International Journal of Information and Communication Sciences
2020; 5(4): 46-68
http://www.sciencepublishinggroup.com/j/ijics
doi: 10.11648/j.ijics.20200504.12
ISSN: 2575-1700 (Print); ISSN: 2575-1719 (Online)

Study the Linear Equivalent of Nonlinear Sequences over *Fp* Where p Is Larger Than Two

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

[1]Department of Mechatronics, College of Mechanical Add Electronical Engineering, Tishreen University, Lattakia, Syria

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

Email address:
Dianamokayes@gmail.com (D. Mokayes), alcheikhaa@yahoo.com (A. H. Al Cheikha)

[*]Corresponding author

To cite this article:
Diana Mokayes, Ahmad Hamza Al Cheikha. Study the Linear Equivalent of Nonlinear Sequences over *Fp* Where p Is Larger Than Two. *International Journal of Information and Communication Sciences*. Vol. 5, No. 4, 2020, pp. 46-68. doi: 10.11648/j.ijics.20200504.12

Received: January 25, 2021; **Accepted**: February 2, 2021; **Published**: February 10, 2021

Abstract: Linear orthogonal binary 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 study the construction of the linear equivalent of a product sequence on two, three, and four degrees over a linear sequences from the field *Fp*, where *p* is larger than two, and answering on the request, how is the maximum length of the linear equivalent of a product sequence (on a linear sequence $\{a_n\}$ over the field *Fp*), is it less than ${}_rN_h$ as the binary sequences?, or can reach it ?, or the length is exceed this value ${}_rN_h$? And is the product sequences are orthogonal? And we show that in some cases, the maximum length ${}_rN_h$ for the binary sequences is not correct for the linear sequences in the finite field *Fp* for *p* larger than two and the result product sequences are not orthogonal, also trying study the product sequence on two different LFSRs, and how can use one shift feedback shift register LFSR as a monitor register of other p registers. In the current time, I think, there is no coders or decoders using the sequences over finite fields *Fp* where *p* is larger than 2 and from this idea this article showing very need for using in the future.

Keywords: Linear Sequences, Finite Field, Linear Feedback Shift Register, Orthogonal Sequences, 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]

The Author Al Cheikha A. H., Studied the case for p=2. [15]

2. Research Method and Materials

M- Linear Recurring Sequences

Let k be a positive integer and $\lambda, \lambda_0, \lambda_1, ..., \lambda_{k-1}$ are elements in the field F_p={0, 1,…,(p-1)} and p >2 then the sequence $a_0, a_1, ...$ is called the nonhomogeneous binary linear recurring sequence of order k (or with the complexity k) *iff*:

$$a_{n+k} = \lambda_{k-1}a_{n+k-1} + \lambda_{k-2}a_{n+k-2} + ... + \lambda_0 a_n + \lambda; \lambda \& \lambda_i \in F_p, i = 0,1,...,k-1$$

Or;

$$a_{n+k} = \sum_{i=0}^{k-1} \lambda_i a_{n+i} + \lambda \quad (1)$$

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

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

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_p with the smallest natural number r is called periodic with the period r *iff*:

$$a_{n+r} = a_n \ ; \ n = 0, 1, ...$$

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

$$\overline{x_i} = (p-1)x_i, \ mod\ p$$

[2, 6-7]

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

$$R_{x,y} = \left| \left(\sum_{i=0}^{n-1} (-1)^{x_i + y_i} \right) - \left(\left[\frac{n+1}{p} \right] - 1 \right) \right| \quad (3)$$

Where $\left[\frac{n+1}{p} \right]$ is the nearest integer of the number $\frac{n+1}{p}$ [13].

*Definition*5. Suppose, $x = (x_0, x_1, ..., x_{n-1})$ and $y = (y_0, y_1, ..., y_{n-1})$ are two vectors of the length n on Fp is said orthogonal if $\sum x = \sum_{i=0}^{n} x_i = 0, \sum y = \sum_{i=0}^{n} y_i = 0 \ mod\ p$, and $R_{x,y} \le 1$. [8-9]

Definition 6. The periodic sequence $(a_i)_{i \in N}$ over F_p with the period $r = p^n - 1$ has the property of "Ideal Auto Correlation" if and only if its periodic auto Correlations $R_a(\tau)$ of the form:

$$a(\tau) = 0 \ \ and \ R_a(\tau) \le 1 \quad (4)$$

When;

$$a(\tau) = \sum_{t=0}^{r-1} a_i(t+\tau) \ mod\ p, \tau = 0,1,...,r; R_a(\tau) = \left| \sum_{t=0}^{r-1} (-1)^{a(t+\tau)+a(t)} - \left(p^{n-1} - 1 \right) \right|, \ for\ \tau \ne \frac{p^n - 1}{2} \quad (5)$$

Because for $\tau = \frac{p^n - 1}{2} \Rightarrow a(t+\tau) = \overline{a(t)}$ [1, 2]

*Definition*7. Suppose G is a set of vectors of length n on the field Fp:

