

# Study the Linear Equivalent of the Binary Nonlinear Sequences

Ahmad Hamza Al Cheikha

Department of Mathematical Science, College of Arts-science and Education, Ahlia University, Manama, Bahrain

**Email address:**

alcheikhaa@yahoo.com

**To cite this article:**

Ahmad Hamza Al Cheikha. Study the Linear Equivalent of the Binary Nonlinear Sequences. *International Journal of Information and Communication Sciences*. Vol. 5, No. 3, 2020, pp. 24-39. doi: 10.11648/j.ijjics.20200503.11

**Received:** July 8, 2020; **Accepted:** July 28, 2020; **Published:** August 27, 2020

**Abstract:** Linear orthogonal sequences, special M-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 links of these channels to sift this information which transmitted and the receivers get the information in a correct form. In current research trying to study the construction of the linear equivalent of a multiplication sequence and answering on the question "why the length of the linear equivalent of a multiplication sequence (on a linear M-sequence  $\{a_n\}$ ), in some cases doesn't reach the maximum length  $rN_h$ , special, when the multiplication is on three or more degrees of the basic sequence  $\{a_n\}$  The multiplication sequence has high complexity and the same period of the basic sequence, or if the multiplication sequence on two different basic sequences then the period of multiplication sequence is equal to multiplication the two periods of the basic sequences, and in the two cases the multiplication sequence is not an orthogonal sequence.

**Keywords:** Linear Sequences, Finite Field, Linear Feedback Shift Register, Orthogonal Sequence, Linear Equivalent, Complexity

## 1. Introduction

The main obstacle to encoding and decoding is the complexity of decoding and decoding. For this reason, efforts have been made to design cryptographic and decoding methods in an easy way. The works of Hocquenghem in 1959, Reed Solomon 1960, Chaudhuri and Bose in 1960, BCH codes or Bose–Chaudhuri–Hocquenghem codes and others as Goppa, and Peterson 1961 were a new starting point for solving this issue. [1-5]

In all stages of the encoding and the decoding, the orthogonal sequences play the main role in these processes, including the sequences with maximum period M-Sequences, Walsh sequences, Reed-Solomon sequences, and other sequences. [6-12]

Sloane, N. J. A., discusses that the multiplication sequence  $\{z_n\}$  on h degrees of  $\{a_n\}$  which has the r complexity the complexity of  $\{z_n\}$  can't be exceeded

$$rN_h = \binom{r}{1} + \binom{r}{2} + \dots + \binom{r}{h}. [8]$$

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 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. [10-12]

Shannon's classic articles, 1948-1949, were followed by many research papers on the question of finding successful ways to encode and successful decoding the media to allow it to be transmitted correctly through jammed channels. [6-8, [13-14].

## 2. Research Method and Materials

### M- Linear Recurring Sequences

Let k be a positive integer and  $\lambda, \lambda_0, \lambda_1, \dots, \lambda_{k-1}$  are elements in the field  $F_2 = \{0, 1\}$  then the sequence  $a_0, a_1, \dots$  is called the nonhomogeneous binary linear recurring sequence of order k (or with the complexity k) iff:

$$a_{n+k} = \lambda_{k-1}a_{n+k-1} + \lambda_{k-2}a_{n+k-2} + \dots + \lambda_0a_n + \lambda; \lambda \& \lambda_i \in F_2, i = 0, 1, \dots, k-1$$

$$\text{or } a_{n+k} = \sum_{i=1}^{k-1} \lambda_i a_{n+i} + \lambda \tag{1}$$

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

$$f(x) = x^k + \lambda_{k-1}x^{k-1} + \dots + \lambda_1x + \lambda_0 \tag{2}$$

Is called the characteristic polynomial. In this study, we are limited to  $\lambda_0 = 1$ .

*Definition 1.* The ultimately sequence  $a_0, a_1, \dots$  in  $F_2$  with the smallest natural number  $r$  is called periodic with the period  $r$  iff:

$$a_{n+r} = a_n ; n = 0, 1, \dots \tag{2-6}$$

*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  $\{a_n\}$  and the register denoted as LFSR.[3]

*Definition 3.* The complement of the binary vector  $X = (x_1, x_2, \dots, x_n), x_i \in F_2 = \{0, 1\}$  is the vector  $\bar{X} = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)$ , where:

$$\bar{x}_i = \begin{cases} 1 & \text{if } x_i = 0 \\ 0 & \text{if } x_i = 1 \end{cases} \tag{2, 6-7}$$

*Definition 4.* Suppose  $x = (x_0, x_1, \dots, x_{n-1})$  and  $y = (y_0, y_1, \dots, y_{n-1})$  are two binary vectors of length  $n$  on  $F_2$ . The coefficient of correlations function of  $x$  and  $y$ , denoted by  $R_{x,y}$ , is:

$$R_{x,y} = \sum_{i=0}^{n-1} (-1)^{x_i+y_i} \tag{3}$$

Where  $x_i + y_i$  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" and each "0" by "1") then [2-9].

$$R_{x,y} = \sum_{i=0}^{n-1} x_i y_i \tag{4}$$

*Definition 5.* Suppose  $x = (x_0, x_1, \dots, x_{n-1})$  and  $y = (y_0, y_1, \dots, y_{n-1})$  are binary vectors of length  $n$  on  $F_2$ , or components belong to  $\{1, -1\}$ , is said orthogonal if  $|R_{x,y}| \leq 1$ .

[8-9]

*Definition 6.* Suppose  $G$  is a set of binary vectors of length  $n$ :

$$G = \{X; X = (x_0, x_1, \dots, x_{n-1}), x_i \in F_2, i = 0, 1, \dots, n-1\}$$

Let's  $1^* = -1$  and  $0^* = 1$ , The set  $G$  is said to be orthogonal if the following two conditions are satisfied:

$$1. \forall X \in G, \left| \sum_{i=0}^{n-1} x_i^* \right| \leq 1, \text{ or } |R_{x,0}| \leq 1. \tag{5}$$

$$2. \forall X, Y \in G (X \neq Y), \left| \sum_{i=0}^{n-1} x_i^* y_i^* \right| \leq 1 \text{ or } |R_{x,y}| \leq 1. \tag{6}$$

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

*Definition 8.* The linear equivalent of a multiplication sequence  $\{z_n\}$ , on a binary linear sequence  $\{a_n\}$  which generated with the linear register LFSR1 and the sequence  $\{z_n\}$  is a multiplication on some terms of  $\{a_n\}$  (that is a result of multiplication circuits over the LFSR1), is a linear shift register LFSR2 generates the same sequence  $\{z_n\}$ . [2, 3, 8]

*Definition 9.* The length of the linear equivalent of a multiplication sequence is the number of its complexity and equal to the degree of the characteristic polynomial which generates the same multiplication sequence, and the multiplication sequence can be generated through the linear equivalent.[8]

*Definition 10.* The maximum length of a linear equivalent is the maximum length of the linear equivalent LFSR2 (it is the number of its complexity) which can be reached and the length of linear equivalent is always less than or equal the maximum length  $r N_h$ . [2, 3, 8]

*Definition 11.* Inverse problem: Finding the sequence  $\{a_n\}$  which  $\{z_n\}$  is a multiplication sequence on it and it is one of the issues at present and it requires a solution. [8]

*Theorem 12.*

- i. If  $a_0, a_1, \dots$  is a homogeneous linear recurring sequence of order  $k$  in  $F_2$ , satisfies (1) then this sequence is periodic.
- ii. If this sequence is a homogeneous linear recurring sequence, periodic with the period  $r$ , and its characteristic polynomial  $f(x)$  then  $r \mid \text{ord } f(x)$ .

If the polynomial  $f(x)$  is primitive then the period of the recurring sequence which has  $f(x)$  as a characteristic polynomial is  $2^k - 1$ , this sequence is called M-Sequence

over  $F_2$ , or briefly M-Sequences.[6, 11-14].

*Lemma 13.* (Fermat's theorem). If  $F$  is a finite field and has  $q$  elements then each element  $a$  of  $F$  satisfies the equation:

$$x^q = x. [6, 10]$$

*Theorem 14.* If  $g(x)$  is a characteristic prime polynomial of the (H. L. R. S.)  $a_0, a_1, \dots$  of degree  $k$ , and  $\alpha$  is a root of  $g(x)$  in any splitting field of  $F_p$  then the general term of this sequence is:

$$a_n = \sum_{i=1}^k C_i (\alpha^{2^{i-1}})^n. [6, 11]$$

*Theorem 15.*

$$i. (q^m - 1) \mid (q^n - 1) \Leftrightarrow m \mid n \quad (7)$$

ii. If  $F_q$  is a field of order  $q = 2^n$  then any subfield of it is of the order  $2^m$  and  $m \mid n$ , and by inverse if  $m \mid n$  then in the field  $F_q$  there is a subfield of order  $2^m$ . [6, 10-14]

*Theorem 16.* The number of irreducible polynomials in  $F_q(x)$  of degree  $m$  and order  $e$  is  $\phi(e)/m$ , 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, 10-14]

\* The study here is limited to the Galois Fields of the form  $F_{2^k}$ , then the period  $r = 2^k - 1$ .

