Applications and Applied Mathematics: An International Journal (AAM)

Volume 19
Issue 3 *Special Issue No. 12 (March 2024)*

Article 9

3-2024

On Constructions of Maximum Distance Separable Pascal-Like Rhotrices over Finite Fields

Neetu Dhiman
Himachal Pradesh University, Shimla, India

Mansi Harish
H.P. University, Shimla, India

Shalini Gupta
H.P. University, Shimla, India

Arun Chauhan
Govt. College Jukhala, Bilaspur, India

Available at
http://pvamu.edu/aam
Appl. Appl. Math.
ISSN: 1932-9466

Applications and Applied Mathematics:
An International Journal
(AAM)

Special Issue No. 12 (March 2024), Article 9, 15 pages

On Constructions of Maximum Distance Separable Pascal-Like Rhotrices over Finite Fields

[1]Neetu Dhiman, [2]Mansi Harish, [3*]Shalini Gupta and [4]Arun Chauhan

[1]Department of Applied Sciences & Humanities
UIT, Himachal Pradesh University, Shimla, India
Email: dhimanneetu278@gmail.com

[2,3]Department of Mathematics & Statistics
H. P. University, Shimla, India
[2]mansihverma16@gmail.com; [3]shalini.garga1970@gmail.com

[4]Govt. College
Jukhala, Bilaspur, India
Email: arunch.925@gmail.com

*Corresponding author

Received: May 1, 2023; Accepted: September 8, 2023

Abstract

Cryptography and coding theory are the important areas where Maximum Distance Separable (MDS) matrices are used extensively. The Pascal matrix plays vital role in combinatorics, matrix theory and its properties provide interesting combinatorial identities. Pascal matrices also have a wide range of applications in cryptography. In this paper, we define Pascal-like rhotrix, and further, we construct MDS Pascal-like rhotrices over finite fields.

Keywords: Pascal matrix; MDS matrix; Coupled matrices; Rhotrix; MDS rhotrix; Pascal-like rhotrix; Cryptography

MSC 2010 No.: 15B99; 20H30

1. Introduction

Rhotrices have been studied more frequently in last few years due to their implementation in other fields such as engineering, coding theory, cryptography, etc. The focus is to identify the relationship between rhotrices and some other fields in algebra. Ajibade (2003) was the first one who defined the rhotrix along with the operations of addition, scalar multiplication and multiplication. The heart-oriented multiplication of rhotrices is given by Ajibade and another method of multiplication of rhotrices is row-column multiplication of rhotrices, which is discussed by Sani (2004). Sani (2007) generalized the row-column multiplication for high dimensional rhotrices. Sani (2008) represented the rhotrix in the form of coupled matrices. This representation of a rhotrix is useful in cryptography to improve the security of cryptosystems. The theoretical development of rhotrices and various properties of rhotrices are discussed by Absalom et al. (2011), Aminu (2009), Mohammed (2011) and Sharma et al. (2012-2015, 2017). Aminu (2012) and Tudunkaya (2013) have studied the system of equations in the case of rhotrices and polynomial rhotrices. An algorithm for heart-oriented multiplication of rhotrices for computing using machines is discussed by Mohammed et al. (2011). Sharma and Kumar (2013) have introduced MDS rhotrices and Gupta et al. (2022) block rhotrices in the literature. Different types of rhotrices such as Vandermonde rhotrices, Sylvester rhotrices, Cauchy rhotrices, circulant rhotrices, Hankel rhotrices, Toeplitz rhotrices, MDS rhotrices and their properties are given by Sharma et al. (2013, 2015, 2017-2020). MDS matrices are studied in the literature by Nakahara and Abrahao (2009), Sarkar and Habeeb (2016, 2017). MDS matrices are derived from Reed-Solomn codes and due to their diffusion property, they are major components of many ciphers such as AES, Two fish & various hash functions as discussed in Alfred et al.(1996). Therefore, the construction of MDS matrices plays significant role for cryptographic algorithms. MDS matrices are constructed by Gupta and Ray (2013) and Sajadieh et al. (2012). As rhotrices are combination of two coupled matrices, therefore MDS rhotrices may double the security of the cryptosystems. The construction of MDS rhotrices using Toeplitz rhotrices are given by Sharma and Gupta (2017).

Pascal matrices have attracted the attention of many researchers because their properties provide many combinatorial identities and are used for the decomposition of matrices. Neamah (2023) proposed an image encryption scheme using Pascal matrix. The applicability of the Pascal matrix motivated us to introduce Pascal-like rhotrices for the algebraic development of the subject as well as to establish a bridge between rhotrix theory and other mathematical fields. In the present paper, we define the Pascal-like rhotrix and construct MDS Pascal-like rhotrices over finite fields.

2. Preliminaries

In this section, we give preliminary results which are used in the subsequent sections. Gupta and Ray in 2013 gave a result related with MDS matrix which states that a square matrix M is an MDS matrix if and only if every square sub-matrix of M is non-singular. That means, all the entries of an MDS matrix must be non-vanishing. On the same analogy, Sharma et al. 2013, proved that a rhotrix R_{2n+1} over $GF(2^n)$ with all non-zero entries is an MDS rhotrix iff its coupled matrices C of order $n+1$ and D of order n are non-singular, and all their entries are non-zero.