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

The set G is said to be orthogonal if the following two conditions are satisfied;

$$1.\ \forall X \in G, X \ne 0; \sum_{i=0}^{n} x_i = 0 \ mod\ p \ \& \ R_X = R_{X,0} \le 1; when\ 0 = (0,0,...,0)_n \quad (6)$$

$$2.\ \forall X,Y \in G(Y \neq X \ \&\ Y \neq \bar{X});\ X+Y \in G \ \&\ R_{X,Y} \leq 1. \quad (7)$$

[6, 9]

Definition 8. (Euler function ϕ). $\phi(n)$ is the number of the all-natural numbers that are relatively prime with *n*. [11-14]

Definition 9. The linear equivalent of a multiplication sequence $\{z_n\}$, on a 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*10. 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 11. 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 ${}_rN_h$. [2, 3, 8]

Definition 12. 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 13.

i. If $a_0, a_1, \ldots$ is a homogeneous linear recurring sequence of order *k* in F_p, 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 $r \mid ord\ f(x)$.

iii. If the polynomial $f(x)$ is primitive then the period of the recurring sequence which has $f(x)$ as a characteristic polynomial is $p^k - 1$, this sequence is called M–Sequence over F_p, or briefly M_p-Sequences. [6, 11-14]

Lemma 14. (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 15. 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:

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

Theorem 16.

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

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

Theorem 17. 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 is limited to the Galois Fields of the form F_{p^k} and $p > 2$, then the period of each sequence in it with prime characteristic polynomial is $r = p^k - 1$.

3. Results and Discussion

3.1. Study Multiplication Sequences on a Recurring M-Sequences over Fp.

Suppose the recurring M-Sequence $\{a_n\}$ over *Fp* 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 *Fp*, its characteristic equation is prime, and α is a root of it (α is prime element in F_p^r) then the general term of the sequence $\{a_n\}$ is;

$$a_n = A_1\alpha^n + A_2(\alpha^{p2-1})^n + \ldots + A_r(\alpha^{p^{r-1}})^n = \sum_{i=1}^{r} A_i(\alpha^{pi-1})^n \quad (8)$$

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 the following;

(1) The first degree is a_n (in another case we can make a shift to the first degree).

(2) The second degree is $b_n = a_{n+\delta}$ as a shift of the first degree 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;

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

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

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

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;

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

Or,

$$\left(\frac{\alpha_j}{\alpha_i}\right)^{\delta} = (p-1) \Rightarrow \left(\frac{\alpha_j^{p^{j-1}}}{\alpha_i^{p^{i-1}}}\right)^{\delta} = (p-1) \Rightarrow \alpha^{\delta p^{j-i}} \neq 1 \; and \in F_p \; \alpha^{\delta p^{j-i}} \in F_p$$

Thus, 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;

$$A_k^2 \alpha^{\delta} \alpha_k^{2n} + A_i A_j \left(\alpha_i^{\delta} + \alpha_j^{\delta}\right)\alpha_i^n \alpha_j^n = 0$$

And it is equivalents the two conditions;

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

2) $A_k^2 \alpha_k^{\delta} + A_i A_j (\alpha_i^{\delta} + \alpha_j^{\delta}) = 0$ or $\alpha_i^{\delta} + \alpha_j^{\delta} = (p-1)\frac{A_k^2}{A_i A_j}\alpha_k^{\delta}$

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

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

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;

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

Or if *i* is the smallest;

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

Or;

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

Thus $2p^{k-i}$ and p^{j-i} are relatively primes and it is a 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 $\binom{r}{1} + \binom{r}{2} = r + \frac{r(r-1)}{2}$.

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

Example 1. Suppose the following sequence $\{a_n\}$, $\forall n \in N; a_n \in F_3$;

$$a_{n+3} + 2a_{n+1} + a_n = 0; a_0 \text{ or } a_{n+3} = a_{n+1} + 2a_n; a_0 = 1, a_1 = 2, a_2 = 0$$

As in the following figure 1;

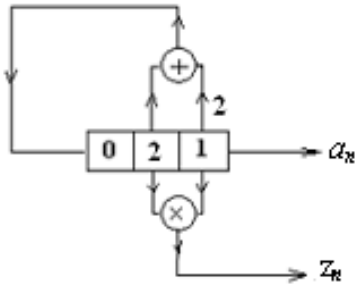

Figure 1. *Product sequence with two degree on F_3.*

The characteristic polynomial of the equation $f(x) = x^3 + 2x + 1$ is a prime and the characteristic equation of the sequence is;

$$x^3 + 2x + 1 = 0$$

If β is a root of the equation then;

$$\beta^3 + 2\beta + 1 = 0$$

And;