### 3. Results and Discussion

#### 3.1. Studying Multiplication Sequences on the Binary Recurring M-Sequences

Suppose the binary recurring M-Sequence  $\{a_n\}$  with the complexity  $r$  and  $\alpha_1, \alpha_2, \dots, \alpha_r$  are its different linear independent roots of the characteristic equation of the sequence then the general term of the sequence is given through the relation;

$$a_n = A_1 \alpha_1^n + A_2 \alpha_2^n + \dots + A_r \alpha_r^n = \sum_{i=1}^r A_i \alpha_i^n$$

$$\sum_{\substack{i=1, j \\ j \neq i}}^r A_i A_j (\alpha_i^\delta + \alpha_j^\delta) \alpha_i^n \alpha_j^n = 0 \Rightarrow \alpha_i^\delta + \alpha_j^\delta = 0 \Rightarrow \alpha_i^\delta = \alpha_j^\delta \Rightarrow \alpha_i = \alpha_j$$

And it is a contradiction, then no term in the second sum is equal to zero and the number of these terms is  $\binom{r}{2} = \frac{r(r-1)}{2}$  and the complexity of the sequence  $\{z_n\}$  is;

If the sequence in  $F_2$ , its characteristic equation is prime, and  $\alpha$  is a root of it ( $\alpha$  is prime element in  $F_2^r$ ) then the general term of the sequence  $\{a_n\}$  is;

$$a_n = A_1 \alpha^n + A_2 (\alpha^{2^{2-1}})^n + \dots + A_r (\alpha^{2^{r-1}})^n = \sum_{i=1}^r A_i (\alpha^{2^{i-1}})^n \quad (8)$$

#### 3.1.1. The Sequence $\{z_n\}$ Is a Multiplication on Two Degrees of the Sequence $\{a_n\}$

Suppose the multiplication sequence  $\{z_n\}$  as multiplication on two different degrees of  $\{a_n\}$  as following;

- (1) The first degree is  $a_n$  (in another case we can make a shift to the first term).
- (2) The second degree is  $b_n = a_{n+\delta}$  as a shift of the first term  $a_n$  by  $\delta$ .

$$b_n = a_{n+\delta} = A_1 \alpha_1^{n+\delta} + A_2 \alpha_2^{n+\delta} + \dots + A_r \alpha_r^{n+\delta} = \sum_{i=1}^r A_i \alpha_i^{n+\delta}$$

Or;

$$b_n = a_{n+\delta} = A_1 \alpha_1^\delta \alpha_1^n + A_2 \alpha_2^\delta \alpha_2^n + \dots + A_r \alpha_r^\delta \alpha_r^n = \sum_{j=1}^r A_j \alpha_j^\delta \alpha_j^n$$

$$z_n = a_n b_n = a_n a_{n+\delta}$$

$$z_n = \left( \sum_{i=1}^r A_i \alpha_i^n \right) \left( \sum_{j=1}^r A_j \alpha_j^{n+\delta} \right) =$$

$$\left( \sum_{i=1}^r A_i^2 \alpha_i^\delta \alpha_i^{2n} \right) + \sum_{\substack{i, j=1 \\ j \neq i}}^r A_i A_j (\alpha_i^\delta + \alpha_j^\delta) \alpha_i^n \alpha_j^n$$

Thus we have the following properties;

P1. Each term of the first sum is not equal to zero and the number of these terms is equal to  $\binom{r}{1} = r$ .

P2. Also, a term of the second sum is equal to zero if and only if;

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

P3. Sum one term of the first sum with one term of the second sum is equal to zero if and only if there is different  $i, j$ ,  $k$  satisfies the two conditions;

$$A_k^2 \alpha_k^\delta \alpha_k^{2n} = A_i A_j (\alpha_i^\delta + \alpha_j^\delta) \alpha_i^n \alpha_j^n$$

And it is equivalent to the two conditions;

- 1)  $\alpha_k^{2n} = \alpha_i^n \alpha_j^n$  or  $\alpha_k^2 = \alpha_i \alpha_j$
- 2)  $A_k^2 \alpha_k^\delta = A_i A_j (\alpha_i^\delta + \alpha_j^\delta)$  or  $\alpha_i^\delta + \alpha_j^\delta = \frac{A_k^2}{A_i A_j} \alpha_k^\delta$

If the sequence  $\{a_n\}$  is linear recurring sequence with prime characteristic polynomial of degree  $r$  and  $\alpha$  is a zero of the characteristic polynomial then the roots of the characteristic equation are  $\alpha, \alpha^2, \dots, \alpha^{2^{r-1}}$  and the general term of the sequence is of the form;

$$a_n = A_1 \alpha^n + A_2 (\alpha^2)^n + \dots + A_r (\alpha^{2^{r-1}})^n = \sum_{i=1}^r A_i (\alpha^{2^{i-1}})^n$$

Thus, for the first condition each of the  $i, j, k$  can't be one, and if there is such other values will be as;

$$\alpha^{2 \cdot 2^{k-1}} = \alpha^{2^{i-1}} \alpha^{2^{j-1}} \Rightarrow \alpha^{2^k} = \alpha^{2^{i-1} + 2^{j-1}}$$

Or if  $i$  is the smallest;

$$\alpha^{2^k} = \alpha^{2^{i-1}(1+2^{j-i})} \Rightarrow \alpha^{2^k} = (\alpha^{(1+2^{j-i})})^{2^{i-1}}$$

Or;

$$\alpha^{\frac{2^k}{2^{i-1}}} = \alpha^{(1+2^{j-i})} \Rightarrow \alpha^{2^{k-i+1}} = \alpha^{(1+2^{j-i})} \Rightarrow 2^{k-i+1} = 1 + 2^{j-i}$$

But  $2^{k-i+1}$  is even number,  $(1+2^{j-i})$  is odd number (or  $2^{k-i+1}$  and  $2^{j-i}$  are relatively primes) and it is contradiction

$$F_{2^4} = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4 = \alpha + 1, \alpha^5 = \alpha^2 + \alpha, \alpha^6 = \alpha^3 + \alpha^2, \alpha^7 = \alpha^3 + \alpha + 1, \alpha^8 = \alpha^2 + 1, \alpha^9 = \alpha^3 + \alpha, \alpha^{10} = \alpha^2 + \alpha + 1, \alpha^{11} = \alpha^3 + \alpha^2 + \alpha, \alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1, \alpha^{13} = \alpha^3 + \alpha^2 + 1, \alpha^{14} = \alpha^3 + 1, \alpha^{15} = 1\} \quad (9)$$

The general term of the sequence is;

$$a_n = A_1 \alpha^n + A_2 \alpha^{2n} + A_3 \alpha^{4n} + A_4 \alpha^{8n}$$

Or;

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

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

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

Or;

then the sum of one term from the first sum with one term from the second sum can't be equal to zero and the linear equivalent reached the maximum length  $\binom{r}{1} + \binom{r}{2} = r + \frac{r(r-1)}{2}$ .

The sequence  $\{z_n\}$  is periodic with the same period of the sequence  $\{a_n\}$ .

*Example 1.* Suppose the binary recurring sequence  $\{a_n\}$  with the complexity 4 as a result of the linear feedback shift register which showing in figure 1;

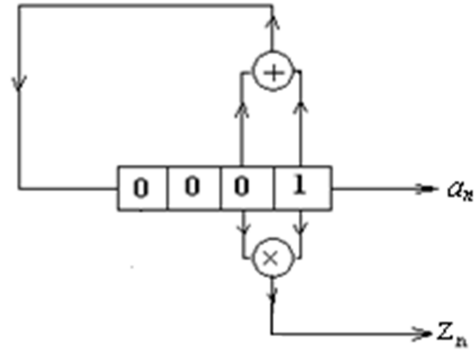


Figure 1. Linear feedback shift register with 4 complexity over  $F_2$ .

Where;

$$a_{n+4} + a_{n+1} + a_n = 0 \text{ or } a_{n+4} = a_{n+1} + a_n$$

Its characteristic polynomial  $f(x) = x^4 + x + 1$  is prime and its characteristic equation is  $x^4 + x + 1 = 0$ , the roots of this equation are;  $\alpha, \alpha^2, \alpha^4 = \alpha + 1, \alpha^8 = \alpha^2 + 1$

All these roots are lie in the field  $F_{2^4}$  where;

$$\begin{cases} A_1 + A_2 + A_3 + A_4 = 1 \\ A_1 \alpha + A_2 \alpha^2 + A_3 (\alpha + 1) + A_4 (\alpha^2 + 1) = 0 \\ A_1 \alpha^2 + A_2 (\alpha + 1) + A_3 (\alpha^2 + 1) + A_4 \alpha = 0 \\ A_1 \alpha^3 + A_2 (\alpha^3 + \alpha^2) + A_3 (\alpha^3 + \alpha^2 + \alpha + 1) + A_4 (\alpha^3 + \alpha) = 0 \end{cases}$$

Solving this system of equation we have;

$$A_1 = \alpha^{14}, A_2 = \alpha^{13}, A_3 = \alpha^{11}, A_4 = \alpha^7$$

Thus, the general term of the sequence is;

$$a_n = \alpha^{14} \cdot \alpha^n + \alpha^{13} \cdot \alpha^{2n} + \alpha^{11} \cdot \alpha^{4n} + \alpha^7 \cdot \alpha^{8n}$$

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

1 0 0 0 1 0 0 1 1 0 1 0 1 1 1 0 0 0 1 0 0 1 1 0 1 0 1 1 1  
1 .....