3. Main Results

In this section, we define a Pascal-like rhotrix over finite fields. Further, we construct Maximum Distance Separable Pascal-like rhotrices over finite fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{3^n}$.

Definition 3.1

A Pascal-like rhotrix of dimension n is defined as $P = \langle C, D \rangle$, where $C = \begin{pmatrix} {}^{i+j}C_i \end{pmatrix}$, $i,j = 1,2,\ldots,t$ and $D = \begin{pmatrix} {}^{i+j}C_i \end{pmatrix}$, $i,j = 1,2,\ldots,t-1$, where γ is the root of irreducible polynomial over $\mathbb{F}_{p^n}$ and $t = \frac{n+1}{2}$.

3.1 Construction of Maximum Distance Separable Pascal-like Rhotrices over Finite Field $\mathbb{F}_{2^n}$

Theorem 3.1

Let $R_5 =< C, D >$ be a Pascal-like rhotrix of dimension 5 whose coupled matrices C and D over $\mathbb{F}_{2^n}$ are defined as $C = \begin{pmatrix} {}^{i+j}C_i \end{pmatrix}$, $i,j = 1,2,3$ and $D = \begin{pmatrix} {}^{i+j}C_i \end{pmatrix}$, $i,j = 1,2$; where γ is the root of an irreducible polynomial over $\mathbb{F}_{2^n}$. Then, C and D form an MDS Pascal-like rhotrix R_5 for $n \geq 3$.

Proof:

Let C and D be the coupled matrices of a Pascal-like rhotrix R_5 which is given by

$$\mathrm{R}_5 = \left\langle \begin{matrix} & & C[1][1] & & \\ & C[2][1] & D[1][1] & C[1][2] & \\ C[3][1] & D[2][1] & C[2][2] & D[1][2] & C[1][3] \\ & C[3][2] & D[2][2] & C[2][3] & \\ & & C[3][3] & & \end{matrix} \right\rangle. \qquad (3.1.1)$$

Since $C = \begin{pmatrix} {}^{i+j}C_i \end{pmatrix}$, $i,j = 1,2,3$ and $D = \begin{pmatrix} {}^{i+j}C_i \end{pmatrix}$, $i,j = 1,2$. Therefore, C and D are given by

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 \\ \gamma^3 & \gamma^6 & \gamma^{10} \\ \gamma^4 & \gamma^{10} & \gamma^{20} \end{bmatrix} \text{ and } D = \begin{bmatrix} \gamma^2 & \gamma^3 \\ \gamma^3 & \gamma^6 \end{bmatrix}.$$

Case 1: For $n = 3$, let γ be a root of the irreducible polynomial $y^3 + y + 1 = 0$. Then,

$$C = \begin{bmatrix} \gamma^2 & \gamma+1 & \gamma^2+\gamma \\ \gamma+1 & \gamma^2+1 & \gamma+1 \\ \gamma^2+\gamma & \gamma+1 & \gamma^2+1 \end{bmatrix}. \tag{3.1.2}$$

Now, determinant$(C) = \gamma^2 + 1 \neq 0$. Also,

$$D = \begin{bmatrix} \gamma^2 & \gamma+1 \\ \gamma+1 & \gamma^2+1 \end{bmatrix}, \tag{3.1.3}$$

and determinant $(D) = \gamma^2 + \gamma + 1 \neq 0$. As all the entries of C and D are non-zero; C and D are non-singular matrices.

Therefore, C and D are MDS matrices. Using (3.1.2) and (3.1.3) in (3.1.1), we get

$$\mathrm{R}_5 = \left\langle \begin{array}{ccccc} & & \gamma^2 & & \\ & \gamma+1 & \gamma^2 & \gamma+1 & \\ \gamma^2+\gamma & \gamma+1 & \gamma^2+1 & \gamma+1 & \gamma^2+\gamma \\ & \gamma+1 & \gamma^2+1 & \gamma+1 & \\ & & \gamma^2+1 & & \end{array} \right\rangle,$$

which is also MDS Pascal-like rhorix.

Case 2: Consider an irreducible polynomial $y^4 + y + 1 = 0$ and let γ be the root of this irreducible polynomial, then the coupled matrix C in this case becomes

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma+1 \\ \gamma^3 & \gamma^3+\gamma^2 & \gamma^2+\gamma+1 \\ \gamma+1 & \gamma^2+\gamma+1 & \gamma^2+\gamma \end{bmatrix}. \tag{3.1.4}$$

The matrix C and all its sub-matrices have non-zero determinant. Therefore, C is an MDS matrix. By the similar argument, the matrix D

$$D = \begin{bmatrix} \gamma^2 & \gamma^3 \\ \gamma^3 & \gamma^3+\gamma^2 \end{bmatrix}, \tag{3.1.5}$$

is an MDS matrix. From (3.1.1), (3.1.4) and (3.1.5), we have

$$R_5 = \left\langle \begin{array}{ccccc} & & \gamma^2 & & \\ & \gamma^3 & \gamma^2 & \gamma^3 & \\ \gamma+1 & \gamma^3 & \gamma^3+\gamma^2 & \gamma^3 & \gamma+1 \\ & \gamma^2+\gamma+1 & \gamma^3+\gamma^2 & \gamma^2+\gamma+1 & \\ & & \gamma^2+\gamma & & \end{array} \right\rangle.$$

Therefore, $R_5 = < C, D >$ is an MDS Pascal-like rhotrix for $n = 4$.

