Matrix Representation of Groups in the Finite Fields $GF(2^n)$

AhmadHamza Al Cheikha

Abstract— ***The representation of mathematical fields can be accomplished by binary rows (or columns) of a binary triangular matrix as the Hamming's matrices, but this representation don't show the basic product properties of the fields, that is the nonzero elements of the fields forms a cyclic multiplicative group.***

In this paper we show that the elements of the fields GF(2^n), and their subgroups, can represent as square matrices by m – sequences, which satisfies the product properties as a cyclic group.

Index Term - Galois fields, m-sequences,cyclic groups, Orthogonal sequences.

I. INTRODUCTION

m- Linear Recurring Sequences

Let k be a positive integer and $\lambda\ ,\lambda_0,\lambda_1,\ldots,\lambda_{k-1}$ are elements in the field F_q , then the sequence $a_0, a_1,\ldots$ is called **non homogeneous linear recurring sequence of order *k*iff :**

$$a_{n+k} = \lambda_{k-1}a_{n+k-1} + \lambda_{k-2}a_{n+k-2} + \ldots + \lambda_0 a_n + \lambda,\ \lambda_i \in F_q\ , i = 0,1,\ldots,k-1$$

$$or \qquad a_{n+k} = \sum_{i=1}^{k-1}\lambda_i a_{n+i} + \lambda \qquad (1)$$

The elements $a_0, a_1,\ldots,a_{k-1}$ are called the **initial values** (or the vector $(a_0, a_1,\ldots,a_{k-1})$ is called **the initial vector**). If $\lambda = 0$ then the sequence $a_0, a_1,\ldots$ is called **homogeneous linear recurring sequence** (**H. L. R. S.),** except the zero initial vector, and the polynomial

$$f(x) = x^k + \lambda_{k-1}x^{k-1} + \ldots + \lambda_1 x + \lambda_0 \qquad (2)$$

is called the **characteristic polynomial. I**n this study, we are limited to $\lambda_0 = 1$. [1]-[3]

II. THE IMPORTANCE OF THIS RESEARCH AND ITS OBJECTIVES

The elements of the fields $GF(2^n)$, and their subgroups, can be represented assquare matrices by m – sequences, which satisfies the multiplicative properties as a cyclic group, that is it will be useful in many other scientific branches. For example orthogonal sets in the forward and the inverse link of communications channels in the CDMA systems especially in the second (IS-95-CDMA), the third…. (CDMA200,…), the pilot channels, the Sync channels, and the Traffics channelsin the present or in many other scientific branches in the future.

III. RESEARCH METHODS AND MATERIALS

Basic Definitions and Theorems

***Definition* 1.**Let S be a nonempty set and $a_0, a_1,\ldots.$ is sequence from S and if there is $r > 0$ such that:

$$a_{n+r} = a_n \quad ; \quad n \geq n_0 \quad ; \quad n_0 \geq 0 \quad (3)$$

Then this sequence is called Ultimately Periodic Sequence, and *r* is called a period of this sequence, the smallest positive integer between these *r*'s is called the period of this sequence, and the smallest non negative n_0 such that:

$$a_{n+r} = a_n \quad ; \quad n \geq n_0 \quad ; \quad n_0 \geq 0,$$

is called **Pre-Period**, [1][4]

***Definition* 2.**The Ultimately Periodic Sequence $a_0, a_1,\ldots.$with the smallest period *r* is called a periodic iff: $a_{n+r} = a_n \ ; \ n = 0,1,\ldots$ [1]-[4]

***Definition* 3.**The complement of the binary vector $X = (x_1, x_2,\ldots,x_n)$ is the vector $\overline{X} = (\overline{x_1}, \overline{x_2},\ldots,\overline{x_n})$,

when $\overline{x_i} = \begin{cases} 1 & if \quad x_i = 0 \\ 0 & if \quad x_i = 1 \end{cases}$. [1]-[4]

***Definition* 4. (Euler function φ).** $\varphi(n)$ is the number of the natural numbers that are relatively prime with*n*.[5]-[8]

***Definition* 5.**AnyPeriodic Sequence $a_0, a_1,\ldots.$over F_q with prime characteristicpolynomial is an orthogonal cyclic code and ideal auto correlation [1]-[10].

***Definition* 6.**The binary periodic sequence $(a_i)_{i\in N}$, with the period r has the property of " Ideal Auto Correlation" if and only if its periodic auto correlation $R_a(\tau)$of the form:

$$R_a(\tau) = \begin{cases} r & ; \quad for\ \tau \equiv 0 \mod(r) \\ -1 & ; \quad otherwise \end{cases}$$

When: $R_a(\tau) = \sum_{t=0}^{r-1}(-1)^{a(\tau+t)+a(t)}$ [1],[2]

Theorem1.

i. If $a_0, a_1,\ldots.$ is a homogeneous linear recurring sequence of order *k* in F_q , satisfies (1) then this sequence is periodic.

Manuscript Received May, 2014

Ahmad Hamza Al Cheikha, Department of Mathematical Science, Ahlia University, Kingdom of Bahrain.

ii. If this sequence is homogeneous linear recurring sequence, periodic with the period r, and its characteristic polynomial $f(x)$ then $r \mid ord\, f(x)$. [6]

iii. If the polynomial $f(x)$ is primitive then the period of the sequence is $q^k - 1$, and this sequence is called m – sequence.

