International Journal of Information and Communication Sciences
2020; 5(3): 17-32
http://www.sciencepublishinggroup.com/j/ijics
doi: 10.11648/j.ijics.20200503.11
ISSN: 2575-1700 (Print); ISSN: 2575-1719 (Online)

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. 17-32. doi: 10.11648/j.ijics.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., discuses 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 ${}_rN_h = \binom{r}{1} + \binom{r}{2} + \ldots + \binom{r}{h}$. [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 $\lambda, \lambda_0, \lambda_1, \ldots, \lambda_{k-1}$ are elements in the field $F_2=\{0, 1\}$ then the sequence $a_0, a_1, \ldots$ is called the nonhomogeneous binary linear recurring sequence of order k (or with the complexity k) *iff*:

$$a_{n+k} = \lambda_{k-1}a_{n+k-1} + \lambda_{k-2}a_{n+k-2} + ... + \lambda_0 a_n + \lambda;\ \lambda\ \&\ \lambda_i \in F_2,\ i = 0,1,...,k-1$$
$$or \qquad a_{n+k} = \sum_{i=1}^{k-1} \lambda_i a_{n+i} + \lambda \tag{1}$$

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

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

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

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

$$a_{n+r} = a_n \ ; \quad n = 0, 1, ... \ [2\text{-}6]$$

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 $X = (x_1, x_2, ..., x_n), x_i \in F_2 = \{0,1\}$ is the vector $\overline{X} = (\overline{x_1}, \overline{x_2}, ..., \overline{x_n})$, where:

$$\overline{x_i} = \begin{cases} 1 & if \quad x_i = 0 \\ 0 & if \quad x_i = 1 \end{cases}. \ [2, 6\text{-}7]$$

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 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 $x = (x_0, x_1, ..., x_{n-1})$ and $y = (y_0, y_1, ..., y_{n-1})$ are binary vectors of length n on F_2, or components belong to {1, -1}, is said orthogonal if $|R_{x,y}| \le 1$. [8-9]

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

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

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

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

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

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 ϕ). $\phi(n)$ 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]

Theorem12.

i. If $a_0, a_1, ...$ 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 $r \mid ord\, f(x)$.

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:

$$x^q = x \text{ . [6, 10]}$$

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

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

Theorem 15.

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

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 $\alpha_1, \alpha_2, \ldots, \alpha_r$ 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;

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

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

$$a_n = A_1\alpha^n + A_2(\alpha^{22-1})^n + \ldots + A_r(\alpha^{2^{r-1}})^n = \sum_{i=1}^{r} A_i(\alpha^{2i-1})^n \quad (8)$$

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 δ.

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

Or;

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

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

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

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

Thus we have the following properties;

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

*P*2. Also, a term of the second sum is equal to zero if and only if;

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

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;

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

*P*3. 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;

$$A_k^2\alpha_k^{\delta}\alpha_k^{2n} = A_iA_j\left(\alpha_i^{\delta}+\alpha_j^{\delta}\right)\alpha_i^n\alpha_j^n$$

And it is equivalents the two conditions;

1) $\alpha_k^{2n} = \alpha_i^n\alpha_j^n$ or $\alpha_k^2 = \alpha_i\alpha_j$

2) $A_k^2\alpha_k^{\delta} = A_iA_j(\alpha_i^{\delta}+\alpha_j^{\delta})$ or $\alpha_i^{\delta}+\alpha_j^{\delta} = \dfrac{A_k^2}{A_iA_j}\alpha_k^{\delta}$

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

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

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

$$\alpha^{2.2^{k-1}} = \alpha^{2^{i-1}}\alpha^{2^{j-1}} \Rightarrow \alpha^{2^k} = \alpha^{2^{i-1}+2^{j-1}}$$

Or if i is the smallest;

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

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

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;

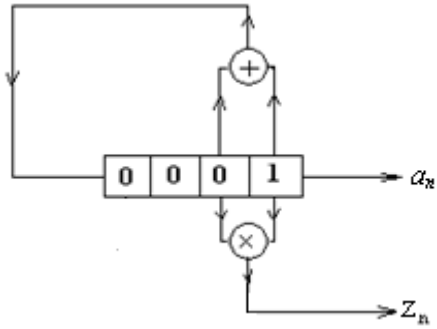

Figure 1. *Linear feedback shift register with 4 complexity over* F_2.