Case 3: For $n = 5$, let $y^5 + y^2 + 1 = 0$ be an irreducible polynomial and γ be its root, then C becomes

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 \\ \gamma^3 & \gamma^3+\gamma & \gamma^4+1 \\ \gamma^4 & \gamma^4+1 & \gamma^3+\gamma^2 \end{bmatrix}. \tag{3.1.6}$$

Here, determinant$(C) = \gamma^2 \neq 0$ and determinant of all square sub-matrices of C are also non-zero. Therefore, C is an MDS matrix. On the basis of similar arguments, the coupled matrix

$$D = \begin{bmatrix} \gamma^2 & \gamma^3 \\ \gamma^3 & \gamma^3+\gamma \end{bmatrix}, \tag{3.1.7}$$

is also an MDS matrix. From equations (3.1.1), (3.1.6) and (3.1.7), we get

$$R_5 = \left\langle \begin{array}{ccccc} & & \gamma^2 & & \\ & \gamma^3 & \gamma^2 & \gamma^3 & \\ \gamma^4 & \gamma^3 & \gamma^3+\gamma & \gamma^3 & \gamma^4 \\ & \gamma^4+1 & \gamma^3+\gamma & \gamma^4+1 & \\ & & \gamma^3+\gamma^2 & & \end{array} \right\rangle.$$

Therefore, $R_5 =< C, D >$ is an MDS Pascal-like rhotrix for $n = 5$. In a similar manner, we can check that R_5 is MDS Pascal-like rhotrix for $n > 5$. Thus, R_5 is an MDS Pascal-like rhotrix for $n \geq 3$. ■

Theorem 3.2

Let $R_7 =< C, D >$ be a Pascal-like rhotrix of dimension 7 whose coupled matrices C and D over $\mathbb{F}_{2^n}$ are defined as $C = \begin{pmatrix} {}^{i+j}C_i \\ \gamma \end{pmatrix}$, $i, j = 1, 2, 3, 4$ and $D = \begin{pmatrix} {}^{i+j}C_i \\ \gamma \end{pmatrix}$, $i, j = 1, 2, 3$. Then, C and D form an MDS Pascal-like rhotrix R_7 for $n \geq 3$.

Proof:

Let C and D be the coupled matrices of a 7-dimensional Pascal-like rhotrix R_7 which is given by

$$R_7 = \left\langle \begin{array}{ccccccc} & & & C[1][1] & & & \\ & & C[2][1] & D[1][1] & C[1][2] & & \\ & C[3][1] & D[2][1] & C[2][2] & D[1][2] & C[1][3] & \\ C[4][1] & D[3][1] & C[3][2] & D[2][2] & C[2][3] & D[1][3] & C[1][4] \\ & C[4][2] & D[3][2] & C[3][3] & D[2][3] & C[2][4] & \\ & & C[4][3] & D[3][3] & C[3][4] & & \\ & & & C[4][4] & & & \end{array} \right\rangle. \tag{3.1.8}$$

Since $C = \begin{pmatrix} {}^{i+j}C_i \\ \gamma \end{pmatrix}$, $i, j = 1, 2, 3, 4$ and $D = \begin{pmatrix} {}^{i+j}C_i \\ \gamma \end{pmatrix}$, $i, j = 1, 2, 3$. Therefore, coupled matrices C and D are given by

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 & \gamma^5 \\ \gamma^3 & \gamma^6 & \gamma^{10} & \gamma^{15} \\ \gamma^4 & \gamma^{10} & \gamma^{20} & \gamma^{35} \\ \gamma^5 & \gamma^{15} & \gamma^{35} & \gamma^{70} \end{bmatrix},$$

and

$$D = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 \\ \gamma^3 & \gamma^6 & \gamma^{10} \\ \gamma^4 & \gamma^{10} & \gamma^{20} \end{bmatrix}.$$

.

Case 1: Consider an irreducible polynomial $y^3 + y + 1 = 0$ of degree 3 over $\mathbb{F}_2$ and let γ be the root of this irreducible polynomial. For $n = 3$, the coupled matrix C is

$$C = \begin{bmatrix} \gamma^2 & \gamma + 1 & \gamma^2 + \gamma & \gamma^2 + \gamma + 1 \\ \gamma + 1 & \gamma^2 + 1 & \gamma + 1 & \gamma \\ \gamma^2 + \gamma & \gamma + 1 & \gamma^2 + 1 & \gamma \\ \gamma^2 + \gamma + 1 & \gamma & \gamma & \gamma^2 \end{bmatrix}. \tag{3.1.9}$$

