Matrix Representation of Groups In the Finite Fields GF(p^n)

Ahmad Hamza 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(pn), 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 :**

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

or

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

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*(p^n), and their subgroups, can be represented as square matrices by m – sequences, which satisfies the multiplicative properties as a cyclic group, that is it will be useful in many other scientific branches.

Most of the existing communication devices (such as coders channels and decoders) for example, orthogonal sets in the forward and the inverse link of communication channels in the CDMA systems especially in the second (IS-95-CDMA), the third…. (CDMA200,…), the pilot channels, the Sync channels, and the Traffic channels uses computational Binary SystemF_2 due to ease of manufacture and affordability which shows how the significance of this research. This study contributes notions for making modern communication devices to be efficient, confidential and safe, although the cost may not be low, using computational $F_p$systems where p> 2, in 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 $r > 0$ such that:

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

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 nonnegative n_0 such that:

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

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 vector:

$X = (x_1, x_2, \ldots, x_n)$, when $x_i \in F_p$,

is the vector $\overline{X} = (\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})$,when

$\overline{x_i} = p - 1 - x_i$, and $-X = (-x_1, -x_2, \ldots, -x_n)$ when $-x_i = p - x_i \bmod p$. [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_p, when p is prime, with prime characteristic polynomial 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:

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

Manuscript received on July, 2014.

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

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

Theorem1.

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

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 p^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 positiveInteger *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. $(q^m-1)\mid(q^n-1)\Leftrightarrow m\mid n$ (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. Also, if $m = e = 1$, and equal to zero else where. [6]-[9]

Theorem 6. If $g(x)$ is a characteristic prime polynomial of the (H. L. R. S.) $a_0,a_1,....$of degree *k*, and α is a root of $g(x)$ in any splitting field of F_2then the general bound of the sequence is: $a_n=\sum_{i=1}^{k}C_i\left(\alpha^{p^{i-1}}\right)^n$. [11]-[13].

*** The study here, is limited to the fields Galois $GF(p^n)$, and $p>2$, then the period $r=p^k-1$ is even.**

IV. RESULTS AND DISCUSSION

A. First step

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

Proof: This sequence is periodic with period $r=p^k-1$. We suppose $\$=\{S_1,S_2,...,S_r\}$ where $S_1=(a_1a_2..a_r)$ is the sequence of the first $r=p^k-1$ bounds, and $S_2=(a_ra_1...a_{r-1}),...,\ S_r=(a_2a_3..a_ra_1)$ are all its cyclic shifts, and we suppose $O=S_0=(0.....0)$, $S=\$\cup\{S_0\}$ and if α is a root of the prime polynomial $f(x)$ and:

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

And the function: $h:GF(p^k)\rightarrow S$ as following:

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

Then *h* is one-to-one corresponding and:

$$\begin{cases} h(\alpha^i+\alpha^j)=h(\alpha^i)+h(\alpha^j) \\ h(m.\alpha^i)=m.h(\alpha^i),\quad m\in F_p \end{cases}$$

And h is Linear Transformation and isomorphism from the additive group $(GF(p^k),+)$to the additive group $(S,+)$, but $\$$ is not closed under the addition as F_{2^n} because:

for $\alpha^i\in F_{p^k}$ then: $h(\alpha^i)\neq 0\ \&\ h(-\alpha^i)=-h(\alpha^i)\neq 0$

and: $h(\alpha^i)+h(-\alpha^i)=0\notin\$$

B. Second Step

Theorem 8: Suppose $a_1,a_2,.....$ is a non zero homogeneouslinear recurring sequence of order *k* in F_p and *f*(*x*) is their primitive characteristic polynomial, S_1 is the initial bounds where $r=p^k-1$ and $\$=\{S_1,S_2,...,S_r\}$ are the all cyclic shifts. Let *A* is a matrix which its rows are elements $\$ respectively, then by $\{A^i,\ i=1,...,r\}$, or by powers of its permutations of *A*we can represent all subgroups in F_{p^k} relatively to product and addition of matrices, having the period of $S_1(x)$ and rows of A^i are the shifts to rows of *A*.

