Original Article

Bulletin of Pure and Applied Sciences.
Vol.36 E (Math & Stat.)), Issue (No.1) 2017: P.70-80
Print version ISSN 0970 6577
Online version ISSN 2320 3226
DOI 10.5958/2320-3226.2017.00009.1

SYLVESTER RHOTRICES AND THEIR PROPERTIES OVER FINITE FIELDS

P.L. Sharma*, Shalini Gupta, Neetu Dhiman***

Author Affiliation:
*Department of Mathematics & Statistics, Himachal Pradesh University, Shimla -5, India
**Bahra University, Solan, (H.P.), India

Corresponding Author:
P.L. Sharma, Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, Himachal Pradesh 171005
E-mail: plsharma1964@gmail.com

Received on 03.06.2017, **Accepted on** 26.06.2017

Abstract

Sylvester matrices play an important role in commutative algebra. We use the coefficients of the polynomials over finite fields to define Sylvester rhotrix. Further, we study the properties of Sylvester rhotrix.

Keywords: Sylvester matrix; Sylvesterrhotrix; Finite field; Determinant; Resultant.

AMS Classification (2010): 15A09, 20H30, 11T71

1. INTRODUCTION

The concept of rhotrix is introduced by Ajibade in 2003, see [2]. A 3×3–dimensional rhotrix is defined in some way, between 2×2–dimensional and 3×3–dimensional matricesas shown below;

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

where a, b, c, d, e are real numbers. Here $h(R_3) = c$ is called the heart of rhotrix R_3. In [2], the following operations of addition and scalar multiplication are discussed;

If $Q_3 = \left\langle \begin{matrix} & f & \\ g & h & j \\ & k & \end{matrix} \right\rangle$, is another 3-dimensional rhotrix, then the addition of two rhotrices is defined as

$$R_3 + Q_3 = \left\langle \begin{matrix} & a & \\ b & c & d \\ & e & \end{matrix} \right\rangle + \left\langle \begin{matrix} & f & \\ g & h & j \\ & k & \end{matrix} \right\rangle = \left\langle \begin{matrix} & a+f & \\ b+g & c+h & d+j \\ & e+k & \end{matrix} \right\rangle,$$

Let α be any real number, then the scalar multiplication of a rhotrix R_3 by α is defined as

$$\alpha R_3 = \alpha \left\langle \begin{array}{ccc} & a & \\ b & c & d \\ & e & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & \alpha a & \\ \alpha b & \alpha c & \alpha d \\ & \alpha e & \end{array} \right\rangle.$$

There are two types of multiplication methods of rhotrices discussed in [2] and [13]. The heart oriented multiplication of rhotrices is discussed in [2] as

$$R_3 \, o \, Q_3 = \left\langle \begin{array}{ccc} & ah + fc & \\ bh + gc & ch & dh + jc \\ & eh + kc & \end{array} \right\rangle.$$

The row-column multiplication of rhotrices as discussed in [13] is given below;

Mohammed et al. [10] discussed an algorithm of heart oriented multiplication method of rhotricesfor

$$R_3 \, o \, Q_3 = \left\langle \begin{array}{ccc} & a & \\ b & c & d \\ & e & \end{array} \right\rangle \left\langle \begin{array}{ccc} & f & \\ g & h & j \\ & k & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & af + dg & \\ bf + eg & ch & aj + dk \\ & bj + ek & \end{array} \right\rangle.$$

computing machines and also generalized the heart oriented multiplication of 3-dimensional rhotrices to n-dimensional rhotrices in [9].

The row-column multiplication of high dimension rhotricesis discussed by Saini in [14] as follows: Consider a n-dimensional rhotrix

$$P_n = \left\langle \begin{array}{ccccccc} & & & a_{11} & & & \\ & & a_{21} & c_{11} & a_{12} & & \\ & a_{31} & c_{21} & a_{22} & c_{12} & a_{13} & \\ . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{t1} & \cdots & \cdots & \cdots & \cdots & \cdots & a_{1t} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & a_{tt-2} & c_{t-1t-2} & a_{t-1t-1} & c_{t-2t-1} & a_{t-2t} & \\ & & a_{tt-1} & c_{t-1t-1} & a_{t-1t} & & \\ & & & a_{tt} & & & \end{array} \right\rangle,$$

where $t = (n+1)/2$ and denote it as $P_n = \langle a_{ij}, c_{lk} \rangle$ with $i, j = 1, 2, ..., t$ and $l, k = 1, 2, ..., t-1$.