Lemma 2.(Fermat's theorem). If F is a finite field and has q elements then every element a of F satisfies the equation: $x^q = x$. [6],[9]

Theorem 3. For any primitive element p and any positive integer n there is a field F, which has p^n elements and any two fields having $q = p^n$ Elements are isomorphic. [6],[9],[11]

Theorem 4.

i. $(q^m - 1)\big|(q^n - 1) \Leftrightarrow m \mid n$ (4)

ii. If F_q is a field of order $q = p^n$ then any subfield of them of the order p^m and $m \mid n$ and by inverse if $m \mid n$ then in the field F_q there is a subfield of order p^m. [6],[9],[11]

Theorem 5. The number of irreducible polynomials in $F_q(x)$ of degree m and order e is $\varphi(e)/m$, if $e \geq 2$, when m is the order of q by mod e, and equal to 2 if $m = e = 1$, and equal to zero elsewhere. [6]-[9]

Theorem 6. If $g(x)$ is a characteristic prime polynomial of the (H. L. R. S.) $a_0, a_1, \ldots$ of degree k, and α is a root of $g(x)$ in any splitting field of F_2 then the general bound of the sequence is: $a_n = \sum_{i=1}^{k} C_i \left(\alpha^{2^{i-1}}\right)^n$. [11],[12].

*** The study here, is limited to the fields Galois $GF(2^n)$**

IV. RESULTS AND DISCUSSION

A. First step

Theorem 7: Suppose $a_0, a_1, \ldots$ is a non zero homogeneous linear recurring sequence of order k over $F_2 = \{0,1\}$ and $f(x)$ is its prime characteristic polynomial then the first $r = 2^k - 1$ bounds with all its cyclic shifts forming an additive group.

Proof: This sequence is periodic with period $r = 2^k - 1$. We suppose $\$ = \{S_1, S_2, \ldots, S_r\}$ where $S_1 = (a_1 a_2 \ldots a_r)$ is the sequence of the first $r = 2^k - 1$ bounds, and $S_2 = (a_r a_1 \ldots a_{r-1}), \ldots,\ S_r = (a_2 a_3 \ldots a_r a_1)$ are all its cyclic shifts, and we suppose $O = S_0 = (0 \ldots\ldots 0)$, $S = \$ \cup \{S_0\}$ and if α is a root of the prime polynomial $f(x)$ and:

$$GF(2^k) = \left\{\alpha^i : \alpha^i = \sum_{j=0}^{k-1} b_j\, \alpha^j,\ i = 0,1,2,\ldots,2^{k-1}\right\} \cup \{0\},\ 0 = \sum_{j=0}^{k-1} 0\alpha^j$$

And the function: $h : GF(2^k) \to S$ as following:

$$h(\alpha^i) = h(i) = h[b_0\ b_1 \ldots b_{k-1}] = [b_0\ b_1\ \ b_{k-1}\ b_k\ \ b_{2^k-2}]$$

Then h is one-to-one corresponding and:

$$\begin{cases} h(\alpha^i + \alpha^j) = h(\alpha^i) + h(\alpha^j) \\ h(m.\alpha^i) = m.h(\alpha^i), \quad m = 0 \text{ or } 1 \end{cases}$$

And h is Linear Transformation and isomorphism from the additive group $(GF(2^k), +)$ to the additive group $(S, +)$.

B. Second Step

Theorem 8: Suppose $a_1, a_2, \ldots$ is a non zero homogeneous linear recurring sequence of order k in F_2 and $f(x)$ is their primitive characteristic polynomial, S_1 is the initial bounds where $r = 2^k - 1$ and $\$ = \{S_1, S_2, \ldots, S_r\}$ are the all cyclic shifts. Let A is a matrix which its rows are elements \$ respectively, then $\{A^i,\ i = 1, \ldots, r\}$ is a cyclic multiplicative group, relatively to product of matrices, having the period of $S_1(x)$ and rows of A^i are the shifts to rows of A.

Proof:

Suppose $A = \begin{bmatrix} S_1 \\ S_2 \\ \ldots \\ S_r \end{bmatrix}$ and we will compute $A^2 = A \cdot A$.

Suppose the first row ω_1 in the matrix A^2 then:

$$\omega_1 = \sum_{i \in I} S_i$$

when I the set of all columns in A which does not start by zero, and we see that:

$$X, Y \in \$\ \&\ X \neq Y \Rightarrow X + Y \in \$$$

Then $\omega_1 = S_l \in \$$

The second row ω_2 in A^2 is a result of shift i by 1 digit to the right, then: $\omega_2 = \sum_{i \in I} S_{i+1} = S_{l+1}$, and respectively we have $\omega_r = \sum_{i \in I} S_{i+r-1} = S_{l+r-1}$, when the indexes computed by $mod\ r$, then the rows of the matrix A^2 are shifts to rows of A, On other hand we suppose that $\$(x) = \{S_1(x), S_2(x), \ldots, S_r(x)\}$ then:

$$\omega_1(x)=\sum_{i\in I} S_i(x)\ ;$$
$$\omega_2(x)=\sum_{i\in I} S_{i+1}(x)=\sum_{i\in I} xS_i(x)\quad ;\ldots$$
$$\omega_r(x)=\sum_{i\in I} x^{r-1}S_i(x)$$

And:

$$\omega_1=\sum_{i\in I} S_i(x)=\sum_{i\in I} x^{i-1}S_1(x)\ \Rightarrow\ \omega_1(x)=S_1^2(x)$$