$$\begin{aligned} F_{3^3} = \{0, \beta^{26} = 1, \beta, \beta^2, \beta^3 = \beta + 2, \beta^4 = \beta^2 + 2\beta, \beta^5 = 2\beta^2 + \beta + 2, \beta^6 = \beta^2 + \beta + 1, \\ \beta^7 = \beta^2 + 2\beta + 2, \beta^8 = 2\beta^2 + 2, \beta^9 = \beta + 1, \beta^{10} = \beta^2 + \beta, \beta^{11} = \beta^2 + \beta + 2 \\ \beta^{12} = \beta^2 + 2, \beta^{13} = 2, \beta^{14} = 2\beta, \beta^{15} = 2\beta^2, \beta^{16} = 2\beta + 1, \beta^{17} = 2\beta^2 + \beta, \\ \beta^{18} = \beta^2 + 2\beta + 1, \beta^{19} = 2\beta^2 + 2\beta + 2, \beta^{20} = 2\beta^2 + \beta + 1, \beta^{21} = \beta^2 + 1, \\ \beta^{22} = 2\beta + 2, \beta^{23} = 2\beta^2 + 2\beta, \beta^{24} = 2\beta^2 + 2\beta + 1, \beta^{25} = 2\beta^2 + 1\} \end{aligned} \quad (9)$$

The general solution of the characteristic equation is;

$$a_n = A_1\beta^n + A_2(\beta^3)^n + A_3(\beta^{3^2})^n$$

Solving the given equation is;

$$\begin{cases} A_1 + A_2 + A_3 = 1 \\ \beta A_1 + \beta^3 A_2 + \beta^9 A_3 = 2 \\ \beta^2 A_1 + \beta^6 A_2 + \beta^{18} A_3 = 0 \end{cases}$$

We have;

$$A_1 = \beta^{20} = 2\beta^2 + \beta + 1, A_2 = \beta^8 = 2\beta^2 + 2, A_3 = \beta^{24} = 2\beta^2 + 2\beta + 1$$

And the general solution of the characteristic equation is;

$$a_n = \beta^{20}(\beta)^n + \beta^8(\beta^3)^n + \beta^{24}(\beta^9)^n$$

Or;

$$a_n = (2\beta^2 + \beta + 1)\beta^n + (2\beta^2 + 2)(\beta + 2)^n + (2\beta^2 + 2\beta + 1)(\beta + 1)^n$$

And the sequence is periodic with the period: 3^3-1=26 and the sequence is;

1 2 0 1 1 1 0 0 2 0 2 1 2 2 1 0 2 2 2 0 0 1 0 1 2 1 1 2 0 1 1 1 0 ….

The multiplication sequence $z_n = a_n.a_{n+1}$ then;

$$a_{n+1} = (2\beta^2 + \beta + 1)\beta^{n+1} + (2\beta^2 + 2)\beta^{3n+3} + (2\beta^2 + 2\beta + 1)\beta^{9n+9}$$

And;

$$z_n = 2\beta^2(\beta^2)^n + \beta^{20}(\beta^4)^n + \beta^{19}(\beta^6)^n + \beta^8(\beta^{10})^n + \beta^{20}(\beta^{12})^n + \beta^5(\beta^{18})^n$$

$$z_n = 2\beta^2(\beta^2)^n + (2\beta^2 + \beta + 1)(\beta^4)^n + (2\beta^2 + 2\beta + 2)(\beta^6)^n + (2\beta^2 + 2)(\beta^{10})^n + (2\beta^2 + \beta + 1)(\beta^{12})^n + (2\beta^2 + \beta + 2)(\beta^{18})^n$$

The characteristic equation is;

$$(x - \beta^2)(x - \beta^4)(x - \beta^6)(x - \beta^{10})(x - \beta^{12})(x - \beta^{18}) = 0$$

We can find that;

$$(-\beta^2)(-\beta^4)(-\beta^6)(-\beta^{10})(-\beta^{12})(-\beta^{18}) = \beta^{52} = 1$$

And the characteristic equation is of the form;

$$x^6 + \mu_5 x^5 + \mu_4 x^4 + \mu_3 x^3 + \mu_2 x^2 + \mu_1 x + 1 = 0$$

Calculated the coefficients we have;

$$\mu_5 = 2, \mu_4 = 2, \mu_3 = 2, \mu_2 = 1, \mu_1 = 2$$

Thus, the characteristic equation is;

$$x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 2x + 1 = 0$$

Or;

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

Where each of $q(x) = x^3 + x^2 + 2$ and $h(x) = x^3 + x^2 + x + 2$ is minimal but not primitive polynomial in $F_3{}^3$ each of them of the order 13. Thus, the recurring sequence $\{z_n\}$ is;

$$z_{n+6} + 2z_{n+5} + 2z_{n+4} + 2z_{n+3} + z_{n+2} + 2z_{n+1} + z_n = 0$$

Or;

$$z_{n+6} = z_{n+5} + z_{n+4} + z_{n+3} + 2z_{n+2} + z_{n+1} + 2z_n$$

is periodic with the period 13 and $\{z_n\}$ reached the maximum length ${}_3N_2$ =6 and this sequence is;

2 0 0 1 1 0 0 0 0 0 2 2 1 2 0 0 1 1 0 0 0 0 0 2 2 1 2 0 0 1 1 0 0 0 0 ……

Figure 2 showing its feedback linear shift register of the sequence $\{z_n\}$.