Suppose the sequence  $\{z_n\}$  is a multiplication sequence on two degrees  $(a_n, \text{ and } a_{n+1})$  of the sequence  $\{a_n\}$  as is showing in figure 1 then;

$$z_n = a_n \cdot a_{n+1}$$

$$a_{n+1} = (\alpha^{14} \cdot \alpha^{n+1} + \alpha^{13} \cdot \alpha^{2n+2} + \alpha^{11} \cdot \alpha^{4n+4} + \alpha^7 \cdot \alpha^{8n+8}) = (\alpha^n + \alpha^{2n} + \alpha^{4n} + \alpha^{8n})$$

Or;

$$z_n = (\alpha^{14} \cdot \alpha^n + \alpha^{13} \cdot \alpha^{2n} + \alpha^{11} \cdot \alpha^{4n} + \alpha^7 \cdot \alpha^{8n}) \cdot (\alpha^{14} \cdot \alpha^{n+1} + \alpha^{13} \cdot \alpha^{2n+2} + \alpha^{11} \cdot \alpha^{4n+4} + \alpha^7 \cdot \alpha^{8n+8})$$

Or;

$$z_n = (\alpha^{14} \cdot \alpha^n + \alpha^{13} \cdot \alpha^{2n} + \alpha^{11} \cdot \alpha^{4n} + \alpha^7 \cdot \alpha^{8n}) \cdot (\alpha^n + \alpha^{2n} + \alpha^{4n} + \alpha^{8n})$$

Or;

$$z_n = \alpha^7 \alpha^n + \alpha^{14} \alpha^{2n} + \alpha^2 \alpha^{3n} + \alpha^{13} \alpha^{4n} + \alpha^{10} \alpha^{5n} + \alpha^4 \alpha^{6n} + \alpha^8 \alpha^{8n} + \alpha^{14} \alpha^{9n} + \alpha^{10} \alpha^{10n} + \alpha^8 \cdot \alpha^{12n}$$

Thus;

$$z_n = (\alpha^3 + \alpha + 1)\alpha^n + (\alpha^3 + 1)\alpha^{2n} + \alpha^2 \alpha^{3n} + (\alpha^3 + \alpha^2 + 1)\alpha^{4n} + (\alpha^2 + \alpha + 1)\alpha^{5n} + (\alpha + 1)\alpha^{6n} + (\alpha^2 + 1)\alpha^{8n} + (\alpha^3 + 1)\alpha^{9n} + (\alpha^2 + \alpha)\alpha^{10n} + (\alpha^2 + 1)\alpha^{12n} \tag{10}$$

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

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

equal to zero and the characteristic equation is;

$$x^{10} + x^5 + x^4 + x^3 + 1 = 0$$

Or;

$$(x^3 + x + 1)(x^7 + x^5 + x^4 + x^3 + x^2 + x + 1) = 0$$

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

$$f(x) = (x - \alpha^n)(x - \alpha^{2n}) \dots (x - \alpha^{12n}) \tag{11}$$

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

$$(x - \alpha^n)(x - \alpha^{2n}) \dots (x - \alpha^{12n}) = 0 \tag{12}$$

We can verify that;

$$\alpha^n \cdot \alpha^{2n} \dots \alpha^{12n} = 1$$

The subsequence as result of  $x^3 + x + 1 = 0$  is periodic with the period  $2^3 - 1 = 8$ ,  $x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$  is a irreducible polynomial. The sequence  $\{z_n\}$ , as a result of the characteristic equation  $x^{10} + x^5 + x^4 + x^3 + 1 = 0$  is periodic with the period  $2^4 - 1 = 15$ , the same period of the sequence  $\{a_n\}$ , and the sequence  $\{z_n\}$  defined by the recurring formula

$$z_{n+10} + z_{n+5} + z_{n+4} + z_{n+3} + z_n = 0 \tag{13}$$

And it is;

The coefficient of  $x^{10}$  and the constant also each of them is equal to one, the other coefficients except;  $x^5, x^4$ , and  $x^3$  are

$$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \dots \tag{14}$$

Thus, the sequence reached its maximum length;

$$\binom{4}{1} + \binom{4}{2} = 4 + \frac{4(4-1)}{2} = 10 \tag{15}$$

And one period, with its cyclic permutations, don't form an orthogonal set. Figure 2 showing the linear feedback shift register which generates  $\{z_n\}$ .

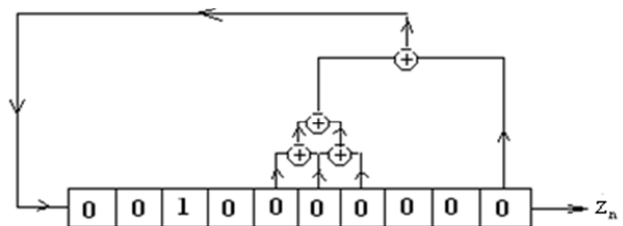


Figure 2. Linear feedback shift register generates the sequence  $\{z_n\}$ .

### 3.1.2. The Sequence $\{z_n\}$ Is a Multiplication on Three Degrees of the Sequence $\{a_n\}$

Suppose the new product sequence  $\{z_n\}$  as a product of three different degrees in  $\{a_n\}$  as following;

- 1) The first degree is  $a_n$  (in another case we can make a shift until to the first term) as in *part1*.
- 2) The second degree is  $b_n = a_{n+\delta}$  (as a result of shift  $n$  by  $\delta$ ).
- 3) The third degree is  $c_n = a_{n+\gamma}$  (as a result of shift the first

by  $\gamma$  and  $\delta \leq r$  &  $\gamma \leq r$ ) then:

$$b_n = a_{n+\delta} = A_1 \alpha_1^\delta \alpha_1^n + A_2 \alpha_2^\delta \alpha_2^n + \dots + A_r \alpha_r^\delta \alpha_r^n = \sum_{i=1}^r A_i \alpha_i^\delta \alpha_i^n$$

$$c_n = a_{n+\gamma} = A_1 \alpha_1^\gamma \alpha_1^n + A_2 \alpha_2^\gamma \alpha_2^n + \dots + A_r \alpha_r^\gamma \alpha_r^n = \sum_{i=1}^r A_i \alpha_i^\gamma \alpha_i^n$$

$$z_n = a_n b_n c_n = \sum_{i=1}^r A_i^3 \alpha_i^{\delta+\gamma} \alpha_i^{3n} + \sum_{\substack{i=1 \\ i \neq j}}^r A_i^2 A_j \left( \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_j^\gamma \right) \alpha_i^{2n} \alpha_j^n + \sum_{\substack{i=1, i \neq j \\ i \neq k, j \neq k}}^r A_i A_j A_k \left( \alpha_j^\delta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\delta + \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_k^\gamma + \alpha_i^\gamma \alpha_k^\delta \right) (\alpha_i^n \alpha_j^n \alpha_k^n)$$

Thus, we have the following properties;

P1. Each term of the first sum, not equal to zero.

P2. For one term of the second sum is equal to zero is equivalent to;

$$\alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_j^\gamma = 0 \quad (16)$$

Or, by division on  $\alpha_i^{\delta+\gamma}$  ;

$$\left( \frac{\alpha_j}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_j}{\alpha_i} \right)^\delta + 1 = 0$$

Suppose;  $A = \left( \frac{\alpha_j}{\alpha_i} \right)$  we have the previous condition is equivalent to;

$$A^\gamma + A^\delta + 1 = 0 \quad (17)$$

P3. For one term of the third sum is equal to zero necessary and sufficient;

$$\alpha_j^\delta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\delta + \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_k^\gamma + \alpha_i^\gamma \alpha_k^\delta = 0 \quad (18)$$

By division on  $\alpha_i^{\delta+\gamma}$  we have;

$$\left( \frac{\alpha_j}{\alpha_i} \right)^\delta \left( \frac{\alpha_k}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_j}{\alpha_i} \right)^\gamma \left( \frac{\alpha_k}{\alpha_i} \right)^\delta + \left( \frac{\alpha_j}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_j}{\alpha_i} \right)^\delta + \left( \frac{\alpha_k}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_k}{\alpha_i} \right)^\delta + 1 = 0 \quad (19)$$

Suppose,  $A = \left( \frac{\alpha_j}{\alpha_i} \right)$  and  $B = \left( \frac{\alpha_k}{\alpha_i} \right)$  then;

conditions;

$$1) \alpha_k^{3n} = \alpha_i^{2n} \alpha_j^n \Rightarrow \alpha_k^3 = \alpha_i^2 \alpha_j^1; \quad (22)$$

$$A^\delta B^\gamma + A^\gamma B^\delta + A^\gamma + A^\delta + B^\gamma + B^\delta + 1 = 0 \quad (20) \quad \text{here, } i, j, k, \text{ are different}$$

This equation is symmetric and can write it as follows;

$$2). A_k^3 \alpha_k^{(\delta+\gamma)} + A_i^2 A_j (\alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_j^\gamma) = 0 \quad (23)$$

$$(A^\delta + 1)(B^\gamma + 1) + (A^\gamma + 1)(B^\delta + 1) = 0 \quad (21)$$

The second condition can be written as;

P4. Sum, one term of the first sum with one term of the second sum, is equal to zero necessary and sufficient the two

$$A_k^3 \left( \frac{\alpha_k}{\alpha_i} \right)^{\delta+\gamma} + A_i^2 A_j \left[ \left( \frac{\alpha_j}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_j}{\alpha_i} \right)^\delta + 1 \right] = 0 \qquad A^\gamma + A^\delta + 1 = \frac{A_k^3}{A_i^2 A_j} B^{\delta+\gamma} \qquad (25)$$

$$\left( \frac{\alpha_j}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_j}{\alpha_i} \right)^\delta + 1 = \frac{A_k^3}{A_i^2 A_j} \left( \frac{\alpha_k}{\alpha_i} \right)^{\delta+\gamma} \qquad (24)$$