Then the multiplication of two rhotrices P_n and Q_n is defined as follows:

$$P_n \, o \, Q_n = \left\langle a_{i_1 j_1}, c_{l_1 k_1} \right\rangle o \left\langle b_{i_2 j_2}, d_{l_2 k_2} \right\rangle = \left\langle \sum_{i_2 j_1 = 1}^{t} \left(a_{i_1 j_1} b_{i_2 j_2} \right), \sum_{l_2 k_1 = 1}^{t-1} \left(c_{l_1 k_1} d_{l_2 k_2} \right) \right\rangle.$$

Sani [15] introduced the rhotrix representation in the form of coupled matrices.An n-dimensional rhotrix R_n can be written in the form of coupled matrices as follows:

$$R_n = \langle A_t, B_{t-1} \rangle, \text{ where } t = \frac{n+1}{2}.$$

This representation of rhotrix in the form of coupled matrices attracts the researchers of cryptography to use the said coupled matrices to increase the security of the cryptosystems, see [5, 21, 25, 26]. Rhotrices over finite fields were discussed by Tudunkaya et al. in [30]. The investigations of rhotricesover matrix theory and polynomials ring theory were discussed in [6, 7, 29]. The extended heart oriented method for rhotrix multiplication was given by Mohammed [9]. Algebra and analysis of rhotrices is discussed in the literature, see [1, 2, 11, 12, 13, 14, 16-28, 30].

The well known structure of Sylvester matrix is used in commutative algebra, see [3, 4, 8]. Now firstly, we recall the definition of the Sylvester matrix then we define the Sylvester rhotrix. Further, in section 2 and 3, we study the properties of Sylvester rhotrix.

Definition 1.1 Let

$$p(x) = p_m x^m + ... + p_2 x^2 + p_1 x + p_0 \; ; (p_m \neq 0),$$

$$q(x) = q_n x^n + ... + q_2 x^2 + q_1 x + q_0 \; ; (q_n \neq 0).$$

be two non-constant univariate polynomials of degree m and n where the coefficients $p_i \, (i = 1, 2, ..., m)$ and $q_j \, (j = 1, 2, ..., n)$ are the elements of the finite field F_{2^k}. Then the Sylvester matrix $\mathrm{M} = \mathrm{syl}(p(\mathrm{x}), q(\mathrm{x}))$ of order $(\mathrm{m} + \mathrm{n})$ is given by

$$\mathrm{M} = \begin{bmatrix} p_m & p_{m-1} & . & . & p_0 & 0 & . & 0 \\ 0 & p_m & . & . & p_1 & p_0 & . & 0 \\ . & . & . & . & p_4 & . & . & p_0 \\ q_n & q_{n-1} & . & . & q_0 & 0 & . & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & q_3 & . & . & q_0 \end{bmatrix}.$$

Definition 1.2 Let

$$p(x) = p_2 x^2 + p_1 x + p_0,$$

$$q(x) = q_1 x + q_0,$$

$$r(x) = r_1 x + r_0,$$

$$s(x) = s_1 x + s_0.$$

Then5-dimensional Sylvester rhotrix $S_5 = \langle A_3, B_2 \rangle$ is defined as

$$S_5 = \left\langle \begin{matrix} & & p_2 & & \\ & q_1 & r_1 & p_1 & \\ 0 & s_1 & q_0 & r_0 & p_0 \\ & q_1 & s_0 & 0 & \\ & & q_0 & & \end{matrix} \right\rangle,$$

where $p_i, \; q_j \; (i = 0, 1, \; 2 \; and \; j = 0, 1)$and $r_l, s_m \; (l, m = 0, 1)$are elements of the finite field of F_{2^k}.

Remark 1 Two coupled matrices of S_5 are

$$A_3 = \begin{bmatrix} p_2 & p_1 & p_0 \\ q_1 & q_0 & 0 \\ 0 & q_1 & q_0 \end{bmatrix} \text{ and } B_2 = \begin{bmatrix} r_1 & r_0 \\ s_1 & s_0 \end{bmatrix}.$$

Definition 1.3 Let $S_{2n+1} = \langle A_{n+1}, B_n \rangle$ be a rhotrix of dimension $(2n+1)$, then the determinant (det) of S_{2n+1} is given by

$$\det S_{2n+1} = \det(A_{n+1}) \times \det(B_n).$$

Remark 2 The determinant of a Sylvester rhotrix is known as its Resultant (Res).

