BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Electrical Science & Engineering
https://ojs.bilpublishing.com/index.php/ese

ARTICLE

Finding Non-liner Register on Binary M-Sequence Generating Binary Multiplication Sequence

Ahmad Al Cheikha[1*] Diana Mokayes[2]

1. Department of Maths and Science, Ahlia University, Bahrain
2. Mechatronics Department, Tishreen University, Syria

ARTICLE INFO

Article history
Received: 30 October 2021
Accepted: 11 November 2021
Published Online: 15 November 2021

Keywords:
Linear sequences
Finite field
linear feedback shift register
Orthogonal sequence
Linear equivalent
Complexity

ABSTRACT

In the current time there is an important problem that is for a received linear or nonlinear binary sequence $\{z_n\}$ how we can find the nonlinear feedback shift register and its linear equivalent which generate this sequence. The linear orthogonal sequences, special M-Sequences, play a big role in these methods for solving this problem. In the current research trying give illuminations about the methods which are very useful for solving this problem under short sequences, and study these methods for finding the nonlinear feedback shift register of a multiplication sequence and its linear equivalent feedback shift register of a received multiplication binary sequence $\{z_n\}$ where the multiplication on *h* degrees of a binary linear sequence $\{a_n\}$, or finding the equivalent linear feedback shift register of $\{z_n\}$, where the sequence $\{z_n\}$of the form M-sequence, and these methods are very effectively. We can extend these methods for the large sequences using programming and modern computers with large memory.

1. Introduction

Sloane, N.J.A., discuses that the multiplication binary sequence {*zn*} on *h* degrees of {*an*} which has the *r* complexity the *r* complexity, the complexity of {zn} can't be exceeded;

$$ {}_rN_h = \binom{r}{1} + \binom{r}{2} + \ldots + \binom{r}{h} . \quad (1)\ [1\text{-}2] $$

Al Cheikha A. H., & Mokayes D., studied the construction of the multiplication Mp-sequences and their complexities, periods, and the lengths of the linear equivalents of these multiplication sequences, where the multiplication will be on one Mp-sequence or on more than one binary sequence [3-8].

Al Cheikha A. H., & Omar Ebtisam Haj, studied the construction of the multiplication binary M-sequences, Mp-Sequences and their reciprocal sequences and their complexities, periods, and the lengths of the linear equivalents of these multiplication sequences, where the multiplication will be on one Mp-sequence or on more than one binary sequence [9].

Al Cheikha A. H., studied the construction of the multiplication binary M-sequences and their complexities, periods, and the lengths of the linear equivalents of these multiplication sequences, where the multiplication will be on one Mp-sequence or on more than one binary sequence [10-14].

Orthogonal Sequences are used widely in the systems communication channels as in the forward links for mixing the information on connection and as in the backward

**Corresponding Author:*
Ahmad Al Cheikha,
Department of Maths and Science, Ahlia University, Bahrain;
Email: alcheikhaa@yahoo.com

 DOI: https://doi.org/10.30564/ese.v3i2.4036

links of these channels to sift this information which transmitted and the receivers get the information in a correct form, especially in the pilot channels, the Sync channels, and the Traffic channel [14-18].

In current article we try to solve the problem; we received the binary sequence $\{z_n\}$, where $\{z_n\}$ is a linear or nonlinear binary sequence then how we can find the basic original binary sequence $\{an\}$ which is under the multiplication operation and the multiplication operation lead to the sequence $\{zn\}$.

It is the inverse problem of finding the sequence $\{z_n\}$ where $\{an\}$ is known.

2. Research Method and Materials

2.1 M- Linear Recurring Sequences

The sequence $\{sn\}$ of the form

$$\begin{aligned} s_{n+k} &= \eta_{k-1}s_{n+k-1} + \eta_{k-2}s_{n+k-2} + ... + \\ &\quad \eta_0 s_n + \eta; \eta \,\&\, \eta_i \in F_2, i = 0,1,...,k-1 \\ or \qquad s_{n+k} &= \sum_{i=0}^{k-1} \eta_i s_{n+i} + \eta \end{aligned} \tag{2}$$

where, $\eta, \eta_0, \eta_1, ..., \eta_{k-1}$ are in the field F_2={0,1} and k is a positive integer is called a binary linear recurring sequence of complexity or order k, *if* $\eta = 0$ then the sequence is called a homogeneous linear recurring sequence (H.L.R.S), in other case the sequence is called non-homogeneous linear homogeneous sequence, the vector $(s_0, s_1, ..., s_{k-1})$ is called the initial vector and the characteristic equation of the sequence is;

$$f(x) = x^k + \eta_{k-1}x^{k-1} + ... + \eta_1 x + \eta_0 \tag{3}$$

We are limited in our article to η_0=1 and the all sequences are binary.

2.2 Definitions and Theorems

Definition 1.

The ultimately sequence $s_0, s_1, \cdots$ in F_2 with the smallest natural number $r \neq 0$ is called periodic with the period r *iff*:

$s_{n+r} = s_n \;\; ; \;\; n = 0, 1, ...$ [2-5]

Definition 2.

The linear register of a linear sequence is a linear feedback shift register with only addition circuits and the number in its output in the impulse n equal to the general term of the sequence $\{an\}$ and the register denoted as LFSR [3].

Definition 3.

The complement of the binary vector $X = (x_1, x_2, ..., x_n)$, $x_i \in F_2$ is the vector $\overline{X} = (\overline{x_1}, \overline{x_2}, ..., \overline{x_n})$, where:

$$\overline{x_i} = \begin{cases} 1 & if \quad x_i = 0 \\ 0 & if \quad x_i = 1 \end{cases} \tag{4}$$ [3,5-8]

Definition 4.

Suppose $x = (x_0, x_1, ..., x_{n-1})$ and $y = (y_0, y_1, ..., y_{n-1})$ are two binary vectors of the length n on F_2. The coefficient of correlations function of x and y, denoted by Rx,y, is

$$R_{x,y} = \sum_{i=0}^{n-1} (-1)^{x_i + y_i} \tag{5}$$

Where $xi + yi$ is computed *mod* 2. It is equal to the number of agreements components minus the number of disagreements corresponding to components or if $x_i, y_i \in \{1, -1\}$ (usually, replacing in binary vectors x and y each "1" by "1*= -1" and each "0" by "0* = 1") then

$$R_{x,y} = \sum_{i=0}^{n-1} x_i^* y_j^* \tag{6}$$ [2-10]

Definition 5.

The two binary vectors $x = (x_0, x_1, ..., x_{n-1})$ and $y = (y_0, y_1, ..., y_{n-1})$ are orthogonal iff;

$$\left| R_{x,y} \right| \leq 1 \tag{7}$$ [11-13]

Definition 6.

The set G, where $G = \{X; X = (x_0, x_1, ..., x_{n-1}), x_i \in F_2, i = 0,1,...,n-1\}$ is orthogonal iff the following two conditions are satisfied:

$$1.\ \forall X \in G, \left| \sum_{i=0}^{n-1} x_i^* \right| \leq 1, \ or \ \left| R_{x,0} \right| \leq 1. \tag{8}$$

$$2.\ \forall X, Y \in G (X \neq Y), \left| \sum_{i=0}^{n-1} x_i^* y_i^* \right| \leq 1 \ or \ \left| R_{x,y} \right| \leq 1. \tag{9}$$

That is, the absolute value of "the number of agreements minus the number of disagreements" is less than or equals one [6,9].