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;

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

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;

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

Or;

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

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;

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

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 1 0 0 0 1 0 0 1 1 0 1 0 1 1 1 …….

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

$$z_n = a_n.a_{n+1}$$

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

Or;

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

Or;

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

Or;

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

Thus;

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

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

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

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

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

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

$$(x-\alpha^n)(x-\alpha^{2n}) \ldots (x-\alpha^{12n}) = 0 \quad (12)$$

We can verify that;

$$\alpha^n.\alpha^{2n} \ldots \alpha^{12n} = 1$$

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 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 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

$$z_{n+10} + z_{n+5} + z_{n+4} + z_{n+3} + z_n = 0 \quad (13)$$

And it is;

0 0 0 0 0 0 0 1 0 0 0 0 1 1 1 0 0 0 0 0 0 0 1 0 0 0 0 1 1 1……. (14)

Thus, the sequence reached its maximum length;

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

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

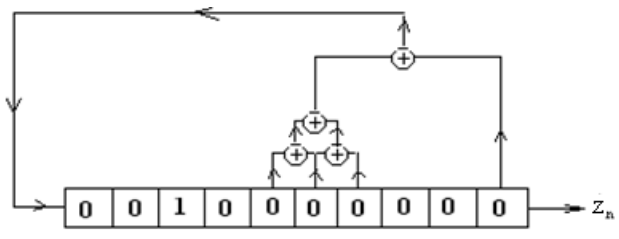

Figure 2. *Linear feedback shift register generates the sequence $\{z_n\}$.*

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 *part*1.
2) The second degree is $b_n = a_{n+\delta}$ (as a result of shift n by δ).
3) The third degree is $c_n = a_n + \gamma$ (as a result of shift the first by γ and $\delta \le r \,\&\, \gamma \le r$) then:

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

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

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

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

Thus, we have the following properties;

*P*1. Each term of the first sum, not equal to zero.

*P*2. For one term of the second sum is equal to zero is equivalent to;

$$\alpha_i^{\delta}\alpha_j^{\gamma} + \alpha_i^{\gamma}\alpha_j^{\delta} + \alpha_i^{\delta}\alpha_i^{\gamma} = 0 \tag{16}$$

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;

$$A^{\gamma} + A^{\delta} + 1 = 0 \tag{17}$$

*P*3. For one term of the third sum is equal to zero necessary and sufficient;

$$\alpha_j^{\delta}\alpha_k^{\gamma} + \alpha_j^{\gamma}\alpha_k^{\delta} + \alpha_i^{\delta}\alpha_j^{\gamma} + \alpha_i^{\gamma}\alpha_j^{\delta} + \alpha_i^{\delta}\alpha_k^{\gamma} + \alpha_i^{\gamma}\alpha_k^{\delta} = 0 \tag{18}$$

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

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

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

$$A^{\delta}B^{\gamma} + A^{\gamma}B^{\delta} + A^{\gamma} + A^{\delta} + B^{\gamma} + B^{\delta} + 1 = 0 \tag{20}$$

This equation is symmetric and can write it as follows;

$$(A^{\delta} + 1)(B^{\gamma} + 1) + (A^{\gamma} + 1)(B^{\delta} + 1) = 0 \tag{21}$$

*P*4. Sum, one term of the first sum with one term of the second sum, is equal to zero necessary and sufficient the two conditions;

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

here, i, j, k, are different

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

The second condition can be written as;

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

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

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

$$A^{\gamma}+A^{\delta}+1=\frac{A_k^3}{A_i^2A_j}B^{\delta+\gamma} \quad (25)$$

*P*5. Sum, one term of the first sum with one term of the third sum, is equal to zero necessary and sufficient the two conditions;

