f(x) = x^3 + 2x^2 + 1$ in $\mathbb{F}_{3^3}$, therefore,

$$\alpha^{27} = \alpha, \alpha^{144} = \alpha^{14}$$

and

$$\alpha^{198} = \alpha^{16}.$$

Also, $M = \langle E,\ F\rangle$ is a diagonal matrix, where matrices C and D are given by

$$E = \begin{bmatrix} \alpha^{14} & 0 & 0 \\ 0 & \alpha^{16} & 0 \\ 0 & 0 & \alpha^{22} \end{bmatrix}$$

and

$$F = \begin{bmatrix} \alpha^{10} & 0 \\ 0 & \alpha^{25} \end{bmatrix}$$

Here,

$$C.E = \begin{bmatrix} \alpha^{14} & \alpha^{16} & \alpha^{22} \\ \alpha^{16} & \alpha^{22} & \alpha^{14} \\ \alpha^{22} & \alpha^{14} & \alpha^{16} \end{bmatrix} \begin{bmatrix} \alpha^{14} & 0 & 0 \\ 0 & \alpha^{16} & 0 \\ 0 & 0 & \alpha^{22} \end{bmatrix}$$

$$C.E = \begin{bmatrix} \alpha^{28} & \alpha^{32} & \alpha^{44} \\ \alpha^{30} & \alpha^{38} & \alpha^{36} \\ \alpha^{36} & \alpha^{30} & \alpha^{38} \end{bmatrix}$$

or

$$C.E = \begin{bmatrix} \alpha^{2} & \alpha^{6} & \alpha^{18} \\ \alpha^{4} & \alpha^{12} & \alpha^{10} \\ \alpha^{10} & \alpha^{4} & \alpha^{12} \end{bmatrix}.$$

det $(C.E) = \alpha^{18} \neq 0$ Therefore, $C.E$ is MDS matrix. Similarly,

$$D.F = \begin{bmatrix} \alpha^{10} & \alpha^{25} \\ \alpha^{4} & \alpha^{23} \end{bmatrix} \begin{bmatrix} \alpha^{10} & 0 \\ 0 & \alpha^{25} \end{bmatrix}$$

$$D.F = \begin{bmatrix} \alpha^{20} & \alpha^{50} \\ \alpha^{14} & \alpha^{48} \end{bmatrix}$$

or,

$$D.F = \begin{bmatrix} \alpha^{20} & \alpha^{24} \\ \alpha^{14} & \alpha^{22} \end{bmatrix}.$$

det$(D.F) = \alpha^{22} \neq 0$ Therefore, $D.F$ is a MDS matrix. Hence,

$$R.M = \langle C,\ D\rangle . \langle E,\ F\rangle$$

$$R.M = \left\langle \begin{array}{ccccc} & & \alpha^{28} & & \\ & \alpha^{30} & \alpha^{20} & \alpha^{32} & \\ \alpha^{36} & \alpha^{14} & \alpha^{38} & \alpha^{24} & \alpha^{44} \\ & \alpha^{30} & \alpha^{22} & \alpha^{36} & \\ & & \alpha^{38} & & \end{array} \right\rangle.$$

Therefore, $R.M$ is a MDS rhotrix. □

Example 2 Let R_5 be a five dimensional an involutory MDS rhotrix, whose coupled matrices $C = \left(c_{ij}\right)_{3\times3}$ and $D = \left(d_{ij}\right)_{2\times2}$ are generated by $q-$ powers of self- dual bases $\{\alpha^{14}, \alpha^{70}, \alpha^{102}\}$ and $\{\alpha^{17}, \alpha^{115}\}$ respectively over $\mathbb{F}_{5^3}$ where α is the root of the irreducible polynomial $p(x) = x^3 + 3x + 2$, (C and D are involutory matrices). And $M = \langle E,\ F\rangle$ be a five-dimensional diagonal rhotrix, where coupled matrices are $E = \left(e_{ij}\right)_{3\times3}$ and $F = \left(f_{ij}\right)_{2\times2}$ whose diagonal entries are basis $\{\alpha^{14}, \alpha^{70}, \alpha^{102}\}$ and $\{\alpha^{17}, \alpha^{115}\}$ respectively, over $\mathbb{F}_{5^3}$. Then $R.M = \langle C,\ D\rangle . \langle E, F\rangle$ is again a MDS rhotrix.