Definition 1.4 Let $S_{2n+1} = \langle A_{n+1}, B_n \rangle$, then the rank of S_{2n+1} is given by

$$\text{rank } S_{2n+1} = \text{rank}(A_{n+1}) + \text{rank}(B_n).$$

2. PROPERTIES OF SYLVESTER RHOTRICES OVER F_{2^2}

In this section, we discuss some properties of Sylvester rhotrices over the finite field F_{2^2}.

Theorem 2.1 Let $S_5 = \langle A_3, B_2 \rangle$ be a Sylvester rhotrix of dimension 5 whose coupled matrices are defined as $A_3 = syl(p(x), q(x))$ and $B_2 = syl(r(x), s(x))$, where

$$p(\mathrm{x}) = \alpha^2 x^2 + \alpha x + 1,$$
$$q(x) = \alpha x + 1,$$
$$r(x) = \alpha^2 x,$$
$$s(x) = x + \alpha$$

and α is the root of irreducible polynomial $g(x) = x^2 + x + 1$ in the extension field of GF(2^2). Then,

(i) determinant of $S_5 = 0$ if either $p(x), q(x)$ or $r(x), s(x)$ have non-constant common divisor and determinant of $S_5 \neq 0$ otherwise.

(ii) degree of $\gcd(p(x), q(x))$ + degree of $\gcd(r(x), s(x))$ = sum of degrees of $p(x), q(x), r(x)$ and $s(x)$ − rank of S_5.

Proof :(i) for given $p(x), q(x), r(x)$ and $s(x)$, the corresponding coefficients matrices are

$$A_3 = \begin{bmatrix} \alpha^2 & \alpha & 1 \\ \alpha & 1 & 0 \\ 0 & \alpha & 1 \end{bmatrix} \text{ and } B_2 = \begin{bmatrix} \alpha^2 & 0 \\ 1 & \alpha \end{bmatrix}.$$

Since,

$$\gcd(p(x), q(x)) = 1 \text{ and } \gcd(r(x), s(x)) = 1. \quad (2.1)$$

Also,

$$\det(A_3) = \begin{vmatrix} \alpha^2 & \alpha & 1 \\ \alpha & 1 & 0 \\ 0 & \alpha & 1 \end{vmatrix} = \alpha^2 \neq 0, \det(B_2) = \begin{vmatrix} \alpha^2 & 0 \\ 1 & \alpha \end{vmatrix} = \alpha^3 = 1 \neq 0.$$

This implies that,

$$\det(S_5) = \det(A_3) \times \det(B_2) = \alpha^2. \quad (2.2)$$

Therefore, the results (2.1) and (2.2) conclude the theorem.

(ii) From part (i) degree of $\gcd(p(x), q(x)) = 0$ and degree of $\gcd(r(x), s(x)) = 0$.

Also, rank of $A_3 = 3$ and rank of $B_2 = 2$.

Therefore, rank of S_5 = rank of A_3 + rank of $B_2 = 5$.

Now,

degree of $\gcd(p(x), q(x))$ + degree of $\gcd(r(x), s(x) = 0$. (2.3)

Also,

sum of degrees of $p(x), q(x), r(x)$ and $s(x)$ − rank of $S_5 = 0$. (2.4)

Using (2.3) and (2.4), we have

degree of $\gcd(p(x), q(x))$ + degree of $\gcd(r(x), s(x))$

=sum of degrees of $p(x), q(x), r(x)$ and $s(x)$ − rank of S_5.

Theorem 2.2 Let $S_7 = \langle A_4, B_3 \rangle$ be a Sylvester rhotrix of dimension 7 whose coupled matrices are defined as $A_4 = syl(p(x), q(x))$ and $B_3 = syl(r(x), s(x))$, where

$$p(x) = x^3 + \alpha^2 x + 1,$$
$$q(x) = x + \alpha,$$
$$r(x) = x^2 + \alpha x + \alpha^2,$$
$$s(x) = x$$

and α is the root of irreducible polynomial $p(x) = x^2 + x + 1$ in the extension field of GF$\left(2^2\right)$. Then,

(i) det of $S_7 = 0$ if either $p(x), q(x)$ or $r(x), s(x)$ have non constant common divisor and $S_7 \neq 0$ otherwise.

(ii) degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x)) =$ sum of degrees of $p(x), q(x), r(x)$ and $s(x) -$ rank of S_7.