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

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

$$2).\ A_m^3(\alpha_m^{\delta+\gamma})=A_iA_jA_k\left(\alpha_j^{\delta}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\delta}+\alpha_i^{\delta}\alpha_j^{\gamma}+\alpha_i^{\gamma}\alpha_j^{\delta}+\alpha_i^{\delta}\alpha_k^{\gamma}+\alpha_i^{\gamma}\alpha_k^{\delta}\right)=0 \quad (27)$$

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

$$A_m^3\left(\frac{\alpha_m}{\alpha_i}\right)^{\delta+\gamma}+A_iA_jA_k\left[\begin{array}{l}\left(\frac{\alpha_j}{\alpha_i}\right)^{\delta}\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_k}{\alpha_i}\right)^{\delta}+\\ \left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha_k}{\alpha_i}\right)^{\delta}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\delta}+\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma}\end{array}\right]=0$$ Suppose, $A=\left(\frac{\alpha_j}{\alpha_i}\right)$, $B=\left(\frac{\alpha_k}{\alpha_i}\right)$, $C=\left(\frac{\alpha_m}{\alpha_i}\right)$ then;

$$A_mC^{\delta+\gamma}+A_iA_jA_k[A^{\delta}B^{\gamma}+A^{\gamma}B^{\delta}+A^{\lambda}+A^{\delta}+B^{\gamma}+B^{\delta}]=0 \quad (28)$$

Or;

$$A^{\delta}B^{\gamma}+A^{\gamma}B^{\delta}+A^{\lambda}+A^{\delta}+B^{\gamma}+B^{\delta}=\frac{A_m}{A_iA_jA_k}C^{\delta+\gamma} \quad (29)$$

*P*6. Sum, one term of the second sum with one term of the third sum, is equal to zero necessary and sufficient the two conditions;

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

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

$$\begin{aligned}2).&A_l^2A_m(\alpha_l^{\delta}\alpha_m^{\gamma}+\alpha_l^{\gamma}\alpha_m^{\delta}+\alpha_l^{\gamma+\delta})+A_iA_jA_k(\alpha_j^{\delta}\alpha_k^{\gamma}+\\ &\alpha_j^{\gamma}\alpha_k^{\delta}+\alpha_i^{\delta}\alpha_j^{\gamma}+\alpha_i^{\gamma}\alpha_j^{\delta}+\alpha_i^{\delta}\alpha_k^{\gamma}+\alpha_i^{\gamma}\alpha_k^{\delta})=0\end{aligned} \quad (31)$$

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;

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

$$=\frac{A_l^2A_m}{A_iA_jA_k}\left[\left(\frac{\alpha_l}{\alpha_i}\right)^{\delta}\left(\frac{\alpha_m}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha_l}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_m}{\alpha_i}\right)^{\delta}+\left(\frac{\alpha_l}{\alpha_i}\right)^{\delta+\gamma}\right]$$

Or;

$$A^{\delta}B^{\gamma}+A^{\gamma}B^{\delta}+A^{\delta}+A^{\gamma}+B^{\delta}+B^{\gamma}=\frac{A_l^2A_m}{A_iA_jA_k}\left[D^{\delta}C^{\gamma}+D^{\gamma}C^{\delta}+D^{\delta+\gamma}\right] \tag{32}$$

*P*7. 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;

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

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

$$\begin{aligned}&2).A_m^3\alpha_m^{\delta+\gamma}+A_h^2A_l(\alpha_h^{\delta}\alpha_l^{\gamma}+\alpha_h^{\gamma}\alpha_l^{\delta}+\alpha_h^{\gamma+\delta})+A_iA_jA_k(\alpha_j^{\delta}\alpha_k^{\gamma}+\\&\alpha_j^{\gamma}\alpha_k^{\delta}+\alpha_i^{\delta}\alpha_j^{\gamma}+\alpha_i^{\gamma}\alpha_j^{\delta}+\alpha_i^{\delta}\alpha_k^{\gamma}+\alpha_i^{\gamma}\alpha_k^{\delta})=0\end{aligned} \tag{34}$$

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

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

$$\begin{aligned}&A_m^3C^{\delta+\gamma}+A_h^2A_l(E^{\delta}D^{\gamma}+E^{\gamma}D^{\delta}+E^{\delta+\gamma})+\\&A_iA_jA_k\left(A^{\delta}B^{\gamma}+A^{\gamma}B^{\delta}+A^{\delta}+A^{\gamma}+B^{\delta}+B^{\gamma}\right)=0\end{aligned} \tag{35}$$

Each of *P*4,…., and *P*7 properties leads to decrease the length of linear equivalent by one (for each case) relatively the maximum length ${}_rN_h$.

