International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 11 No. I (April, 2017), pp. 19-35

ON IDENTIFICATION OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS WITH CHARACTERISTIC p

P. L. SHARMA[1] AND SHABNAM SHARMA[2]
[1,2] Department of Mathematics and Statistics,
Himachal Pradesh University, Shimla - 171005, India

Abstract

We give two different structures of $\mathbb{F}_{p^n}^*$,where p is prime and n is a positive integer. Further, we characterize the elements of both the structures of $\mathbb{F}_{p^n}^*$ to identify the irreducible polynomials of degree n over finite fields $\mathbb{F}_p$. Also, we show the correspondence of the elements of these structures.

1. Introduction

Irreducible polynomials play an important role to construct the elements of extension fields and have wide applications in many areas such as design theory [10, 11, 15], combinatorics [8] and cryptography [6, 8, 9, 12, 13, 16]. Irreducible polynomials are also used to form the generator polynomials which are important in the construction of cyclic codes and BCH codes in coding theory over binary and non-binary finite fields, see [1, 3, 4, 7]. The security of many cryptographic schemes, such as identity-based encryption, attribute-based encryption, keyword searchable encryption, short signature,

---

Key Words : *Irreducible polynomials, Conjugates, Finite field, Primitive element.*
AMS Subject Classification : 11T06, 12E05.

functional encryption depends on the difficulty of the discrete logarithm problem (DLP) over finite fields $GF(3)$, see [5, 22]. Beuchat et al.[2] discuss irreducible polynomials over $GF(3)$ to develop an accelerator for pairing-based cryptosystem. Several authors have studied the counting and construction of irreducible polynomials over finite fields. Sharma et al. [17] discuss the counting of irreducible polynomials with some prescribed coefficients, and show the construction of infinite sequences of irreducible polynomials, see [18] and references therein.

In case of F_{2^n}, the non zero elements of $F^*_{2^n} = \{\alpha, \alpha^2, ..., \alpha^{2^n-2}, \alpha^{2^n-1}\}$ are arranged as follows [20],

$$
\begin{array}{cccccccc}
\alpha & & & & & & & \\
\alpha^2 & & & & \alpha^3 & & & \\
\alpha^{2^2} & & \alpha^5 & & \alpha^6 & & \alpha^7 & \\
\alpha^{2^3} & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} & \alpha^{15} \\
\ldots & & & & & & &
\end{array}
$$

Structure of $\mathbb{F}^*_{2^n}$

The structure of $\mathbb{F}^*_{3^n}$ is also discussed in [20]. The characterization of the structure $\mathbb{F}^*_{2^n}$ to obtain the irreducible polynomials is discussed in [21]. Further, Sharma et al. [19] discuss the characterization of the structure $\mathbb{F}^*_{3^n}$ to identify the irreducible polynomials of degree n over $\mathbb{F}_3$. In this paper we arrange the non zero elements of $\mathbb{F}_{p^n}$ that is $\mathbb{F}^*_{p^n} = \{\alpha, \alpha^2, \alpha^3, \alpha^4, ..., \alpha^{p^n-2}, \alpha^{p^n-1}\}$ in two different structures. We construct these structures by begining with elements α and α^{p^n-1} respectively. Further, we characterize both the structures in conjugate classes. Let $[\alpha^i]$ or $[[i]]$ be the conjugate classes of α^i, and $[[[i]]]$ be the i^{th} row containing α^i. Therefore, we show that

$$\left[\alpha^{p^{n-1}+r}\right] = \left[\alpha^{pr+1}\right] \tag{1}$$

that is $\alpha^{p^{n-1}+r}$, α^{pr+1} lie in the same conjugate class for $r = 0, 1, \ldots, ((p-1).p^{n-1})-1$.We also show that

$$[\alpha^{p^n-r}] \;=\; [\alpha^{p^n-(pr-p+1)}] \tag{2}$$

for $r = 1, 2, 3, ..., (p-1)p^{n-1}$. The conjugate classes (1) and (2) help to identify the irreducible polnomials of degree n over $\mathbb{F}_p$ respectively for both the structures. Further, we give the correspondence between the elements of each column and the elements of the n^{th} row for these structures.

2. Structure of $\mathbb{F}^*_{p^n}$

In this section, we discuss the structure

$$\mathbb{F}^*_{p^n} = \{\alpha, \alpha^2, \alpha^3, \alpha^4, ..., \alpha^{p^n-2}, \alpha^{p^n-1}\}$$

in two different ways. First structure begin with the element α and the second one begin with α^{p^n-1} as discussed below.