Proof: (i)For given $p(x), q(x), r(x)$ and $s(x)$, the corresponding coefficients matrices are

$$A_4 = \begin{bmatrix} 1 & 0 & \alpha^2 & 1 \\ 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \\ 0 & 0 & 1 & \alpha \end{bmatrix} \text{and } B_3 = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Since, $\gcd(p(x), q(x)) = 1$ and $\gcd(r(x), s(x)) = 1.$ (2.5)

Also,

$$\det(A_4) = \begin{vmatrix} 1 & 0 & \alpha^2 & 1 \\ 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \\ 0 & 0 & 1 & \alpha \end{vmatrix} = \alpha^3 + \alpha^3 - 1 = 1 \neq 0,$$

and

$$\det(B_3) = \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{vmatrix} = 1(0) - \alpha(0) + \alpha^2 = \alpha^2 \neq 0.$$

This implies that,

$$\det(S_7) = \det(A_4) \times \det(B_3) = 1 \times \alpha^2 = \alpha^2 \neq 0. \quad (2.6)$$

It follows from (2.5) and (2.6) that $p(x), q(x)$ or $r(x), s(x)$ have nonon-constant common divisor and $\det(S_7)$ is non –zero.

(ii) From part (i) degree of $\gcd(p(x), q(x)) = 0$ and degree of $\gcd(r(x), s(x)) = 0$.

Also, rank of $A_4 = 4$ and rank of $B_3 = 3$.

Therefore, rank of $S_7 =$ rank of A_4 + rank of $B_3 = 7$.

Now, degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x)) = 0$.

Also,

Sum of degrees of $p(x), q(x), r(x)$ and $s(x) -$ rank of $S_5 = 0$.

Hence,

Degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x))$

$=$Sum of degrees of $p(x), q(x), r(x)$ and $s(x) -$ rank of S_7.

Theorem 2.3 Let $S_7 = \langle A_4, B_3 \rangle$ be a Sylvester rhotrix of dimension 7 whose coupled matrices are defined as $A_4 = syl(p(x), q(x))$ and $B_3 = syl(r(x), s(x))$, where

$$p(x) = \alpha^2 x^2 + \alpha x + 1,$$
$$q(x) = x^2 + \alpha^2 x + \alpha$$
$$r(x) = \alpha x^2 + \alpha x + \alpha^2,$$
$$s(x) = \alpha x$$

and α is the root of irreducible polynomial $p(x) = x^2 + x + 1$ in the extension field of GF(2^2). Then ,

(i) det of $S_7 = 0$ if either $p(x), q(x)$ or $r(x), s(x)$ have non constant common divisor and det $S_7 \neq 0$ otherwise.

(ii) Degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x)) =$ sum of degrees of $p(x), q(x), r(x)$ and $s(x) -$ rank of S_7.

Proof: (i) For given $p(x), q(x), r(x)$ and $s(x)$, the corresponding coefficients matrices are

$$A_4 = \begin{bmatrix} \alpha^2 & \alpha & 1 & 0 \\ 0 & \alpha^2 & \alpha & 1 \\ 1 & \alpha^2 & \alpha & 0 \\ 0 & 1 & \alpha^2 & \alpha \end{bmatrix} \text{ and } B_3 = \begin{bmatrix} \alpha & \alpha & \alpha^2 \\ \alpha & 0 & 0 \\ 0 & \alpha & 0 \end{bmatrix}.$$

Since, $\gcd(p(x), q(x)) = x^2 + \alpha^2 x + \alpha$ and $\gcd(r(x), s(x)) = 1.$ (2.7)

Also,

$$\det(A_4) = \begin{vmatrix} \alpha^2 & \alpha & 1 & 0 \\ 0 & \alpha^2 & \alpha & 1 \\ 1 & \alpha^2 & \alpha & 0 \\ 0 & 1 & \alpha^2 & \alpha \end{vmatrix} = 0,$$

and

$$\det(B_3) = \begin{vmatrix} \alpha & \alpha & \alpha^2 \\ \alpha & 0 & 0 \\ 0 & \alpha & 0 \end{vmatrix} = \alpha \neq 0.$$

This implies that,

$$\det(S_7) = \det(A_4) \times \det(B_3) = 0 \times \alpha = 0. \quad (2.8)$$

It follows from (2.7) and (2.8) that $p(x), q(x)$ or $r(x), s(x)$ have non-constant common divisor and $\det(S_7)$ is zero.

(ii) From part (i) degree of $\gcd(p(x), q(x)) = 2$ and degree of $\gcd(r(x), s(x)) = 0$.

Also, rank of $A_4 = 2$ and rank of $B_3 = 3$.

Therefore, rank of $S_7 =$ rank of A_4 + rank of $B_3 = 5$

Now, degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x)) = 2$.