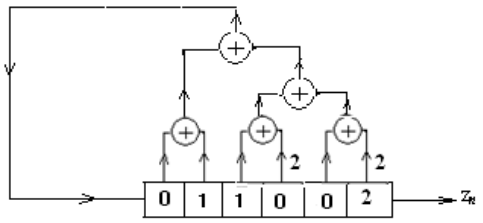

Figure 2. *Linear Equivalent of $\{z_n\}$ with 6 complexity on F_3.*

For one period w_0=(2 0 0 1 1 0 0 0 0 0 2 2 1) and for all its permutations $S=\{w_0, w_1, \ldots, w_{12}\}$ when;

w_1=(1 2 0 0 1 1 0 0 0 0 0 2 2), w_2=(2 1 2 0 0 1 1 0 0 0 0 0 2), w_3=(2 2 1 2 0 0 1 1 0 0 0 0 0),

w_4=(0 2 2 1 2 0 0 1 1 0 0 0 0), w_5=(0 0 2 2 1 2 0 0 1 1 0 0 0), w_6=(0 0 0 2 2 1 2 0 0 1 1 0 0),

w_7=(0 0 0 0 2 2 1 2 0 0 1 1 0), w_8=(0 0 0 0 0 2 2 1 2 0 0 1 1), w_9=(1 0 0 0 0 0 2 2 1 2 0 0 1)

w_{10}=(1 1 0 0 0 0 0 2 2 1 2 0 0), w_{11}=(0 1 1 0 0 0 0 0 2 2 1 2 0), w_{12}=(0 0 1 1 0 0 0 0 0 2 2 1 2)

From equations (4) and (5);

$$w_i(\tau) = 0 \; and \; R_{w_i}(\tau) = 3 \; ; i = 0,1,...,12$$

And; $w_{0+1}=w_0 + w_1$=(0 2 0 1 2 1 0 0 0 0 2 1 0) thus;

$$w_{0+1} \notin S, \sum_{w_{0+1}} = 0, \; and \; R_{w_0, w_1} = 3$$

And; $w_{2+3}=w_2+ w_3$=(1 0 0 2 0 1 2 1 0 0 0 0 2) thus;

$$w_{2+3} \notin S, \sum_{w2+3} = 0, \text{ and } R_{w_2,w_3} = 3$$

Thus; the set S is not an orthogonal set.

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 to we arrive at the first degree) as in 3.1..

2) The second degree is $b_n = a_{n+\delta}$ (as a result of shift n by δ *and* $\delta < r$).

3) The third degree is $c_n = a_{n+\gamma}$ (as a result of shift n by γ) and $\delta < \gamma$ *and* $\gamma < r$, 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 is not equal to zero.

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

$$\alpha_i^{\delta}\alpha_j^{\gamma} + \alpha_i^{\gamma}\alpha_j^{\delta} + \alpha_i^{\delta}\alpha_i^{\gamma} = 0 \tag{10}$$

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;

$$A^{\gamma} + A^{\delta} + 1 = 0 \tag{11}$$

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

$$\alpha_j^{\delta}\alpha_k^{\gamma} + \alpha_j^{\gamma}\alpha_k^{\delta} + \alpha_i^{\delta}\alpha_j^{\gamma} + \alpha_i^{\gamma}\alpha_j^{\delta} + \alpha_i^{\delta}\alpha_k^{\gamma} + \alpha_i^{\gamma}\alpha_k^{\delta} = 0 \tag{12}$$

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

$$\left(\frac{\alpha_j}{\alpha_i}\right)^{\delta}\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma} + \left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_k}{\alpha_i}\right)^{\delta} + \left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma} + \left(\frac{\alpha_j}{\alpha_i}\right)^{\delta} + \left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma} + \left(\frac{\alpha_k}{\alpha_i}\right)^{\delta} = 0 \tag{13}$$

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

$$A^{\delta}B^{\gamma} + A^{\gamma}B^{\delta} + A^{\gamma} + A^{\delta} + B^{\gamma} + B^{\delta} = 0 \tag{14}$$

This equation is symmetric and can write it as follows;

$$(A^{\delta} + 1)(B^{\gamma} + 1) + (A^{\gamma} + 1)(B^{\delta} + 1) + 1 = 0 \tag{15}$$

*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;

$$1).\ \alpha_k^{3n} = \alpha_i^{2n}\alpha_j^n \Rightarrow \alpha_k^3 = \alpha_i^2\alpha_j^1, \text{ Where } i, j, k \text{ are different} \tag{16}$$

$$2).\ A_k^3\alpha_k^{(\delta+\gamma)} + A_i^2 A_j(\alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_i^\gamma) = 0 \tag{17}$$

The second condition can be written as;

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

Or;

$$\left(\frac{\alpha_j}{\alpha_i}\right)^\gamma + \left(\frac{\alpha_j}{\alpha_i}\right)^\delta + 1 = (p-1)\frac{A_k^3}{A_i^2 A_j}\left(\frac{\alpha_k}{\alpha_i}\right)^{\delta+\gamma} \tag{18}$$