Definition 7. (Euler function φ).

$\varphi(n)$ is the number of the all-natural numbers that are relatively prime with n [11-14].

Definition 8.

Inverse problem: Finding the sequence $\{an\}$ which $\{zn\}$ is a linear or multiplication sequence on it and it is one of the issues at present and it requires a solutions [10].

Theorem 9.

If $g(x)$ is a characteristic prime polynomial of the (H. L. R. S.), $s_0, s_1, \cdots$ of degree k, and α is a root of $g(x)$ in any splitting field of F_2 then the general term of this sequence is:

DOI: https://doi.org/10.30564/ese.v3i2.4036

$$s_n = \sum_{i=1}^{k} C_i \left(\alpha^{2^{i-1}} \right)^n \quad (10)\ [6,12]$$

Theorem10.

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 [8,14-18].

***** The study here is limited to the finite fields of the form F_{2^k}, then the period of M-Sequence is of the form $r = 2^k - 1$.

3. Results and Discussion

Strategies finding the origin nonlinear feedback shift register and linear equivalent for nonlinear sequences.

Our strategies here as the method of the factorization natural number to their prime factors and If the origin feedback shift register of the sequence $\{z_n\}$ is a linear or nonlinear then we can accomplished it as the following:

1) If the period of the sequence $\{z_n\}$ is of the form $r = 2k\text{-}1$ and the set of all periodic permutations of one period of the sequence $\{z_n\}$ is orthogonal then the sequence $\{z_n\}$ is a M-Sequence and their feedback shift register is a linear, its characteristic polynomial is comfortable with a prime polynomial of degree k, and we can find it through the first k terms of the sequence $\{z_n\}$ by finding the coefficients of the characteristic equation using the recurrent sequence;

$$z_{n+k} + \lambda_{k-1} z_{n+k-1} + \ldots + \lambda_1 z_{n+1} + z_n = 0 \quad (11)$$

In other cases, if $r = 2k\text{-}1$ and the set of all periodic permutations of one period of the sequence $\{z_n\}$ is not orthogonal then we can go to the second step which we can make it by one of the two following strategies namely 2 or 3;

2) We find the origin sequence binary recurring M-Sequence $\{an\}$ with the complexity k and the initial vector $\alpha_0, \alpha_1, \ldots, \alpha k\text{-}_1$ (and the best try; $\alpha_0, \alpha_1, \ldots, \alpha k\text{-}_1 = z_0, z_1, \ldots, zk\text{-}_1$ respectively), the number of degrees h (where $h = 2,3,..,k$ starting with 2 until we come to the sequence $\{z_n\}$ or by inverse starting with $h = k$ until we come to the sequence $\{z_n\}$) and the terms (which they are under the multiplication operation) are sufficient for finding the nonlinear feedback shift register which will be generate the nonlinear sequence $\{z_n\}$.

The value h is one value between 2 and k and we need take the all prime polynomials of degree k and for each of them we will try, one by one, give h the values from 2 to k until we get the comfortable prime polynomial, h and the terms under the multiplication operation of the sequence $\{an\}$ will give us the sequence $\{z_n\}$, after that we can find the general term of the sequence $\{z_n\}$ which will define the length of the linear equivalent and through element the sequence $\{z_n\}$ by solving one algebraic linear system.

3) If the period of the sequence $\{z_n\}$ is of the form $r = 2k\text{-}1$ or divides it and the set of all periodic permutations of one period of the sequence $\{z_n\}$ is not orthogonal then the sequence $\{z_n\}$ is nonlinear, not M-Sequence and their equivalent linear feedback shift register comfortable with the first m terms in the sequence $\{z_n\}$, we can find the coefficients of the characteristic equation of the equivalent linear feedback shift register as following;

$$x^m + \mu_{m-1} x^{m-1} + \ldots + \mu_1 x + 1 = 0 \quad (12)$$

of the recurrent sequence;

$$y_{m+k} + \mu_{k-1} y_{m+k-1} + \ldots + \mu_1 y_{m+1} + y_m = 0 \quad (13)$$

Where m is one value between $\binom{k}{1} + \binom{k}{2}$ and ${}_kN_k = \binom{k}{1} + \binom{k}{2} + \ldots + \binom{k}{k} = \sum_{i=1}^{k} \binom{k}{i}$ starting through $m = \binom{k}{1} + \binom{k}{2}$ until we coming (and maybe with some shifting of the indexes) to the sequence $\{yn\} = \{z_n\}$ or by inverse starting with $h =$ until (and maybe with some shifting of the indexes) we coming to the sequence $\{yn\} = \{z_n\}$), thus, we can go to finding the equivalent feedback shift register generating the sequence $\{z_n\}$ specially, m the complexity of the equivalent linear register of the sequence $\{z_n\}$.

Finding h: As very known that $m \leq \binom{k}{1} + \ldots + \binom{k}{h} = {}_kN_h$ then h is larger than or equal to j where j is the smallest natural number for $m \leq \binom{k}{1} + \ldots + \binom{k}{j} = {}_kN_j$ and if $m = \binom{k}{1} + \binom{k}{2}$ then $h = 2$ or 3.

Usually, $h = j$ or $j+1$. We will try solve some problems through the two strategies 2 and 3.

Example 1.

Suppose the following sequence $\{sn\}$;

0 1 0 0 1 1 0 1 0 1 1 1 1 0 0, 0 1 0 0 1 1 0 1 0 1 0 0 1 1 0, … (14)

We can look that the sequence is a periodic sequence with the period $r = 2^4 - 1 = 15$, here k = 4, and the set of the all cyclic permutations of one period is $S = \{ m_0, m_1, \ldots, m_{14} \}$ is;

$m_0 =$ 0 1 0 0 1 1 0 1 0 1 1 1 1 0 0

$xm_1 =$ 0 0 1 0 0 1 1 0 1 0 1 1 1 1 0

m_2 = 0 0 0 1 0 0 1 1 0 1 0 1 1 1 1
m3 = 1 0 0 0 1 0 0 1 1 0 1 0 1 1 1
m4 = 1 1 0 0 0 1 0 0 1 1 0 1 0 1 1
m5 = 1 1 1 0 0 0 1 0 0 1 1 0 1 0 1
m6 = 1 1 1 1 0 0 0 1 0 0 1 1 0 1 0
m7 = 0 1 1 1 1 0 0 0 1 0 0 1 1 0 1
m_8 = 1 0 1 1 1 1 0 0 0 1 0 0 1 1 0
m_9 = 0 1 0 1 1 1 1 0 0 0 1 0 0 1 1
m_{10} = 1 0 1 0 1 1 1 1 0 0 0 1 0 0 1
m_{11} = 1 1 0 1 0 1 1 1 1 0 0 0 1 0 0
m_{12} = 0 1 1 0 1 0 1 1 1 1 0 0 0 1 0
m_{13} = 0 0 1 1 0 1 0 1 1 1 1 0 0 0 1
m_{14} = 1 0 0 1 1 0 1 0 1 1 1 1 0 0 0

we can check that each m_i, i = 0,1,…, 14 has 8 of the "1" and 7 of the "0" and $m_i + m_j \in S, mod\ 2$, for example;

$$m_2 + m_9 = 010011010111100 = m_0$$

Thus, S is an orthogonal set.