Example 2. Suppose the sequence $\{a_n\}$ as a result of the linear feedback shift register which showing in the figure 1 as in example1and the sequence $\{z_n\}$ is a multiplication on three degrees of $\{a_n\}$ as showing in figure 3;

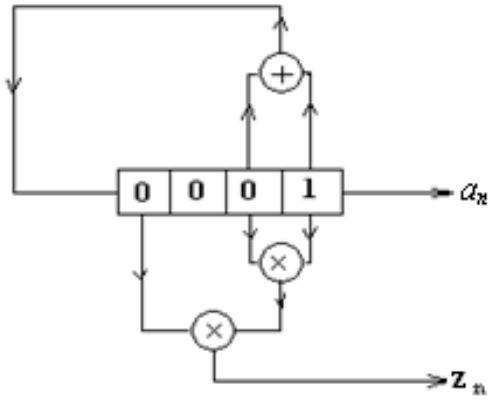

Figure 3. *Linear feedback shift register generates the sequence $\{z_n\}$.*

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;

$$z_n=a_n.a_{n+1}.a_{n+3}$$

Or;

$$\begin{aligned}z_n=&\left(\alpha^{14}.\alpha^n+\alpha^{13}.\alpha^{2n}+\alpha^{11}.\alpha^{4n}+\alpha^7.\alpha^{8n}\right).\\&.\left(\alpha^{14}.\alpha^{n+1}+\alpha^{13}.\alpha^{2n+2}+\alpha^{11}.\alpha^{4n+4}+\alpha^7.\alpha^{8n+8}\right).\\&.\left(\alpha^{14}.\alpha^{n+3}+\alpha^{13}.\alpha^{2n+6}+\alpha^{11}.\alpha^{4n+12}+\alpha^7.\alpha^{8n+24}\right)\end{aligned}$$

Or;

$$\begin{aligned}z_n=&\left(\alpha^{14}.\alpha^n+\alpha^{13}.\alpha^{2n}+\alpha^{11}.\alpha^{4n}+\alpha^7.\alpha^{8n}\right).\left(\alpha^n+\alpha^{2n}+\alpha^{4n}+\alpha^{8n}\right).\\&.\left(\alpha^2.\alpha^n+\alpha^4.\alpha^{2n}+\alpha^8.\alpha^{4n}+\alpha.\alpha^{8n}\right)\end{aligned}$$

Or;

$$\begin{aligned}z_n=&\alpha^{13}\alpha^n+\alpha^{11}\alpha^{2n}+\alpha^7\alpha^{4n}+\alpha^5\alpha^{5n}+\alpha\alpha^{7n}+\\&\alpha^{14}\alpha^{8n}+\alpha^{10}\alpha^{10n}+\alpha^8\alpha^{11n}+\alpha^4.\alpha^{13n}+\alpha^2\alpha^{14n}\end{aligned}$$

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;

$$f(x)=(x-\alpha^n)(x-\alpha^{2n})\ldots..(x-\alpha^{14n}) \tag{36}$$

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

$$(x-\alpha^n)(x-\alpha^{2n})\ldots..(x-\alpha^{14n})=0 \tag{37}$$

We can check that;

$$\alpha^n.\alpha^{2n}\ldots..\alpha^{14n}=1$$

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;

$$x^{10}+x^5+1=0 \tag{38}$$

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,

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;

$$0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\ldots\ldots. \tag{40}$$

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 *P*2 of *Part*2, 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) $A_k^3\alpha_k^{(\delta+\gamma)}+A_i^2A_j(\alpha_i^\delta\alpha_j^\gamma+\alpha_i^\gamma\alpha_j^\delta+\alpha_i^\delta\alpha_i^\gamma)=0$