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

and the first row ω_1 in the matrix *A* then: $\omega_1=\sum_{i\in I}\alpha_i S_i\neq O$ When *I* the set of all columns in *A* which does not start by zero and the of i^{th} is $a_i\neq 0$ then $\omega_1=S_l\in\$$, because multiplying any element of

$\$$ by any element of $GF(p)$ is an element of $\$$, the sum of any two elements of $\$$ is in $\$$ and $\varpi_1 \neq 0$.

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

$$\omega_1(x) = \sum_{i\in I}\alpha_i\, S_i(x) \quad ;$$

$$\omega_2(x) = \sum_{i\in I}\alpha_{i+1}\, S_{i+1}(x) = \sum_{i\in I}\alpha_{i+1}\, x S_i(x) \quad ;....$$

$$;..., \omega_r = \sum_{i\in I}\alpha_{i+r-1}\, x^{r-1} S_i(x)$$

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

When: $S_1^2(x) \in \$(x)$, and the calculations are done by $\left(\mathrm{mod}\left(x^{p^k-1}-1\right)\right)$, And we have: $\omega_2(x) = xS_1^2(x)$; … ; $\omega_r(x) = x^{r-1}S_1^2(x)$

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

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

$$; \; A^i = \begin{bmatrix} S_1^i(x) \\ xS_1^i(x) \\ . \\ x^{r-1}S_1^i(x) \end{bmatrix}, \; i = 1,2,....,r \quad \text{When: } S_1^i(x) \in \$(x); i = 1, ..., r \,,$$

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

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

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

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

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

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

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

C. Third Step

Example 1: If α is a root of the prime polynomial $f(x) = x^2 + x + 2$ and generates $GF(3^2)$ then the then the representation of the elements of $GF(3^2)$ in F_3 is:

$\alpha \rightarrow (1) = [0\,1]$; $\alpha^5 = 2\alpha \rightarrow (5) = [0\,2]$

$\alpha^2 = 1 + 2\alpha \rightarrow (2) = [1\,2]$; $\alpha^6 = 2 + \alpha \rightarrow (6) = [2\,1]$

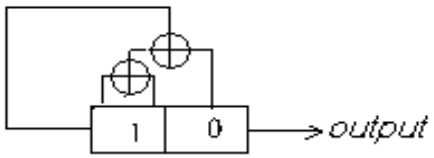
$\alpha^3 = 2 + 2\alpha \rightarrow (3) = [2\,2]$; $\alpha^7 = 1 + \alpha \rightarrow (7) = [1\,1]$

$\alpha^4 = 2 \rightarrow (4) = [2\,0]$; $\alpha^8 = 1 \rightarrow (1) = [1\,0]$

Where $(i), i = 0, 1, 2, ..., 8$ is the symbol of the sequence *i*.

The divisors of the number 8 are 1, 2, 4, and 8, consequently, $GF(3^2)$ contains four multiplicative subgroups are: <1>, $GF^*(3)$, fourth order multiplicative subgroup $= <\alpha^2>$, and $GF^*(3^2)$, and the divisors of 9 are: 1, 3, and 9 .Then $GF(3^2)$ contains three additive subgroups are: one first order additive subgroups, one third order additive subgroups, and one ninth order additive subgroups, consequently the field $GF(3^2)$ contains two subfields are : $GF(3)$ and the same $GF(3^2)$. Suppose the Linear Recurring Sequence be:

$$a_{n+2} + a_{n+1} + 2a_n = 0 \quad or \quad a_{n+2} = 2a_{n+1} + a_n \qquad (5)$$



Figure(1): Linear feedback register of degree2 generates sequence (5)

With the characteristic equation $x^2 + x + 2 = 0$ and the characteristic polynomial $f(x) = x^2 + x + 2$,which is a prime and generates F_{3^2} and if $\bar{x} = \alpha \in GF(3^2)$ is a root of $f(x)$ then the solutions of characteristic equation are $\{\alpha^n, \alpha^{3n}\}$.