When: $S_1^2(x)\in \$(x)$, and the calculations are done by $\left(\bmod\left(x^{2^k-1}-1\right)\right)$, And we have:

$\omega_2(x)=xS_1^2(x);\ \ldots\ ;\omega_r(x)=x^{r-1}S_1^2(x)$

Suppose $[f_i(x)]$ denotes the row of coefficients of $f_i(x)$, respectively to increasing exponents of x, and which has the length r, then:

$$A=\begin{bmatrix}S_1(x)\\ S_2(x)\\ .\\ S_r(x)\end{bmatrix}=\begin{bmatrix}S_1(x)\\ xS_1(x)\\ .\\ x^{r-1}S_1(x)\end{bmatrix}\ ;\ A^2=\begin{bmatrix}S_1^2(x)\\ xS_1^2(x)\\ .\\ x^{r-1}S_1^2(x)\end{bmatrix};\ldots;$$

$$A^i=\begin{bmatrix}S_1^i(x)\\ xS_1^i(x)\\ .\\ x^{r-1}S_1^i(x)\end{bmatrix}\ ,\ i=1,2,\ldots,r$$

When: $S_1^i(x)\in \$(x);\ i=1,\ldots,r$, then:

$$A=\begin{bmatrix}S_1(x)\\ S_2(x)\\ .\\ S_r(x)\end{bmatrix}=\begin{bmatrix}1\\ x\\ .\\ x^{r-1}\end{bmatrix}S_1(x)\ ,\ A^2=\begin{bmatrix}1\\ x\\ .\\ x^{r-1}\end{bmatrix}S_1^2(x),\ldots$$

$$\ldots,A^i=\begin{bmatrix}1\\ x\\ .\\ x^{r-1}\end{bmatrix}S_1^i(x)\ ,i=1,2,\ldots,r$$

Result 1: The period of the sequence $A,A^2,A^3,\ldots$ is equal to $ord(S_1(x))$ and divides 2^k-1.

Result 2: If $ord(S_1(x))=2^k-1$ then S is representation to the field $GF(2^k)$.

Result 3: If $ord(S_1(x))=l\ and\ l\,|\,2^k-1$ then $l=2^m-1$ and $<A>$ is a representation to one subgroup of order l in the field $GF(2^k)$

Result 4: If $ord(S_1(x))+1=2^l\ and\ l\,|\,k$ then : $<A>\cup\{O\}$ is representation to the Subfield $GF(2^l)$.

Result 5: If 2^k-1 is prime then all elements of $S_i(x)$ are of the order 2^k-1 except only one of them that is of the order one

C. Third Step

Example 1: If α is a root of the prime polynomial $f(x)=x^3+x+1$ and generates $GF(2^3)$ then the Binary representation of the elements of $GF(2^3)$ is:

$$\begin{array}{llll}
\alpha & \rightarrow(1)=[010]\ ; & \alpha^5=1+\alpha+\alpha^2 & \rightarrow(5)=[111]\\
\alpha^2 & \rightarrow(2)=[001]\ ; & \alpha^6=1+\alpha^2 & \rightarrow(6)=[101]\\
\alpha^3=1+\alpha & \rightarrow(3)=[110]\ ; & \alpha^7=1 & \rightarrow(7)=[100]\\
\alpha^4=\alpha+\alpha^2 & \rightarrow(4)=[011]\ ; & 0 & \rightarrow(0)=[000]
\end{array}$$

Where $(i), i=0,1,2,\ldots,7$ is the symbol of the sequence i.

The field $GF(2^3)$ contains two subfields : $GF(2)$ and the same $GF(2^3)$ and the divisorsof the number 7 are 1 and 7 consequently $GF(2^3)$ contains twomultiplicativesubgroups are: $GF^*(2)$ and $GF^*(2^3)$.

Suppose the Linear Recurring Sequence be

$a_{n+3}=a_{n+1}+a_n$ or $a_{n+3}+a_{n+1}+a_n=0$ (1)

Figure(1): Linear feedback register of degree3 generates sequence (1)

With the characteristic equation $x^3+x+1=0$ and the characteristic polynomial $f(x)=x^3+x+1$,which is a prime and generates F_{2^3} and if $\bar{x}=\alpha\in GF(2^3)$ is a root of $f(x)$ then the solutions of characteristic equation are $\{\alpha^n,\alpha^{2n},\alpha^{4n}\}$. The general solution of equation (1) isgiven by $a_n=\alpha^2\cdot\alpha^n+\alpha^4\cdot\alpha^{2n}+\alpha\cdot\alpha^{4n}$, and thesequence is periodic with the period $2^3-1=7$.

For the initial position: $a_1=1, a_2=0,\ a_3=0$, then $S_1=(1\ 0\ 0\ 1\ 0\ 1\ 1)$ and by the cyclic permutationson S_1 we have $\$=\{S_1,S_2,S_3,S_4,S_5,S_6,S_7\}$ where:

$S_2=(1\ 1\ 0\ 0\ 1\ 0\ 1)$; $S_3=(1\ 1\ 1\ 0\ 0\ 1\ 0)$; $S_4=(0\ 1\ 1\ 1\ 0\ 0\ 1)$
$S_5=(1\ 0\ 1\ 1\ 1\ 0\ 0)$; $S_6=(0\ 1\ 0\ 1\ 1\ 1\ 0)$; $S_7=(0\ 0\ 1\ 0\ 1\ 1\ 1)$

The first three digits in each sequence are the initial position of the feedback register.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The matrix A of the cyclic permutations of S_1 is:

$$A=\begin{bmatrix}1&0&0&1&0&1&1\\1&1&0&0&1&0&1\\1&1&1&0&0&1&0\\0&1&1&1&0&0&1\\1&0&1&1&1&0&0\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{bmatrix} \text{ or briefly } A=A_1=\begin{bmatrix}1&0&0&1&0&1&1\\1&1&0&0&1&0&1\\-&-&-&-&-&-&-\\0&0&1&0&1&1&1\end{bmatrix}$$

The first row in this matrix is called ***The head row***.