2.1 Structure of the elements of $\mathbb{F}^*_{p^n}$ beginning with the primitive element α

The elements of $\mathbb{F}^*_{p^n}$ are arranged in $(p^n - p^{n-1})$ columns and n rows. The elements in the first column are ranging from α to $\alpha^{p^{n-1}}$and every element (except the first) in each column is the conjugate of the previous element of the same column. The elements in the rows are in geometric progression with common ratio α. In the $(p+1)^{th}$ column , we obtain one more element in the $(n-1)^{th}$ row whose conjugate lies in the same column under the n^{th} row. Similarly, in the $(p^2+1)^{th}$ column , we obtain one more element in $(n-2)^{th}$ row whose conjugate lies in the same column under the $(n-1)^{th}$ row. The structure of $\mathbb{F}^*_{p^n}$ beginning from the element α is as follows:

$$\begin{array}{llllllll}
\alpha & & & & & & & \\
\alpha^p & & & & & & & \\
\alpha^{p^2} & & & & & & & \\
\alpha^{p^3} & & & & & & & \\
\vdots & & & & & & & \\
\alpha^{p^{n-3}} & & & & & & & \\
\alpha^{p^{n-2}} & & & & \alpha^{p^{n-2}+1} & & & \alpha^{p^{n-2}+2} \\
\alpha^{p^{n-1}} & \alpha^{p^{n-1}+1} & \alpha^{p^{n-1}+2} & ... & \alpha^{p^{n-1}+p} & \alpha^{p^{n-1}+p+1} & \alpha^{p^{n-1}+p+2} & ... \alpha^{p^{n-1}+p+p}
\end{array}$$

Structure of $\mathbb{F}^*_{p^n} - (I) - Part(1)$

$$\begin{array}{cccccccc} & & & & \alpha^{p^{n-3}+1} & & & \\ & & & \alpha^{p^{n-2}+3} & & \alpha^{p^{n-2}+p} & & \\ \alpha^{p^{n-1}+2p+1} & \alpha^{p^{n-1}+2p+2}... & \alpha^{p^{n-1}+2p+p}... & & \alpha^{p^{n-1}+p.p} & ... & \alpha^{p^{n-1}+p^2+1} & \alpha^{p^{n-1}+p^2+2}... \end{array}$$

Structure of $\mathbb{F}^*_{p^n} - (I) - Part(2)$

$$\begin{array}{cccccc} \alpha^{p^{n-2}+p+1} & & & & \alpha^{p^{n-2}+p+2} & \\ \alpha^{p^{n-1}+p^2+p} & \alpha^{p^{n-1}+p^2+p+1} & \alpha^{p^{n-1}+p^2+p+2}... & \alpha^{p^{n-1}+p^2+p+p} & \alpha^{p^{n-1}+p^2+2p+1} & \end{array}$$

Structure of $\mathbb{F}^*_{p^n} - (I) - Part(3)$

$$\begin{array}{cccccccc} & & & & \alpha^{p^{n-3}+2} & & & \\ & & & \alpha^{p^{n-2}+p+3} & ... & \alpha^{p^{n-2}+p+p} & & \\ \alpha^{p^{n-1}+p^2+2p+2} & ... & \alpha^{p^{n-1}+p^2+2p+p} & ... & \alpha^{p^{n-1}+p^2+p.p} & & \alpha^{p^{n-1}+p^2+p^2+1}... & \end{array}$$

Structure of $\mathbb{F}^*_{p^n} - (I) - Part(4)$.

2.2 Structure of the elements of $\mathbb{F}^*_{p^n}$ beginning **with the element** α^{p^n-1}

The elements of the structure of $\mathbb{F}^*_{p^n}$ are arranged in $(p^n - p^{n-1})$ columns and n rows beginning from the element α^{p^n-1}. In the p^{th} column, we obtain one more element in the $(n-1)^{th}$ row whose conjugate lies in the same column under the n^{th} row, and in the $\left(p^2\right)^{th}$ column, we obtain one element in $(n-2)^{th}$ row whose conjugate lies in the same column under the $(n-1)^{th}$ row. Also, the elements in the rows are in geometric progression with common ratio $1/\alpha$. The structure of $\mathbb{F}^*_{p^n}$ beginning from the element α^{p^n-1} is as follows:

$$\begin{array}{cccccccccc} & & & & \alpha^{p^{n-1}-1} & & & & & \alpha^{p^{n-1}-2} \\ \alpha^{p^n-1} & \alpha^{p^n-2} & \alpha^{p^n-3}... & \alpha^{p^n-p} & \alpha^{p^n-p-1} & \alpha^{p^n-p-2} & \alpha^{p^n-p-3}... & \alpha^{p^n-p-p} & & \end{array}$$

Structure of $\mathbb{F}_{p^n}^* - (II) - Part(1)$

$$\begin{array}{ccccccccccc} & & & & \alpha^{p^{n-2}-1} & & & & & & \\ & & & & \alpha^{p^{n-1}-p} & & & & \alpha^{p^{n-1}-p-1} & & \\ \alpha^{p^n-2p-1} & \alpha^{p^n-2p-2} & \ldots & \alpha^{p^n-p.p} & \alpha^{p^n-p^2-1} & \alpha^{p^n-p^2-2} & \ldots & \alpha^{p^n-p^2-p} & \ldots & & \end{array}$$

Structure of $\mathbb{F}_{p^n}^* - (II) - Part(2)$

$$\begin{array}{ccccccccc} & & & & & \alpha^{p^{n-1}-p-2} & & & \\ \alpha^{p^n-p^2-p-1} & \alpha^{p^n-p^2-p-2} & \alpha^{p^n-p^2-p-3} & \ldots & \alpha^{p^n-p^2-p-p} & \alpha^{p^n-p^2-2p-1} & \ldots & & \end{array}$$