The general solution of equation (1) is given by

$$a_n = 2\alpha \cdot \alpha^n + (1+\alpha) \cdot \alpha^{3n} \,,$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

and the sequence is periodic with the period $3^2-1=8$.
For the initial position: $a_1=0, a_2=1$, then
$S_1=(0\,1\,2\,2\,0\,2\,1\,1)$ and by the cyclic permutationsonS_1
we have $\$=\{S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8\}$where:
$S_2=(1\,0\,1\,2\,2\,0\,2\,1)$; $S_3=(1\,1\,0\,1\,2\,2\,0\,2)$; $S_4=(2\,1\,1\,0\,1\,2\,2\,0)$
$S_5=(0\,2\,1\,1\,0\,1\,2\,2)$; $S_6=(2\,0\,2\,1\,1\,0\,1\,2)$; $S_7=(2\,2\,0\,2\,1\,1\,0\,1)$
$S_8=(1\,2\,2\,0\,2\,1\,1\,0)$
The first two digits in each sequence are the initial position of the feedback register.
In this example the resulting sequences is:
0 1 2 2 0 2 1 1 0 1 2 2 0 2 …
The matrix *A* of the cyclic permutations of S_1 is:

$$B_1=A=\begin{bmatrix}0&1&2&2&0&2&1&1\\1&0&1&2&2&0&2&1\\1&1&0&1&2&2&0&2\\2&1&1&0&1&2&2&0\\0&2&1&1&0&1&2&2\\2&0&2&1&1&0&1&2\\2&2&0&2&1&1&0&1\\1&2&2&0&2&1&1&0\end{bmatrix}$$

Or briefly: $B_1=\begin{bmatrix}0&1&2&2&0&2&1&1\\1&0&1&2&2&0&2&1\\-&-&-&-&-&-&-&-\\1&2&2&0&2&1&1&0\end{bmatrix}$

The first row in this matrix is called ***The head row***.
If the function $h:GF(3^2)\to\$$ 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 $(GF(3^2),+)$ on the group $(\$,+)$.

I- In this matrix the head row is: $S_1=[\,0\,1\,2\,2\,0\,2\,1\,1\,]$ and the head polynomial is:
$h(1)=S_1(x)=x+2x^2+2x^3+2x^5+x^6+x^7$. Thus

$$B_2=B_1^2=\begin{bmatrix}2&2&0&2&1&1&0&1\\2&2&0&2&2&1&1&0\\-&-&-&-&-&-&-&-\\2&0&2&1&1&0&1&0\end{bmatrix}$$

In this matrix the head row is: $h(3)=S_7=[2\,2\,0\,2\,1\,1\,0\,1]$ and the corresponding head polynomial is: $S_7(x)=2+2x+2x^3+x^4+x^5+x^7$, Thus

$$B_3=B_1^3=\begin{bmatrix}0&2&1&1&0&1&2&2\\2&0&2&1&1&0&1&2\\-&-&-&-&-&-&-&-\\2&1&1&0&1&2&2&0\end{bmatrix}$$

In this matrix the head row is: $h(5)=S_5=[0\,2\,1\,1\,0\,1\,2\,2]$ and the corresponding head polynomial is: $S_5(x)=2x+x^2+x^3+x^5+2x^6+2x^7$, Thus

$$B_4=B_1^4=\begin{bmatrix}1&1&0&1&2&2&0&2\\2&1&1&0&1&2&2&0\\-&-&-&-&-&-&-&-\\1&0&1&1&2&0&2&1\end{bmatrix}$$

In this matrix the head row is: $h(7)=S_3=[1\,1\,0\,1\,2\,2\,0\,2]$ and the corresponding head polynomial is: $S_3(x)==1+x+x^3+2x^4+2x^5+2x^7$, Thus $B_1^5=B_1$ and the set $B^*=\{B_1,B_2,B_3,B_4\}$ is fourth order multiplicative group and the set
$B=\{O,B_1,B_2,B_3,B_4\}$ is not additive group as is shown by the table 1.
Then *B* is not a field, and we see that:
$ord(B_1)=ord(B_3)=4$

II- We suppose that;

$$C_1=\begin{bmatrix}2&2&0&2&1&1&0&1\\1&2&1&0&2&1&1&0\\-&-&-&-&-&-&-&-\\2&0&2&1&1&0&1&2\end{bmatrix}$$

In this matrix the head row is: $h(3)=S_7=[2\,2\,0\,2\,1\,1\,0\,1]$ and the corresponding head polynomial is: $S_7(x)=2+2x+2x^3+x^4+x^5+x^7$, Thus

$$C_2=C_1^2=\begin{bmatrix}1&1&0&1&2&2&0&2\\2&1&1&0&1&2&2&0\\-&-&-&-&-&-&-&-\\1&0&1&1&2&0&2&1\end{bmatrix}$$