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 *P*1 and *P*4 from *Part*2 is realized for the following values of *i*, *j* and *k* (but the other properties *P*2, *P*3, *P*5, *P*6 and *P*7 are not realized);

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

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

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

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

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

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

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

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

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;

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

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

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

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

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

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

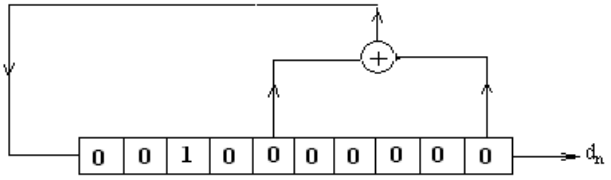

Figure 4. *Linear equivalent of product sequence on three degrees of $\{a_n\}$.*

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 β), third term is $c_n=a_{n+\mu}$ (as a result of shift the first term by μ), forth term is $d_n=a_{n+\gamma}$ (as a result of shift the first term by γ) (the all β,μ,γ are less than or equal to *r*), thus;

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

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

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

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

$$z_n=a_nb_nc_nd_n$$
$$=\sum_{i=1}^{r}A_i^4\alpha_i^{\beta+\mu+\gamma}\alpha_i^{4n}+$$
$$+\sum_{\substack{i,j=1\\ i\neq j}}^{r}A_i^3A_j(\alpha_i^{\beta+\mu}\alpha_j^r+\alpha_i^{\beta+\gamma}\alpha_j^{\mu}+\alpha_i^{\mu+\gamma}\alpha_j^{\beta}+\alpha_i^{\beta+\mu+\gamma})\alpha_i^{3n}\alpha_j^n+$$
$$+\sum_{\substack{i,j,k=1,i\neq j\\ i\neq k\,\&\,j\neq k}}^{r}A_i^2A_jA_k\begin{bmatrix}\alpha_i^{\beta}\left(\alpha_j^{\mu}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\mu}\right)+\alpha_i^{\mu}\left(\alpha_j^{\beta}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\beta}\right)+\\ \alpha_i^{\gamma}\left(\alpha_j^{\beta}\alpha_k^{\mu}+\alpha_j^{\mu}\alpha_k^{\beta}\right)+\alpha_i^{\beta+\mu}\left(\alpha_j^{\gamma}+\alpha_k^{\gamma}\right)+\\ +\alpha_i^{\beta+\gamma}\left(\alpha_j^{\mu}+\alpha_k^{\mu}\right)+\alpha_i^{\mu+\gamma}\left(\alpha_j^{\beta}+\alpha_k^{\beta}\right)\end{bmatrix}\alpha_i^{2n}\alpha_j^n\alpha_k^n$$

$$+\sum_{\substack{i,j,k,l=1,\\ i,j,k,l\,are\,different}}^{r}A_iA_jA_kA_l\begin{bmatrix}\sum_{(j,k,l)}\left(\alpha_j^{\beta}\alpha_k^{\mu}\alpha_l^{\gamma}\right)+\alpha_i^{\beta}\left(\alpha_j^{\mu}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\mu}\right)+\\ \alpha_i^{\mu}\left(\alpha_j^{\gamma}\alpha_l^{\beta}+\alpha_j^{\beta}\alpha_l^{\mu}\right)+\alpha_i^{\gamma}\left(\alpha_k^{\beta}\alpha_l^{\mu}+\alpha_k^{\mu}\alpha_l^{\beta}\right)\end{bmatrix}(\alpha_i\alpha_j\alpha_k\alpha_l)^n$$

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

*P*1. Each term of the first sum is not equal to zero.