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

$$A^\gamma + A^\delta + 1 = (p-1)\frac{A_k^3}{A_i^2 A_j}B^{\delta+\gamma} \tag{19}$$

*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;

$$1).\ \alpha_m^{3n} = (\alpha_i\alpha_j\alpha_k)^n \Rightarrow \alpha_m^3 = \alpha_i\alpha_j\alpha_k \tag{20}$$

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

$$2).\ A_m^3(\alpha_m^{\delta+\gamma}) + A_i A_j A_k\left(\alpha_j^\delta\alpha_k^\gamma + \alpha_j^\gamma\alpha_k^\delta + \alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_k^\gamma + \alpha_i^\gamma\alpha_k^\delta\right) = 0 \tag{21}$$

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

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

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;

$$A_m^3 C^{\delta+\gamma} + A_i A_j A_k[A^\delta B^\gamma + A^\gamma B^\delta + A^\lambda + A^\delta + B^\gamma + B^\delta] = 0 \tag{22}$$

Or;

$$A^\delta B^\gamma + A^\gamma B^\delta + A^\lambda + A^\delta + B^\gamma + B^\delta = (p-1)\frac{A_m^3}{A_i A_j A_k}C^{\delta+\gamma} \tag{23}$$

*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;

$$1).\ \alpha_l^2\alpha_m = \alpha_i\alpha_j\alpha_k, \text{ Where, no two between the indexes } i, j, k, m \text{ and } l \text{ are equal, and;} \tag{24}$$

$$2).\ A_l^2 A_m(\alpha_l^\delta \alpha_m^\gamma + \alpha_l^\gamma \alpha_m^\delta + \alpha_l^{\gamma+\delta}) + A_i A_j A_k(\alpha_j^\delta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\delta + \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + +\alpha_i^\delta \alpha_k^\gamma + \alpha_i^\gamma \alpha_k^\delta) = 0 \quad (25)$$

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;

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

$$= (p-1)\frac{A_l^2 A_m}{A_i A_j A_k}\left[\left(\frac{\alpha_l}{\alpha_i}\right)^\delta \left(\frac{\alpha_m}{\alpha_i}\right)^\gamma + \left(\frac{\alpha_l}{\alpha_i}\right)^\gamma \left(\frac{\alpha_m}{\alpha_i}\right)^\delta + \left(\frac{\alpha_l}{\alpha_i}\right)^{\delta+\gamma}\right]$$

Or;

$$A^\delta B^\gamma + A^\gamma B^\delta + A^\delta + A^\gamma + B^\delta + B^\gamma = (p-1)\frac{A_l^2 A_m}{A_i A_j A_k}\left[D^\delta C^\gamma + D^\gamma C^\delta + D^{\delta+\gamma}\right] \quad (26)$$

*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;

$$1).\ \alpha_m^{3n} + \alpha_h^{2n}\alpha_l^n + (\alpha_i \alpha_j \alpha_k)^n \quad (27)$$

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

$$2).\ A_m^3 \alpha_m^{\delta+\gamma} + A_h^2 A_l(\alpha_h^\delta \alpha_l^\gamma + \alpha_h^\gamma \alpha_l^\delta + \alpha_h^{\gamma+\delta}) + A_i A_j A_k(\alpha_j^\delta \alpha_k^\gamma + \alpha_j^\gamma \alpha_k^\delta + \alpha_i^\delta \alpha_j^\gamma + \alpha_i^\gamma \alpha_j^\delta + \alpha_i^\delta \alpha_k^\gamma + \alpha_i^\gamma \alpha_k^\delta) = 0 \quad (28)$$

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;

$$A_m^3 C^{\delta+\gamma} + A_h^2 A_l(E^\delta D^\gamma + E^\gamma D^\delta + E^{\delta+\gamma}) + A_i A_j A_k\left(A^\delta B^\gamma + A^\gamma B^\delta + A^\delta + A^\gamma + B^\delta + B^\gamma\right) = 0 \quad (29)$$

Each of *P*4 or …. or *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 $\{z_n\}$ as a multiplication on three degrees of $\{a_n\}$ as in figure 3 (see *Example* 1) where; $z_n = b_n a_{n+2} = a_n a_{n+1} a_{n+2}$