P5. Sum, one term of the first sum with one term of the third sum, is equal to zero necessary and sufficient the two conditions;

$$1). \alpha_m^{3n} = (\alpha_i \alpha_j \alpha_k)^n \Rightarrow \alpha_m^3 = \alpha_i \alpha_j \alpha_k \qquad (26)$$

Suppose;  $A = \left( \frac{\alpha_j}{\alpha_i} \right)$  and  $B = \left( \frac{\alpha_k}{\alpha_i} \right)$  then;

Where, no two between the indexes  $i, j, k,$  and  $m$  are equal, and;

$$2). A_m^3 (\alpha_m^{\delta+\gamma}) = A_i A_j A_k (\alpha_j^\delta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\delta + \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_k^\gamma + \alpha_i^\gamma \alpha_k^\delta) = 0 \qquad (27)$$

Or, by division on  $\alpha_i^{\delta+\gamma}$ , the second condition can be written as;

$$A_m^3 \left( \frac{\alpha_m}{\alpha_i} \right)^{\delta+\gamma} + A_i A_j A_k \left[ \begin{aligned} &\left( \frac{\alpha_j}{\alpha_i} \right)^\delta \left( \frac{\alpha_k}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_j}{\alpha_i} \right)^\gamma \left( \frac{\alpha_k}{\alpha_i} \right)^\delta + \\ &\left( \frac{\alpha_j}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_k}{\alpha_i} \right)^\delta + \left( \frac{\alpha_j}{\alpha_i} \right)^\delta + \left( \frac{\alpha_k}{\alpha_i} \right)^\gamma \end{aligned} \right] = 0 \text{ Suppose, } A = \left( \frac{\alpha_j}{\alpha_i} \right), B = \left( \frac{\alpha_k}{\alpha_i} \right), C = \left( \frac{\alpha_m}{\alpha_i} \right) \text{ then;}$$

$$A_m^3 C^{\delta+\gamma} + A_i A_j A_k [A^\delta B^\gamma + A^\gamma B^\delta + A^\lambda + A^\delta + B^\gamma + B^\delta] = 0 \qquad (28)$$

Or;

$$A^\delta B^\gamma + A^\gamma B^\delta + A^\lambda + A^\delta + B^\gamma + B^\delta = \frac{A_m^3}{A_i A_j A_k} C^{\delta+\gamma} \qquad (29)$$

P6. Sum, one term of the second sum with one term of the third sum, is equal to zero necessary and sufficient the two conditions;

$$1). \alpha_l^2 \alpha_m = \alpha_i \alpha_j \alpha_k \qquad (30)$$

Where, no two between the indexes  $i, j, k, m$  and  $l$  are equal, and

$$2). A_l^2 A_m (\alpha_i^\delta \alpha_m^\gamma + \alpha_i^\gamma \alpha_m^\delta + \alpha_i^{\gamma+\delta}) + A_i A_j A_k (\alpha_j^\delta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\delta + \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_k^\gamma + \alpha_i^\gamma \alpha_k^\delta) = 0 \qquad (31)$$

By division on  $\alpha_i^{\delta+\gamma}$  and suppose,  $A = \left( \frac{\alpha_j}{\alpha_i} \right), B = \left( \frac{\alpha_k}{\alpha_i} \right), C = \left( \frac{\alpha_m}{\alpha_i} \right), D = \left( \frac{\alpha_l}{\alpha_i} \right)$  We have;

$$\begin{aligned} &\left( \frac{\alpha_j}{\alpha_i} \right)^\delta \left( \frac{\alpha_k}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_j}{\alpha_i} \right)^\gamma \left( \frac{\alpha_k}{\alpha_i} \right)^\delta + \left( \frac{\alpha_j}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_k}{\alpha_i} \right)^\delta + \left( \frac{\alpha_j}{\alpha_i} \right)^\delta + \left( \frac{\alpha_k}{\alpha_i} \right)^\gamma = \\ &= \frac{A_l^2 A_m}{A_i A_j A_k} \left[ \left( \frac{\alpha_l}{\alpha_i} \right)^\delta \left( \frac{\alpha_m}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_l}{\alpha_i} \right)^\gamma \left( \frac{\alpha_m}{\alpha_i} \right)^\delta + \left( \frac{\alpha_l}{\alpha_i} \right)^{\delta+\gamma} \right] \end{aligned}$$

Or;

$$A^\delta B^\gamma + A^\gamma B^\delta + A^\delta + A^\gamma + B^\delta + B^\gamma = \frac{A_l^2 A_m}{A_i A_j A_k} [D^\delta C^\gamma + D^\gamma C^\delta + D^{\delta+\gamma}] \quad (32)$$

P7. Sum, one term of the first sum, with one term of the second sum, and with one term of the third sum, is equal to zero, necessary and sufficient the two conditions;

$$1). \alpha_m^{3n} = \alpha_h^{2n} \alpha_l^n = (\alpha_i \alpha_j \alpha_k)^n \quad (33)$$

where, no two indexes between  $i, j, k, h, l,$  and  $m$  are equal

$$2). A_m^3 \alpha_m^{\delta+\gamma} + A_h^2 A_l (\alpha_h^\delta \alpha_l^\gamma + \alpha_h^\gamma \alpha_l^\delta + \alpha_h^{\gamma+\delta}) + A_i A_j A_k (\alpha_j^\delta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\delta + \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_k^\gamma + \alpha_i^\gamma \alpha_k^\delta) = 0 \quad (34)$$

By division on  $\alpha_i^{\delta+\gamma}$  and suppose

$$A = \left( \frac{\alpha_j}{\alpha_i} \right), B = \left( \frac{\alpha_k}{\alpha_i} \right), C = \left( \frac{\alpha_m}{\alpha_i} \right), D = \left( \frac{\alpha_l}{\alpha_i} \right), E = \left( \frac{\alpha_h}{\alpha_i} \right) \text{ then;}$$

$$A_m^3 C^{\delta+\gamma} + A_h^2 A_l (E^\delta D^\gamma + E^\gamma D^\delta + E^{\delta+\gamma}) + A_i A_j A_k (A^\delta B^\gamma + A^\gamma B^\delta + A^\delta + A^\gamma + B^\delta + B^\gamma) = 0 \quad (35)$$

Each of P4, ..., and P7 properties leads to decrease the length of linear equivalent by one (for each case) relatively the maximum length  $r, N_h$ .

*Example 2.* Suppose the sequence  $\{a_n\}$  as a result of the linear feedback shift register which showing in the figure 1 as in example 1 and the sequence  $\{z_n\}$  is a multiplication on three degrees of  $\{a_n\}$  as showing in figure 3;

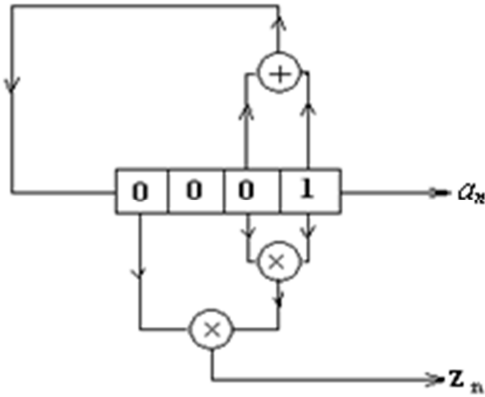


Figure 3. Linear feedback shift register generates the sequence  $\{z_n\}$ .

Where  $a_{n+4} + a_{n+1} + a_n = 0$  and the general term of it is  $\alpha^{14} \alpha^n + \alpha^{13} \alpha^{2n} + \alpha^{11} \alpha^{4n} + \alpha^7 \alpha^{8n}$

And;

$$z_n = a_n \cdot a_{n+1} \cdot a_{n+3}$$

Or;

$$z_n = (\alpha^{14} \alpha^n + \alpha^{13} \alpha^{2n} + \alpha^{11} \alpha^{4n} + \alpha^7 \alpha^{8n}) \cdot (\alpha^{14} \alpha^{n+1} + \alpha^{13} \alpha^{2n+2} + \alpha^{11} \alpha^{4n+4} + \alpha^7 \alpha^{8n+8}) \cdot (\alpha^{14} \alpha^{n+3} + \alpha^{13} \alpha^{2n+6} + \alpha^{11} \alpha^{4n+12} + \alpha^7 \alpha^{8n+24})$$

Or;

$$z_n = (\alpha^{14} \alpha^n + \alpha^{13} \alpha^{2n} + \alpha^{11} \alpha^{4n} + \alpha^7 \alpha^{8n}) \cdot (\alpha^n + \alpha^{2n} + \alpha^{4n} + \alpha^{8n}) \cdot (\alpha^2 \alpha^n + \alpha^4 \alpha^{2n} + \alpha^8 \alpha^{4n} + \alpha \alpha^{8n})$$

Or;

$$z_n = \alpha^{13} \alpha^n + \alpha^{11} \alpha^{2n} + \alpha^7 \alpha^{4n} + \alpha^5 \alpha^{5n} + \alpha \alpha^{7n} + \alpha^{14} \alpha^{8n} + \alpha^{10} \alpha^{10n} + \alpha^8 \alpha^{11n} + \alpha^4 \alpha^{13n} + \alpha^2 \alpha^{14n}$$

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

$$\alpha^n, \alpha^{2n}, \alpha^{4n}, \alpha^{5n}, \alpha^{7n}, \alpha^{8n}, \alpha^{10n}, \alpha^{11n}, \alpha^{13n}, \alpha^{14n}$$

And the characteristic polynomial of the sequence  $\{z_n\}$  defined through the formula;

$$f(x) = (x - \alpha^n)(x - \alpha^{2n}) \dots (x - \alpha^{14n}) \quad (36)$$

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

$$(x - \alpha^n)(x - \alpha^{2n}) \dots (x - \alpha^{14n}) = 0 \quad (37)$$

We can check that;

$$\alpha^n \cdot \alpha^{2n} \dots \alpha^{14n} = 1$$

And the coefficient of  $x^{10}$  and  $x^5$  also is equal to one but the other coefficients of the characteristic equation are equal to zero, or;

$$x^{10} + x^5 + 1 = 0 \quad (38)$$

Or;

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



The subsequence as a result of the characteristic equation  $x^2 + x + 1=0$  is periodic with the period  $2^2-1=3$  and the each subsequence as a result of each of the characteristic equation  $x^4 + x + 1=0$  and  $x^4 + x^3 + 1=0$  is periodic with the period  $2^4-1=15$  then the sequence  $\{z_n\}$  is as a result of the characteristic equation  $x^{10} + x^5 + 1=0$  is periodic with the period  $2^4-1=15$ ,

$$00000001000010000000000010000100..... \tag{40}$$

The complexity of the sequence is 10 and doesn't achieve its maximum length  ${}_4N_3 = 14$ , and the set of all cyclic permutations of one period of  $\{z_n\}$  is not orthogonal set.