*P*2. For one term of the second sum is equal to zero to necessary and sufficient;

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

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;

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

*P*3. For one term of the third sum is equal to zero is necessary and sufficient realized;

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

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;

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

Or;

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

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

$$\left[1+\left(\frac{\alpha_l}{\alpha_i}\right)^{\beta}\right]\left[\left(\frac{\alpha_j}{\alpha_i}\right)^{\mu}\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha^j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_k}{\alpha_i}\right)^{\mu}\right]+$$
$$\left[1+\left(\frac{\alpha_k}{\alpha_i}\right)^{\mu}\right]\left[\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_l}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\beta}\left(\frac{\alpha_l}{\alpha_i}\right)^{\gamma}\right]+$$
$$\left[1+\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\right]\left[\left(\frac{\alpha_k}{\alpha_i}\right)^{\beta}\left(\frac{\alpha_l}{\alpha_i}\right)^{\mu}+\left(\frac{\alpha_k}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_l}{\alpha_i}\right)^{\mu}\right]=0$$

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;

$$(1+C^{\beta})(A^{\mu}B^{\gamma}+A^{\gamma}B^{\mu})+(1+B^{\mu})(A^{\gamma}C^{\beta}+A^{\beta}C^{\gamma})+$$
$$(1+A^{\gamma})(B^{\beta}C^{\mu}++B^{\mu}C^{\beta})=0 \quad (46)$$

*P*5. 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) $A_k^4\alpha_k^{\beta+\mu+\gamma}+A_i^3A_k(\alpha_i^{\beta+\mu}\alpha_j^{\gamma}+\alpha_i^{\beta+\gamma}\alpha_j^{\mu}+\alpha_i^{\mu+\gamma}\alpha_j^{\beta}+\alpha_i^{\beta+\mu+\gamma})=0$

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;

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

*P*6. 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;

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

$$A_l^4\alpha_l^{\beta+\mu+\gamma}+A_i^2A_jA_k\begin{bmatrix}\alpha_i^{\beta}\left(\alpha_j^{\mu}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\mu}\right)+\alpha_i^{\mu}\left(\alpha_j^{\beta}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\beta}\right)+\\ \alpha_i^{\gamma}\left(\alpha_j^{\beta}\alpha_k^{\mu}+\alpha_j^{\mu}\alpha_k^{\beta}\right)+\alpha_i^{\beta+\mu}\left(\alpha_j^{\gamma}+\alpha_k^{\gamma}\right)+\\ +\alpha_i^{\beta+\gamma}\left(\alpha_j^{\mu}+\alpha_k^{\mu}\right)+\alpha_i^{\mu+\gamma}\left(\alpha_j^{\beta}+\alpha_k^{\beta}\right)\end{bmatrix}=0 \quad (48)$$

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;

$$A_l^4C^{\beta+\mu+\gamma}+A_i^2A_jA_k\begin{bmatrix}A^{\mu}B^{\gamma}+A^{\gamma}B^{\mu}+A^{\beta}B^{\gamma}+A^{\gamma}B^{\beta}+A^{\beta}B^{\mu}+A^{\mu}B^{\beta}+\\ +(A^{\beta}+A^{\mu}+A^{\gamma})+(B^{\beta}+B^{\mu}+B^{\gamma})\end{bmatrix}=0 \quad (49)$$

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

1. Sum one term from the second sum with one term from the third sum is equal to zero.
2. Sum one term from the second sum with one term from the forth sum is equal to zero.
3. Sum one term from the third sum with one term from the forth sum is equal to zero.
4. The sum of three terms from the different four sums is equal to zero.
5. 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 α & β 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 α 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 β 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 $\{z_n\}=\{a_n.b_n\}$ are in the field $F_{2^{r.s}}$ and this sequence has the period $2^{r.s}$-1.