There are to ways for finding the linear shift register of the sequence;

First way:

There are only tow prime polynomials of degree 4 are; $f(x) = x^4 + x + 1$ and its reciprocal $g(x) = x^4 + x^3 + 1$ and we will check each of them if can be generate this sequence (with some shift of the indexes).

a) For the prime polynomial $g(x) = x^4 + x^3 + 1$ which corresponding with the recurrent sequence $y_{n+4} + y_{n+3} + y_n = 0$ or $y_{n+4} = y_{n+3} + y_n$ and their comfortable linear shift register for the first initial vector(0 1 1 0)is the following;

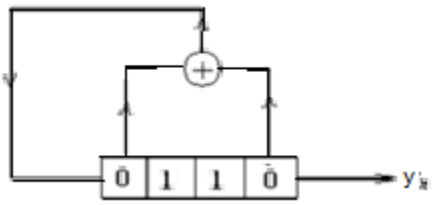

Figure 1. Linear feedback shift register with 4 complexity over F_2

This feedback shift register generates the following periodic sequence;

0 1 1 0 0 1 0 0 0 1 1 1 1 0 1, 0 1 1 0 0 1 0 0 0 1 1 1 1 0 1 (15)

And we can see that this sequence is not the same of received sequence.

b) For the prime polynomial $f(x) = x^4 + x + 1$ which corresponding with the recurrent sequence $y_{n+4} + y_{n+1} + y_n = 0$ or $y_{n+4} = y_{n+1} + y_n$ and their comfortable linear shift register for the first initial vector(0 1 1 0)is the following;

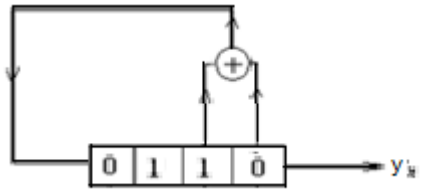

Figure 2. Linear feedback shift register with 4 complexity over F_2

This feedback shift register generates the following periodic sequence;

0 1 1 0 1 0 1 1 1 1 0 0 0 1 0 0 1 1 0 1 0 1 1 1 1 0 0 0 1 0 … (16)

And we can see that this sequence is the same of the received sequence with shift of the index by 14.

Second way:

Suppose the characteristic equation is of the form; $x^4 + \alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + 1 = 0$ and the recurrent formula is the following; $y_{n+4} + \alpha_3 y_{n+3} + \alpha_2 y_{n+2} + \alpha_1 y_{n+1} + 1 y_n = 0$, and y_0= 0, y_1 = 1, y_2= 0, y_3= 0, y_4= 1, y_5= 1, y_6= 0, y_7=1. Thus;

$$for\ n = 0 \Rightarrow y_4 + \alpha_3 y_3 + \alpha_2 y_2 + \alpha_1 y_1 + 1 y_0 = 0$$

$$for\ n = 1 \Rightarrow y_5 + \alpha_3 y_4 + \alpha_2 y_3 + \alpha_1 y_2 + 1 y_1 = 0$$

$$for\ n = 2 \Rightarrow y_6 + \alpha_3 y_5 + \alpha_2 y_4 + \alpha_1 y_3 + 1 y_2 = 0$$

$$for\ n = 3 \Rightarrow y_7 + \alpha_3 y_6 + \alpha_2 y_5 + \alpha_3 y_4 + 1 y_3 = 0$$

From the first three equations we have; $\alpha_3 = 0, \alpha_2 = 0, \alpha_1 = 1$ and the characteristic equation is $x^4 + x + 1 = 0$ and the recurrent equation is; $y_{n+4} + y_{n+1} + y_n = 0$ and it is the same what we get in the first way.

Example 2.

Given the following received periodic sequence $\{z_n\}$;

0 0 1 0 1 0 1 1 0 0 0 0 0 0 0, 0 0 1 0 1 0 1 1….. (17)

The period of the sequence is $r = 2^4$-1 = 15 and as showing is not orthogonal that is the sequence $\{z_n\}$ is nonlinear sequence and we need find the nonlinear feedback shift register and the linear equivalent which generates it that are; origin sequence $\{a_n\}$, the terms of it which they are under the multiplication operation, finding *h* the number of these terms which under the multiplication operations, and the linear equivalent to the nonlinear register.

There are only two prime polynomials of degree 4 they are; $g(x) = x^4 + x^3 + 1$ and $f(x) = x^4 + x + 1$.

We will study the nonlinear sequences generated by given nonlinear feedback shift register corresponding to the polynomials under the multiplication operation on two degrees, three degrees, and four degrees for each of them one by one.

DOI: https://doi.org/10.30564/ese.v3i2.4036

First step.

For the first polynomial $g(x) = x^4 + x^3 + 1$ and the origin sequence $\{a_n\}$ generated with the characteristic polynomial $g(x)$, the initial vector (0010) and the sequence is under the multiplication operation.

The origin sequence $\{a_n\}$ which has $g(x)$ as a characteristic polynomial and satisfies the recurrent formula $a_{n+4} + a_{n+3} + a_n = 0$ is orthogonal and periodic with the period $r = 2^4$-1=15 and is showing in the Figure 3;

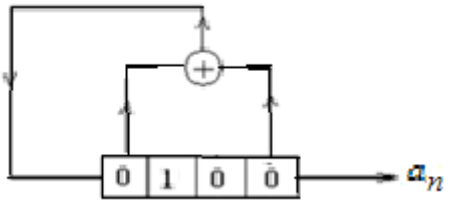

Figure 3. Linear feedback shift register with 4 complexity over F_2

And it is;

0 0 1 0 0 0 1 1 1 1 0 1 0 1 1, 0 0 1 0 0 0 1 1……. (18)

Suppose $u_n^{(i,j)}$ is the nonlinear sequence generated under the multiplication operation on the tow degrees i and j of the feedback shift register, and we have $h = 2$;

$u_n^{(0,1)}$ = 0 0 0 0 0 0 1 1 1 0 0 0 0 1 0 0 0 0 0 0 0 1…..

$u_n^{(0,2)}$ = 0 0 0 0 0 0 1 1 0 1 0 1 0 0 0 0 0 0 0 …..

$u_n^{(0,3)}$ = 0 0 0 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 0 ……

$u_n^{(1,2)}$ = 0 0 0 0 0 1 1 1 0 0 0 0 1 0 0 0 0 0 0 …..

$u_n^{(1,3)}$ = 0 0 0 0 0 0 1 1 0 1 0 0 0 0 0 0 0 0 0 …..

$u_n^{(2,3)}$ = 0 0 0 0 1 1 10 0 0 0 1 0 0 0 0 0 0 0 0 …..

Thus, no any of the previously sequences is equal to the sequence $\{z_n\}$.

Second step.

For the polynomial $f(x) = x^4 + x + 1$ the origin sequence $\{b_n\}$ generated with the characteristic function $f(x)$ and has the initial vector (0010) and the sequence is under the multiplication operation.

The origin sequence $\{b_n\}$ which has $f(x)$ as a characteristic polynomial and satisfies the recurrent formula

$b_{n+4} + b_{n+1} + b_n = 0$ is orthogonal and periodic with the period $r = 2^4$-1=15 and is showing in the Figure 4;

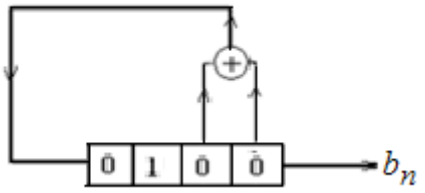

Figure 4. Linear feedback shift register generating the sequence $\{b_n\}$

And it is;

0 0 1 0 0 1 1 0 1 0 1 1 1 1 0, 0 0 1 0 0 1 1 0 1 0……. (19)

Suppose $w_n^{(i,j)}$ is the nonlinear sequence generated under the multiplication operation on the tow cells i and j of the feedback shift register, and we have $h = 2$;

$w_n^{(0,1)}$ = 0 0 0 0 0 1 0 0 0 0 1 1 1 0 0…..