From *P2* of *Part2*, For the one term of the second sum is equal to zero necessary?

- 1)  $\alpha_k^{3n} = \alpha_i^{2n} \alpha_j^n \Rightarrow \alpha_k^3 = \alpha_i^2 \alpha_j^1; i \neq j, i \neq k, j \neq k$
- 2)  $A_k^3 \alpha_k^{(\delta+\gamma)} + A_i^2 A_j (\alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_i^\gamma) = 0$

The recurring sequence  $\{z_n\}$  is defined by formula;

$$z_{n+10} + z_{n+5} + z_n = 0 \tag{39}$$

And the sequence  $\{z_n\}$  is;

Here;

$$\begin{cases} A_1 = \alpha^{14}, A_2 = \alpha^{13}, A_3 = \alpha^{11}, A_4 = \alpha^7 \\ \alpha_1 = \alpha, \alpha_2 = \alpha^2, \alpha_3 = \alpha^4, \alpha_4 = \alpha^8 \end{cases}; \delta = 1, \gamma = 3$$

Properties *P1* and *P4* from *Part2* is realized for the following values of  $i, j$  and  $k$  (but the other properties *P2, P3, P5, P6* and *P7* are not realized);

$$a) i = 1, j = 3, k = 2 \Rightarrow (\alpha^2)^{3n} = \alpha^{6n} \ \& \ (\alpha)^{2n} (\alpha^4)^n = \alpha^{6n} \ \text{and};$$

$$(\alpha^{13})^3 (\alpha^2)^{1+3} + (\alpha^{14})^2 (\alpha^{11}) \left( (\alpha)^1 (\alpha^4)^3 + (\alpha)^3 (\alpha^4)^1 + (\alpha^4)^4 \right) = 0$$

$$b) i = 2, j = 4, k = 3 \Rightarrow (\alpha^4)^{3n} = \alpha^{12n} \ \& \ (\alpha^2)^{2n} (\alpha^8)^n = \alpha^{12n} \ \text{and};$$

$$(\alpha^{11})^3 (\alpha^4)^4 + (\alpha^{13})^2 (\alpha^7) \left( (\alpha^2)^1 (\alpha^8)^3 + (\alpha^2)^3 (\alpha^8)^1 + (\alpha^4)^4 \right) = \alpha^{49} + \alpha^{33} (\alpha) = 0$$

$$c) i = 3, j = 1, k = 4 \Rightarrow (\alpha^8)^{3n} = \alpha^{9n} \ \& \ (\alpha^4)^{2n} (\alpha)^n = \alpha^{9n} \ \text{and};$$

$$(\alpha^7)^3 (\alpha^8)^4 + (\alpha^{11})^2 (\alpha^{14}) \left( (\alpha^4)^1 (\alpha)^3 + (\alpha^4)^3 (\alpha)^1 + (\alpha^4)^4 \right) = 0$$

$$d) i = 4, j = 2, k = 1 \Rightarrow (\alpha)^{3n} = \alpha^{3n} \ \& \ (\alpha^8)^{2n} (\alpha^2)^n = \alpha^{3n} \ \text{and};$$

$$(\alpha^{14})^3 (\alpha)^4 + (\alpha^7)^2 (\alpha^{13}) \left( (\alpha^8)^1 (\alpha^2)^3 + (\alpha^8)^3 (\alpha^2)^1 + (\alpha^8)^4 \right) = 0$$

We can see that each of the property; 2, 3, 4, 5, 6, 7 are not realized, for example; For  $i=2, j=3, k=4$  we have;

\* Each term from the first sum is not equal to zero;

$$\sum_{i=1}^r A_i^3 \alpha_i^{\delta+\gamma} \alpha_i^{3n} = \sum_{i=1}^r A_i^3 \alpha_i^5 \alpha_i^{3n}$$

\* Each term from the second sum is not equal to zero, special;

$$\begin{aligned} \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_i^\gamma &= \alpha_2^\delta \alpha_3^\gamma + \alpha_2^\gamma \alpha_3^\delta + \alpha_2^\delta \alpha_2^\gamma \\ &= (\alpha^2)^1 (\alpha^4)^3 + (\alpha^2)^3 (\alpha^4)^1 + \alpha^{1+3} \\ &= \alpha^{14} + \alpha^{10} + \alpha^4 = \alpha^3 + \alpha^2 \\ &= \alpha^9 \neq 0 \end{aligned}$$

\* Each term from the third sum is not equal to zero, special;

$$\begin{aligned}
& \alpha_j^\delta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\delta + \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_k^\gamma + \alpha_i^\gamma \alpha_k^\delta = \\
& = (\alpha^4)^1 (\alpha^8)^3 + (\alpha^4)^3 (\alpha^8)^1 + (\alpha^2)^1 (\alpha^4)^3 + (\alpha^2)^3 (\alpha^4)^1 + (\alpha^2)^1 (\alpha^8)^3 + (\alpha^2)^3 (\alpha^8)^1 \\
& = \alpha^{28} + \alpha^{20} + \alpha^{14} + \alpha^{10} + \alpha^{26} + \alpha^{14} = \alpha \neq 0
\end{aligned}$$

\* Sum one term of the first sum with one term of the second sum is;

$$\begin{aligned}
& A_k^3 \alpha_k^{(\delta+\gamma)} + A_i^2 A_j (\alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_i^\gamma) = \\
& = (\alpha^7)^3 (\alpha^8)^{1+3} + (\alpha^{13})^2 (\alpha^{11}) \left( (\alpha^2)^1 (\alpha^4)^3 + (\alpha^2)^3 (\alpha^4)^1 + (\alpha^2)^4 \right) \\
& = \alpha^{45} + \alpha^{37} (\alpha^7) = \alpha^3 + \alpha + 1 \neq 0
\end{aligned}$$

The same is true for the other properties, and thus, the length of the linear equivalent generated  $\{z_n\}$  is;

$${}_4N_3 - 4 = \binom{4}{1} + \binom{4}{2} + \binom{4}{3} - 4 = 10 \quad (41)$$

The linear equivalent of  $\{z_n\}$  is showing in figure 4;

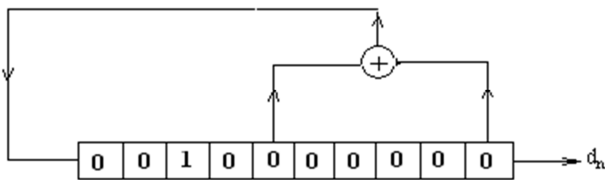


Figure 4. Linear equivalent of product sequence on three degrees of  $\{a_n\}$ .

### 3.1.3. Suppose, the Sequence $\{z_n\}$ Is a Result of

#### Multiplication on Four Terms from the Sequence $\{a_n\}$

As the following; the first term from  $\{a_n\}$  is  $a_n$  (in another

case, we can shift the terms to the first term) second term is  $b_n = a_{n+\beta}$  (as a result of shift the first term by  $\beta$ ), third term is  $c_n = a_{n+\mu}$  (as a result of shift the first term by  $\mu$ ), fourth term is  $d_n = a_{n+\gamma}$  (as a result of shift the first term by  $\gamma$ ) (the all  $\beta, \mu, \gamma$  are less than or equal to  $r$ ), thus;

$$\begin{aligned}
a_n &= A_1 \alpha_1^n + A_2 \alpha_2^n + \dots + A_r \alpha_r^n = \sum_{i=1}^r A_i \alpha_i^n \\
b_n &= A_1 \alpha_1^\beta \alpha_1^n + A_2 \alpha_2^\beta \alpha_2^n + \dots + A_r \alpha_r^\beta \alpha_r^n = \sum_{i=1}^r A_i \alpha_i^{n+\beta} \\
c_n &= A_1 \alpha_1^\mu \alpha_1^n + A_2 \alpha_2^\mu \alpha_2^n + \dots + A_r \alpha_r^\mu \alpha_r^n = \sum_{i=1}^r A_i \alpha_i^{n+\mu} \\
d_n &= A_1 \alpha_1^\gamma \alpha_1^n + A_2 \alpha_2^\gamma \alpha_2^n + \dots + A_r \alpha_r^\gamma \alpha_r^n = \sum_{i=1}^r A_i \alpha_i^{n+\gamma}
\end{aligned}$$