Here, all the entries of C are non-zero, determinant $(C) = \gamma^2 + 1 \neq 0$ and the determinants of all the square sub-matrices of C are non-zero. So, C is an MDS matrix. Similarly, we see that the coupled matrix

$$D = \begin{bmatrix} \gamma^2 & \gamma+1 & \gamma^2+\gamma \\ \gamma+1 & \gamma^2+1 & \gamma+1 \\ \gamma^2+\gamma & \gamma+1 & \gamma^2+1 \end{bmatrix}, \tag{3.1.10}$$

is an MDS matrix. Hence, from (3.1.8), (3.1.9) and (3.1.10), the 7-dimensional rhotrix

$$R_7 = \left\langle \begin{array}{ccccccc} & & & \gamma^2 & & & \\ & & \gamma+1 & \gamma^2 & \gamma+1 & & \\ & \gamma^2+\gamma & \gamma+1 & \gamma^2+1 & \gamma+1 & \gamma^2+\gamma & \\ \gamma^2+\gamma+1 & \gamma^2+\gamma & \gamma+1 & \gamma^2+1 & \gamma+1 & \gamma^2+\gamma & \gamma^2+\gamma+1 \\ & \gamma & \gamma+1 & \gamma^2+1 & \gamma+1 & \gamma & \\ & & \gamma & \gamma^2+1 & \gamma & & \\ & & & \gamma^2 & & & \end{array} \right\rangle.$$

is an MDS Pascal-like rhotrix for $n = 3$.

Case 2: Let $y^4 + y + 1 = 0$ be an irreducible polynomial of degree 4 over $\mathbb{F}_2$ and let γ be the root of this irreducible polynomial. Therefore, for $n = 4$, the coupled matrix C is given by

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma+1 & \gamma^2+\gamma \\ \gamma^3 & \gamma^3+\gamma^2 & \gamma^2+\gamma+1 & 1 \\ \gamma+1 & \gamma^2+\gamma+1 & \gamma^2+\gamma & \gamma^2+\gamma \\ \gamma^2+\gamma & 1 & \gamma^2+\gamma & \gamma^2+\gamma+1 \end{bmatrix}. \tag{3.1.11}$$

Here, each entry of C is non-zero. Also, determinant $(C) = \gamma^3 + \gamma^2 + \gamma \neq 0$ and the determinants of all the square sub-matrices of C are also non-zero. Therefore, the matrix C is an MDS matrix. Similar argument gives that

$$D = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma+1 \\ \gamma^3 & \gamma^3+\gamma^2 & \gamma^2+\gamma+1 \\ \gamma+1 & \gamma^2+\gamma+1 & \gamma^2+\gamma \end{bmatrix}. \tag{3.1.12}$$

is an MDS matrix. From (3.1.8), (3.1.11) and (3.1.12), the 7-dimensional rhotrix

$$R_7 = \left\langle \begin{array}{ccccccc} & & & \gamma^2 & & & \\ & & \gamma^3 & \gamma^2 & \gamma^3 & & \\ & \gamma+1 & \gamma^3 & \gamma^3+\gamma^2 & \gamma^3 & \gamma+1 & \\ \gamma^2+\gamma & \gamma+1 & \gamma^2+\gamma+1 & \gamma^3+\gamma^2 & \gamma^2+\gamma+1 & \gamma+1 & \gamma^2+\gamma \\ & 1 & \gamma^2+\gamma+1 & \gamma^2+\gamma & \gamma^2+\gamma+1 & 1 & \\ & & \gamma^2+\gamma & \gamma^2+\gamma & \gamma^2+\gamma & & \\ & & & \gamma^2+\gamma+1 & & & \end{array} \right\rangle.$$

is an MDS Pascal-like rhotrix for $n = 4$.

Case 3: Let γ be the root of irreducible polynomial $y^5 + y^2 + 1 = 0$ of degree 5 over $\mathbb{F}_2$. Therefore, for $n = 5$, the coupled matrix C is

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 & \gamma^2+1 \\ \gamma^3 & \gamma^3+\gamma & \gamma^4+1 & \gamma^4+\gamma^3+\gamma^2+\gamma+1 \\ \gamma^4 & \gamma^4+1 & \gamma^3+\gamma^2 & \gamma^4 \\ \gamma^2+1 & \gamma^4+\gamma^3+\gamma^2+\iota+1 & \gamma^4 & \gamma^3+\gamma^2+1 \end{bmatrix}. \qquad (3.1.13)$$

Since all the entries of C are non-zero, determinant $(C) = \gamma^4 + \gamma^2 + \gamma + 1 \neq 0$ and the determinants of all the square sub-matrices of C are non-zero. Therefore, C is an MDS matrix. Using the same arguments, we see that the coupled matrix

$$D = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 \\ \gamma^3 & \gamma^3+\gamma & \gamma^4+1 \\ \gamma^4 & \gamma^4+1 & \gamma^3+\gamma^2 \end{bmatrix}, \qquad (3.1.14)$$

is also an MDS matrix.