If the function $h: GF(2^3) \to \$$ where:

$h(\alpha^i)=h(i)=h_i=$ [The row of the matrix A corresponding of the initial position I].

Then h_i is isomorphism from the group $(GF(2^3),+)$ on the group $(\$,+)$.

I- In this matrix the head row is: $S_1=[1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1]$ and the head polynomial is:

$h(1)=S_1(x)=1+x^3+x^5+x^6$.

We see that: $A_2=A^2=A$ and $\{O,A\}$ is a representation of the field $GF(2)$, where O is zero matrix.

II- We suppose that;

$$B=B_1=\begin{bmatrix}1&1&0&0&1&0&1\\1&1&1&0&0&1&0\\-&-&-&-&-&-&-\\1&0&0&1&0&1&1\end{bmatrix}$$

In this matrix the head row is:

$h(3)=S_2=[1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1]$ and the corresponding head polynomial is: $S_2(x)=1+x+x^4+x^6$, Thus

$$B_2=B^2=\begin{bmatrix}1&1&1&0&0&1&0\\0&1&1&1&0&0&1\\-&-&-&-&-&-&-\\1&1&0&0&1&0&1\end{bmatrix}$$

In this matrix the head row is:

$h(5)=S_3=[1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0]$ and the corresponding head polynomial is: $S_2^2(x)=1+x+x^2+x^5$, Thus

$$B_3=B^3=\begin{bmatrix}0&1&1&1&0&0&1\\1&0&1&1&1&0&0\\-&-&-&-&-&-&-\\1&1&1&0&0&1&0\end{bmatrix}$$

In this matrix the head row is: $h(4)=S_4=[0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1]$ and the corresponding head polynomial is: $S_2^3(x)=x+x^2+x^3+x^6$, Thus

$$B_4=B^4=\begin{bmatrix}1&0&1&1&1&0&0\\0&1&0&1&1&1&0\\-&-&-&-&-&-&-\\0&1&1&1&0&0&1\end{bmatrix}$$

In this matrix the head row is:

$h(6)=S_5=[1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0]$ and the corresponding head polynomial is: $S_2^4(x)=1+x^2+x^3+x^4$, Thus

$$B_5=B^5=\begin{bmatrix}0&1&0&1&1&1&0\\0&0&1&0&1&1&1\\-&-&-&-&-&-&-\\1&0&1&1&1&0&0\end{bmatrix}$$

In this matrix the head row is:

$h(1)=S_6=[0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0]$ and the corresponding head polynomial is: $S_2^5(x)=x+x^3+x^4+x^5$, Thus

$$B_6=B^6=\begin{bmatrix}0&0&1&0&1&1&1\\1&0&0&1&0&1&1\\-&-&-&-&-&-&-\\0&1&0&1&1&1&0\end{bmatrix}$$

In this matrix the head row is:

$h(2)=S_7=[0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1]$ and the corresponding head polynomial is: $S_2^6(x)=x^2+x^4+x^5+x^6$, Thus

$$B_7=B^7=\begin{bmatrix}1&0&0&1&0&1&1\\1&1&0&0&1&0&1\\-&-&-&-&-&-&-\\0&0&1&0&1&1&1\end{bmatrix}$$

In this matrix the head row is:

$h(7)=S_1=[1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1]$ and the corresponding head polynomial is: $S_2^7(x)=1+x^3+x^5+x^6$, and

$B_8=B^8=B$.

We see that $\{O,B_1,B_2,B_3,B_4,B_5,B_6,B_7\}$ is a representation of $GF(2^3)$ and

$ord(B_1)=ord(B_2)=ord(B_3)=ord(B_4)=ord(B_5)=ord(B_6)=7$

The field F_{2^3} contains $\varphi(2^k-1)/k=\varphi(2^3-1)/3=2$ third degree irreducible polynomials that are:

$f(x)=x^3+x+1$ and its conjugate $g(x)=x^3+x^2+1$, and $g(x)$ is a prime polynomial then we can represent F_{2^3} by two different ways.