Structure of $\mathbb{F}_{p^n}^* - (II) - Part(3)$

$$\begin{array}{ccccccccc} \alpha^{p^{n-2}-2} & & & & & & & & \\ \alpha^{p^{n-1}-p-p} & & & & \alpha^{p^{n-1}-2p-1} & & & & \\ \alpha^{p^n-p^2-p.p} & \alpha^{p^n-p^2-p^2-1} & \alpha^{p^n-p^2-p^2-2} & \ldots & \alpha^{p^n-2p^2-p} & & \alpha^{p^n-2p^2-p-1} & & \end{array}$$

Structure of $\mathbb{F}_{p^n}^* - (II) - Part\ (4)$

$$\begin{array}{ccccccccc} & & & & & & \alpha^{p^{n-3}-1} & & \\ & & & \alpha^{p^{n-2}-3} & & & \alpha^{p^{n-2}-p} & & \\ & & & \alpha^{p^{n-1}-2p-p} & & \alpha^{p^{n-1}-3p-1} & \alpha^{p^{n-1}-p.p} & & \\ \alpha^{p^n-2p^2-p-2} & \ldots & \alpha^{p^n-2p^2-p-p} & \ldots & \alpha^{p^n-2p^2-p.p} & \alpha^{p^n-2p^2-p^2-1} & \ldots & \alpha^{p^n-3p^2-p} & \ldots \quad \alpha^{p^n-p^3} \ldots \end{array}$$

Structure of $\mathbb{F}_{p^n}^* - (II) - Part\ (5)$.

3. Characterization of the Structure $\mathbb{F}_{p^n}^*$ beginning with the element α

In this section,we characterize the structure of $\mathbb{F}_{p^n}^* - (I)$ and show some conjugate classes. We also give an illustration which show the identification of irreducible polynomials of degree 2 over $\mathbb{F}_5$.

Proposition 3.1 : The elements $\alpha^{p^{n-1}+r}$ and α^{pr+1} are in the same conjugate class for $r = 0, 1, \ldots, ((p-1).p^{n-1}) - 1$.

Proof :

$$\begin{aligned}[\alpha^{p^{n-1}+r}] &= [(\alpha^{p^{n-1}+r})^p] \\ &= [\alpha^{p.p^{n-1}+pr}] \\ &= [\alpha^{p^n+pr}].\end{aligned}$$

Since,

$$\alpha^{p^n} = \alpha^1$$

Therefore,

$$[\alpha^{p^{n-1}+r}] = [\alpha^{pr+1}]. \tag{3.1.1}$$

3.1 Classes of type $[[p^{n-1}+r]]$ **for** $r = 0, 1, \ldots, ((p-1).p^{n-1}) - 1$.

From the above proposition, we get the conjugates of every element in the n^{th} row as below:

For $r = 0$, the equation (3.1.1) becomes

$$[\alpha^{p^{n-1}}] = [\alpha^1] = [\alpha^{p^n}].$$

The length of $[[[1]]]$ is n and there are n conjugates of $\alpha^{p^{n-1}}$ in $[[[1]]]$.

For $r = 1$, the equation (3.1.1) becomes

$$[\alpha^{p^{n-1}+1}] = [\alpha^{p+1}].$$

The length of $[[[p+1]]]$ is $n - \lfloor \log_p(p+1) \rfloor$ and there are $n - \lfloor \log_p(p+1) \rfloor$ conjugates of $\alpha^{p^{n-1}+1}$ in $[[[p+1]]]$.

For $r = 2$, the equation (3.1.1) becomes

$$[\alpha^{p^{n-1}+2}] = [\alpha^{2p+1}].$$

The length of $[[[2p+1]]]$ is $n - \lfloor \log_p(2p+1) \rfloor$ and there are $n - \lfloor \log_p(2p+1) \rfloor$ conjugates of $\alpha^{p^{n-1}+2}$ in $[[[2p+1]]]$.

$\vdots$

For $r = p^{n-1}$, the equation (3.1.1) becomes

$$[\alpha^{p^{n-1}+p^{n-1}}] = [\alpha^{p.p^{n-1}+1}] = [\alpha^{p^n+1}] = [\alpha^2].$$

The length of $[[[p^n+1]]]$ is $n-\lfloor \log_p(2)\rfloor$ and there are $n-\lfloor \log_p(2)\rfloor$ conjugates of $\alpha^{p^{n-1}+p^{n-1}}$ in $[[[p^n+1]]]$.

For $r=p^{n-1}+1$,the equation (3.1.1) becomes

$$[\alpha^{p^{n-1}+p^{n-1}+1}]=[\alpha^{p.(p^{n-1}+1)+1}]=[\alpha^{p^n+p+1}] \ =[\alpha^{p+2}].$$

The length of $[[[p+2]]]$ is $n-\lfloor \log_p(p+2)\rfloor$.

$\vdots$

For $r=p^{n-1}+p^{n-1}$, the equation (3.1.1) becomes

$$[\alpha^{p^{n-1}+p^{n-1}+p^{n-1}+1}]=[\alpha^{p.(p^{n-1}+p^{n-1})+1}]=[\alpha^{p^n+p^n+1}] \ =[\alpha^3].$$

The length of $[[[p^n+p^n+1]]]$ is $n-\lfloor \log_p(p^n+p^n+1)\rfloor$.

and so on.