Hence, equations (3.1.8), (3.1.13) and (3.1.14), the 7-dimensional rhotrix given by

$$R_7 = \left\langle \begin{array}{ccccccc} & & & \gamma^2 & & & \\ & & \gamma^3 & \gamma^2 & \gamma^3 & & \\ & \gamma^4 & \gamma^3 & \gamma^3+\gamma & \gamma^3 & \gamma^4 & \\ \gamma+1 & \gamma^4 & \gamma^4+1 & \lambda^3+\gamma & \gamma^4+1 & \gamma^4 & \gamma+1 \\ & \gamma^4+\gamma^3+\gamma^2+\gamma+1 & \gamma^4+1 & \gamma^3+\gamma^2 & \gamma^4+1 & \gamma^4+\gamma^3+\gamma^2+\gamma+1 & \\ & & \gamma^4 & \gamma^3+\gamma^2 & \gamma^4 & & \\ & & & \gamma^3+\gamma^2+1 & & & \end{array} \right\rangle.$$

is an MDS Pascal-like rhotrix for $n = 5$. Similarly, we can prove the results for any $n > 5$. Thus, R_7 is an MDS Pascal-like rhotrix over $\mathbb{F}_{2^n}$ for $n \geq 3$. ■

3.2 Construction of Maximum Distance Separable Pascal-like Rhotrices over Finite Field $\mathbb{F}_{3^n}$

Theorem 3.3

Let $R_5 =< C, D >$ be a 5- dimensional Pascal-like rhotrix, whose coupled matrices C and D over $\mathbb{F}_{3^n}$ are defined as $C = \begin{pmatrix} \gamma^{i+j}C_i \end{pmatrix}$, $i,j = 1,2,3$ and $D = \begin{pmatrix} \gamma^{i+j}C_i \end{pmatrix}$, $i,j = 1,2$; where γ is root of irreducible polynomial over $\mathbb{F}_{3^n}$. Then, C and D form an MDS Pascal-like rhotrix R_5 for $n \geq 3$.

Proof:
Let R_5 be a 5-dimensional Pascal-like rhotrix formed by the coupled matrices C and D as defined in (3.1.1). Since $C = \begin{pmatrix} \gamma^{i+j}C_i \end{pmatrix}$, $i,j = 1,2,3$ and $D = \begin{pmatrix} \gamma^{i+j}C_i \end{pmatrix}$, $i,j = 1,2$. Therefore, coupled matrices C and D are given by

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 \\ \gamma^3 & \gamma^6 & \gamma^{10} \\ \gamma^4 & \gamma^{10} & \gamma^{20} \end{bmatrix} \text{ and } D = \begin{bmatrix} \gamma^2 & \gamma^3 \\ \gamma^3 & \gamma^6 \end{bmatrix}.$$

Case 1: Consider γ is the root of irreducible polynomial $y^3 + 2y + 1 = 0$. Then, for $n = 3$, the matrices C and D are given by

$$C = \begin{bmatrix} \gamma^2 & \gamma + 2 & \gamma^2 + 2\gamma \\ \gamma + 2 & \gamma^2 + \gamma + 1 & \gamma^2 + \gamma \\ \gamma^2 + 2\gamma & \gamma^2 + \gamma & \gamma^2 + 2\gamma + 1 \end{bmatrix}, \tag{3.2.1}$$

and

$$D = \begin{bmatrix} \gamma^2 & \gamma + 2 \\ \gamma + 2 & \gamma^2 + \gamma + 1 \end{bmatrix}. \tag{3.2.2}$$

Now, determinant$(C) = 2\gamma^2 + 2\gamma + 1 \neq 0$ and determinant $(D) = \alpha^2 + 2\alpha + 1 \neq 0$. Here, all the entries of C and D are non-zero and the determinants of all the sub-matrices of C and D are also non-zero. Therefore, C and D are MDS matrices. Using (3.2.1) and (3.2.2), the 5-dimensional rhotrix given in (3.1.1) becomes

$$\mathrm{R}_5 = \left\langle \begin{array}{ccccc} & & \gamma^2 & & \\ & \gamma+2 & \gamma^2 & \gamma+2 & \\ \gamma^2+2\gamma & \gamma+2 & \gamma^2+\gamma+1 & \gamma+2 & \gamma^2+2\gamma \\ & \gamma^2+\gamma & \gamma^2+\gamma+1 & \gamma^2+\gamma & \\ & & \gamma^2+2\gamma+1 & & \end{array} \right\rangle,$$

which is an MDS Pascal-like rhotrix.

Case 2: Let $y^4 + 2y + 2 = 0$ be an irreducible polynomial and γ be its root. Then, for $n = 4$, we have

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma+1 \\ \gamma^3 & \gamma^3+\gamma^2 & 2\gamma^3+\gamma^2+\gamma+1 \\ \gamma+1 & 2\gamma^3+\gamma^2+\gamma+1 & \gamma^3+2\gamma^2+2\gamma \end{bmatrix}, \tag{3.2.3}$$

and

$$D = \begin{bmatrix} \gamma^2 & \gamma^3 \\ \gamma^3 & \gamma^3+\gamma^2 \end{bmatrix}. \tag{3.2.4}$$

The determinant$(C) = 2\gamma^3 + \gamma^2 + 2\gamma \neq 0$ and determinant $(D) = 2\gamma^3 + 2\gamma + 1 \neq 0$. Since entries of C and D are non-zero, therefore C and D are MDS matrices. Hence, by using (3.2.3) and (3.2.4) in (3.1.1), we get

$$\mathrm{R}_5 = \left\langle \begin{array}{ccccc} & & \gamma^2 & & \\ & \gamma^3 & \gamma^2 & \gamma^3 & \\ \gamma+1 & \gamma^3 & \gamma^3+\gamma^2 & \gamma^3 & \gamma+1 \\ & 2\gamma^3+\gamma^2+\gamma+1 & \gamma^3+\gamma & 2\gamma^3+\gamma^2+\gamma+1 & \\ & & \gamma^3+2\gamma^2+2\gamma & & \end{array} \right\rangle,$$

is an MDS Pascal-like rhorix.