$w_n^{(0,2)}$ = 0 0 0 0 0 0 1 0 1 0 1 1 0 0 0…..

Thus, we can see that $w_n^{(0,2)}$ is a permutation of $\{z_n\}$ by 4 cyclic and the sequence is a nonlinear sequence over two degrees which are the first and the third degrees of the linear shift register of the sequence $\{b_n\}$ and Figure 5 showing the nonlinear feedback shift register for the sequence;

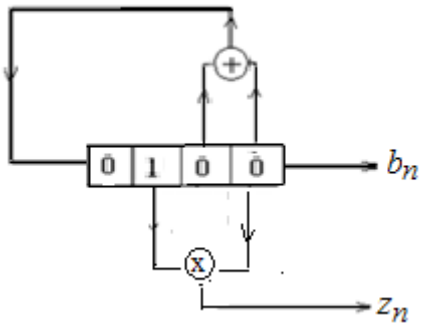

Figure 5. Nonlinear feedback shift register generating the sequence $\{z_n\}$

We can find the linear equivalent of the sequence by other way through the sequence $\{b_n\}$as following;

The sequence $\{b_n\}$satisfies the recurrent formula $b_{n+4} + b_{n+1} + b_n = 0$ *or* $b_{n+4} = b_{n+1} + b_n$ and its characteristic equation is $x^4 + x + 1 = 0$ and $f(x) = x^4 + x + 1$ is a prime polynomial, if β is a root of the characteristic equation then the roots of the characteristic equation (in F_2^4) are $\beta, \beta^2, \beta^4, \beta^8$ and the general solution of the characteristic equation which that is the general term of the sequence $\{bn\}$is;

 DOI: https://doi.org/10.30564/ese.v3i2.4036

$$b_n = A_1\beta^n + A_2\beta^{2n} + A_3\beta^{4n} + A_4\beta^{8n} \quad \text{o r}$$

$$b_n = A_1\beta^n + A_2\beta^{2n} + A_3(\beta+1)^n + A_4(\beta^2+1)^n$$

The elements of the $F_2{}^4$are;

$$\begin{aligned} F_{2^4} = \{&0, \beta, \beta^2, \beta^3, \beta^4 = \beta+1, \beta^5 = \beta^2+\beta, \beta^6 = \beta^3+\beta^2, \\ &\beta^7 = \beta^3+\beta+1, \beta^8 = \beta^2+1, \beta^9 = \beta^3+\beta, \beta^{10} = \beta^2+\beta+1, \\ &\beta^{11} = \beta^3+\beta^2+\beta, \beta^{12} = \beta^3+\beta^2+\beta+1, \beta^{13} = \beta^3+\beta^2+1, \\ &\beta^{14} = \beta^3+1, \beta^{15} = 1\} \end{aligned} \tag{20}$$

The sequence $\{b_n\}$is periodic with the period $r = 2^4\text{-}1 = 15$ and;

$$\begin{aligned} &n=0 \Rightarrow A_1 + A_2 + A_3 + A_4 = 0 \\ &n=1 \Rightarrow A_1\beta + A_2\alpha^2 + A_3\beta^4 + A_4\beta^8 = 0 \\ &n=2 \Rightarrow A_1\beta^2 + A_2\beta^4 + A_3\beta^8 + A_4\beta^{16} = 1 \\ &n=3 \Rightarrow A_1\beta^3 + A_2\beta^6 + A_3\beta^{12} + A_4\beta^{24} = 0 \end{aligned} \quad \text{or}$$

$$\begin{aligned} &n=0 \Rightarrow A_1 + A_2 + A_3 + A_4 = 0 \\ &n=1 \Rightarrow A_1\beta + A_2\beta^2 + A_3\beta^4 + A_4\beta^8 = 0 \\ &n=2 \Rightarrow A_1\beta^2 + A_2\beta^4 + A_3\beta^8 + A_4\beta = 1 \\ &n=3 \Rightarrow A_1\beta^3 + A_2\beta^6 + A_3\beta^{12} + A_4\beta^9 = 0 \end{aligned}$$

Solving this system of equations we have;

$$A_1 = \beta, A_2 = \beta^2, A_3 = \beta^4, A_4 = \beta^8$$

Thus, the general term of the sequence $\{bn\}$ is;

$$b_n = \beta.\beta^n + \beta^2.\beta^{2n} + \beta^4.\beta^{4n} + \beta^8.\beta^{8n} \tag{21}$$

and $\{b_n\}$ is a M-Sequence with period $2^4\text{-}1 = 15$, and one period with its cyclic permutations form an orthogonal set;

0 0 1 0 0 1 1 0 1 0 1 1 1 1 0, 0 0 1 0 0 1 0 0 0……. (22)

Suppose the sequence $\{zn\}$is a multiplication sequence on two degrees of $\{bn\}$, b_n and bn_{+2} of the sequence $\{bn\}$ as is showing in Figure 5, then;

$$z_n = b_n.b_{n+2}$$

$$b_{n+2} = \left(\beta^3\beta^n + \beta^6\beta^{2n} + \beta^{12}\beta^{4n} + \beta^9\beta^{8n}\right)$$

Or;

$$z_n = \left(\beta.\beta^n + \beta^2.\beta^{2n} + \beta^4.\beta^{4n} + \beta^8.\beta^{8n}\right)$$
$$\left(\beta^3\beta^n + \beta^6\beta^{2n} + \beta^{12}\beta^{4n} + \beta^9\beta^{8n}\right)$$

Or;

$$\begin{aligned} z_n = {} & \beta^2\beta^n + \beta^4\beta^{2n} + \beta^{13}\beta^{3n} + \beta^8\beta^{4n} + \\ & \beta^5\beta^{5n} + \beta^{11}\beta^{6n} + \beta^{16}\beta^{8n} + \beta^{14}\beta^{9n} + \\ & \beta^{10}\beta^{10n} + \beta^7.\beta^{12n} \end{aligned} \tag{23}$$

Thus, the zeros of the characteristic polynomial of the sequence $\{zn\}$are;

$$\beta^n, \beta^{2n}, \beta^{3n}, \beta^{4n}, \beta^{5n}, \beta^{6n}, \beta^{8n}, \beta^{9n}, \beta^{10n}, \beta^{12n}$$

The characteristic polynomial of the sequence $\{zn\}$ is finding through the formula;

$$h(x) = (x-\beta^n)(x-\beta^{2n}).....(x-\beta^{12n}) \tag{24}$$

Thus, the characteristic equation of the sequence $\{zn\}$ is;

$$(x-\beta^n)(x-\beta^{2n}).....(x-^{12n}) = 0 \tag{25}$$

We can verify that;

$$\beta^n.\beta^{2n}.....\beta^{12n} = \beta^{60n} = 1$$

And;

$$h(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 \tag{26}$$

And the characteristic equation for the equivalent of the nonlinear sequence s;

$$x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 = 0 \tag{27}$$

The equivalent feedback shift register is showing in the following Figure 6;