D. Fourth step

Example 2: If α is a root of the prime polynomial $f(x)=x^4+x+1$ and generates $GF(2^4)$ then the binary representation of the elements of $GF(2^4)$ is:

$\alpha \to (1)=[0100]$; $\alpha^9=\alpha+\alpha^3 \to (5)=[0101]$

$\alpha^2 \to (2)=[0010]$; $\alpha^{10}=1+\alpha+\alpha^2 \to (10)=[1110]$

$\alpha^3 \to (3)=[0001]$; $\alpha^{11}=\alpha+\alpha^2+\alpha^3 \to (11)=[0111]$

$\alpha^4=1+\alpha \to (4)=[1100]$; $\alpha^{12}=1+\alpha+\alpha^2+\alpha^3 \to (12)=[1111]$

$\alpha^5=\alpha+\alpha^2 \to (5)=[0110]$; $\alpha^{13}=1+\alpha^2+\alpha^3 \to (13)=[1011]$

$\alpha^6=\alpha^2+\alpha^3 \to (6)=[0011]$; $\alpha^{14}=1+\alpha^3 \to (14)=[1001]$

$\alpha^7=1+\alpha+\alpha^3 \to (7)=[1101]$; $\alpha^{15}=1 \to (15)=[1000]$

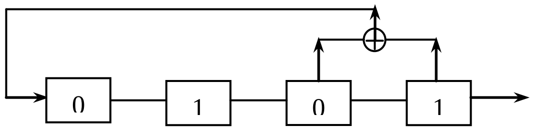
$\alpha^8=1+\alpha^2 \to (8)=[1010]$; $0 \to (0)=[0000]$

Where $(i), i=0,1,2,\ldots,15$ is the symbol of the sequence i.

The field $GF(2^4)$ contains three subfields are: $GF(2)$,

$GF(2^2)$ and the same $GF(2^4)$ and the divisors of the number 15 are 1, 3, 5 and 15 consequently $GF(2^4)$ contains four multiplicative subgroups : $GF^*(2)$, $GF^*(2^2)$, one group of the order 5 and $GF^*(2^4)$ .Suppose the Linear Recurring Sequence:

$a_{n+4} = a_{n+1} + a_n$ or $a_{n+4} + a_{n+1} + a_n = 0$ **(2)**



Figure(2): Linear feedback register of degree 4 generates sequence (2)

With the characteristic equation $x^4 + x + 1 = 0$ and the characteristic polynomial $f(x) = x^4 + x + 1$, which is prime and generates F_{2^4} and if $\bar{x} = \alpha \in GF\left(2^4\right)$ is a root of $f(x)$ then the solutions of characteristic equation are $\{\alpha, \alpha^2, \alpha^4, \alpha^8 = \alpha^2 + 1\}$ and the general solution of equation (2) is given by:

$$a_n = c_1\alpha^n + c_2 a^{2n} + c_3\alpha^{4n} + c_4\alpha^{8n}$$

For $a_1 = 1$, $a_2 = 0$, $a_3 = 1$, $a_4 = 0$ we have:

$$a_n = \alpha^9\alpha^n + \alpha^{12}a^{2n} + \alpha^9\alpha^{4n} + \alpha^3\alpha^{8n}$$

and the sequence is periodic with the period $2^4 - 1 = 15$.

$$s_1 = (1,0,1,0,1,1,1,1,0,0,0,1,0,0,1); s_2 = (1,1,0,1,0,1,1,1,1,0,0,0,1,0,0);..$$
$$.....; s_{15} = (0,1,0,1,1,1,1,0,0,0,1,0,0,1,1)$$

The first four digits in each sequence are the initial position of the feedback register.

The matrix of the cyclic permutations of S_1 is the following matrix:

$$A = \begin{bmatrix} 1&0&1&0&1&1&1&1&0&0&0&1&0&0&1 \\ 1&1&0&1&0&1&1&1&1&0&0&0&1&0&0 \\ 0&1&1&0&1&0&1&1&1&1&0&0&0&1&0 \\ 0&0&1&1&0&1&0&1&1&1&1&0&0&0&1 \\ 1&0&0&1&1&0&1&0&1&1&1&1&0&0&0 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \\ 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \\ 1&1&0&0&0&1&0&0&1&1&0&1&0&1&1 \\ 1&1&1&0&0&0&1&0&0&1&1&0&1&0&1 \\ 1&1&1&1&0&0&0&1&0&0&1&1&0&1&0 \\ 0&1&1&1&1&0&0&0&1&0&0&1&1&0&1 \\ 1&0&1&1&1&1&0&0&0&1&0&0&1&1&0 \\ 0&1&0&1&1&1&1&0&0&0&1&0&0&1&1 \end{bmatrix}$$

Or briefly:

$$A = A_1 = \begin{bmatrix} 1&0&1&0&1&1&1&1&0&0&0&1&0&0&1 \\ 1&1&0&1&0&1&1&1&1&0&0&0&1&0&0 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 0&1&0&1&1&1&1&0&0&0&1&0&0&1&1 \end{bmatrix}$$

The first row in this matrix is called ***The head row***.

If the function $h: GF(2^4) \to \$$ where:

$h(\alpha^i) = h(i) = h_i$ = [The row of the matrix A corresponding of the initial position i], then h_i is isomorphism from the additive group $(GF(2^4),+)$ on the additive group $(\$,+)$.

In this matrix the head row is:

$h(8) = S_1 = [1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1]$

And the corresponding head polynomial is:

$S_1(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^7 + x^{11} + x^{14}$, Thus:

$$A_2 = A^2 = \begin{bmatrix} 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \\ 1&1&0&0&0&1&0&0&1&1&0&1&0&1&1 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \end{bmatrix}$$

In this matrix the head row is:

$h(15) = S_9 = [1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1]$

and the corresponding head polynomial is:

$S_1^3(x) = 1 + x + x^3 + x^5 + x^6 + x^7 + x^8 + x^{12}$ Thus:

$$A_3 = A^3 = \begin{bmatrix} 1&1&0&1&0&1&1&1&1&0&0&0&1&0&0 \\ 0&1&1&0&1&0&1&1&1&1&0&0&0&1&0 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 1&0&1&0&1&1&1&1&0&0&0&1&0&0&1 \end{bmatrix}$$