Case 3: Let $y^5 + 2y + 1 = 0$ be an irreducible polynomial and let γ be its root. So, for $n = 5$, the coupled matrices C and D are

$$C = \begin{bmatrix} \lambda^2 & \gamma^3 & \gamma^4 \\ \gamma^3 & \gamma^2+2\gamma & \gamma^2+\gamma+1 \\ \gamma^4 & \gamma^2+\gamma+1 & \gamma^4+2\gamma^3+2\gamma+1 \end{bmatrix}, \tag{3.2.5}$$

and

$$D = \begin{bmatrix} \gamma^2 & \gamma^3 \\ \gamma^3 & \gamma^2+2\gamma \end{bmatrix}. \tag{3.2.6}$$

All the elements of C and D are non-zero. Also, determinant$(C) = \gamma^4 + \gamma^3 + \gamma^2 + 1 \neq 0$ and determinant$(D) = \gamma^4 + 2\gamma^3 + 2\gamma^2 + \gamma \neq 0$. Further, the determinants of all the sub-matrices of C and D are non-zero.

Therefore, C and D are MDS matrices. From equations (3.1.1), (3.2.5) and (3.2.6), the 5-dimensional Pascal rhotrix becomes

$$R_5 = \left\langle \begin{array}{ccccc} & & \gamma^2 & & \\ & \gamma^3 & \gamma^2 & \gamma^3 & \\ \gamma^4 & \gamma^3 & \gamma^2+2\gamma & \gamma^3 & \gamma^4 \\ & \gamma^2+\gamma+1 & \gamma^2+2\gamma & \gamma^2+\gamma+1 & \\ & & \gamma^4+2\gamma^3+2\gamma+1 & & \end{array} \right\rangle.$$

Therefore, $R_5 =< C, D >$ is an MDS Pascal-like rhotrix for $n = 5$. In the similar manner, we can verify that R_5 is an MDS Pascal- like rhotrix $n > 5$. Thus, R_5 is an MDS Pascal-like rhotrix over $\mathbb{F}_{3^n}$ for $n \geq 3$. ■

Theorem 3.4

Let $R_7 =< C, D >$ be the Pascal-like rhotrix of dimension 7, whose coupled matrices C and D over $\mathbb{F}_{3^n}$ are defined as $C = \left(\gamma^{\,i+j}C_i\right)$, $i, j = 1, 2, 3, 4$ and $D = \left(\gamma^{\,i+j}C_i\right)$, $i, j = 1, 2, 3$. Then, C and D form an MDS Pascal-like rhotrix R_7 for $n \geq 3$.

Proof:

Consider a 7-dimensional Pascal-like rhotrix R_7 as defined in (3.1.8). Here C and D are coupled matrices of R_7. Since $C = \left(\gamma^{\,i+j}C_i\right)$, $i, j = 1, 2, 3, 4$ and $D = \left(\gamma^{\,i+j}C_i\right)$, $i, j = 1, 2, 3$. Therefore, the coupled matrices C and D are given by

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 & \gamma^5 \\ \gamma^3 & \gamma^6 & \gamma^{10} & \gamma^{15} \\ \gamma^4 & \gamma^{10} & \gamma^{20} & \gamma^{35} \\ \gamma^5 & \gamma & \gamma^{35} & \gamma^{70} \end{bmatrix},$$

and

$$D = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 \\ \gamma^3 & \gamma^6 & \gamma^{10} \\ \gamma^4 & \gamma^{10} & \gamma^{20} \end{bmatrix}.$$

Case 1: Consider an irreducible polynomial $y^3 + 2y + 1 = 0$ of degree 3. Let γ be the root of $y^3 + 2y + 1 = 0$. Therefore, for $n = 3$, the matrix C becomes

$$C = \begin{bmatrix} \gamma^2 & \gamma+2 & \gamma^2+2\gamma & 2\gamma^2+\gamma+2 \\ \gamma+2 & \gamma^2+\gamma+1 & \gamma^2+\gamma & 2\gamma^2 \\ \gamma^2+2\gamma & \gamma^2+\gamma & 2\gamma^2+\gamma+1 & \gamma+1 \\ 2\gamma^2+\gamma+2 & 2\gamma^2 & \gamma+1 & \gamma^2+2\gamma+1 \end{bmatrix}. \tag{3.2.7}$$

Here, the entries of C are all non-zero and the determinant of C and all its sub-matrices are also non-zero. Therefore, C is an MDS matrix. Using similar arguments, the matrix

$$D = \begin{bmatrix} \gamma^2 & \gamma+2 & \gamma^2+2\gamma \\ \gamma+2 & \gamma^2+\gamma+1 & \gamma^2+\lambda \\ \gamma^2+2\gamma & \gamma^2+\gamma & 2\gamma^2+\gamma+1 \end{bmatrix}, \tag{3.2.8}$$

is also an MDS matrix.