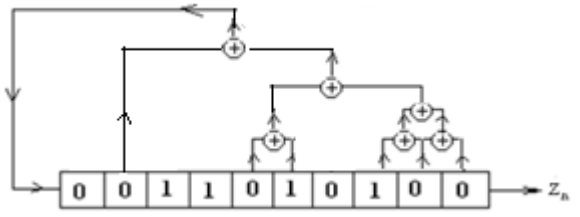

Figure 6. The equivalent linear feedback register generating the sequence $\{z_n\}$

Or, the characteristic equation can be written as;

$$\begin{aligned} &((x-\beta^5)(x-\beta^{10}))((x-\beta)(x-\beta^2)(x-\beta^4)(x-\beta^8)) \\ &((x-\beta^3)(x-\beta^6)(x-\beta^9)(x-\beta^{12})) = 0 \end{aligned} \tag{28}$$

$$(x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1) = 0 \tag{29}$$

The subsequence as result of the characteristic equation $x^2 + x + 1$is periodic with the period $2^2\text{-}1 = 4$, $x^4 + x + 1$ and $x^4 + x^3 + x^2 + x + 1$, each of them is prime with the period $2^4\text{-}1 = 15$, Thus the sequence $\{zn\}$, as a result of the characteristic equation $x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 = 0$, is periodic with the period $2^4\text{-}1 = 15$, the same period of the sequence $\{bn\}$, and the sequence $\{zn\}$ defined by the recurring formula

DOI: https://doi.org/10.30564/ese.v3i2.4036

$$z_{n+10}+z_{n+8}+z_{n+5}+z_{n+4}+z_{n+2}+z_{n+1}+z_n=0 \quad (30)$$

And it is;

0 0 1 0 1 0 1 1 0 0 0 0 0 0 0, 0 0 1 0 1 0 1 1, 0 0 1 0 1 0 1 1 0 0 0 0 0 0 0, 0 0 1 0 1 0 1 1….. (31)

Thus, the sequence reached its maximum length;

$$\binom{4}{1}+\binom{4}{2}=4+\frac{4(4-1)}{2}=10 \quad (32)$$

Or;

The length of the linear equivalent of the nonlinear sequence $\{z_n\}$ is $m=\binom{4}{1}+\binom{4}{2}=10.$

The characteristic equation of the linear equivalent shift register is of the form;

$$x^{10}+\mu_9x^9+\mu_8x^8+\mu_7x^7+\mu_6x^6+\mu_5x^5+\mu_4x^4 +\mu_3x^3+\mu_2x^2+\mu_1x+1=0 \quad (33)$$

Or from the recurrent formula;

$$z_{n+10}+\mu_9z_{n+9}+\mu_8z_{n+8}+\mu_7z_{n+7}+\mu_6z_{n+6}+\mu_5z_{n+5} +\mu_4z_{n+4}+\mu_3z_{n+3}+\mu_2z_{n+2}+\mu_1z_{n+1}+z_n=0 \quad (34)$$

We need solve system of 9 equations (or we can take more equations if it is need) using the terms of the sequence $\{z_n\}$and the previously characteristic equation that are for n = 0,1, ….,8 as following;

For $n=0\rightarrow$ $z_{10}+\mu_9z_9+\mu_8z_8+\mu_7z_7+\mu_6z_6+\mu_5z_5+\mu_4z_4 +\mu_3z_3+\mu_2z_2+\mu_1z_1+z_0=0$

For $n=1\rightarrow$ $z_{11}+\mu_9z_{10}+\mu_8z_9+\mu_7z_8+\mu_6z_7+\mu_5z_6+\mu_4z_5 +\mu_3z_4+\mu_2z_3+\mu_1z_2+z_1=0$

For $n=2\rightarrow$ $z_{12}+\mu_9z_{11}+\mu_8z_{10}+\mu_7z_9+\mu_6z_8+\mu_5z_7+\mu_4z_6 +\mu_3z_5+\mu_2z_4+\mu_1z_3+z_2=0$

For $n=3\rightarrow$ $z_{13}+\mu_9z_{12}+\mu_8z_{11}+\mu_7z_{10}+\mu_6z_9+\mu_5z_8+\mu_4z_7 +\mu_3z_6+\mu_2z_5+\mu_1z_4+z_3=0$

For $n=4\rightarrow$ $z_{14}+\mu_9z_{13}+\mu_8z_{12}+\mu_7z_{11}+\mu_6z_{10}+\mu_5z_9+\mu_4z_8 +\mu_3z_7+\mu_2z_6+\mu_1z_5+z_4=0$

For $n=5\rightarrow$ $z_{15}+\mu_9z_{14}+\mu_8z_{13}+\mu_7z_{12}+\mu_6z_{11}+\mu_5z_{10}+\mu_4z_9 +\mu_3z_8+\mu_2z_7+\mu_1z_6+z_5=0$

For $n=6\rightarrow$ $z_{16}+\mu_9z_{15}+\mu_8z_{14}+\mu_7z_{13}+\mu_6z_{12}+\mu_5z_{11}+\mu_4z_{10} +\mu_3z_9+\mu_2z_8+\mu_1z_7+z_6=0$

For $n=7\rightarrow$ $z_{17}+\mu_9z_{16}+\mu_8z_{15}+\mu_7z_{14}+\mu_6z_{13}+\mu_5z_{12}+\mu_4z_{11} +\mu_3z_{10}+\mu_2z_9+\mu_1z_8+z_7=0$

For $n=8\rightarrow$ $z_{18}+\mu_9z_{17}+\mu_8z_{16}+\mu_7z_{15}+\mu_6z_{14}+\mu_5z_{13}+\mu_4z_{12} +\mu_3z_{11}+\mu_2z_{10}+\mu_1z_9+z_8=0$

For $n=9\rightarrow$ $z_{19}+\mu_9z_{18}+\mu_8z_{17}+\mu_7z_{16}+\mu_6z_{15}+\mu_5z_{14} +\mu_4z_{13}+\mu_3z_{12}+\mu_2z_{11}+\mu_1z_{10}+z_9=0$

Solving these equations we have;

$$\mu_9=0,\mu_8=1,\mu_7=\mu_6=0,\mu_5=\mu_4=1, \mu_3=0,\mu_2=\mu_1=1 \quad (35)$$

Thus, the equivalent linear shift register as showing previosly in the Figure 6.

Example 3.

Given the following received periodic sequence $\{z_n\}$;

000001000010000, 000001000010000….. (36)

The period of the sequence is 2^4-1 = 15 and as showing is not orthogonal t. e. is nonlinear sequence and we need find the nonlinear feedback shift register which generates it and the linear equivalent to it that are; origin sequence $\{a_n\}$, the terms of it which they are under the multiplication operation, finding h the number of these terms, and the linear equivalent to the nonlinear shift register.

There are to prime polynomials of degree 4 they are; $g(x)=x^4+x^3+1$ and $f(x)=x^4+x+1$.

We will study the nonlinear sequences generated by given nonlinear feedback shift register corresponding to the polynomials under the multiplication operation on four degrees and there are only one sequence for each of the prime polynomial, after that three degrees and there are only 4 sequences for each of the prime polynomial, and after that for two degrees for each of them one by one.

First step.

For the polynomial $g(x) = x^4 + x^3 + 1$ and the origin sequence $\{a_n\}$ generated with the characteristic function $g(x)$ and has the initial vector (0010) and the sequence is under the multiplication operation.