Also,

sum of degrees of $p(x), q(x), r(x)$ and $s(x) -$ rank of $S_7 = 7 - 5 = 2$.

Hence,

degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x))$

=sum of degrees of $p(x), q(x), r(x)$ and $s(x)-$ rank of S_7.

3. PROPERTIES OF SYLVESTER RHOTRICES OVER F_{2^3}

In this section we use the appropriate polynomials for the Sylvester rhotrices over the finite field F_{2^3}. Further, we discuss some properties of Sylvester rhotrices.

Theorem 3.1 Let $S_5 = \langle A_3, B_2 \rangle$ be a Sylvester rhotrix of dimension 5 whose coupled matrices are defined as $A_3 = syl(p(x), q(x))$ and $B_2 = syl(r(x), s(x))$,where

$$p(x) = x^2 + \alpha^4 x + \alpha^5,$$
$$q(x) = \alpha^6 x,$$
$$r(x) = \alpha^3 x + 1$$

and

$$s(x) = \alpha^4 x + \alpha^2.$$

The coefficients of $p(x), q(x), r(x)$ and $s(x)$ are defined over GF$(2^3)$and α is the root of irreducible polynomial $g(x) = x^3 + x + 1$ in the extension fieldof GF(2^3). Then,

(i) determinant of $S_5 = 0$ if either $p(x), q(x)$ or $r(x), s(x)$ have common divisor and determinant of $S_5 \neq 0$ otherwise.

(ii) degree of $\gcd(p(x), q(x))$ + degree of $\gcd(r(x), s(x))$ = sum of degrees of $p(x), q(x), r(x)$ and $s(x)$ − rank of S_5.

Proof: (i)For given $p(x), q(x), r(x)$ and $s(x)$, the corresponding coefficients matrices are

$$A_3 = \begin{bmatrix} 1 & \alpha^4 & \alpha^5 \\ \alpha^6 & 0 & 0 \\ 0 & \alpha^6 & 0 \end{bmatrix} \text{ and } B_2 = \begin{bmatrix} \alpha^3 & 1 \\ \alpha^4 & \alpha^2 \end{bmatrix}.$$

Since, $\gcd(p(x), q(x)) = 1$ and $\gcd(r(x), s(x)) = 1.$ (3.1)

Also,

$$\det(A_3) = \begin{vmatrix} 1 & \alpha^4 & \alpha^5 \\ \alpha^6 & 0 & 0 \\ 0 & \alpha^6 & 0 \end{vmatrix} = \alpha^5 \times \alpha^{12} = \alpha^{17} = \alpha^3 \neq 0,$$

and

$$\det(B_2) = \begin{vmatrix} \alpha^3 & 1 \\ \alpha^4 & \alpha^2 \end{vmatrix} = \alpha^5 - \alpha^4 = 1 \neq 0.$$

Now, $\det(S_5) = \det(A_3) \times \det(B_2) = \alpha^3 \neq 0.$ (3.2)

It follows from (3.1) and (3.2) that $p(x), q(x)$ or $r(x), s(x)$ have no non-constant common divisor and $\det(S_5)$ is non –zero.

(ii) From part (i) degree of $\gcd(p(x), q(x)) = 0$ and degree of $\gcd(r(x), s(x)) = 0$.

Also, rank of $A_3 = 3$ and rank of $B_2 = 2$.

Therefore, rank of S_5 = rank of A_3 + rank of $B_2 = 5$.

Now,

degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x) = 0$.

Also,

sum of degrees of $p(x), q(x), r(x)$ and $s(x) -$ rank of $S_5 = 0$.

Hence,

degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x))$

$=$Sum of degrees of $p(x), q(x), r(x)$ and $s(x) -$ rank of S_5.

Theorem 3.2 Let $S_7 = \langle A_4, B_3 \rangle$ be a Sylvester rhotrix of dimension 7 whose coupled matrices are defined as $A_4 = syl(p(x), q(x))$ and $B_3 = syl(r(x), s(x))$, where

$$p(x) = \alpha^2 x^2 + \alpha^5 x + \alpha,$$
$$q(x) = \alpha^2 x^2 + \alpha x + 1,$$
$$r(x) = \alpha^6 x^2 + \alpha^2,$$
$$s(x) = x$$

and α is the root of irreducible polynomial $g(x) = x^3 + x + 1$ in the extension field of GF(2^3). Then,

(i) determinant of $S_7 = 0$ if either $p(x), q(x)$ or $r(x), s(x)$ have non-constant common divisor and det $S_7 \neq 0$ otherwise.