From (3.1.8), (3.2.7) and (3.2.8), the 7-dimensioanl rhotrix R_7 given below is an MDS Pascal-like rhotrix

$$R_7 = \left\langle \begin{array}{ccccccc} & & & \gamma^2 & & & \\ & & \gamma+2 & \gamma^2 & \gamma+2 & & \\ & \gamma^2+2\gamma & \gamma+2 & \gamma^2+\gamma+1 & \gamma+2 & \gamma^2+2\gamma & \\ 2\gamma^2+\gamma+2 & \gamma^2+2\gamma & \gamma^2+\gamma & \gamma^2+\gamma+1 & \gamma^2+\gamma & \gamma^2+2\gamma & 2\gamma^2+\gamma+2 \\ & 2\gamma^2 & \gamma^2+\gamma & 2\gamma^2+\gamma+1 & \gamma^2+\gamma & 2\gamma^2 & \\ & & \gamma+1 & 2\gamma^2+\gamma+1 & \gamma+1 & & \\ & & & \gamma^2+2\gamma+1 & & & \end{array} \right\rangle.$$

Case 2: Let γ be the root of irreducible polynomial $y^4 + 2y + 2 = 0$. Therefore, for $n = 4$, the matrix C in this case becomes

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma+1 & \gamma^2+\gamma \\ \gamma^3 & \gamma^3+\gamma^2 & 2\gamma^3+\gamma^2+\gamma+1 & 2\gamma^2+\gamma \\ \gamma+1 & 2\gamma^3+\gamma^2+\gamma+1 & \gamma^3+2\gamma^2+2\gamma & \gamma^2+\gamma+2 \\ \gamma^2+\gamma & 2\gamma^2+\gamma & \gamma^2+\gamma+2 & 2\gamma^3+2\gamma^2+2\gamma+2 \end{bmatrix}. \tag{3.2.9}$$

As the entries of C and the determinant of C are non-zero Further, the determinants of all sub-matrices of C are also all non-zero. Hence, C is an MDS matrix. Similarly,

$$D = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma+1 \\ \gamma^3 & \gamma^3+\gamma^2 & 2\gamma^3+\gamma^2+\gamma+1 \\ \gamma+1 & 2\gamma^3+\gamma^2+\gamma+1 & \gamma^3+2\gamma^2+2\gamma \end{bmatrix}, \tag{3.2.10}$$

is also an MDS matrix. From equations (3.1.8), (3.2.9) and (3.2.10), we get

$$R_7 = \left\langle \begin{array}{ccccccc} & & & g^2 & & & \\ & & g^3 & g^2 & g^3 & & \\ & g+1 & g^3 & g^3+g^2 & g^3 & g+1 & \\ g^2+g & g+1 & 2g^3+g^2+g+1 & g^3+g^2 & 2g^3+g^2+g+1 & g+1 & g^2+g \\ & 2g^2+g & 2g^3+g^2+g+1 & g^3+2g^2+2g & 2g^3+g^2+g+1 & 2g^2+g & \\ & & g^2+g+2 & g^3+2g^2+2g & g^2+g+2 & & \\ & & & 2g^3+2g^2+2g+2 & & & \end{array} \right\rangle,$$

which is an MDS Pascal-like rhotrix.

Case 3: Consider an irreducible polynomial $y^5 + 2y + 1 = 0$. Let γ be the root of $y^5 + 2y + 1 = 0$. Therefore, for $n = 5$, the coupled matrices C and D are given by

$$C = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 & \gamma+2 \\ \gamma^3 & \gamma^2+2\gamma & \gamma^2+\gamma+1 & \gamma^3+2 \\ \gamma^4 & \gamma^2+\gamma+1 & \gamma^4+2\gamma^3+2\gamma+1 & \gamma^4+\gamma^2+2\gamma+2 \\ \gamma+2 & \gamma^3+2 & \gamma^4+\gamma^2+2\gamma+2 & 2\gamma \end{bmatrix}, \tag{3.2.11}$$

and

$$D = \begin{bmatrix} \gamma^2 & \gamma^3 & \gamma^4 \\ \gamma^3 & \gamma^2+2\gamma & \gamma^2+\gamma+1 \\ \gamma^4 & \gamma^2+\gamma+1 & \gamma^4+2\gamma^3+2\gamma+1 \end{bmatrix}. \tag{3.2.12}$$

Using the arguments given in the previous case, we see that C and D are MDS matrices. From (3.1.8), (3.2.11) and (3.2.12), R_7 is an MDS Pascal-like rhotrix and is given by

$$R_7 = \left\langle \begin{array}{ccccccc} & & & \gamma^2 & & & \\ & & \gamma^3 & \gamma^2 & \gamma^3 & & \\ & \gamma^4 & \gamma^3 & \gamma^2+2\gamma & \gamma^3 & \gamma^4 & \\ \gamma+2 & \gamma^4 & \gamma^2+\gamma+1 & \gamma^2+2\gamma & \gamma^2+\gamma+1 & \gamma^4 & \gamma+2 \\ & \gamma^3+2 & \gamma^2+\gamma+1 & \gamma^4+2\gamma^3+2\gamma+1 & \gamma^2+\gamma+1 & \gamma^3+2 & \\ & & \gamma^4+\gamma^2+2\gamma+2 & \gamma^4+2\gamma^3+2\gamma+1 & \gamma^4+\gamma^2+2\gamma+2 & & \\ & & & 2\gamma & & & \end{array} \right\rangle.$$

In the similar manner, we can prove that R_5 is an MDS Pascal- like rhotrix $n > 5$. ■

4. Conclusion

In this paper, we defined Pascal-like rhotrix over finite fields. Further, we constructed MDS Pascal- like rhotrices over finite field $\mathbb{F}_{p^n}$. This work can be extended to block Pascal-like rhotrix. Also, MDS block Pascal-like rhotrices can be constructed with the help of generalised elements from normal bases or self-dual bases of finite field $\mathbb{F}_{p^n}$. These constructions may have vast applications in the field of cryptography and coding theory.