The origin sequence $\{a_n\}$ which has $g(x)$ as a characteristic polynomial and satisfies the recurrent formula $a_{n+4}+a_{n+3}+a_n=0$ is orthogonal and periodic with the period 2^4-1=15 and is showing in the Figure 7;

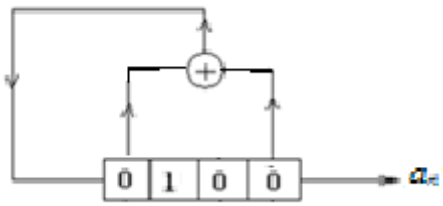

Figure 7. Linear feedback shift register with 4 complexity over F_2

And it is;

001000111101011,001000111101011……. (37)

Thus the nonlinear sequence which as a result of multiplication on all degrees of the linear shift register in the Figure 7 is;

0 0 0 0 0 0 1 0 1 0 0 1 0 0 1, 0 0 0 0 0 0 1 0 1 0 0 (38)

And it is not the same sequence $\{z_n\}$.

 DOI: https://doi.org/10.30564/ese.v3i2.4036

Second step.

For the polynomial $f(x) = x^4 + x + 1$ and the origin sequence $\{b_n\}$ generated with the characteristic function $f(x)$ and has the initial vector (0010) and the sequence is under the multiplication operation.

The origin sequence $\{b_n\}$ which has $f(x)$ as a characteristic polynomial and satisfies the recurrent formula $b_{n+4} + b_{n+1} + b_n = 0$ is orthogonal and periodic with the period 2^4-1=15 and is showing in the Figure 8;

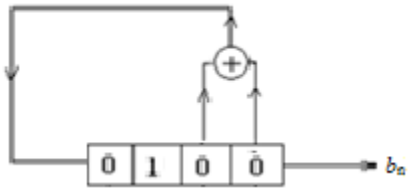

Figure 8. Linear feedback shift register generating the sequence $\{b_n\}$

And it is;

0 0 1 0 0 1 1 0 1 0 1 1 1 1 0, 0 0 1 0 0 1 1 0 1 0 1 1 1 1 0……. (39)

Thus the nonlinear sequence which as a result of multiplication on all cells of the linear shift register in the Figure 7 is;

0 0 1 0 0 1 0 0 1 0 1 0 0 0 0 0 0 1 0 0, 1 0 0 1 0 0 0 0 1 0 1 0 0 (40)

And it is not the same sequence $\{z_n\}$.

Third step.

We will go for finding $u_n^{(i,j,k)}$ and $w_n^{(i,j,k)}$ the nonlinear sequences over three cells of the sequences $\{a_n\}$ and $\{b_n\}$respectively which are in the previously first step one by one and we have the following;

$a)\ u_n^{(0,1,2)} = 0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0, 0\,0\,01\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\ldots$

$w_n^{(0,1,2)} = 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0, 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\ldots$

And both of $u_n^{(0,1,2)}$ & $w_n^{(0,1,2)}$ is not the same sequence $\{z_n\}$.

$b)\ u_n^{(0,1,3)} = 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0, 0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\ldots$

$w_n^{(0,1,3)} = 0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0, 0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\ldots$

We can see that $u_n^{(0,1,3)}$ is not the same $\{z_n\}$ but the sequence $w_n^{(0,1,3)}$ is the same and the following nonlinear shift register generates the sequence $\{z_n\}$;

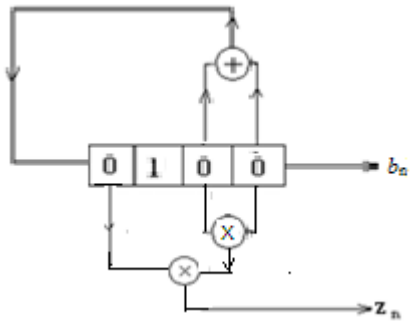

Figure 9. Nonlinear feedback shift register generating the sequence $\{z_n\}$

From (20);

$$b_n = \beta.\beta^n + \beta^2.\beta^{2n} + \beta^4.\beta^{4n} + \beta^8.\beta^{8n}$$

$$b_{n+1} = \beta^2.\beta^n + \beta^4.\beta^{2n} + \beta^8.\beta^{4n} + \beta.\beta^{8n}$$

$$b_{n+3} = \left(\beta^4\beta^n + \beta^8\beta^{2n} + \beta\beta^{4n} + \beta^2\beta^{8n}\right)$$

$$z_n = b_n.b_{n+1}.b_{n+3}$$

$$z_n = (\beta.\beta^n + \beta^2.\beta^{2n} + \beta^4.\beta^{4n} + \beta^8.\beta^{8n}).$$
$$(\beta^2.\beta^n + \beta^4.\beta^{2n} + \beta^8.\beta^{4n} + \beta.\beta^{8n}.$$
$$(\beta^5\beta^n + \beta^{10}\beta^{2n} + \beta^5\beta^{4n} + \beta\beta^{8n}$$

Or;

$$z_n = \beta^n + \beta^{2n} + \beta^{4n} + \beta^8\beta^{5n} + \beta^{7n} + \beta^{8n} + \beta^{10} + \beta^{11n} + \beta^{13n} + \beta^{14n} \quad (41)$$

Thus;

The zeros of the characteristic polynomial of the sequence $\{zn\}$are;

$$\beta^n, \beta^{2n}, \beta^{4n}, \beta^{5n}, \beta^{7n}, \beta^{8n}, \beta^{10}, \beta^{11n}, \beta^{13n}, \beta^{14n} \quad (42)$$

The characteristic polynomial of the sequence $\{zn\}$ is finding through the formula;

$$f(x) = (x - \beta^n)(x - \beta^{2n}) \ldots\ldots (x - \beta^{14n}) \quad (43)$$

Thus, the characteristic equation of the sequence $\{zn\}$is;

$$(x - \beta^n)(x - \beta^{2n}) \ldots\ldots (x - \beta^{14n}) = 0 \quad (44)$$

We can verify that;

$$\beta.\beta^2.\beta^4.\beta^5.\beta^7.\beta^8.\beta^{10}.\beta^{11}.\beta^{13}.\beta^{14n} = \beta^{75} = 1 \quad (45)$$

And the characteristic equation of the sequence $\{zn\}$is ;

DOI: https://doi.org/10.30564/ese.v3i2.4036

$$((x-\beta^5)(x-\beta^{10}))((x-\beta)(x-\beta^2)(x-\beta^4)(x-\beta^8)) \\ ((x-\beta^7)(x-\beta^{11})(x-\beta^{13})(x-\beta^{14}))=0 \quad (46)$$

Or;

$$x^{10}+x^5+1=0 \quad (47)$$

And the characteristic function of the linear equivalent of the nonlinear sequence $\{z_n\}$ is;

$$f(x)=x^{10}+x^5+1 \quad (48)$$

The linear equivalent feedback shift register of $\{z_n\}$ is showing in the following Figure 10;

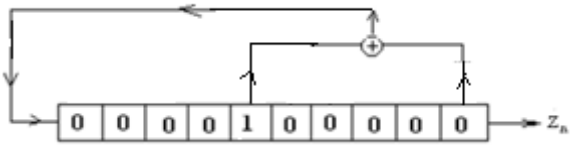

Figure 10. The equivalent linear feedback register generating sequence $\{z_n\}$

Or by inverse, we define the equivalent linear register, after that we define *h* the number of terms which are under the multiplication operation and after that we define the basic sequence which is under under the multiplication operation, namely as following;

The length of the linear equivalent of the nonlinear sequence $\{z_n\}$ is $h=\binom{4}{1}+\binom{4}{2}=10$.