Proof. Here coupled matrices $C = \left(c_{ij}\right)_{3\times 3}$ and $D = \left(d_{ij}\right)_{2\times 2}$ are generated by $q-$ powers of self- dual bases $\{\alpha^{14}, \alpha^{70}, \alpha^{102}\}$ and $\{\alpha^{17}, \alpha^{115}\}$ respectively.
Therefore, matrices A and B are given by

$$C = \begin{bmatrix} \alpha^{14} & \alpha^{70} & \alpha^{102} \\ (\alpha^{14})^{5} & (\alpha^{70})^{5} & (\alpha^{102})^{5} \\ (\alpha^{14})^{5^2} & (\alpha^{70})^{5^2} & (\alpha^{102})^{5^2} \end{bmatrix}$$

or

$$C = \begin{bmatrix} \alpha^{14} & \alpha^{70} & \alpha^{102} \\ \alpha^{70} & \alpha^{350} & \alpha^{510} \\ \alpha^{350} & \alpha^{1750} & \alpha^{2550} \end{bmatrix}$$

implies,

$$C = \begin{bmatrix} \alpha^{14} & \alpha^{70} & \alpha^{102} \\ \alpha^{70} & \alpha^{102} & \alpha^{14} \\ \alpha^{102} & \alpha^{14} & \alpha^{70} \end{bmatrix}$$

and

$$D = \begin{bmatrix} \alpha^{17} & \alpha^{115} \\ (\alpha^{17})^{5} & (\alpha^{115})^{5} \end{bmatrix}$$

or

$$D = \begin{bmatrix} \alpha^{17} & \alpha^{115} \\ \alpha^{85} & \alpha^{575} \end{bmatrix}$$

$$D = \begin{bmatrix} \alpha^{17} & \alpha^{115} \\ \alpha^{85} & \alpha^{79} \end{bmatrix}.$$

To show that A is involutory matrix, we find AA^T

$$CC^T = \begin{bmatrix} \alpha^{14} & \alpha^{70} & \alpha^{102} \\ \alpha^{70} & \alpha^{102} & \alpha^{14} \\ \alpha^{102} & \alpha^{14} & \alpha^{70} \end{bmatrix} \begin{bmatrix} \alpha^{14} & \alpha^{70} & \alpha^{102} \\ \alpha^{70} & \alpha^{102} & \alpha^{14} \\ \alpha^{102} & \alpha^{14} & \alpha^{70} \end{bmatrix}$$

implies,

$$CC^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Hence, C is involutory matrix. Similarly, we can show that D is an involutory matrix.
Therefore, $R_5 = \langle C,\ D \rangle$ is given by

$$R_5 = \left\langle \begin{array}{ccccc} & & \alpha^{14} & & \\ & \alpha^{70} & \alpha^{17} & \alpha^{70} & \\ \alpha^{102} & \alpha^{85} & \alpha^{102} & \alpha^{115} & \alpha^{102} \\ & \alpha^{14} & \alpha^{79} & \alpha^{14} & \\ & & \alpha^{70} & & \end{array} \right\rangle.$$

As α is the root of the irreducible polynomial $f(x) = x^3 + 3x + 2$ in $\mathbb{F}_{5^3}$, therefore,

$$\alpha^{124} = 1, \alpha^{575} = \alpha^{79}$$

and

$$\alpha^{1750} = \alpha^{14}.$$

Also, $M = \langle E,\ F\rangle$ is a diagonal matrix, where matrices E and F are given by

$$E = \begin{bmatrix} \alpha^{14} & 0 & 0 \\ 0 & \alpha^{70} & 0 \\ 0 & 0 & \alpha^{102} \end{bmatrix}$$

and

$$F = \begin{bmatrix} \alpha^{17} & 0 \\ 0 & \alpha^{115} \end{bmatrix}.$$

Here,

$$C.E = \begin{bmatrix} \alpha^{14} & \alpha^{70} & \alpha^{102} \\ \alpha^{70} & \alpha^{102} & \alpha^{14} \\ \alpha^{102} & \alpha^{14} & \alpha^{70} \end{bmatrix} \begin{bmatrix} \alpha^{14} & 0 & 0 \\ 0 & \alpha^{70} & 0 \\ 0 & 0 & \alpha^{102} \end{bmatrix}$$