(ii) degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x)) =$ sum of degrees of $p(x), q(x), r(x)$ and $s(x) -$ rank of S_7.

Proof:(i) For given $p(x), q(x), r(x)$ and $s(x)$, the corresponding coefficients matrices are

$$A_4 = \begin{bmatrix} \alpha^2 & \alpha^5 & \alpha & 0 \\ 0 & \alpha^2 & \alpha^5 & \alpha \\ \alpha^3 & \alpha & 1 & 0 \\ 0 & \alpha^3 & \alpha & 0 \end{bmatrix} \text{and } B_3 = \begin{bmatrix} \alpha^6 & 0 & \alpha^2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Since, $\gcd(p(x), q(x)) = \alpha^2 x + \alpha$ and $\gcd(r(x), s(x)) = 1$. (3.3)

Also,

$$\det(A_4) = \begin{vmatrix} \alpha^2 & \alpha^5 & \alpha & 0 \\ 0 & \alpha^2 & \alpha^5 & \alpha \\ \alpha^3 & \alpha & 1 & 0 \\ 0 & \alpha^3 & \alpha & 0 \end{vmatrix} = 0,\ \det(B_3) = \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{vmatrix} = \alpha^2 \neq 0.$$

Now, $\det(S_7) = \det(A_4) \times \det(B_3) = 0 \times \alpha^2 = 0$. (3.4)

It is clear from (3.3)and (3.4)that for non-constant divisor of either $p(x), q(x)$ or $r(x), s(x)$ the $\det(S_7)$ is zero.

(ii) From part (i) degree of $\gcd(p(x), q(x)) = 1$ and degree of $\gcd(r(x), s(x)) = 0$.

Also, rank of $A_4 = 3$ and rank of $B_3 = 3$.

Therefore, rank of $S_7 =$ rank of A_4 + rank of $B_3 = 6$.

degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x)) = 1$.

Also,

sum of degrees of $p(x), q(x), r(x)$ and $s(x) -$ rank of $S_5 = 1$.

Hence,

degree of $\gcd(p(x), q(x)) +$ degree of $\gcd(r(x), s(x))$

$=$Sum of degrees of $p(x), q(x), r(x)$ and $s(x) -$ rank of S_7.

Theorem 3.3 Let $S_7 = \langle A_4, B_3 \rangle$ be a Sylvester rhetoric of dimension 7 over GF (2^3) whose coupled matrices are defined as $A_4 = syl\,(p(x), q(x))$ and $B_3 = syl\,(r(x), s(x))$, where

$$p(x) = a_2\, x^2 + a_1\, x + a_0$$
$$q(x) = b_2\, x^2 + b_1\, x + b_0,$$
$$r(x) = c_2\, x^2 + c_1\, x + c_0$$
$$s(x) = \; d_1\, x + d_0$$

Then, Res($p(x), q(x), r(x), s(x))$

$$= a_2^2\, b_2^2\, c_2^1\, d_1^2\, (\beta_1 - \chi_1)(\beta_1 - \chi_2)(\beta_2 - \chi_1)(\beta_2 - \chi_2)(\delta_1 - t_1)(\delta_2 - t_1), \text{(3.5)}$$

where $p(\beta_i) = 0$ for $1 \le i \le 2$, $q(\chi_j) = 0$ for $1 \le j \le 2$, $r(\delta_u) = 0$ for $1 \le u \le 2$ and $s(t_v) = 0$ for $v = 1$.

Proof: Since the polynomials $p(x), q(x), r(x)$ and $s(x)$ are over $\mathrm{GF}(2^3)$.
Let

$$a_2 = \alpha,\; a_1 = \alpha^5,\; a_0 = \alpha^6,$$
$$b_2 = \alpha^2,\; b_1 = 0, b_0 = \alpha^4,$$
$$c_2 = \alpha^6,\; c_1 = 0, c_0 = \alpha^2,$$
$$d_1 = 1, d_0 = 0.$$

Therefore, given polynomials become

$$p(\mathrm{x}) = \alpha\, x^2 + \alpha^5 x + \alpha^6,$$
$$q(x) = \alpha^2 x^2 + \alpha^4,$$
$$r(x) = \alpha^6 x^2 + \alpha^2,$$
$$s(x) = x,$$

where α is the root of irreducible polynomial $g(x) = x^3 + x + 1$ in the extension field of GF$\left(2^3\right)$.
Clearly, the roots of $p(x)$, $q(x)$ and $r(x)$ are respectively 1 and α^5, α^2 and α^2, α^5 and α^5.The root of $s(x)$ is 0.
Therefore,

$$\beta_1 = 1,\; \beta_2 = \alpha^5,\; \chi_1 = \alpha^2,\; \chi_2 = \alpha^2,\; \delta_1 = \alpha^5,\; \delta_2 = \alpha^5 \text{ and } t_1 = 0.$$