The characteristic equation of the linear equivalent shift register is of the form;

$$x^{10}+\mu_9x^9+\mu_8x^8+\mu_7x^7+\mu_6x^6+\mu_5x^5+\mu_4x^4 \\ +\mu_3x^3+\mu_2x^2+\mu_1x+1=0 \quad (49)$$

Or from the recurrent formula;

$$z_{n+10}+\mu_9z_{n+9}+\mu_8z_{n+8}+\mu_7z_{n+7}+\mu_6z_{n+6}+\mu_5z_{n+5} \\ +\mu_4z_{n+4}+\mu_3z_{n+3}+\mu_2z_{n+2}+\mu_1z_{n+1}+z_n=0$$

We need solve system of 9 equations (or we can take more equations if it is need) using the terms of the sequence $\{z_n\}$and the previously characteristic equation that are for $n = 0,1, \ldots,8$ as following;

$$\text{For } n=0 \rightarrow z_{10}+\mu_9z_9+\mu_8z_8+\mu_7z_7+\mu_6z_6+\mu_5z_5+\mu_4z_4 \\ +\mu_3z_3+\mu_2z_2+\mu_1z_1+z_0=0$$

$$\text{For } n=1 \rightarrow z_{11}+\mu_9z_{10}+\mu_8z_9+\mu_7z_8+\mu_6z_7+\mu_5z_6+\mu_4z_5 \\ +\mu_3z_4+\mu_2z_3+\mu_1z_2+z_1=0$$

$$\text{For } n=2 \rightarrow z_{12}+\mu_9z_{11}+\mu_8z_{10}+\mu_7z_9+\mu_6z_8+\mu_5z_7+\mu_4z_6 \\ +\mu_3z_5+\mu_2z_4+\mu_1z_3+z_2=0$$

$$\text{For } n=3 \rightarrow z_{13}+\mu_9z_{12}+\mu_8z_{11}+\mu_7z_{10}+\mu_6z_9+\mu_5z_8+\mu_4z_7 \\ +\mu_3z_6+\mu_2z_5+\mu_1z_4+z_3=0$$

$$\text{For } n=4 \rightarrow z_{14}+\mu_9z_{13}+\mu_8z_{12}+\mu_7z_{11}+\mu_6z_{10}+\mu_5z_9+\mu_4z_8 \\ +\mu_3z_7+\mu_2z_6+\mu_1z_5+z_4=0$$

$$\text{For } n=5 \rightarrow z_{15}+\mu_9z_{14}+\mu_8z_{13}+\mu_7z_{12}+\mu_6z_{11}+\mu_5z_{10}+\mu_4z_9 \\ +\mu_3z_8+\mu_2z_7+\mu_1z_6+z_5=0$$

$$\text{For } n=6 \rightarrow z_{16}+\mu_9z_{15}+\mu_8z_{14}+\mu_7z_{13}+\mu_6z_{12}+\mu_5z_{11}+\mu_4z_{10} \\ +\mu_3z_9+\mu_2z_8+\mu_1z_7+z_6=0$$

$$\text{For } n=7 \rightarrow z_{17}+\mu_9z_{16}+\mu_8z_{15}+\mu_7z_{14}+\mu_6z_{13}+\mu_5z_{12}+\mu_4z_{11} \\ +\mu_3z_{10}+\mu_2z_9+\mu_1z_8+z_7=0$$

$$\text{For } n=8 \rightarrow z_{18}+\mu_9z_{17}+\mu_8z_{16}+\mu_7z_{15}+\mu_6z_{14}+\mu_5z_{13}+\mu_4z_{12} \\ +\mu_3z_{11}+\mu_2z_{10}+\mu_1z_9+z_8=0$$

$$\text{For } n=9 \rightarrow z_{19}+\mu_9z_{18}+\mu_8z_{17}+\mu_7z_{16}+\mu_6z_{15}+\mu_5z_{14}+\mu_4z_{13} \\ +\mu_3z_{12}+\mu_2z_{11}+\mu_1z_{10}+z_9=0$$

Solving these equations we have;

$$\mu_9=\mu_8=\mu_7=\mu_6=\mu_4=\mu_3=0, \mu_5=1 \quad (50)$$

And the characteristic equation is;

$$x^{10}+\ x^5++1=0 \quad (51)$$

Or;

$$(x^2+x+1)(x^4+x+1)(x^4+x^3+1)=0 \quad (52)$$

Or, the recurrent formula of the sequence $\{z_n\}$ is;

$$z_{n+10}+z_{n+5}++z_n=0 \quad (53)$$

We can check that the recurrent sequence generates the same nonlinear sequence $\{z_n\}$.

Thus, the equivalent linear shift register as showing in the previously Figure 10.

From the length of the equivalent linear shift register, which equal to 10 we can guess that the nonlinear shift register has the length 4 (4 degrees) and;

$$\binom{4}{1}+\binom{4}{2}=10 \ \& \ \binom{4}{1}+\binom{4}{2}+\binom{4}{3}=14 \quad (54)$$

Thus, h =2 or 3 and we can go to the first step for finding the exactly the degree of multiplication operation h.

4. Conclusions

1) If the received sequence $\{z_n\}$ is orthogonal and periodic with the period $r = 2k$-1 then the sequence is linear and has linear shift feedback register with the complexity (length) equal to k and we can find the linear feedback shift register using the initial vector ($\alpha_0, \alpha_1, \ldots, \alpha k\text{-}_1 = z_0, z_1, \ldots, zk\text{-}_1$).

2) If $\{z_n\}$is periodic with the period $2k$ -1, the linear equivalent of sequence $\{z_n\}$ has the length;

 DOI: https://doi.org/10.30564/ese.v3i2.4036

$$_rN_2 = \binom{r}{1} + \binom{r}{2} = r + \frac{r(r-1)}{2}$$

and then the set of all cyclic permutations of one period of $\{z_n\}$ is not an orthogonal set then $\{z_n\}$ is multiplication on only two degrees of recurring sequence $\{an\}$ and the characteristic polynomial of the sequence $\{an\}$ is prime polynomial of degree k.

3) If the multiplication sequence $\{z_n\}$ is periodic with the period $2k$ -1 or divide it and the linear equivalent register of $\{z_n\}$ has the complexity m where $m \le {}_kN_t$ (t is the latest natural for the inequality is true) then $h \ge t$ (h is the number of terms of the original recurring sequence $\{an\}$ which are under the multiplication operation) and the characteristic polynomial of the sequence $\{an\}$ is prime polynomial of degree k. Thus from the period of $\{z_n\}$ we can define k the degree of the characteristic polynomial of the original sequence $\{a_n\}$ and then from the length of the linear equivalent of $\{z_n\}$ we can define h the number of terms from $\{z_n\}$ which are under the multiplication operation.

4) If the multiplication sequence $\{z_n\}$ is periodic with the period $2k$ -1 or divide it then we can define k the degree of

characteristic polynomial of the sequence $\{an\}$ which is a prime polynomial and after that we can define the original sequence $\{an\}$ and the terms of it which are under the multiplication operation that is we can define h then through these terms we can define m the complexity of linear equivalent register of the multiplication sequence $\{z_n\}$. Thus from the period of $\{z_n\}$ we can define k the degree of the characteristic polynomial of the original sequence $\{a_n\}$ and then from k we can define h the number of the terms which are under the multiplication operation after that we can find m the complexity of linear equivalent of the sequence $\{z_n\}$.