$$\begin{aligned}
z_n &= a_n b_n c_n d_n \\
&= \sum_{i=1}^r A_i^4 \alpha_i^{\beta+\mu+\gamma} \alpha_i^{4n} + \\
&+ \sum_{\substack{i,j=1 \\ i \neq j}}^r A_i^3 A_j (\alpha_i^{\beta+\mu} \alpha_j^\gamma + \alpha_i^{\beta+\gamma} \alpha_j^\mu + \alpha_i^{\mu+\gamma} \alpha_j^\beta + \alpha_i^{\beta+\mu+\gamma}) \alpha_i^{3n} \alpha_j^n + \\
&+ \sum_{\substack{i,j,k=1, i \neq j \\ i \neq k \& j \neq k}}^r A_i^2 A_j A_k \left[ \begin{aligned} & \alpha_i^\beta (\alpha_j^\mu \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\mu) + \alpha_i^\mu (\alpha_j^\beta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\beta) + \\ & \alpha_i^\gamma (\alpha_j^\beta \alpha_k^\mu + \alpha_j^\mu \alpha_k^\beta) + \alpha_i^{\beta+\mu} (\alpha_j^\gamma + \alpha_k^\gamma) + \\ & + \alpha_i^{\beta+\gamma} (\alpha_j^\mu + \alpha_k^\mu) + \alpha_i^{\mu+\gamma} (\alpha_j^\beta + \alpha_k^\beta) \end{aligned} \right] \alpha_i^{2n} \alpha_j^n \alpha_k^n \\
&+ \sum_{\substack{i,j,k,l=1, \\ i,j,k,l \text{ are different}}}^r A_i A_j A_k A_l \left[ \begin{aligned} & \sum_{(j,k,l)} (\alpha_j^\beta \alpha_k^\mu \alpha_l^\gamma) + \alpha_i^\beta (\alpha_j^\mu \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\mu) + \\ & \alpha_i^\mu (\alpha_j^\gamma \alpha_k^\beta + \alpha_j^\beta \alpha_k^\mu) + \alpha_i^\gamma (\alpha_k^\beta \alpha_l^\mu + \alpha_k^\mu \alpha_l^\beta) \end{aligned} \right] (\alpha_i \alpha_j \alpha_k \alpha_l)^n
\end{aligned}$$

Where  $(j, k, l)$  is the set of permutations of  $\{j, k, l\}$ . Thus, we have the following properties;

P1. Each term of the first sum is not equal to zero.

P2. For one term of the second sum is equal to zero to necessary and sufficient;

$$\alpha_i^{\beta+\mu} \alpha_j^\gamma + \alpha_i^{\beta+\gamma} \alpha_j^\mu + \alpha_i^{\mu+\gamma} \alpha_j^\beta + \alpha_i^{\beta+\mu+\gamma} = 0 \quad (42)$$

Or (by division on  $\alpha_i^{\beta+\mu+\gamma}$  and arranging the order of the terms);

$$\left(\frac{\alpha_j}{\alpha_i}\right)^\beta + \left(\frac{\alpha_j}{\alpha_i}\right)^\mu + \left(\frac{\alpha_j}{\alpha_i}\right)^\gamma + 1 = 0 \tag{43}$$

Suppose  $A = \frac{\alpha_j}{\alpha_i}$  then;

$$A^\beta + A^\mu + A^\gamma + 1 = 0 \tag{44}$$

P3. For one term of the third sum is equal to zero is necessary and sufficient realized;

$$\alpha_i^\beta (\alpha_j^\mu \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\mu) + \alpha_i^\mu (\alpha_j^\beta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\beta) + \alpha_i^\gamma (\alpha_j^\beta \alpha_k^\mu + \alpha_j^\mu \alpha_k^\beta) + \alpha_i^{\beta+\mu} (\alpha_j^\gamma + \alpha_k^\gamma) + \alpha_i^{\beta+\gamma} (\alpha_j^\mu + \alpha_k^\mu) + \alpha_i^{\mu+\gamma} (\alpha_j^\beta + \alpha_k^\beta) = 0$$

Or; (by division on  $\alpha_i^{\beta+\mu+\gamma}$  and arrange the terms as necessary);

$$\left(\frac{\alpha_j}{\alpha_i}\right)^\beta \left(\frac{\alpha_k}{\alpha_i}\right)^\mu + \left(\frac{\alpha_j}{\alpha_i}\right)^\mu \left(\frac{\alpha_k}{\alpha_i}\right)^\beta + \left(\frac{\alpha_j}{\alpha_i}\right)^\beta \left(\frac{\alpha_k}{\alpha_i}\right)^\gamma + \left(\frac{\alpha_j}{\alpha_i}\right)^\gamma \left(\frac{\alpha_k}{\alpha_i}\right)^\beta + \left(\frac{\alpha_j}{\alpha_i}\right)^\mu \left(\frac{\alpha_k}{\alpha_i}\right)^\gamma + \left(\frac{\alpha_j}{\alpha_i}\right)^\gamma \left(\frac{\alpha_k}{\alpha_i}\right)^\mu + \left(\frac{\alpha_j}{\alpha_i}\right)^\beta + \left(\frac{\alpha_k}{\alpha_i}\right)^\mu + \left(\frac{\alpha_j}{\alpha_i}\right)^\gamma + \left(\frac{\alpha_k}{\alpha_i}\right)^\beta + \left(\frac{\alpha_j}{\alpha_i}\right)^\mu + \left(\frac{\alpha_k}{\alpha_i}\right)^\gamma = 0$$

Suppose;  $A = \frac{\alpha_j}{\alpha_i}$ ,  $B = \frac{\alpha_k}{\alpha_i}$  then;

$$A^\beta B^\mu + A^\mu B^\beta + A^\beta B^\gamma + A^\gamma B^\beta + A^\mu B^\gamma + A^\gamma B^\mu + (A^\beta + A^\mu + A^\gamma) + (B^\beta + B^\mu + B^\gamma) = 0 \tag{45}$$

And it is a symmetric equation and can writ it as following;

$$(A^\beta + 1)(B^\mu + 1) + (A^\mu + 1)(B^\beta + 1) + (A^\beta + 1)(B^\gamma + 1) + (A^\gamma + 1)(B^\beta + 1) + (A^\mu + 1)(B^\gamma + 1) + (A^\gamma + 1)(B^\mu + 1) + (A^\beta + A^\mu + A^\gamma) + (B^\beta + B^\mu + B^\gamma) = 0$$

P4. For one term from the forth sum is equal to zero is necessary and sufficient realized;

$$\sum_{(j,k,l)} (\alpha_j^\beta \alpha_k^\mu \alpha_l^\gamma) + \alpha_i^\beta (\alpha_j^\mu \alpha_k^\gamma \alpha_l^\mu) + \alpha_i^\mu (\alpha_j^\gamma \alpha_k^\beta \alpha_l^\mu) + \alpha_i^\mu (\alpha_k^\beta \alpha_l^\mu + \alpha_k^\mu \alpha_l^\beta) = 0$$

Or;

$$(\alpha_i^\beta + \alpha_l^\beta) (\alpha_j^\mu \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\mu) + (\alpha_i^\mu + \alpha_k^\mu) (\alpha_j^\gamma \alpha_l^\beta + \alpha_j^\beta \alpha_l^\gamma) + (\alpha_i^\gamma + \alpha_k^\gamma) (\alpha_k^\beta \alpha_l^\mu + \alpha_k^\mu \alpha_l^\beta) = 0$$

By division on  $\alpha_i^{\beta+\mu+\gamma}$  then the latest equation can be written as;

$$\begin{aligned} & \left[ 1 + \left( \frac{\alpha_l}{\alpha_i} \right)^\beta \right] \left[ \left( \frac{\alpha_j}{\alpha_i} \right)^\mu \left( \frac{\alpha_k}{\alpha_i} \right)^\gamma + \left( \frac{\alpha_j}{\alpha_i} \right)^\gamma \left( \frac{\alpha_k}{\alpha_i} \right)^\mu \right] + \\ & \left[ 1 + \left( \frac{\alpha_k}{\alpha_i} \right)^\mu \right] \left[ \left( \frac{\alpha_j}{\alpha_i} \right)^\gamma \left( \frac{\alpha_l}{\alpha_i} \right)^\beta + \left( \frac{\alpha_j}{\alpha_i} \right)^\beta \left( \frac{\alpha_l}{\alpha_i} \right)^\gamma \right] + \\ & \left[ 1 + \left( \frac{\alpha_j}{\alpha_i} \right)^\gamma \right] \left[ \left( \frac{\alpha_k}{\alpha_i} \right)^\beta \left( \frac{\alpha_l}{\alpha_i} \right)^\mu + \left( \frac{\alpha_k}{\alpha_i} \right)^\beta + \left( \frac{\alpha_l}{\alpha_i} \right)^\mu \right] = 0 \end{aligned}$$

Suppose;  $A = \frac{\alpha_j}{\alpha_i}$ ,  $B = \frac{\alpha_k}{\alpha_i}$ ,  $C = \frac{\alpha_l}{\alpha_i}$  then the latest equation can be written as;

$$\begin{aligned} & (1 + C^\beta)(A^\mu B^\gamma + A^\gamma B^\mu) + (1 + B^\mu)(A^\gamma C^\beta + A^\beta C^\gamma) + \\ & (1 + A^\gamma)(B^\beta C^\mu + B^\mu C^\beta) = 0 \end{aligned} \tag{46}$$

P5. For the sum of one term from the first sum with one term from the second sum is equal to zero is necessary and sufficient the following two conditions;