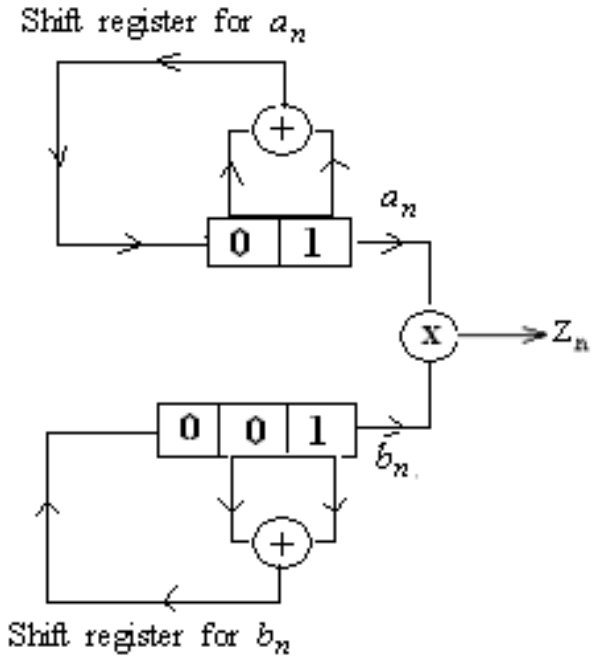

Figure 5. *Feedback shift registers for the sequences $\{a_n\}$, and $\{b_n\}$.*

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 $\{z_n\}=\{a_n. b_n\}$ as in the following figure 5, which shows the feedback shift registers 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 α is a root of $f(x)$ then α 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=1we 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 β is a root to $g(x)$ then β generate F_{2^3} and;

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

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;

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

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 $z_n = a_n.b_n$ we have;

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

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;

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

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

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

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;

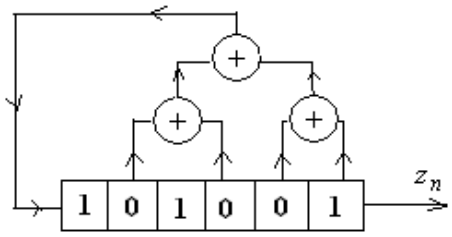

Figure 6. *The linear feedback register of the sequence $\{z_n\}$.*

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

In other hand the polynomial $h(x)=x^6+x+1$ is a prime polynomial and if γ is a root of $h(x)$ in $F_2{}^6$ then γ 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;

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

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;

$$(\gamma^{15})(\gamma^{30})(\gamma^{39})(\gamma^{51})(\gamma^{57})(\gamma^{60})^n=\gamma^{252}=\gamma^{4(63)}=1$$

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

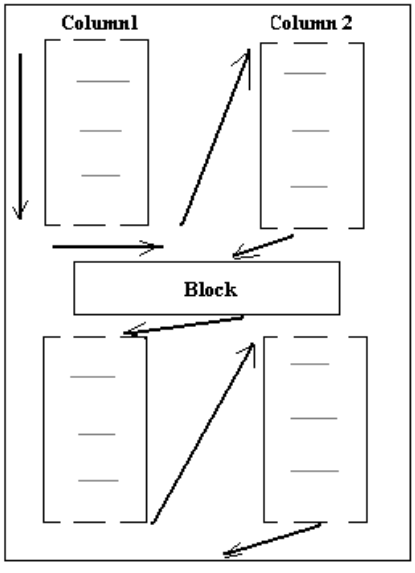

Figure 7. *Method reading page with block.*

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

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

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.

Limitation: This method of compose sequences is useful for only binary sequences and the addition on the sequences computed by "*mod* 2 " also used Microsoft Word 2010 and the Microsoft equation 3.0 for written the math equations.

The method for reading a page which has a block will be according to the following direction as in figure 1.