In this matrix the head row is: $h(7)=S_3=[1\,1\,0\,1\,2\,2\,0\,2]$ and the corresponding head polynomial is: $S_3(x)==1+x+x^3+2x^4+2x^5+2x^7$, Thus $C_1^3=C_1$.
And the $C^*=\{C_1,C_2\}$ is second order multiplicative group and $C=\{O,C_1,C_2\}$ is an additive group as showing in the table2.
We see that *C* is a representation of the subfield $F_3=GF(3^2)$ and: $ord(C_1)=2$ and $ord(C_2)=1$.

III. We suppose that:

$$D_1=\begin{bmatrix}1&0&1&2&2&0&2&1\\1&1&0&1&2&2&0&2\\-&-&-&-&-&-&-&-\\0&1&2&2&0&2&1&1\end{bmatrix}$$

In this matrix the head row is: $h(8)=S_2=[1\,0\,1\,2\,2\,0\,2\,1]$ and the corresponding head polynomial is: $S_2(x)=1+x^2+2x^3+2x^4+2x^6+x^7$, Thus

$$D_2=D_1^2=\begin{bmatrix}0&1&2&2&0&2&1&1\\1&0&1&2&2&0&2&1\\-&-&-&-&-&-&-&-\\1&2&2&0&2&1&1&0\end{bmatrix}$$

In this matrix the head row is: $h(1)=S_1=(0\,1\,2\,2\,0\,2\,1\,1]$

and the corresponding head polynomial is: $S_1(x) = x + 2x^2 + 2x^3 + 2x^5 + x^6 + x^7$, Thus

$$D_3 = D_1^3 = \begin{bmatrix} 1 & 2 & 2 & 0 & 2 & 1 & 1 & 0 \\ 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 \\ - & - & - & - & - & - & - & - \\ 2 & 2 & 0 & 2 & 1 & 1 & 0 & 1 \end{bmatrix}$$

In this matrix the head row is: $h(2) = S_8 = [1\,2\,2\,0\,2\,1\,1\,0]$ and the corresponding head polynomial is: $S_8(x) = 1 + 2x + 2x^2 + 2x^4 + x^5 + x^6$, Thus

$$D_4 = D_1^4 = \begin{bmatrix} 2 & 2 & 0 & 2 & 1 & 1 & 0 & 1 \\ 1 & 2 & 2 & 0 & 2 & 1 & 1 & 0 \\ - & - & - & - & - & - & - & - \\ 2 & 0 & 2 & 1 & 1 & 0 & 1 & 2 \end{bmatrix}$$

In this matrix the head row is: $h(3) = S_7 = [2\,2\,0\,2\,1\,1\,0\,1]$ and the corresponding head polynomial is: $S_7(x) = 2 + 2x + 2x^3 + x^4 + x^5 + x^7$, Thus

$$D_5 = D_1^5 = \begin{bmatrix} 2 & 0 & 2 & 1 & 1 & 0 & 1 & 2 \\ 2 & 2 & 0 & 2 & 1 & 1 & 1 & 1 \\ - & - & - & - & - & - & - & - \\ 0 & 2 & 1 & 1 & 0 & 1 & 2 & 2 \end{bmatrix} 0$$

In this matrix the head row is:
$h(4) = S_6 = [2\,0\,2\,1\,1\,0\,1\,2]$
and the corresponding head polynomial is: $S_6(x) = 2 + 2x^2 + x^3 + x^4 + x^6 + 2x^7$, Thus

$$D_6 = D_1^6 = \begin{bmatrix} 0 & 2 & 1 & 1 & 0 & 1 & 2 & 2 \\ 2 & 0 & 2 & 1 & 1 & 0 & 1 & 2 \\ - & - & - & - & - & - & - & - \\ 2 & 1 & 1 & 0 & 1 & 2 & 2 & 0 \end{bmatrix}$$