Now using Proposition 3.1, we give an illustration which shows the identification of the irreducible polynomials of the structure of $\mathbb{F}^*_{5^n}$.

3.2 Illustration: Identification of irreducible polynomials of degree 2 over $\mathbb{F}_5$: Here, we illustrate the structure discussed in 2.1 for $\mathbb{F}^*_{p^n}-(I)$, where $p=5$ and $n=2$. Futher, we identify all the irreducible polynomials of degree 2 over $\mathbb{F}_5$. We allocate the number for each column ranging from $(0-9)$ in the brackets and empty bracket ( ) according to the Proposition 3.1. The elements lying in the same conjugate class are denoted by the same number. Further, using these elements of the same conjugate class, we obtain irreducible polynomials as discussed above. The illustration of the structure is as follows:

α					α^2					α^3	
α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	α^{15}	α^{16}
(0)	( )	(1)	(2)	(3)	(4)	(1)	( )	(5)	(6)	(7)	(2)

Structure of $\mathbb{F}^*_{5^2}-Part(1)$

			α^4				
α^{17}	α^{18}	α^{19}	α^{20}	α^{21}	α^{22}	α^{23}	α^{24}
(5)	( )	(8)	(9)	(3)	(6)	(8)	( )

Structure of $\mathbb{F}_{5^2}^* - Part(2)$

Proposition 3.1 suggests that the elements α^7 and α^{11} lie in the same conjugate class. Therefore, we denote the conjugates of the same class by the same number. Here α^7 and α^{11}, we denote by (1) and so on. Such elements are combined to obtain an irreducible polynomial as shown below in $p_1(x)$. The empty bracket "( )" indicates that no irreducible polynomial can be formed by using the corresponding element. Thus, we obtain the irreducible polynomials of degree 2 over $\mathbb{F}_5$ as follows:

$$\begin{aligned}
p_0(x) &= (x-\alpha)(x-\alpha^5) = (x^2+4x+2),\\
p_1(x) &= (x-\alpha^7)(x-\alpha^{11}) = (x^2+3x+3),\\
p_2(x) &= (x-\alpha^8)(x-\alpha^{16}) = (x^2+x+1),\\
p_3(x) &= (x-\alpha^9)(x-\alpha^{21}) = (x^2+2),\\
p_4(x) &= (x-\alpha^2)(x-\alpha^{10}) = (x^2+3x+4),\\
p_5(x) &= (x-\alpha^{13})(x-\alpha^{17}) = (x^2+x+2),\\
p_6(x) &= (x-\alpha^{14})(x-\alpha^{22}) = (x^2+2x+4),\\
p_7(x) &= (x-\alpha^3)(x-\alpha^{15}) = (x^2+3),\\
p_8(x) &= (x-\alpha^{19})(x-\alpha^{23}) = (x^2+2x+3),
\end{aligned}$$

and

$$p_9(x) = (x-\alpha^4)(x-\alpha^{20}) = (x^2+4x+1).$$

4. Characterization of the Structure $\mathbb{F}_{p^n}^*$ beginning with the element α^{p^n-1}

Here, first we discuss the conjugate classes and then show the irreducible polynomial of degree 2 over $\mathbb{F}_7$ with the help of an illustration.

Proposition 4.1 : The elements α^{p^n-r} and $\alpha^{p^n-(pr-p+1)}$are in the same conjugate class, for $r = 1, 2, 3, \ldots, (p-1)p^{n-1}$.

Proof : Let

$$\beta = \alpha^{p^n-r}$$

then

$$\begin{aligned}\beta^p &= (\alpha^{p^n-r})^p \\ &= (\alpha^{p.p^n-p.r}) \\ &= (\alpha^{p^n+p^n+p^n+.....p^n(p\ tmes)-p.r}) \\ &= (\alpha^{p^n+(p-1)-p.r}) \\ &= \alpha^{p^n-(pr-p+1)}.\end{aligned}$$

□

Theorem 4.2 : Let $l_1, l_2, l_3, ..., l_t$ be positive integers such that $l_1 > l_2 > l_3 > ...l_t \geq 0$and $r + l \leq n - 2$, where r is a non negative integer. Then conjugate of

$$\alpha^{p^n-(p^{r+l_1}+p^{r+l_2}+p^{r+l_3}+...+p^{r+l_t}+1)}$$

is

$$\alpha^{p^n-(p^{r+l_1+1}+p^{r+l_2+1}+p^{r+l_3+1}+...+p^{r+lt+1}+1)}.$$

Also,

$$\begin{aligned}[[p^n-(p^{l_1}+p^{l_2}+p^{l_3}+...p^{l_t}+1]] &= [[p^n-(p^{l_1+1}+p^{l_2+1}+p^{l_3+1}+...p^{l_t+1}+1]] \\ &= [[p^n-(p^{l_1+2}+p^{l_2+2}+p^{l_3+2}+...p^{l_t+2}+1]] \\ &= ...\end{aligned}$$