$$C.E = \begin{bmatrix} \alpha^{28} & \alpha^{140} & \alpha^{204} \\ \alpha^{84} & \alpha^{172} & \alpha^{116} \\ \alpha^{116} & \alpha^{84} & \alpha^{172} \end{bmatrix}$$

or

$$C.E = \begin{bmatrix} \alpha^{28} & \alpha^{16} & \alpha^{80} \\ \alpha^{84} & \alpha^{48} & \alpha^{116} \\ \alpha^{116} & \alpha^{84} & \alpha^{48} \end{bmatrix}.$$

$\det(C.E) = \alpha^{106} \neq 0$ Therefore, $C.E$ is MDS matrix. Similarly,

$$D.F = \begin{bmatrix} \alpha^{17} & \alpha^{115} \\ \alpha^{85} & \alpha^{72} \end{bmatrix} \begin{bmatrix} \alpha^{17} & 0 \\ 0 & \alpha^{115} \end{bmatrix}$$

$$D.F = \begin{bmatrix} \alpha^{34} & \alpha^{230} \\ \alpha^{102} & \alpha^{194} \end{bmatrix}$$

or

$$D.F = \begin{bmatrix} \alpha^{34} & \alpha^{106} \\ \alpha^{102} & \alpha^{70} \end{bmatrix}.$$

$\det(D.F) = \alpha^{70} \neq 0$ Therefore, $D.F$ is a MDS matrix. Hence,

$$R.M = \langle C,\ D\rangle . \langle E,\ F\rangle$$

$$R.M = \left\langle \begin{array}{ccccc} & & \alpha^{28} & & \\ & \alpha^{84} & \alpha^{34} & \alpha^{16} & \\ \alpha^{116} & \alpha^{102} & \alpha^{48} & \alpha^{106} & \alpha^{80} \\ & \alpha^{84} & \alpha^{70} & \alpha^{116} & \\ & & \alpha^{48} & & \end{array} \right\rangle.$$

Therefore, $R.M$ is a MDS rhotrix. □

6. Conclusion

Maximum Distance Separable involutory rhotrices are constructed from self- dual bases over $\mathbb{F}_{3^3}$, $\mathbb{F}_{5^3}$ and $\mathbb{F}_{2^4}$ using irreducible polynomials $p(x) = x^3 + 2x^2 + 1$ and $p(x) = x^3 + 3x + 2$ respectively. Similar constructions can be done over higher dimensional finite fields. An MDS involutory rhotrix is also constructed using elements of irreducible polynomial $p(x) = x^4 + x + 1$ over $\mathbb{F}_{2^4}$ and it is also shown that multiplication of an involutory rhotrix with a diagonal rhotrix using self-dual basis is again an MDS rhotrix.

Conflicts of Interest: The authors declare no conflict of interest.

References

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

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

[3] A. Aminu, *On the linear system over rhotrices*, Notes Number Theory Discret. Math., **15** (2009) 7-12.

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

[5] K.C. Gupta and I.G. Ray, *On constructions of MDS matrices from circulant-like matrices for lightweight cryptography*, Applied Statistics Unit, Indian Statistical Institute, Calcuta, India, (2014).

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

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

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

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

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

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

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

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

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

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

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

[17] P.L. Sharma and R.K. Kanwar, *On involutory and pascal rhotrices*, International J. of Math. Sci. & Engg. Appls., **7** (2013) 133-146.

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

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

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

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

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

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

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

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

[26] S. Usaini, *On Construction of Involutory Rhotrices*, International J. of Math. Edu. In Sci. & Tech., **43** (2012) 510-515.

S. Gupta, Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, India
e-mail: shalini.garga1970@gmail.com

R. Narang, Department of Mathematics, G. C. Karsog, District Mandi, Himachal Pradesh, India
e-mail: ruchinarang8878@gmail.com

M. Harish, Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, India
e-mail: mansihverma16@gmail.com