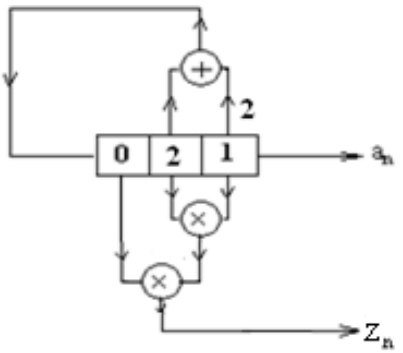

Figure 3. *Multiplication sequence $\{z_n\}$ on three degrees over F_3.*

Thus, from example 1;

$$a_n = \beta^{20}(\beta)^n + \beta^8(\beta^3)^n + \beta^{24}(\beta^9)^n$$

$$a_{n+1} = \beta^{21}\beta^n + \beta^{11}\beta^{3n} + \beta^7\beta^{9n}$$

$$b_n = a_n a_{n+1} = 2\beta^2(\beta^2)^n + \beta^{20}(\beta^4)^n + \beta^{19}(\beta^6)^n + \beta^8(\beta^{10})^n + \beta^{20}(\beta^{12})^n + \beta^5(\beta^{18})^n$$

$$a_{n+2} = (2\beta+2)\beta^n + 2\beta(\beta^3)^n + (2\beta+1)(\beta^9)^n$$

$$z_n = \beta^{21}\beta^n + \beta^{11}(\beta^3)^n + \beta^{23}(\beta^5)^n + 2(\beta^7)^n + \beta^7(\beta^9)^n + 2(\beta^{11})^n + \beta^{17}(\beta^{15})^n + \\ + \beta^{25}(\beta^{19})^n + 2(\beta^{21})$$

Or;

$$z_n = (\beta^2+1)\beta^n + (\beta^2+\beta+2)(\beta+2)^n + (2\beta^2+2\beta)(2\beta^2+\beta+2)^n + 2(\beta^2+2\beta+2)^n + \\ (\beta^2+2\beta+2)(\beta+1)^n + 2(\beta^2+\beta+2)^n + (2\beta^2+\beta)(2\beta^2)^n + (2\beta^2+1)(2\beta^2+2\beta+2)^n + 2(\beta^2+1)$$

The characteristic equation of the sequence is;

$$(x-\beta)(x-\beta^3)(x-\beta^7)...(x-\beta^{21}) = 0$$

We can see that;

$$(-\beta)(-\beta^3)(-\beta^5)(-\beta^7)(-\beta^9)(-\beta^{11})(-\beta^{15})(-\beta^{19})(-\beta^{21}) = -\beta^{91} = -\beta^{13} = -2 = 1$$

And the characteristic equation is of the form;

$$x^9 + \mu_8 x^8 + \mu_7 x^7 + \mu_6 x^6 + \mu_5 x^5 + \mu_4 x^4 + \mu_3 x^3 + \mu_2 x^2 + \mu_1 x + 1 = 0$$

Calculated the coefficient we have;

$$\mu_8 = 0, \mu_7 = 1, \mu_6 = 2, \mu_5 = 0, \mu_4 = 1, \mu_3 = 0, \mu_2 = 2, \mu_1 = 2$$

Or;

$$x^9 + x^7 + 2x^6 + x^4 + 2x^2 + 2x + 1 = 0$$

Or;

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

the recurring formula of the sequence $\{z_n\}$ is;

$$z_{n+9} + z_{n+7} + 2z_{n+6} + z_{n+4} + 2z_{n+2} + 2z_{n+1} + z_n = 0$$

The sequence is periodic and has the complexity 9 and is;

0 0 0 1 0 0 0 0 0 0 1 1 1 0 0 0 2 0 0 0 0 0 0 2 2 2 0 0 0 1 0 0 0 0 0 0 1 1 1 ……

Thus as showing the sequence $\{z_n\}$ is periodic with the period 26 which is equal to same of the period of sequence $\{a_n\}$ and the length of the linear equivalent is the complexity 9 which larger than the expected maximum length ${}_3N_3 = 7$ (which is mentioned in [2]).

Figure 4, illustrated the linear feedback shift register of the sequence $\{z_n\}$;

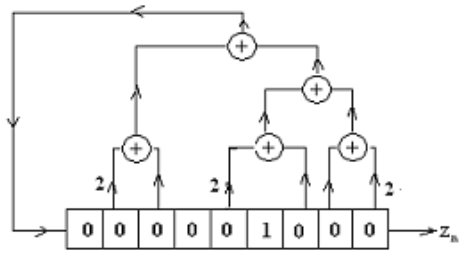

Figure 4. *Linear Equivalent of the sequence $\{z_n\}$ with the complexity 9.*

In other side for one period of the sequence;
w_0=(0 0 0 1 0 0 0 0 0 0 1 1 1 0 0 0 2 0 0 0 0 0 0 2 2 2)
and the all its permutations are;
w_1=(2 0 0 0 1 0 0 0 0 0 0 1 1 1 0 0 0 2 0 0 0 0 0 0 2 2)
w_2=(2 2 0 0 0 1 0 0 0 0 0 0 1 1 1 0 0 0 2 0 0 0 0 0 0 2)
w_3=(2 2 2 0 0 0 1 0 0 0 0 0 0 1 1 1 0 0 0 2 0 0 0 0 0 0)
w_4=(0 2 2 2 0 0 0 1 0 0 0 0 0 0 1 1 1 0 0 0 2 0 0 0 0 0)
⋮
From equations (4) and (5);

$$w_i(\tau) = 0 \; and \; R_{w_i}(\tau) = 10 \; ; i = 0,1,...,12$$

And; $w_{0+1}=w_0 + w_1$=(2 0 0 1 1 0 0 0 0 0 1 2 2 1 0 0 2 2 0 0 0 0 0 2 1 1) thus;

$$w_{0+1} \notin S, \sum_{w_{0+1}} = 0, \; and \; R_{w_0,w_1} = 10$$

And; $w_{1+2}=w_1+ w_2$=(1 2 0 0 1 1 0 0 0 0 0 1 2 2 1 0 0 2 2 0 0 0 0 0 2 1) thus;

$$w_{1+2} \notin S, \sum_{w_{1+2}} = 0, \; and \; R_{w_2,w_3} = 10$$

Thus; the set S is not an orthogonal set.