Proof : Since,

$$\begin{aligned}(\alpha^{p^n-(p^{r+l_1}+p^{r+l_2}+p^{r+l_3}+.....+p^{r+lt}+1)})^p &= \alpha^{p^{n+1}-(p^{r+l_1+1}+p^{r+l_2+1}+p^{r+l_3+1}+...+p^{r+lt+1}+p)} \\ &= \alpha^{p.p^n-(p^{r+l_1+1}+p^{r+l_2+1}+p^{r+l_3+1}+...+p^{r+lt+1}+p)} \\ &= \frac{\alpha^{p^n+p^n+p^n+...+p^n(p\ times)}}{\alpha^{p^{r+l_1+1}+p^{r+l_2+1}+p^{r+l_3+1}+...+p^{r+lt+1}+p}} \\ &= \alpha^{p^n+(p-1)-(p^{r+l_1+1}+p^{r+l_2+1}+p^{r+l_3+1}+...+p^{r+lt+1}+p)} \\ &= \alpha^{p^n-(p^{r+l_1+1}+p^{r+l_2+1}+p^{r+l_3+1}+...+p^{r+lt+1}+1)},\end{aligned}$$

and

$$\begin{aligned}[[p^n-(p^{l_1}+p^{l_2}+p^{l_3}+...p^{l_t}+1)]] &= [[p^n-(p(p^{l_1}+p^{l_2}+p^{l_3}+...p^{l_t}+1)-(p-1)]] \\ &= [[p^n-(p^{l_1+1}+p^{l_2+1}+p^{l_3+1}+...p^{l_t+1}+p-p+1)]] \\ &= [[p^n-(p^{l_1+1}+p^{l_2+1}+p^{l_3+1}+...p^{l_t+1}+1)]].\end{aligned}$$

□

Now, we discuss the special cases of the above theorem.

Classes of type $\alpha^{p^n-(p^r+1)}$: Theorem 4.2, suggests that the conjugates of α^{p^n-2} are given by $\alpha^{p^n-(p^r+1)}$ for $r = 0, 1, 2, \ldots, n-1$,that is,

$$\begin{aligned}[[p^n-2]] &= [[p^n-(p+1)]] \\ &= [[p^n-(p^2+1)]] \\ &\quad . \\ &\quad . \\ &\quad . \\ &= [[p^n-(p^{n-1}+1)]].\end{aligned}$$

Therefore, the irreducible polynomial is

$$\prod_{r=0}^{n-1}(x-\alpha^{p^n-(p^r+1)}).$$

In the same way, we obtain the following irreducible polynomials:

Class of type $\alpha^{p^n-(p^{r+1}+p^r+1)}$: The irreducible polynomial is

$$\prod_{r=0}^{n-1}(x-\alpha^{p^n-(p^{r+1}+p^r+1)}).$$

Class of type $\alpha^{p^n-(p^{r+2}+p^r+1)}$: The irreducible polynomial is

$$\prod_{r=0}^{n-1}(x-\alpha^{p^n-(p^{r+2}+p^r+1)}).$$

Class of type $\alpha^{p^n-(p^{r+3}+p^r+1)}$: The irreducible polynomial is

$$\prod_{r=0}^{n-1}(x-\alpha^{p^n-(p^{r+3}+p^r+1)}).$$

Class of type $\alpha^{p^n-(p^{r+4}+p^r+1)}$: The irreducible polynomial is

$$\prod_{r=0}^{n-1}(x-\alpha^{p^n-(p^{r+4}+p^r+1)}).$$

4.3 Illustration : Identification of irreducible polynomials of degree 2 over $\mathbb{F}_7$:

Here, we illustrate the structure discussed in 2.2 for $\mathbb{F}_{p^n}^* - (II)$, where $p = 7$ and $n = 2$. Further, we identify all the irreducible polynomials of degree 2 over $\mathbb{F}_7$.We allocate the number for each column ranging from $(0 - 20)$ in the brackets and empty bracket ( ) according to the Proposition 4.1. The elements lying in the same conjugate class are denoted by the same number. Further, using the elements of the same conjugate class, we obtain irreducible polynomials as discussed above. The illustration of the structure is as follows:

						α^6					
α^{48}	α^{47}	α^{46}	α^{45}	α^{44}	α^{43}	α^{42}	α^{41}	α^{40}	α^{39}	α^{38}	α^{37}
( )	(1)	(2)	(3)	(4)	(5)	(6)	(1)	()	(7)	(8)	(9)

Structure of $\mathbb{F}_{7^2}^* - Part\ (1)$

	α^5							α^4			
α^{36}	α^{35}	α^{34}	α^{33}	α^{32}	α^{31}	α^{30}	α^{29}	α^{28}	α^{27}	α^{26}	α^{25}
(10)	(11)	(2)	(7)	( )	(12)	(13)	(14)	(15)	(3)	(8)	(12)

Structure of $\mathbb{F}_{7^2}^* - Part\ (2)$

			α^3							α^2	
α^{24}	α^{23}	α^{22}	α^{21}	α^{20}	α^{19}	α^{18}	α^{17}	α^{16}	α^{15}	α^{14}	α^{13}
( )	(16)	(17)	(18)	(4)	(9)	(13)	(16)	( )	(19)	(20)	(5)