REFERENCES

Absalom, E. E., Sani, B. and Sahalu, J. B. (2011). The concept of heart-oriented rhotrix multiplication, Global Journal of Science Frontier Research, Vol. 11, No. 2, pp. 35-42.

Ajibade, A. O. (2003). The concept of rhotrices in mathematical enrichment, International Journal of Mathematical Education in Science and Technology, Vol. 34, No. 2, pp. 175-179.

Alfred, J. M., Paul, C., Van, O. and Scott, A. V. (1996). *Handbook of Applied Cryptography* (third edition), CRC Press.

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

Aminu, A. (2012). A note on the rhotrix system of equation, Journal of the Nigerian Association of Mathematical Physics, Vol. 21, pp. 289-296.

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, Lecture Notes in Computer Science, Vol. 8128, pp. 29-43.

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- Mathematics and Statistics, Vol. 41 E, No. 2, pp. 184-198.

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

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, Vol. 2, pp. 46-49.

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

Neamah, A. A. (2023). An image encryption scheme based on a seven-dimensional hyperchaotic system and Pascal's matrix, Journal of King Saud University-Computer and Information Sciences, Vol. 35, No. 3, pp. 238-248.

Sajadieh, M., Dakhilian, M., Mala, H. and Omoomi, B. (2012). On construction of involutory MDS matrices from Vandermonde matrices, Designs, Codes and Cryptography, Vol. 64, pp. 287-308.

Sani, B. (2004). An alternative method for multiplication of rhotrices, International Journal of Mathematical Education in Science and Technology, Vol. 35, No. 5, pp. 777-781.

Sani, B. (2007). The row-column multiplication for high dimensional rhotrices, International Journal of Mathematical Education in Science and Technology, Vol. 38, pp. 657-662.

Sani, B. (2008). Conversion of a rhotrix to a coupled matrix, International Journal of Mathematical

Education in Science and Technology, Vol. 39, pp. 244-249.

Sarkar, S. and Syed, H. (2016). Light weight diffusion layer: Importance of Toeplitz matrices, IACR Transactions on Symmetric Cryptology, Vol. 2016, No. 1, pp. 95–113.

Sarkar, S. and Syed, H. (2017). Analysis of Toeplitz MDS matrices, Australasian Conference on Information Security and Privacy, Cham: Springer International Publishing, pp. 3-18.

Sharma, P. L., Gupta, S. (2017). Constructions of maximum distance separable Toeplitz rhotrices over Finite Fields, Journal of Combinatorics, Information & System Sciences, Vol. 42, No. (1-4), pp. 89-110.

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 Applications, Vol. 168, No. 9, pp. 8-17.

Sharma, P. L., Gupta, S. and Dhiman, N. (2017). Sylvester rhotrices and their properties over finite field, Bulletin of Pure and Applied Sciences- Mathematics and Statistics, Vol. 36 E, No. 1, pp. 70-80.

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, Vol. 3, No. 2, pp. 25-43.

Sharma, P. L., Gupta, S. and Rehan, M. (2017). On circulant like rhotrices over finite fields, Applications and Applied Mathematics: An International Journal, Vol. 12, No. 1, pp. 509-520.

Sharma, P. L., Kumar, A. and Gupta, S. (2018). Maximum distance separable Hankel rhotrices over finite fields, Journal of Combinatorics, Information & System Sciences, Vol. 43, No. 1-4, pp. 13-48.

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: An International Journal, Vol. 14, No. 2, pp. 1197-1214.

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 and Statistics, Vol. 39 E, No. 1, pp. 165–175.

Sharma, P. L. and Kumar, S. (2013). On construction of MDS rhotrices from companion rhotrices over finite field, International Journal of Mathematical Sciences, Vol. 12, No. (3-4), pp. 271-286.

Sharma, P. L. and Kumar, S. (2014). Some applications of Hadamard rhotrices to design balanced incomplete block, International Journal of Mathematical Sciences and Engineering Applications, Vol. 8, No. 2, pp. 389- 406.

Sharma, P. L. and Kumar, S. (2014). Balanced incomplete block design (BIBD) using Hadamard rhotrices, International Journal of Technology, Vol. 4, No. 1, pp. 62-66.

Sharma, P. L., Kumar, S. and Rehan, M. (2013). On Vandermonde and MDS rhotrices over GF(2^q), International Journal of Mathematics and Analysis, Vol. 5, No. 2, pp. 143-160.

Tudunkaya, S. M. (2013). Rhotrix polynomial and polynomial rhotrix, Pure and Applied Mathematics Journal, Vol. 2, pp. 38-41.