Now,

$$a_2^2\, b_2^2\, c_2^1\, d_1^2\, (\beta_1 - \chi_1)(\beta_1 - \chi_2)(\beta_2 - \chi_1)(\beta_2 - \chi_2)(\delta_1 - t_1)(\delta_2 - t_1)$$
$$= (\alpha)^2\, (\alpha^2)^2\, (\alpha^6)^1\, 1^2 (1-\alpha^2)\,(1-\alpha^2)(\alpha^5 - \alpha^2)(\alpha^5 - \alpha^2)\,(\alpha^5 - 0)(\alpha^5 - 0)$$
$$= \alpha^4 + \alpha + \alpha^5 + \alpha^2 = \alpha^5 \qquad \text{(3.6)}$$

We know that, Res ($p(x), q(x), r(x), s(x)) = \mathrm{Res}(p(x), q(x)) \times \mathrm{Res}(r(x), s(x))$, where Res ($p(x), q(x), r(x), s(x)) = \det(S_7)$, Res$(p(x), q(x)) = \det(A_4)$ and
Res $(r(x), s(x)) = \det(B_3)$.
Since,

$$A_4 = \begin{bmatrix} \alpha & \alpha^2 & \alpha^5 & 0 \\ 0 & \alpha & \alpha^2 & \alpha^5 \\ \alpha^2 & 0 & \alpha^4 & 0 \\ 0 & \alpha^2 & 0 & \alpha^4 \end{bmatrix} \text{ and } B_3 = \begin{bmatrix} \alpha^6 & 0 & \alpha^2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Clearly, $\det(A_4) = \alpha^3$, $\det(B_3) = \alpha^2$.

Therefore, Res($(p(x), q(x)$)= α^3 and Res($r(x), s(x)$)= α^2
which gives

Res ($p(x), q(x), r(x), s(x)) = \alpha^3 . \alpha^2 = \alpha^5$. (3.7)

It follows from (3.6) and (3.7) that

Res ($p(x), q(x), r(x), s(x))$

$$= a_2^2\, b_2^2\, c_2^1\, d_1^2\, (\beta_1 - \chi_1)(\beta_1 - \chi_2)(\beta_2 - \chi_1)(\beta_2 - \chi_2)(\delta_1 - t_1)(\delta_2 - t_1).$$

4. CONCLUSION

In this paper we defined the Sylvester rhotrix. The elements in the rhotricesare from the finite fields GF (2^2) and GF (2^3). Using such rhotrices, we have proved some properties of Sylvester rhotrices over the finite fields GF (2^2) and GF (2^3).

ACKNOWLEDGEMENT Authors thankfully acknowledge the support of UGC - SAP.

REFERENCES

1. Absalom, E. E., Sani, B. and Sahalu, J. B. (2011). The concept of heart-oriented rhotrix multiplication, *Global J. Sci. Fro. Research*, Vol. 11(No. 2): 35-42.
2. Ajibade, A. O. (2003). The concept of rhotrices in mathematical enrichment, *Int. J. Math. Educ. Sci. Tech.*, Vol. 34(No. 2): 175-179.
3. Akritas, A. G. (1993). Sylvester's Forgotten Form of the Resultant, *Fib. Quart.*, Vol. 31: 325-332.
4. Akritas, A. G. (1991). Sylvester's Form of the Resultant and the Matrix-Triangularization Subresultantprs Method, *Proceedings of the Conference on Computer Aided Proofs in Analysis, Cincinnati, Ohio, March, 1989* (Ed. K. R. Meyer and D. S. Schmidt.) IMA Volumes in Mathematics and its Applications, Vol. 28: 5-11.
5. Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone. (1996, Third Edition). *Hand book of Applied Cryptography*, CRC Press.
6. Aminu, A. (2009). On the linear system over rhotrices, *Notes on Number Theory and Discrete Mathematics*, Vol. 15: 7-12.
7. Aminu, A. (2012). A note on the rhotrix system of equation, *Journal of the Nigerian association of Mathematical Physics*, Vol. 21: 289-296.
8. Laidacker, M. A. (1969). Another Theorem Relating Sylvester's Matrix and the Greatest Common Divisor, *Math. Mag.*, Vol. 42: 126-128.
9. Mohammed, A. (2011). Theoretical development and applications of rhotrices, Ph. D. Thesis, Ahmadu Bello University, Zaria.
10. 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: 46-49.
11. Nakahara, J. and Abrahao, E. (2009). A new involutory MDS matrix for the AES. *In: International Journal of Computer Security*, Vol. 9: 109-116.
12. Sajadieh, M., Dakhilian, M., Mala, H. and Omoomi, B. (2012). On construction of involutry MDS matrices from Vandermonde matrices, *Des. Codes and Cry.* Vol. 64: 287-308.
13. Sani, B. (2004). An alternative method for multiplication of rhotrices, *Int. J. Math. Educ. Sci. Tech.*, Vol. 35 (No. 5): 777-781.
14. Sani, B. (2007). The row-column multiplication for high dimensional rhotrices, *Int. J. Math. Educ. Sci. Technol*, Vol. 38: 657-662.
15. Sani, B. (2008). Conversion of a rhotrix to a coupled matrix, *Int. J. Math. Educ. Sci. Technol.*, Vol. 39: 244-249.