In this matrix the head row is:
$h(5) = S_5 = [0\,2\,1\,1\,0\,1\,2\,2]$
and the corresponding head polynomial is: $S_5(x) = 2x + x^2 + x^3 + x^5 + 2x^6 + 2x^7$, Thus

$$D_7 = D_1^7 = \begin{bmatrix} 2 & 1 & 1 & 0 & 1 & 2 & 2 & 0 \\ 0 & 2 & 1 & 1 & 0 & 1 & 2 & 2 \\ - & - & - & - & - & - & - & - \\ 1 & 1 & 0 & 1 & 1 & 2 & 0 & 2 \end{bmatrix}$$

In this matrix the head row is: $h(6) = S_4 = [2\,1\,1\,0\,1\,2\,2\,0]$ and the corresponding head polynomial is: $S_4(x) = 2 + x + x^2 + x^4 + 2x^5 + 2x^6$, Thus

$$D_8 = D_1^8 = \begin{bmatrix} 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 \\ 2 & 1 & 1 & 0 & 1 & 2 & 2 & 0 \\ - & - & - & - & - & - & - & - \\ 1 & 0 & 1 & 1 & 2 & 0 & 2 & 1 \end{bmatrix};$$

$D_9 = D_1$

In this matrix the head row is: $h(7) = S_3 = [1\,1\,0\,1\,2\,2\,0\,2]$ and the corresponding head polynomial is: $S_3(x) = = 1 + x + x^3 + 2x^4 + 2x^5 + 2x^7$

.

And $D^* = \{D_1, D_2, D_3, D_4, D_5, D_6, D_7, D_8\}$ is a multiplicative group of order 8, and $D = \{O, D_1, D_2, D_3, D_4, D_5, D_6, D_7, D_8\}$ is additive group as shown in table 3.

Consequently, D is a field and representation of the field $GF(3^2)$.

The field $GF(3^2)$ contains $\varphi(3^2 - 1)/2 = 2$ third degree irreducible polynomials are $f(x) = x^2 + x + 2$ and $g(x) = x^2 + 2x + 2$.

V. RESULTS AND RECOMMENDATIONS

1. The fields $GF(p^n)$ and their subfield can be represented by square matrices.
2. The multiplicative group $GF^*(p^n)$ and their subgroups can be represented by square matrices.
3. The equations of the degree less than or equal to n on $GF(p)$ 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: The Addition in B^*

+	B_1	B_2	B_3	B_4
B_1	B_3	$\notin B$	O	$\notin B$
B_2	$\notin B$	B_4	$\notin B$	O
B_3	O	$\notin B$	B_1	$\notin B$
B_4	$\notin B$	O	$\notin B$	B_2

Table 2: The Addition in C^*

+	C_1	C_2
C_1	C_2	O
C_2	O	C_1

Table 3: Addition in D^*

+	□	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8
□	□	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8
D_1	D_1	D_5	D_3	D_8	D_7	□	D_4	D_6	D_2
D_2	D_2	D_3	D_6	D_4	D_1	D_8	□	D_5	D_7
D_3	D_3	D_8	D_4	D_7	D_5	D_2	D_1	□	D_6
D_4	D_4	D_7	D_1	D_5	D_8	D_6	D_3	D_2	□
D_5	D_5	□	D_8	D_2	D_6	D_1	D_7	D_4	D_3
D_6	D_6	D_4	□	D_1	D_3	D_7	D_2	D_8	D_5
D_7	D_7	D_6	D_5	□	D_2	D_4	D_8	D_3	D_1
D_8	D_8	D_2	D_7	D_6	□	D_3	D_5	D_1	D_4

ACKNOWLEDGMENT

The author express his gratitude to Prof. Abdulla Yousuf AlHawaj, 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 2n-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.& Niderreiter, H., "Introduction to Finite Fields and Their Application," Cambridge university USA, 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., "TeoriaKodirovania,"Mir(MOSCOW), 1978.
11. David, J., "Introductory Modern Algebra, "Clark University U. S. A, 2008.
12. SLOANE,N.J.A., "An Analysis Of The Stricture And Complexity Of Nonlinear Binary Sequence Generators," IEEE Trans. Information TheoryVol. It 22 No 6,1976, PP 732-736.
13. Al Cheikha A. H. " Matrix Representation of Groups in the finite Fields GF(2n) ," International Journal of Soft Computing and Engineering, Vol. 4, Issue 2, May 2014, PP 118-125.

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.