In this matrix the head row is:

$h(15) = S_9 = [1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1]$

and the corresponding head polynomial is:

$S_1^3(x) = 1 + x + x^3 + x^5 + x^6 + x^7 + x^8 + x^{12}$ Thus:

$$A_4 = A^4 = \begin{bmatrix} 1&1&0&0&0&1&0&0&1&1&0&1&0&1&1 \\ 1&1&1&0&0&0&1&0&0&1&1&0&1&0&1 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \end{bmatrix}$$

In this matrix the head row is:

$h(4) = S_{10} = [1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1]$

and the corresponding head polynomial is:

$S_1^4(x) = 1 + x + x^5 + x^8 + x^9 + x^{11} + x^{13} + x^{14}$ Thus:

$$A_5 = A^5 = \begin{bmatrix} 0&1&1&0&1&0&1&1&1&1&0&0&0&1&0 \\ 0&0&1&1&0&1&0&1&1&1&1&0&0&0&1 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 1&1&0&1&0&1&1&1&1&0&0&0&1&0&0 \end{bmatrix}$$

In this matrix the head row is:

$h(5) = S_3 = [0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0]$

and the corresponding head polynomial is: $S_1^5(x) = x + x^2 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{13}$ Thus:

$$A_6 = A^6 = \begin{bmatrix} 1&1&1&0&0&0&1&0&0&1&1&0&1&0&1 \\ 1&1&1&1&0&0&0&1&0&0&1&1&0&1&0 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 1&1&0&0&0&1&0&0&1&1&0&1&0&1&1 \end{bmatrix}$$

In this matrix the head row is:

$h(10) = S_{11} = [1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1]$

and the corresponding head polynomial is: $S_1^6(x) = 1 + x + x^2 + x^6 + x^9 + x^{10} + x^{12} + x^{14}$ Thus:

$$A_7 = A^7 = \begin{bmatrix} 0&0&1&1&0&1&0&1&1&1&1&0&0&0&1 \\ 1&0&0&1&1&0&1&0&1&1&1&1&0&0&0 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 0&1&1&0&1&0&1&1&1&1&0&0&0&1&0 \end{bmatrix}$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

In this matrix the head row is:
$h(6) = S_4 = [0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1]$
and the corresponding head polynomial is: $S_1^7(x) = x^2 + x^3 + x^5 + x^7 + x^8 + x^9 + x^{10} + x^{14}$ Thus:

$$A_8 = A^8 = \begin{bmatrix} 1&1&1&1&0&0&0&1&0&0&1&1&0&1&0 \\ 0&1&1&1&1&0&0&0&1&0&0&1&1&0&1 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 1&1&1&0&0&0&1&0&0&1&1&0&1&0&1 \end{bmatrix}$$

In this matrix the head row is:
$h(12) = S_{12} = [1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0]$
and the corresponding head polynomial is: $S_1^8(x) = 1 + x + x^2 + x^3 + x^7 + x^{10} + x^{11} + x^{13}$ Thus:

$$A_9 = A^9 = \begin{bmatrix} 1&0&0&1&1&0&1&0&1&1&1&1&0&0&0 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 0&0&1&1&0&1&0&1&1&1&1&0&0&0&1 \end{bmatrix}$$

In this matrix the head row is:
$h(8) = S_5 = [1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0]$
and the corresponding head polynomial is: $S_1^9(x) = 1 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{10} + x^{11}$ Thus:

$$A_{10} = A^{10} = \begin{bmatrix} 0&1&1&1&1&0&0&0&1&0&0&1&1&0&1 \\ 0&0&1&1&1&1&0&0&0&1&0&1&1&1&0 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 1&1&1&1&0&0&0&1&0&0&1&1&0&1&0 \end{bmatrix}$$

In this matrix the head row is:
$h(11) = S_{13} = [0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1]$
and the corresponding head polynomial is: $S_1^{10}(x) = x + x^2 + x^3 + x^4 + x^8 + x^{11} + x^{12} + x^{14}$ Thus:

$$A_{11} = A^{11} = \begin{bmatrix} 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 1&0&0&1&1&0&1&0&1&1&1&1&0&0&0 \end{bmatrix}$$

In this matrix the head row is:
$h(1) = S_6 = [0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0]$
and the corresponding head polynomial is: $S_1^{11}(x) = x + x^4 + x^5 + x^7 + x^9 + x^{10} + x^{11} + x^{12}$ Thus:

$$A_{12} = A^{12} = \begin{bmatrix} 1&0&1&1&1&1&0&0&0&1&0&0&1&1&0 \\ 0&1&0&1&1&1&1&0&0&0&1&0&0&1&1 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 0&1&1&1&1&0&0&0&1&0&0&1&1&0&1 \end{bmatrix}$$

In this matrix the head row is:
$h(12) = S_{14} = [1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0]$
and the corresponding head polynomial is: $S_1^{12}(x) = 1 + x^2 + x^3 + x^4 + x^5 + x^9 + x^{12} + x^{13}$ Thus:

$$A_{13} = A^{13} = \begin{bmatrix} 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \end{bmatrix}$$