Structure of $\mathbb{F}_{7^2}^* - Part\ (3)$

					α^1
α^{12}	α^{11}	α^{10}	α^9	α^8	α^7
(10)	(14)	(17)	(19)	( )	(0)

Structure of $\mathbb{F}_{7^2}^* - Part\ (4)$

Proposition 4.1 suggests that the elements α^{47} and α^{41} lie in the same conjugate class. Therefore, we denote the conjugates of the same class by the same number. Here α^{47} and α^{41}, we denote by (1) and so on. Such elements are combined to obtain an irreducible polynomial. The empty bracket "( )" indicates that no irreducible polynomial can be formed by using the corresponding element. Therefore, the irreducible polynomials of degree 2 over $\mathbb{F}_7$ are as follows:

$$\begin{aligned}
p_0(x) &= (x-\alpha)(x-\alpha^7) = (x^2+x+3),\\
p_1(x) &= (x-\alpha^{41})(x-\alpha^{47}) = (x^2+5x+5),\\
p_2(x) &= (x-\alpha^{34})(x-\alpha^{46}) = (x^2+6x+4),\\
p_3(x) &= (x-\alpha^{27})(x-\alpha^{45}) = (x^2+x+6),\\
p_4(x) &= (x-\alpha^{20})(x-\alpha^{44}) = (x^2+2),\\
p_5(x) &= (x-\alpha^{13})(x-\alpha^{43}) = (x^2+2x+3),\\
p_6(x) &= (x-\alpha^{6})(x-\alpha^{42}) = (x^2+4x+1),\\
p_7(x) &= (x-\alpha^{33})(x-\alpha^{39}) = (x^2+4x+6),
\end{aligned}$$

$$\begin{aligned}
p_8(x) &= (x-\alpha^{26})(x-\alpha^{38}) = (x^2+2x+2),\\
p_9(x) &= (x-\alpha^{19})(x-\alpha^{37}) = (x^2+5x+3),\\
p_{10}(x) &= (x-\alpha^{12})(x-\alpha^{36}) = (x^2+1),\\
p_{11}(x) &= (x-\alpha^{5})(x-\alpha^{35}) = (x^2+3x+5),\\
p_{12}(x) &= (x-\alpha^{25})(x-\alpha^{31}) = (x^2+6x+3),\\
p_{13}(x) &= (x-\alpha^{18})(x-\alpha^{30}) = (x^2+3x+1),\\
p_{14}(x) &= (x-\alpha^{11})(x-\alpha^{29}) = (x^2+4x+5),\\
p_{15}(x) &= (x-\alpha^{4})(x-\alpha^{28}) = (x^2+4),\\
p_{16}(x) &= (x-\alpha^{17})(x-\alpha^{23}) = (x^2+2x+5),\\
p_{17}(x) &= (x-\alpha^{10})(x-\alpha^{22}) = (x^2+x+4),\\
p_{18}(x) &= (x-\alpha^{3})(x-\alpha^{21}) = (x^2+6x+6),\\
p_{19}(x) &= (x-\alpha^{9})(x-\alpha^{15}) = (x^2+3x+6),
\end{aligned}$$

and $p_{20}(x) = (x - \alpha^2)(x - \alpha^{14}) = (x^2 + 5x + 2)$.

5. Correspondence Between the Elements of Columns and Rows of Structure $\mathbb{F}^*_{p^n} - (I)$

The elements of $F^*_{p^n} - (I)$ are arranged in its structure with some criteria and are associated with some correspondence which is discussed in this section. Let

$$\alpha(i,\ j,\ k) = \alpha^{p^{i-1}+pj-k}$$

be the elements introduced in new columns of the i^{th} row, where $i = 1, 2, ..., n$ and j stands for number of spells in which new columns are to be introduced (for example, in first row of the structure $F^*_{5^2}$ has four spells),

$j = \left\{ \begin{array}{ll} 1 & \text{for } i = 1 \\ 1, 2, ..., p^{i-2}(p-1) & \text{for } i \qquad\quad 1 \end{array} \right\}$;

$k = 1, 2, ...,\ (p-1)$.

Now, we consider n^{th} row and $(n-1)^{th}$ row for detail description.

For i = n;

$j = 1,\ 2, ...,\ p^{i-2}(p-1);\ k = 1,\ 2, ...,\ (p-1)$,

the elements in the new columns are introduced as follows:

Let us take $j = 1;\ k = 1, 2, ..., (p-1)$, therefore $\alpha(i,\ j, k)$ becomes

$$\begin{aligned} \alpha^{p^{i-1}+pj-1} &= \alpha^{p^{n-1}+p.1-1} = \alpha^{p^{n-1}+p-1}, \\ \alpha^{p^{i-1}+pj-2} &= \alpha^{p^{n-1}+p.1-2} = \alpha^{p^{n-1}+p-2}, \\ &\vdots \\ \alpha^{p^{i-1}+pj-(p-1)} &= \alpha^{p^{n-1}+p.1-(p-1)} = \alpha^{p^{n-1}+1}. \end{aligned}$$