- 1)  $\alpha_k^{4n} = \alpha_i^{3n} \alpha_j^n$  where I, j, k are different
- 2)  $A^4 \alpha_k^{\beta+\mu+\gamma} + A_i^3 A_k (\alpha_i^{\beta+\mu} \alpha_j^\gamma + \alpha_i^{\beta+\gamma} \alpha_j^\mu + \alpha_i^{\mu+\gamma} \alpha_j^\beta + \alpha_i^{\beta+\mu+\gamma}) = 0$

By division on  $\alpha_i^{\beta+\mu+\gamma}$  and suppose,  $A = \frac{\alpha_j}{\alpha_i}$ ,  $B = \frac{\alpha_k}{\alpha_i}$  then the latest equation can be written

as;

$$A_k^4 B^{\beta+\mu+\gamma} + A_i^3 A_j (A^\beta + A^\mu + A^\gamma + 1) = 0$$

P6. For the sum of one term from the first sum with one term from the third sum is equal to zero is necessary and sufficient the two conditions;

$$\alpha_i^{4n} = \alpha_i^{2n} \alpha_j^n \alpha_k^n \text{ Where } i, j, k, \text{ and } l \text{ are different} \tag{47}$$

$$\begin{aligned} & A_i^4 \alpha_i^{\beta+\mu+\gamma} + A_i^2 A_j A_k \left[ \begin{aligned} & \alpha_i^\beta (\alpha_j^\mu \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\mu) + \alpha_i^\mu (\alpha_j^\beta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\beta) + \\ & \alpha_i^\gamma (\alpha_j^\beta \alpha_k^\mu + \alpha_j^\mu \alpha_k^\beta) + \alpha_i^{\beta+\mu} (\alpha_j^\gamma + \alpha_k^\gamma) + \\ & + \alpha_i^{\beta+\gamma} (\alpha_j^\mu + \alpha_k^\mu) + \alpha_i^{\mu+\gamma} (\alpha_j^\beta + \alpha_k^\beta) \end{aligned} \right] = 0 \end{aligned} \tag{48}$$

By division on  $\alpha_i^{\beta+\mu+\gamma}$  and suppose  $A = \frac{\alpha_j}{\alpha_i}$ ,  $B = \frac{\alpha_k}{\alpha_i}$ ,  $C = \frac{\alpha_l}{\alpha_i}$  then the latest equation can be written as;

$$\begin{aligned} & A_i^4 C^{\beta+\mu+\gamma} + A_i^2 A_j A_k \left[ \begin{aligned} & A^\mu B^\gamma + A^\gamma B^\mu + A^\beta B^\gamma + A^\gamma B^\beta + A^\beta B^\mu + A^\mu B^\beta + \\ & + (A^\beta + A^\mu + A^\gamma) + (B^\beta + B^\mu + B^\gamma) \end{aligned} \right] = 0 \end{aligned} \tag{49}$$

Thus, as the same, we have the corresponding relations for the following cases;

- 7) Sum one term from the second sum with one term from the third sum is equal to zero.
- 8) Sum one term from the second sum with one term from the forth sum is equal to zero.
- 9) Sum one term from the third sum with one term from the forth sum is equal to zero.
- 10) The sum of three terms from the different four sums is equal to zero.
- 11) The sum of four terms from the different four sums is

equal to zero.

### 3.2. Multiplication Sequence on Two Linear Sequences Generated by Different LFSR

Suppose  $\alpha \in F_{2^r}$  &  $\beta \in F_{2^s}$ , and  $\alpha$  &  $\beta$  are not in  $F_2$  then  $\alpha.\beta$  is in  $F_{2^t}$ , where  $t$  is the lowest common multiple (*lcm*) of  $m$  and  $n$ , in special case if  $r, s$  are relatively prime then  $t = r.s$ .

Suppose the recurrent binary sequence  $\{a_n\}$  which has the

complexity  $r$  and  $\alpha$  is a primitive root of its characteristic equation then this sequence is periodic and its period is  $2^r - 1$ ,  $\{b_n\}$  is other binary sequence which has the complexity  $s$  and  $\beta$  is a primitive root of its characteristic equation then this sequence is periodic and its period is  $2^s - 1$ , and suppose, for easily,  $r$  and  $s$  are relatively prime then the roots of the characteristic equation of the binary sequence  $\{z_n\} = \{a_n \cdot b_n\}$  are in the field  $F_{2^{r \cdot s}}$  and this sequence has the period  $2^{r \cdot s} - 1$ .

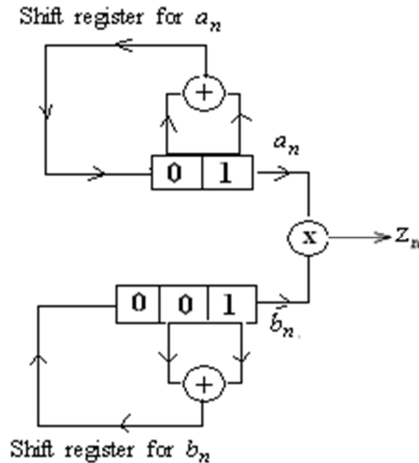


Figure 5. Feedback shift registers for the sequences  $\{a_n\}$ , and  $\{b_n\}$ .

Example 3. Suppose, the linearly binary recurring sequence  $\{a_n\}$  defining through the recurring formula  $a_{n+2} + a_{n+1} + a_n = 0$  or  $a_{n+2} = a_{n+1} + a_n$  and the linearly binary recurring sequence  $\{b_n\}$  defining through the recurring formula  $b_{n+3} + b_{n+1} + b_n = 0$  or  $b_{n+3} = b_{n+1} + b_n$  and  $\{z_n\} = \{a_n \cdot b_n\}$  as in the following figure 5, which shows the feedback shift registers

$$F_{2^3} = \{0, \beta^7 = 1, \beta, \beta^2, \beta^3 = \beta + 1, \beta^4 = \beta^2 + \beta, \beta^5 = \beta^2 + \beta + 1, \beta^6 = \beta^2 + 1\}$$

The general term of the sequence  $\{b_n\}$  is of the form  $b_n = c_1\beta^n + c_2\beta^{2n} + c_3\beta^{4n}$ , by solving the following system for  $n=0, n=1$ , and  $n=2$  we have;

$$\begin{cases} c_1 + c_2 + c_3 = 1 \\ c_1\beta + c_2\beta^2 + c_3\beta^4 = 0 \\ c_1\beta^2 + c_2\beta^4 + c_3\beta^8 = 0 \end{cases}$$

$$z_n = \alpha^2(\alpha\beta)^n + \alpha^2(\alpha\beta^2)^n + \alpha^2(\alpha\beta^4)^n + \alpha(\alpha^2\beta)^n + \alpha(\alpha^2\beta^2)^n + \alpha(\alpha^2\beta^4)^n$$

Thus, the complexity of the sequence  $\{z_n\}$  is 6 and;

$$(\alpha\beta)(\alpha\beta^2)(\alpha\beta^4)(\alpha^2\beta)(\alpha^2\beta^2)(\alpha^2\beta^4) = \alpha^9\beta^{14} = 1$$

And its characteristic equation is of the form;

$$x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + 1 = 0$$

We can find the coefficients  $c_1, c_2, \dots, c_5$  through solving the following recurring system for  $n=0, 1, \dots, 4$  and initial value of  $z_n$  corresponding to them;

for the sequences  $\{a_n\}$ ,  $\{b_n\}$ , and the product sequence  $\{z_n\}$ .

The characteristic equation of the sequence  $\{a_n\}$  is  $x^2 + x + 1 = 0$  and its characteristic polynomial is the prime polynomial  $f(x) = x^2 + x + 1$ . If  $\alpha$  is a root of  $f(x)$  then  $\alpha$  generate the field  $F_{2^2}$  and;

$$F_{2^2} = \{0, \alpha^3 = 1, \alpha, \alpha^2 = \alpha + 1\}$$

The general term of the sequence  $\{a_n\}$  is of the form  $a_n = c_1\alpha^n + c_2\alpha^{2n}$  by solving the following system for  $n=0$  and for  $n=1$  we have;

$$\begin{cases} c_1 + c_2 = 1 \\ c_1\alpha + c_2\alpha^2 = 0 \end{cases}$$

Thus;  $c_1 = \alpha^2 = \alpha + 1$ ,  $c_2 = \alpha$  and the general term of the sequence is  $a_n = \alpha^2\alpha^n + \alpha\alpha^{2n}$

Or;

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

And this sequence is periodic with the period  $2^2 - 1 = 3$  and it is 1 0 1 1 0 1... and the all cyclic permutations of one period form an orthogonal set.

The characteristic equation of the sequence  $\{b_n\}$  is  $x^3 + x + 1 = 0$ , the characteristic polynomial  $g(x) = x^3 + x + 1$  is prime, and if  $\beta$  is a root to  $g(x)$  then  $\beta$  generate  $F_{2^3}$  and;

Thus;  $c_1 = 1, c_2 = 1, c_3 = 1$  and the general term of the sequence  $\{b_n\}$  is  $b_n = \beta^n + \beta^{2n} + \beta^{4n}$

The sequence is periodic with the period  $2^3 - 1 = 7$  and it is 1 0 0 1 0 1 1 1 0 0 1 0 1 1..., and the all cyclic permutations of one period form an orthogonal set.