In this matrix the head row is:
$h(2) = S_7 = [0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0]$
and the corresponding head polynomial is: $S_1^{13}(x) = x^2 + x^5 + x^6 + x^8 + x^{10} + x^{11} + x^{12} + x^{13}$ Thus:

$$A_{14} = A^{14} = \begin{bmatrix} 0&1&0&1&1&1&1&0&0&0&1&0&0&1&1 \\ 0&0&1&0&1&1&1&1&0&0&0&1&0&0&1 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 1&0&1&1&1&1&0&0&0&1&0&0&1&1&0 \end{bmatrix}$$

In this matrix the head row is:
$h(9) = S_{15} = [0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1]$
and the corresponding head polynomial is: $S_1^{14}(x) = x + x^3 + x^4 + x^5 + x^6 + x^{10} + x^{13} + x^{14}$ Thus:

$$A_{15} = A^{15} = \begin{bmatrix} 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \\ 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \end{bmatrix}$$

In this matrix the head row is:
$h(3) = S_8 = [0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1]$
and the corresponding head polynomial is: $S_1^{15}(x) = x^3 + x^6 + x^7 + x^9 + x^{11} + x^{12} + x^{13} + x^{14}$ Thus: $A_{16} = A^{16} = A$.

By considering $h_0 = O$ we see that:

$$ord(A_1) = ord(A_2) = ord(A_4) = ord(A_7) = ord(A_8) = \\ = ord(A_{11}) = ord(A_{13}) = ord(A_{14}) = 15$$

According to above calculations:
The set: **A** = $\{O, A, A_2, A_3, \ldots, A_{15}\}$ is an additive group (Table 1) and the set **A*** = $\{A, A_2, A_3, \ldots, A_{15}\}$ is a multiplicative group of order 15 the identity is A_{15} (Table 2).

Then the set **A** is a representation of $GF(2^4)$.

The field F_{2^4} contains $\varphi(2^k - 1)/k = \varphi(2^4 - 1)/4 = 2$ third degree irreducible polynomials that are $f(x) = x^4 + x + 1$ and its conjugate $g(x) = x^4 + x^3 + 1$, also $g(x)$ is a prime polynomial then we can represent F_{2^4} by two different ways.

II- Suppose the matrix:

$$B = B_1 = \begin{bmatrix} 1&1&0&1&0&1&1&1&1&0&0&0&1&0&0 \\ 0&1&1&0&1&0&1&1&1&1&0&0&0&1&0 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 1&0&1&0&1&1&1&1&0&0&0&1&0&0&1 \end{bmatrix}$$

In this matrix the head row is:
$h(7) = S_2 = [1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0]$
and the corresponding head polynomial is: $S_2(x) = 1 + x + x^3 + x^5 + x^6 + x^7 + x^8 + x^{12}$ Thus:

$$B_2 = B^2 = \begin{bmatrix} 1&1&1&0&0&0&1&0&0&1&1&0&1&0&1 \\ 1&1&1&1&0&0&0&1&0&0&1&1&0&1&0 \\ -&-&-&-&-&-&-&-&-&-&-&-&-&-&- \\ 1&1&0&0&0&1&0&0&1&1&0&1&0&1&1 \end{bmatrix}$$

In this matrix the head row is:
$h(10) = S_{11} = [1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1]$
and the corresponding head polynomial is: $S_2^2(x) = 1 + x + x^2 + x^6 + x^9 + x^{10} + x^{12} + x^{14}$ Thus:

$$B_3 = B^3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ - & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

In this matrix the head row is:

$h(8) = S_5 = [1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0]$

and the corresponding head polynomial is: $S_2^3(x) = 1 + x + x^3 + x^5 + x^6 + x^7 + x^8 + x^{12}$ Thus:

$$B_4 = B^4 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ - & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

In this matrix the head row is:

$h(12) = S_{14} = [1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0]$

and the corresponding head polynomial is: $S_2^4(x) = 1 + x^2 + x^3 + x^4 + x^5 + x^9 + x^{12} + x^{13}$ Thus:

$$B_5 = B^5 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ - & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

In this matrix the head row is:

$h(3) = S_8 = [0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1]$

and the corresponding head polynomial is: $S_2^5(x) = x^3 + x^6 + x^7 + x^9 + x^{11} + x^{12} + x^{13} + x^{14}$

Thus: $B_6 = B^6 = B$.

Then the set **B** = $\{O, B_1, B_2, B_3, B_4, B_5\}$ is not an additive group because $B + B_2$ does not belongs to the set and: $ord(B_1) = ord(B_2) = ord(B_3) = ord(B_4) = 5$. Also, **B*** = $\{B_1, B_2, B_3, B_4, B_5\}$ is a multiplicative group of order 5 and the identity in their is $B_5 = A_{15}$.(Table 3).

The field F_{2^4} contains $\varphi(2^k - 1)/k = \varphi(2^4 - 1)/4 = 2$ third degree irreducible polynomials that are:

$f(x) = x^4 + x + 1$ and its conjugate $g(x) = x^4 + x^3 + 1$.

Also, $g(x)$ is a prime polynomial then we can represent the group $\{B, B_2, B_3, B_4, B_5\}$ by two different ways.