For $j = 2;\ k = 1, 2, ..., (p-1)$, $\alpha(i,\ j, k)$ becomes

$$\begin{aligned} \alpha^{p^{i-1}+pj-1} &= \alpha^{p^{n-1}+p.2-1} = \alpha^{p^{n-1}+2p-1}, \\ \alpha^{p^{i-1}+pj-2} &= \alpha^{p^{n-1}+p.2-2} = \alpha^{p^{n-1}+2p-2}, \\ &\vdots \\ \alpha^{p^{i-1}+pj-(p-1)} &= \alpha^{p^{n-1}+p.2-(p-1)} = \alpha^{p^{n-1}+p+1}. \end{aligned}$$

Likewise, we can obtain the corresponding elements for $j = 3, 4, ..., p^{i-2}(p-1)$. Here, the number of new columns introduced for $i = n$ are $p^{n-1}(p-2) + p^{n-2}$.

For i = n − 1.

Let us take $j = 1$; $k = 1, 2, ..., (p-1)$, therefore $\alpha(i,\, j, k)$ becomes

$$\begin{aligned}
\alpha^{p^{i-1}+pj-1} &= \alpha^{p^{n-1-1}+p.1-1} = \alpha^{p^{n-2}+p-1},\\
\alpha^{p^{i-1}+pj-2} &= \alpha^{p^{n-1-1}+p.1-2} = \alpha^{p^{n-2}+p-2},\\
&\vdots\\
\alpha^{p^{i-1}+pj-(p-1)} &= \alpha^{p^{n-1-1}+p.1-(p-1)} = \alpha^{p^{n-2}+1}.
\end{aligned}$$

For $j = 2$; $k = 1, 2, ..., (p-1)$, $\alpha(i,\, j, k)$ becomes

$$\begin{aligned}
\alpha^{p^{i-1}+pj-1} &= \alpha^{p^{n-1-1}+p.2-1} = \alpha^{p^{n-2}+2p-1},\\
\alpha^{p^{i-1}+pj-2} &= \alpha^{p^{n-1-1}+p.2-2} = \alpha^{p^{n-2}+2p-2},\\
&\vdots\\
\alpha^{p^{i-1}+pj-(p-1)} &= \alpha^{p^{n-1-1}+p.2-(p-1)} = \alpha^{p^{n-2}+p+1}.
\end{aligned}$$

Likewise, we can obtain the corresponding elements for $j = 3, 4, ...,\ p^{i-2}(p-1)$. Here, the number of new columns introduced for $i = n-1$ are $p^{n-2}(p-2) + p^{n-3}$.
Similarly, we can proceed for $i = (n-2),\ (n-3), ..., 3,\ 2,\ 1$. The number of columns introduced for $i = 3,\ 2,\ 1$ are respectively $p^2(p-2)+p,\ p(p-2)+1,\ p-2$.

6. Correspondence Between the Elements of Columns and Rows of Structure $F^*_{p^n} - (II)$

The elements of $F^*_{p^n} - (II)$ are associated with some correspondence in the structure which is discussed in this section. Let

$$\alpha(i, j, k) = \alpha^{p^i+pj-k}$$

be the elements introduced in new columns of the i^{th} row, where $i = 1,\ 2, ..., n$ and j stands for number of spells in which new columns are to be introduced (for example, in first row of the structure $F^*_{7^2}$ has six spells,

$j = \left\{ \begin{array}{ll} 1 & \text{for } i = 1 \\ 0, -1, -2, ..., -[p^{i-2}(p-1)-1] & \text{for } i \qquad 1 \end{array} \right\}$;
$k = 1, 2, ..., (p-1)$.

We consider n^{th} row and $(n-1)^{th}$ row for detail description.

For i = n;

$j = 0, -1, -2, ..., -[p^{i-2}(p-1)-1]$; $k = 1, 2, ..., (p-1)$,

the elements in the new columns are introduced as follows:
Let us take $j = 0$; $k = 1, 2, ..., (p-1)$, therefore $\alpha(i, j, k)$ becomes

$$\begin{aligned} \alpha^{p^i+pj-1} &= \alpha^{p^n-1}, \\ \alpha^{p^i+pj-2} &= \alpha^{p^n-2}, \\ &\vdots \\ \alpha^{p^i+pj-(p-1)} &= \alpha^{p^n-p+1}. \end{aligned}$$

For $j = -1$; $k = 1, 2, ..., (p-1)$, $\alpha(i, j, k)$ becomes

$$\begin{aligned} \alpha^{p^i+pj-1} &= \alpha^{p^n-p.1-1} = \alpha^{p^n-p-1}, \\ \alpha^{p^i+pj-2} &= \alpha^{p^n-p.1-2} = \alpha^{p^n-p-2}, \\ &\vdots \\ \alpha^{p^i+pj-(p-1)} &= \alpha^{p^n-p.1-(p-1)} = \alpha^{p^n-2p+1}. \end{aligned}$$