Appendix: Elements F_{2^6}

F_{2^6}		
0	$\gamma^{20} = \gamma^5 + \gamma^4 + \gamma^3 + \gamma^2$	$\gamma^{41} = \gamma^4 + \gamma^3 + \gamma^2 + 1$
$\gamma^{63} = 1$	$\gamma^{21} = \gamma^5 + \gamma^4 + \gamma^3 + \gamma + 1$	$\gamma^{42} = \gamma^5 + \gamma^4 + \gamma^3 + \gamma$
γ	$\gamma^{22} = \gamma^5 + \gamma^4 + \gamma^2 + 1$	$\gamma^{43} = \gamma^5 + \gamma^4 + \gamma^2 + \gamma = 1$
γ^2	$\gamma^{23} = \gamma^5 + \gamma^3 + 1$	$\gamma^{44} = \gamma^5 + \gamma^3 + \gamma^2 + 1$
γ^3	$\gamma^{24} = \gamma^4 + 1$	$\gamma^{45} = \gamma^4 + \gamma^3 + 1$
γ^4	$\gamma^{25} = \gamma^5 + \gamma$	$\gamma^{46} = \gamma^5 + \gamma^4 + \gamma$
γ^5	$\gamma^{26} = \gamma^2 + \gamma + 1$	$\gamma^{47} = \gamma^5 + \gamma^3 + \gamma + 1$
$\gamma^6 = \gamma + 1$	$\gamma^{27} = \gamma^3 + \gamma^2 + \gamma$	$\gamma^{48} = \gamma^3 + \gamma^2 + 1$
$\gamma^7 = \gamma^2 + \gamma$	$\gamma^{28} = \gamma^4 + \gamma^3 + \gamma^2$	$\gamma^{49} = \gamma^4 + \gamma^3 + \gamma$
$\gamma^8 = \gamma^3 + \gamma^2$	$\gamma^{29} = \gamma^5 + \gamma^4 + \gamma^3$	$\gamma^{50} = \gamma^5 + \gamma^4 + \gamma^2$
$\gamma^9 = \gamma^4 + \gamma^3$	$\gamma^{30} = \gamma^5 + \gamma^4 + \gamma + 1$	$\gamma^{51} = \gamma^5 + \gamma^3 + \gamma + 1$
$\gamma^{10} = \gamma^5 + \gamma^4$	$\gamma^{31} = \gamma^5 + \gamma^2 = 1$	$\gamma^{52} = \gamma^4 + \gamma^2 + 1$
$\gamma^{11} = \gamma^5 + \gamma + 1$	$\gamma^{32} = \gamma^3 + 1$	$\gamma^{53} = \gamma^5 + \gamma^3 + \gamma$
$\gamma^{12} = \gamma^2 + 1$	$\gamma^{33} = \gamma^4 + \gamma$	$\gamma^{54} = \gamma^4 + \gamma^2 + \gamma + 1$
$\gamma^{13} = \gamma^3 + \gamma$	$\gamma^{34} = \gamma^5 + \gamma^2$	$\gamma^{55} = \gamma^5 + \gamma^3 + \gamma^2 + \gamma$
$\gamma^{14} = \gamma^4 + \gamma^2$	$\gamma^{35} = \gamma^3 + \gamma + 1$	$\gamma^{56} = \gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1$
$\gamma^{15} = \gamma^5 + \gamma^3$	$\gamma^{36} = \gamma^4 + \gamma^2 + \gamma$	$\gamma^{57} = \gamma^5 + \gamma^4 + \gamma^3 + \gamma^2 + \gamma$
$\gamma^{16} = \gamma^4 + \gamma + 1$	$\gamma^{37} = \gamma^5 + \gamma^3 + \gamma^2$	$\gamma^{58} = \gamma^5 + \gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1$
$\gamma^{17} = \gamma^5 + \gamma^2 + \gamma$	$\gamma^{38} = \gamma^4 + \gamma^3 + \gamma + 1$	$\gamma^{59} = \gamma^5 + \gamma^4 + \gamma^3 + \gamma^2 + 1$
$\gamma^{18} = \gamma^3 + \gamma^2 + \gamma + 1$	$\gamma^{39} = \gamma^5 + \gamma^4 + \gamma^2 + \gamma$	$\gamma^{60} = \gamma^5 + \gamma^4 + \gamma^3 + 1$
$\gamma^{19} = \gamma^4 + \gamma^3 + \gamma^2 + \gamma$	$\gamma^{40} = \gamma^5 + \gamma^3 + \gamma^2 + \gamma + 1$	$\gamma^{61} = \gamma^5 + \gamma^4 + 1$; $\gamma^{62} = \gamma^5 + 1$

References

[1] Yang K, Kg Kim y Kumar l. 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-1with Ideal Autocorrelation*, "IEEE Trans. Information Theory*, Vol. 44 No 2, PP 814-817.

[3] Golamb 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 Wiliams, 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.