16. Sharma, P. L. and Kanwar, R. K. (2011). A note on relationship between invertible rhotricesand associated invertible matrices, *Bulletin of Pure and Applied Sciences*, Vol. 30 E (Math & Stat.) (No.2): 333-339.
17. Sharma, P. L. and Kanwar, R. K. (2012a). Adjoint of a rhotrix and its basic properties, *International J. Mathematical Sciences*, Vol. 11(No. (3-4)): 337-343.
18. Sharma, P.L. and Kanwar, R.K. (2012b). On inner product space and bilinear forms over rhotrices, *Bulletin of Pure and Applied Sciences*, Vol. 31E (No. 1): 109-118.
19. Sharma, P. L. and Kanwar, R. K. (2012c). The Cayley-Hamilton theorem for rhotrices, International *Journal Mathematics and Analysis*, Vol. 4(No. 1): 171-178.
20. Sharma, P.L. and Kanwar, R.K. (2013). On involutory and pascalrhotrices, *International J. of Math. Sci. &Engg. Appls. (IJMSEA)*, Vol. 7 (No. IV): 133-146.
21. Sharma, P. L. and Kumar, S. (2014a). Some applications of Hadamardrhotrices to design balanced incomplete block. *International J. of Math. Sci. &Engg. Appls. (IJMSEA)*, Vol. 8(No. II): 389-406.
22. Sharma, P. L. and Kumar, S. (2014b). Balanced incomplete block design (BIBD) using Hadamardrhotrices, *International J. Technology*, and Vol. 4 (No. 1): 62-66.
23. Sharma, P. L. and Kumar, S. (2014c). On a special type of Vandermonderhotrix and its decompositions, *Recent Trends in Algebra and Mechanics*, Indo-American Books Publisher, New Delhi: 33-40.
24. Sharma, P. L., Kumar, S. and Rehan, M. (2014). On construction of Hadamard codes using Hadamardrhotrices, *International Journal of Theoretical & Applied Sciences*, Vol. 6 (No. 1): 102-111.
25. Sharma, P. L., Kumar, S. and Rehan, M. (2013a). On Hadamardrhotrix over finite field, *Bulletin of Pure and Applied Sciences*, Vol. 32 E (Math & Stat.) (No. 2): 181-190.
26. Sharma, P. L., Kumar, S. and Rehan, M. (2013b). On Vandermonde and MDS rhotrices over GF (2^q), *International Journal of Mathematics and Analysis*, Vol. 5 (No. 2): 143-160.
27. Sharma, P. L., Gupta, S. and Rehan, M. (2015). Construction of MDS rhotrices using specialtype of circulantrhotrices over finite fields, *Himachal Pradesh University Journal*, Vol.3 (No. 2): 25-43.
28. Sharma, P. L., Gupta, S. and Rehan, (2017). On circulant like rhotrices over finite fields, Accepted for publication in Applications and Applied Mathematics: *An International Journal (AAM)*.
29. Tudunkaya, S. M. (2013). Rhotrix polynomial and polynomial rhotrix, *Pure and Applied mathematics Journal*, Vol. 2: 38-41.
30. Tudunkaya, S.M. and Makanjuola, S.O. (2010). Rhotrices and the construction of finite fields, *Bulletin of Pure and Applied Sciences*, Vol. 29 E(No. 2): 225-229.