Likewise, we can obtain the corresponding elements for $j = -2, ..., -[p^{i-2}(p-1)-1]$.
Here, the number of new columns introduced for $i = n$ are $p^{n-1}(p-2) + p^{n-2}$.
For $\mathbf{i = n-1}$.
Let us take $j = 0$; $k = 1, 2, ..., (p-1)$, thereore $\alpha(i, j, k)$ becomes

$$\begin{aligned} \alpha^{p^i+pj-1} &= \alpha^{p^{n-1}-1}, \\ \alpha^{p^i+pj-2} &= \alpha^{p^{n-1}-2}, \\ &\vdots \\ \alpha^{p^i+pj-(p-1)} &= \alpha^{p^{n-1}-(p-1)} = \alpha^{p^{n-1}-p+1}. \end{aligned}$$

For $j = -1$; $k = 1, 2, ..., (p-1)$, $\alpha(i, j, k)$ becomes

$$\begin{aligned} \alpha^{p^i+pj-1} &= \alpha^{p^n-p.1-1} = \alpha^{p^{n-1}-p-1}, \\ \alpha^{p^i+pj-2} &= \alpha^{p^n-p.1-2} = \alpha^{p^{n-1}-p-2}, \\ &\vdots \\ \alpha^{p^i+pj-(p-1)} &= \alpha^{p^{n-1}-p.1-(p-1)} = \alpha^{p^{n-1}-2p+1}. \end{aligned}$$

Likewise, we can obtain the corresponding elements for $j = -2, -3, ..., -[p^{i-2}(p-1)-1]$.
Here, the number of new columns introduced for $i = n-1$ are $p^{n-2}(p-2) + p^{n-3}$.

Similarly, we can proceed for $i = (n-2), (n-3), ..., 3,\ 2,\ 1$. The number of columns introduced for $i = 3,\ 2,\ 1$ are respectively $p^2(p-2)+p$, $p(p-2)+1$, $p-1$.

Acknowledgment

Authors gratefully acknowledge the support of UGC-SAP. They also wish to thank here the organizing team of International Conference on Finite Field (Fq12).

References

[1] Ashikhmin A. E. and Litsyn S. N., Fast decoding of non-binary first order Reed-Mullar codes, AAECC, 7 (1996), 299-308.

[2] Beuchat J. L., Brisebarre N., Detrey J. and Okamoto E., Arithmetic operators for pairing-based cryptography, CHES, (2007), LNCS, 4727 (2007), 239-255.

[3] Charpin P., Tietavainen A. and Zinoviev V., On binary cyclic codes with minimum distance three, Problems of Information Transmission, 33 (1997), 3-14.

[4] Geer G. V. D., Schoof R. and Vlugt M. V. D., Weight formulas for Ternary Melas codes, Mathematics of Computation, 58(198) (1992),781-792.

[5] Hayashi T., Shimoyama T., Shinohara N. and Takagi T., Breaking pairing based cryptosystem using η_T pairing over $F(3^{97})$, ASIACRYPT, (2012), 43-60.

[6] Lidl R. and Niederreiter H., Finite Fields, Cambridge University Press, (1983).

[7] Mac Williams F. J. and Sloane N. J. A., The Theory of Error-Correcting Codes, North-Holland, New York, (1986).

[8] Mullen G. L. and Panario D., Handbook of Finite Fields, CRC Press, (2013).

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

[10] Sharma P. L. and Kumar S., Balanced incomplete block design (BIBD) using hadamard Rhotrices, International Journal of Technology, 4(1) (2014), 62-66.

[11] Sharma P. L. and Kumar S., Some applications of hadamard Rhotrices to design balanced incomplete block, International J. of Math Sci.& Engg Appls, 8(II) (2014), 389-404.

[12] Sharma P. L. and Rehan M., On security of Hill Cipher using finite fields, International Journal of Computer Applications, 71(4) (2013), 30-33.

[13] Sharma P. L. and Rehan M., Modified Hill Cipher using Vandermonde matrix and finite field, International Journal of Technology, 4(1) (2014), 252-256.

[14] Sharma P. L. and Sharma S., An application of finite field in Hill Cipher, International Journal of Technology, 4(1) (2014), 248-251.

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

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

[17] Sharma P. L., Rehan M. and Sharma S., Counting irreducible Polynomials over $GF(3)$ with first and third coefficients given, Asian European Journal of Mathematics, 8(1) (2015), 1550-1527.

[18] Sharma P. L., Sharma S. and Dhiman N., Construction of Iniinite sequences of irreducible polynomials using Kloosterman sums, Bulletin of Pure and Applied Sciences, 33E(2), (Math. & Stat.), (2014),161-168.

[19] Sharma P. L., Sharma S. and Rehan M., On Construction of irreducible polynomials over finite field F_3, Journal of Discrete Mathematical Sciences and Cryptography, 18(4) (2015), 335-347.

[20] Sharma R. K., Shukla W. and Ramasamy S., On trace structure of $F(2^n)$, Journal of Communication and Computer, 8 (2011), 329-334.

[21] Sharma R. K., Shukla W. and Ramasamy S., A note on identification of irreducible polynomials over F_2, International Electronic Journal of Pure and Applied Mathematics, 4(2) (2012), 59-70.

[22] Shinohara N., Shimoyama T., Hayashi T. and Takagi T., Key length estimation of pairing-based cryptosystems using η_T pairing, ISPEC 2012, LNCS 7232 (2012), 228-244.