III- Suppose the matrix:

$$C = C_1 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ - & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

In this matrix the head row is:

$h(5) = S_3 = [0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0]$

And the corresponding head polynomial is:

$S_3(x) = x + x^2 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{13}$ Thus:

$$C_2 = C^2 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ - & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

In this matrix the head row is:

$h(11) = S_{13} = [0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1]$

and the corresponding head polynomial is:

$S_3^2(x) = x + x^2 + x^3 + x^4 + x^8 + x^{11} + x^{12} + x^{14}$ Thus:

$$C_3 = C^3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ - & - & - & - & - & - & - & - & - & - & - & - & - & - & - \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

In this matrix the head row is:

$h(3) = S_8 = [0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1]$

And the corresponding head polynomial is:

$S_3^3(x) = x^3 + x^6 + x^7 + x^9 + x^{11} + x^{12} + x^{13} + x^{14}$

Also, $C_4 = C^4 = C$, and we see that:

$ord(C_1) = ord(C_2) = 2$ but $ord(C_3) = 1$

Thus, we have for the sets : **C** = $\{O, C_1, C_2, C_3\}$ and **C*** = $\{O, C_1, C_2, C_3\}$. (Table 4)

IV- From the previous table we see that:

+	C_3
C_3	O

•	C_3
C_3	C_3

And the set $\{O, C_3\}$ represent the field $\{O, C_3\}$. Thus we can represent it by two different ways.

V. Results and Recommendations

1. The fields $GF(2^n)$ and their subfield can be represented by square matrices.
2. The multiplicative group $GF^*(2^n)$ and their subgroups can be represented by square matrices.
3. The equations of the degree less than or equal to *n* on $GF(2)$ can also be solved by square matrices.
4. Building encoders on the field F_q when $q \mid n$ are recommended for further study.

Appendix

Table 1: Addition on the additive group A

•	A	A_2	A_3	A_4	A_5	A_6	A_7
A	A_2	A_3	A_4	A_5	A_6	A_7	A_8
A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9
A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}
A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}
A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}
A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}
A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}
A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}
A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}	A
A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}	A	A_2
A_{11}	A_{12}	A_{13}	A_{14}	A_{15}	A	A_2	A_3
A_{12}	A_{13}	A_{14}	A_{15}	A	A_2	A_3	A_4
A_{13}	A_{14}	A_{15}	A	A_2	A_3	A_4	A_5
A_{14}	A_{15}	A	A_2	A_3	A_4	A_5	A_6
A_{15}	A	A_2	A_3	A_4	A_5	A_6	A_7

Table 2:Multiplication on the multiplicative group A*

A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}
A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}	A
A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}	A	A_2
A_{11}	A_{12}	A_{13}	A_{14}	A_{15}	A	A_2	A_3
A_{12}	A_{13}	A_{14}	A_{15}	A	A_2	A_3	A_4
A_{13}	A_{14}	A_{15}	A	A_2	A_3	A_4	A_5
A_{14}	A_{15}	A	A_2	A_3	A_4	A_5	A_6
A_{15}	A	A_2	A_3	A_4	A_5	A_6	A_7
A	A_2	A_3	A_4	A_5	A_6	A_7	A_8
A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9
A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}
A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}
A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}
A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}
A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}
A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}

Table 3:Multiplication on multiplicative group B*

+	C	C_2	C_3
C	O	C_3	C_2
C_2	C_3	O	C
C_3	C_2	C	O

•	C	C_2	C_3
C	C_2	C_3	C
C_2	C_3	C	C_2
C_3	C	C_2	C_3

Tables 4: Addition on C and multiplication on C*

ACKNOWLEDGMENT

The author express his gratitude to Prof. Abdulla Yousuf Al Hawaj, President of Ahlia University for all the support provided.

REFERENCES

1. Yang K , Kg Kim y Kumar l. d ,"Quasi – orthogonal Sequences for code - Division Multiple Access Systems ," *IEEE Trans .information theory* , Vol. 46 NO3, 200, PP 982-993
2. Jong-Seon No, Solomon W& Golomb, "Binary Pseudorandom Sequences For period 2^n-1 with Ideal Autocorrelation*," IEEE Trans. Information Theory*, Vol. 44 No 2, 1998, PP 814-817
3. Lee J.S &Miller L.E, " *CDMA System Engineering Hand Book, "* Artech House. Boston, London,1998.
4. Yang S.C,"*CDMA RF System Engineering,"* Artech House.Boston-London,1998.
5. LIDL,R.& PILZ,G., "*Applied Abstract Algebra*," Springer – Verlage New York, 1984.
6. Lidl, R. & Niderrreiter, H., " Introduction to Finite Fields and Their Application," *Cambridge university* U SA, 1994.
7. Thomson W. Judson , "*Abstract Algebra: Theory and Applications* ," Free Software Foundation,2013.
8. FRALEIGH,J.B., "A First course In Abstract Algebra, *Fourth printing. Addison-Wesley publishing company* USA,1971.
9. Mac WILIAMS,F.G& SLOANE,N.G.A., "*The Theory Of Error-Correcting Codes,"* North-Holland, Amsterdam, 2006.
10. KACAMI,T.&TOKORA, H., "Teoria Kodirovania," *Mir*(*MOSCOW*), 1978.
11. David, J., "Introductory Modern Algebra," *Clark University* USA, 2008.
12. SLOANE,N.J.A., "An Analysis Of The Stricture And Complexity Of Nonlinear Binary Sequence Generators," *IEEE Trans. Information Theory* Vol. It 22 No 6,1976, PP 732-736.

AUTHORS PROFILE

Dr. Ahmad Hamza Al Cheikha. His Research interests are Design Orthogonal sequences with variable length, Finite Fields, Linear and Non Linear codes, Co-positive Matrices and Fuzzy Sets.
(E-mail :alcheikhaa@yahoo.com).