For studying the decreasing in the length of the linear equivalent needed return to the theoretical study of the properties from 1 to 7 of the comfortable values of i, j, k, namely;

1) i=1, j=2, k=3; 3) i=2, j=1, k=3; 5) i=3, j=1, k=2
2) i=1, j=3, k=2; 4) i=2, j=3, k=1; 6) i=3, j=2, k=1

Remembering the that the general term of the sequence is;

$$a_n = \beta^{20}(\beta)^n + \beta^8(\beta^3)^n + \beta^{24}(\beta^9)^n$$

Here;

$$\begin{cases} A_1 = \beta^{20}, A_2 = \beta^8, A_3 = \beta^{24} \\ \alpha_1 = \beta, \alpha_2 = \beta^3, \alpha_3 = \beta^9 \end{cases} ; \delta = 1, \gamma = 2$$

And $\{z_n\}$ of the form;

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

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

P1. We can see that no term of the first sum for each *i*, namely $A_i^3 \alpha_i^{\delta+\gamma}$, is equal to zero and studying the properties 2, 3, 4 for each set of *i*, *j* and *k*.

P2. Is there any term of the third sum is equal to zero?

a) for *i*=1, *j*=2, *k*=3;

1) From the second sum;

$$\alpha_i^{\delta} \alpha_j^{\gamma} + \alpha_i^{\gamma} \alpha_j^{\delta} + \alpha_i^{\delta} \alpha_i^{\gamma} = (\beta)^1 (\beta^3)^2 + (\beta)^2 (\beta^3)^1 + (\beta)^{1+2} = \beta \neq 0$$

2) From the third sum;

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

$$= (\beta^3)^1(\beta^9)^2 + (\beta^3)^2(\beta^9)^1 + (\beta)^1(\beta^3)^2 + (\beta)^2(\beta^3)^1 + (\beta)^1(\beta^9)^2 + (\beta)^2(\beta^9)^1$$

$$= \beta^{21} + \beta^{15} + \beta^7 + \beta^5 + \beta^{19} + \beta^{11} = 0$$

3) Sum one term of the first sum with one term of the second sum, $A_i^3\alpha_i^{\delta+\gamma} + A_i^2 A_j\left(\alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_i^\gamma\right) =$

$(\beta^{24})^3(\beta)^3 + (\beta^{20})^2(\beta^8)^1\left((\beta)^1(\beta^3)^2 + (\beta)^2(\beta^3)^1 + (\beta)^3\right) = \beta^{99} + \beta^{49} = \beta^{16} \neq 0$

b) for i=1, j=3, k=2;

4) $\alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_i^\gamma = (\beta)^1(\beta^9)^2 + (\beta)^2(\beta^9)^1 + (\beta)^{1+2} = \beta \neq 0$,

5) $\alpha_j^\delta\alpha_k^\gamma + \alpha_j^\gamma\alpha_k^\delta + \alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_k^\gamma + \alpha_i^\gamma\alpha_k^\delta =$

$= (\beta^9)^1(\beta^3)^2 + (\beta^9)^2(\beta^3)^1 + (\beta)^1(\beta^9)^2 + (\beta)^2(\beta^9)^1 + (\beta)^1(\beta^3)^2 + (\beta)^2(\beta^3)^1$

$= \beta^{15} + \beta^{21} + \beta^{19} + \beta^{11} + \beta^7 + \beta^5 = 0$

for i=2, j=1, k=3;

6) $\alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_i^\gamma = (\beta^3)^1(\beta)^2 + (\beta^3)^2(\beta)^1 + (\beta^3)^{1+2} = \beta + 2 \neq 0$,

7) $\alpha_j^\delta\alpha_k^\gamma + \alpha_j^\gamma\alpha_k^\delta + \alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_k^\gamma + \alpha_i^\gamma\alpha_k^\delta =$

$= (\beta)^1(\beta^9)^2 + (\beta)^2(\beta^9)^1 + (\beta^3)^1(\beta)^2 + (\beta^3)^2(\beta)^1 + (\beta^3)^1(\beta^9)^2 + (\beta^3)^2(\beta^9)^1$

$= \beta^{19} + \beta^{11} + \beta^5 + \beta^7 + \beta^{21} + \beta^{15} = 0$

for i=2, j=3, k=1;