From the relation  $z_n = a_n \cdot b_n$  we have;

$$z_{n+6} + c_5z_{n+5} + c_4z_{n+4} + c_3z_{n+3} + c_2z_{n+2} + c_1z_{n+1} + z_n = 0$$

Thus, we have;  $c_1 = c_2 = c_4 = 1$  &  $c_3 = c_5 = 0$  and, in result, the recurring equation of  $\{z_n\}$  is;

$$z_{n+6} + z_{n+4} + z_{n+2} + z_{n+1} + z_n = 0$$

The characteristic equation of  $\{z_n\}$  is;

$$x^6 + x^4 + x^2 + x + 1 = 0$$

The linear feedback shift register of the sequence  $\{z_n\}$  is showing in the following figure 6;

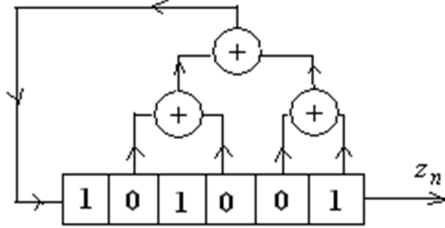


Figure 6. The linear feedback register of the sequence  $\{z_n\}$ .

Thus, the sequence  $\{z_n\}$  is periodic with the period 3 (7)=21 and the set of all cyclic permutations of one period is

$$z_n = \gamma^{42}(\gamma^{21}\gamma^9)^n + \gamma^{42}(\gamma^{21}\gamma^{18})^n + \gamma^{42}(\gamma^{21}\gamma^{36})^n + \gamma^{21}(\gamma^{42}\gamma^9)^n + \gamma^{21}(\gamma^{42}\gamma^{18})^n + \gamma^{21}(\gamma^{42}\gamma^{36})^n$$

Or;

$$z_n = \gamma^{42}(\gamma^{30})^n + \gamma^{42}(\gamma^{39})^n + \gamma^{42}(\gamma^{57})^n + \gamma^{21}(\gamma^{51})^n + \gamma^{21}(\gamma^{60})^n + \gamma^{21}(\gamma^{15})^n$$

Or;

$$z_n = \gamma^{21}(\gamma^{15})^n + \gamma^{42}(\gamma^{30})^n + \gamma^{42}(\gamma^{39})^n + \gamma^{21}(\gamma^{51})^n + \gamma^{42}(\gamma^{57})^n + \gamma^{21}(\gamma^{60})^n$$

We can see that;

$$(\gamma^{15})(\gamma^{30})(\gamma^{39})(\gamma^{51})(\gamma^{57})(\gamma^{60})^n = \gamma^{252} = \gamma^{A(63)} = 1$$

And  $\{z_n\}$  has the complexity 6.

not orthogonal set and the sequence is;

$$1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ \dots$$

In other hand the polynomial  $h(x) = x^6 + x + 1$  is a prime polynomial and if  $\gamma$  is a root of  $h(x)$  in  $F_2^6$  then  $\gamma$  generates  $F_2^6$ ,  $\alpha = \gamma^{21} = \gamma^5 + \gamma^4 + \gamma^3 + \gamma + 1$  generates  $F_2^2$ , and  $\beta = \gamma^9 = \gamma^4 + \gamma^3$  generates  $F_2^3$  (see Appendix).

Thus the general term of the sequence  $\{z_n\}$  can be written through the elements of  $F_2^6$  as following;

less than or equal its maximum length  ${}_rN_h$  and maybe can't reach it where;

$${}_rN_h = \binom{r}{1} + \dots + \binom{r}{h} = r + \frac{r(r-1)}{2} + \dots + \frac{r!}{h!(r-h)!} \quad (51)$$

### 4. Conclusion

1) If the sequence  $\{z_n\}$  is multiplication on only two degrees of the recurring sequence  $\{a_n\}$  and the characteristic polynomial of the sequence  $\{a_n\}$  is prime of degree  $r$  then the equivalent LFSR of  $\{z_n\}$  reached its maximum length

$${}_rN_2 = \binom{r}{1} + \binom{r}{2} = r + \frac{r(r-1)}{2} \quad (50)$$

2) If the sequence  $\{z_n\}$  is multiplication on only two degrees of the recurring sequence  $\{a_n\}$  and the characteristic polynomial of the sequence  $\{a_n\}$  is prime of degree  $r$  then the sequence  $\{z_n\}$  is also periodic and has the same period of  $\{a_n\}$  which equal to  $2^r - 1$  but the cyclic permutations of one period of  $\{z_n\}$  is don't form an orthogonal sequence as the sequence  $\{a_n\}$ .

3) If the sequence  $\{z_n\}$  is multiplication on  $h$  degrees of the recurring sequence  $\{a_n\}$  and the characteristic polynomial of the sequence  $\{a_n\}$  is prime of degree  $r$  then the length of equivalent LFSR of  $\{z_n\}$  usually is

4) Length of the multiplication sequence  $\{z_n\}$  on  $h$  degrees of the linear recurring sequence  $\{a_n\}$  is pending not only with the roots of the characteristic equation of the sequence  $\{a_n\}$  but also pending with the coefficients of the terms in the general solution of the sequence  $\{a_n\}$  and with the shifts of the terms of the sequence  $\{a_n\}$  which on them occur the multiplication.

5) If the sequence  $\{z_n\}$  is a multiplication on two recurring sequences;  $\{a_n\}$  which its characteristic polynomial is prime of degree  $r$  and  $\{b_n\}$  which its characteristic polynomial is prime of degree  $s$  and if  $r$  and  $s$  are relatively prime then the sequence  $\{z_n\}$  is periodic with the period  $(2^r - 1)(2^s - 1)$ , and has the complexity  $r.s$ . I think, if  $r$  and  $s$  are not relatively prime then the period of the sequence  $\{z_n\}$  is  $(2^{lcm(r,s)} - 1)$  and its complexity is  $lcm(r,s)$ .

6) Using multiplication operation on different sequences operation leads to getting sequences with high complexity and with a high period but not orthogonal.



$$\gamma^{13} = \gamma^3 + \gamma$$

$$\gamma^{14} = \gamma^4 + \gamma^2$$

$$\gamma^{15} = \gamma^5 + \gamma^3$$

$$\gamma^{16} = \gamma^4 + \gamma + 1$$

$$\gamma^{17} = \gamma^5 + \gamma^2 + \gamma$$

$$\gamma^{18} = \gamma^3 + \gamma^2 + \gamma + 1$$

$$\gamma^{19} = \gamma^4 + \gamma^3 + \gamma^2 + \gamma$$

$$\gamma^{34} = \gamma^5 + \gamma^2$$

$$\gamma^{35} = \gamma^3 + \gamma + 1$$

$$\gamma^{36} = \gamma^4 + \gamma^2 + \gamma$$

$$\gamma^{37} = \gamma^5 + \gamma^3 + \gamma^2$$

$$\gamma^{38} = \gamma^4 + \gamma^3 + \gamma + 1$$

$$\gamma^{39} = \gamma^5 + \gamma^4 + \gamma^2 + \gamma$$

$$\gamma^{40} = \gamma^5 + \gamma^3 + \gamma^2 + \gamma + 1$$

$$\gamma^{55} = \gamma^5 + \gamma^3 + \gamma^2 + \gamma$$

$$\gamma^{56} = \gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1$$

$$\gamma^{57} = \gamma^5 + \gamma^4 + \gamma^3 + \gamma^2 + \gamma$$

$$\gamma^{58} = \gamma^5 + \gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1$$

$$\gamma^{59} = \gamma^5 + \gamma^4 + \gamma^3 + \gamma^2 + 1$$

$$\gamma^{60} = \gamma^5 + \gamma^4 + \gamma^3 + 1$$

$$\gamma^{61} = \gamma^5 + \gamma^4 + 1, \gamma^{62} = \gamma^5 + 1$$

## References

- 
- [1] Yang K, Kg Kim y Kumar I. d, (2000), "Quasi-orthogonal Sequences for code -Division Multiple Access Systems," *IEEE Trans. information theory*, Vol. 46, No3, PP 982-993.
- [2] Jong-Seon No, Solomon W. & Golomb, (1998), "Binary Pseudorandom Sequences For period  $2^n-1$  with Ideal Autocorrelation," *IEEE Trans. Information Theory*, Vol. 44 No 2, PP 814-817.
- [3] Golomb S. W. (1976), *Shift Register Sequences*, San Francisco – Holden Day.
- [4] Lee J. S & Miller L. E, (1998), "*CDMA System Engineering Hand Book*," Artech House. Boston, London.
- [5] Yang S. C, "*CDMA RF* (1998), *System Engineering*," Artech House. Boston- London.
- [6] Mac Williams, F. G & Sloane, N. G. A., (2006), "*The Theory of Error- Correcting Codes*," North-Holland, Amsterdam.
- [7] Kasami, T. & Tokora, H., (1978), "Teoria Kodirovania," *Mir (Moscow)*.
- [8] 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.
- [9] Al Cheikha A. H. (May 2014), "Matrix Representation of Groups in the finite Fields  $GF(p^n)$ ," *International Journal of Soft Computing and Engineering*, Vol. 4, Issue 2, PP 118-125.
- [10] Lidl, R. & Pilz, G., (1984), "*Applied Abstract Algebra*," Springer – Verlage New York, 1984.
- [11] Lidl, R. & Niderreiter, H., (1994), "Introduction to Finite Fields and Their Application," *Cambridge university USA*.
- [12] Thomson W. Judson, (2013), "*Abstract Algebra: Theory and Applications*," Free Software Foundation.
- [13] Fraleigh, J. B., (1971), "A First course In Abstract Algebra, *Fourth printing*. Addison- Wesley publishing company USA.
- [14] David, J., (2008), "Introductory Modern Algebra," *Clark University USA*.