5) Knowing he construction of the nonlinear register of the original sequence $\{a_n\}$ giving us all codes (or commands) which sending through it and how we can to influence it.

References

[1] Sloane, N.J.A., (1976), "An Analysis Of The Stricture And Complexity of Nonlinear Binary Sequence Generators," *IEEE Trans. Information Theory* Vol. It 22 No 6, PP 732-736.

[2] Mac Wiliams, F. G & Sloane,N.G.A., (2006), "*The Theory of Error- Correcting Codes,"*North- Holland, Amsterdam.

[3] Mokayes D. Al Cheikha A. H., (2021- February) Study the Linear Equivalent of Nonlinear Sequences over *Fp* Where p is larger than two, *International Journal of Information and Communication* Sciences, ISSN: 2575-1700, Vol. 5, Issue 4, pp 53-75.

[4] Al Cheikha A. H. (September,2014). Some Properties of M-Sequences Over Finite Field Fp. *International Journal of Computer Engineering & Technology*. IJCET. ISSN 0976- 6367(Print),ISSN 0976 - 6375(Online),Vol.5, Issue 9. Pp. 61-72.

[5] Al Cheikha A. H. (May 2014), " Matrix Representation of Groups in the finite Fields GF(*pn*) "International Journal of Soft Computing and Engineering, Vol. 4, Issue 2, PP 118-125.

[6] Al Cheikha A. H. (2018).Generation New Binary Sequences using Quotient Ring Z/*pm*Z. *Research Journal of Mathematics and Computer Science. RJMCS*. ISSN: 2576 -3989, Vol.2, Issue 11. Pp. 0001- 0013.

[7] Al Cheikha A. H. (May 5, 2014). Matrix Representation of Groups in the Finite Fields GF(p^n). *International Journal of Soft Computing and Engineering*, IJSCE, ISSN:2231- 2307, Vol. 4, Issue 2, pp. 1-6.

[8] Al Cheikha, A. H., (2019), Placement of M-Sequences over the Field *Fp* in the Space *Rn*, International Journal of Information and Communication Science, IJICS, ISSN: 2575-1700 (Print); ISSN: 2575-1719 (Online), Vol. 4, No.1, Pp. 24-34.

[9] Al Cheikha A. H., Omar Ebtisam. Haj., "Study the Multiplication M-sequences and its Reciprocal Sequences", *Journal of Electronic & Information Systems*. ISSN: 2661-3204,Vol. 03, Issue. 0, Pp. 13-22.

[10] Al Cheikha, A.H. (April 26, 2014). Matrix Representation of Groups in the Finite Fields GF(2^n). *International Journal of Soft Computing and Engineering*, IJSCE, ISSN: 2231- 2307, Vol. 4, Issue 2. pp. 118-125

[11] Al Cheikhaa A. H. A Theoretical Study for the Linear Homogenous Orthogonal Recurring Sequences. (5 May, 2004). In Almanara Journal, Alalbayt University, Jordan. No 2, 285/2004. (in Arabic), In English: www. researchgate.net/profile/Ahmad_Al_Cheikha/publications After select: Ahmad Al Cheikha | Ahlia University | Department of ... – Research Gate after select: Research, and after select: Article, or Faulltexts, and the article.

[12] Golamb S. W. (1976), Shift Register Sequences, San Francisco – Holden Day.

[13] Lee J.S &Miller L.E, (1998)"*CDMA System Engineering Hand Book, "*Artech House. Boston, London.

[14] Yang S.C,"*CDMA RF* , (1998), *System Engineering,"*Artech House. Boston-London.

[15] Lidl, R.& Pilz, G., (1984), "*Applied Abstract Alge-*

DOI: https://doi.org/10.30564/ese.v3i2.4036

bra," Springer – Verlage New York, 1984.
[16] Lidl, R. & Niderreiter, H., (1994), "Introduction to Finite Fields and Their Application," *Cambridge university* USA.
[17] Thomson W. Judson, (2013), "*Abstract Algebra: Theory and Applications*," Free Software Foundation.
[18] Fraleigh, J.B., (1971), "A First course In Abstract Algebra, *Fourth printing. Addison- Wesley publishing company* USA.

Appendix 1.

List of the primitive polynomials on F_2^n

x^2 + x^1 + 1
x^3 + x^1 + 1
x^4 + x^1 + 1
x^5 + x^2 + 1
x^5 + x^4 + x^2 + x^1 + 1
x^5 + x^4 + x^3 + x^2 + 1
x^6 + x^1 + 1
x^6 + x^5 + x^2 + x^1 + 1
x^6 + x^5 + x^3 + x^2 + 1
x^7 + x^1 + 1
x^7 + x^3 + 1
x^7 + x^3 + x^2 + x^1 + 1
x^7 + x^4 + x^3 + x^2 + 1
x^7 + x^5 + x^4 + x^3 + x^2 + x^1 + 1
x^7 + x^6 + x^3 + x^1 + 1
x^7 + x^6 + x^4 + x^2 + 1
x^7 + x^6 + x^5 + x^2 + 1
x^7 + x^6 + x^5 + x^4 + x^2 + x^1 + 1
x^8 + x^4 + x^3 + x^2 + 1
x^8 + x^5 + x^3 + x^1 + 1
x^8 + x^6 + x^4 + x^3 + x^2 + x^1 + 1
x^8 + x^6 + x^5 + x^1 + 1
x^8 + x^6 + x^5 + x^2 + 1
x^8 + x^6 + x^5 + x^3 + 1
x^8 + x^7 + x^6 + x^1 + 1
x^8 + x^7 + x^6 + x^5 + x^2 + x^1 + 1
x^9 + x^4 + 1
x^9 + x^5 + x^3 + x^2 + 1
x^9 + x^6 + x^4 + x^3 + 1
x^9 + x^6 + x^5 + x^3 + x^2 + x^1 + 1
x^9 + x^6 + x^5 + x^4 + x^2 + x^1 + 1
x^9 + x^7 + x^6 + x^4 + x^3 + x^1 + 1
x^9 + x^8 + x^4 + x^1 + 1
x^9 + x^8 + x^5 + x^4 + 1
x^9 + x^8 + x^6 + x^5 + 1
x^9 + x^8 + x^6 + x^5 + x^3 + x^1 + 1
x^9 + x^8 + x^7 + x^2 + 1
x^9 + x^8 + x^7 + x^3 + x^2 + x^1 + 1
x^9 + x^8 + x^7 + x^6 + x^5 + x^1 + 1
x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + 1
x^10 + x^3 + 1
x^10 + x^4 + x^3 + x^1 + 1
x^10 + x^6 + x^5 + x^3 + x^2 + x^1 + 1
x^10 + x^8 + x^3 + x^2 + 1
x^10 + x^8 + x^4 + x^3 + 1
x^10 + x^8 + x^5 + x^1 + 1
x^10 + x^8 + x^5 + x^4 + 1
x^10 + x^8 + x^7 + x^6 + x^5 + x^2 + 1
x^10 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^1 + 1
x^10 + x^9 + x^4 + x^1 + 1
x^10 + x^9 + x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 1
x^10 + x^9 + x^8 + x^6 + x^3 + x^2 + 1
x^10 + x^9 + x^8 + x^6 + x^5 + x^1 + 1
x^10 + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1

 DOI: https://doi.org/10.30564/ese.v3i2.4036