8) $\alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_i^\gamma = (\beta^3)^1(\beta^9)^2 + (\beta^3)^2(\beta^9)^1 + (\beta^3)^{1+2} = \beta^3 \neq 0$,

9) $\alpha_j^\delta\alpha_k^\gamma + \alpha_j^\gamma\alpha_k^\delta + \alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_k^\gamma + \alpha_i^\gamma\alpha_k^\delta =$

$= (\beta^9)^1(\beta)^2 + (\beta^9)^2(\beta)^1 + (\beta^3)^1(\beta^9)^2 + (\beta^3)^2(\beta^9)^1 + (\beta^3)^1(\beta)^2 + (\beta^3)^2(\beta)^1$

$= \beta^{11} + \beta^{19} + \beta^{21} + \beta^{15} + \beta^5 + \beta^7 = 0$

e) for i=3, j=1, k=2;

10) $\alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_i^\gamma = (\beta^9)^1(\beta)^2 + (\beta^9)^2(\beta)^1 + (\beta^9)^{1+2} = \beta^9 \neq 0$,

11) $\alpha_j^\delta\alpha_k^\gamma + \alpha_j^\gamma\alpha_k^\delta + \alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_k^\gamma + \alpha_i^\gamma\alpha_k^\delta =$

$= (\beta)^1(\beta^3)^2 + (\beta)^2(\beta^3)^1 + (\beta^9)^1(\beta)^2 + (\beta^9)^2(\beta)^1 + (\beta^9)^1(\beta^3)^2 + (\beta^9)^2(\beta^3)^1$

$= \beta^7 + \beta^5 + \beta^{11} + \beta^{19} + \beta^{15} + \beta^{21} = 0$

f) for i=3, j=2, k=1;

12) $\alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_i^\gamma = (\beta^9)^1(\beta^3)^2 + (\beta^9)^2(\beta^3)^1 + (\beta^9)^{1+2} = \beta^9 \neq 0$,

13) $\alpha_j^\delta\alpha_k^\gamma + \alpha_j^\gamma\alpha_k^\delta + \alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_k^\gamma + \alpha_i^\gamma\alpha_k^\delta =$

$= (\beta^3)^1(\beta)^2 + (\beta^3)^2(\beta)^1 + (\beta^9)^1(\beta^3)^2 + (\beta^9)^2(\beta^3)^1 + (\beta^9)^1(\beta)^2 + (\beta^9)^2(\beta)^1$

$= \beta^5 + \beta^7 + \beta^{15} + \beta^{21} + \beta^{11} + \beta^{19} = 0$

There are no other different i, j, and k as; sum one term from the first sum with one term from the second sum or sum one term from the first sum with one term from the third sum or sum one term from the first sum with one term from the second sum with one term from the third sum satisfies the first condition for $P4$ to $P7$.

P3. Is there any term of the third sum is equal to zero?

Or;

$$\alpha_j^\delta\alpha_k^\gamma + \alpha_j^\gamma\alpha_k^\delta + \alpha_i^\delta\alpha_j^\gamma + \alpha_i^\gamma\alpha_j^\delta + \alpha_i^\delta\alpha_k^\gamma + \alpha_i^\gamma\alpha_k^\delta = 0$$

We can check that only for case from a), to f) there is only one case and the sum of them is 6 cases and the other properties $P4$,…, $P7$ are not satisfied.

Thus, in result the length of linear equivalent in our case is 9 only (and this length is larger than the mentioned maximum length ${}_3N_3 = 7$ as in [2]) also, the expected maximum length in this case is 9 + 6=15 and it is greater than the mentioned maximum length ${}_3N_3 = 7$ as in [2].

3.1.3. The Sequence {z_n} Is a Multiplication on Four Degrees of the Sequence {a_n}

Suppose the sequence $\{z_n\}$ is a result of product four terms from the sequence $\{a_n\}$ as the following; First term from $\{a_n\}$ a_n (in other case we can shift the term to the first), 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 (as a result of shift the first term by γ) and the all β, γ, and μ are less than or equal to r *and* $\beta < \mu < \gamma$, that is;

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

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

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

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

$$\begin{aligned} z_n &= a_n b_n c_n d_n \\ &= \sum_{i=1}^{r} A_1^4\alpha_1^{\beta+\mu+\gamma}\alpha_1^n + \quad + \sum_{\substack{i=1 \\ i\neq j}}^{r} A_1^3 A_j(\alpha_i^{\beta+\mu}\alpha_j^r + \alpha_i^{\beta+\gamma}\alpha_j^{\mu} + \alpha_i^{\mu+\gamma}\alpha_j^{\beta} + \alpha_i^{\beta+\mu+\gamma})\alpha_i^{3n}\alpha_j^r \end{aligned}$$

$$+ \sum_{\substack{i=1, i\neq j \\ i\neq k \,\&\, j\neq k}}^{r} A_1^2 A_j A_k \begin{bmatrix} \alpha_i^{\beta}\left(\alpha_j^{\mu}\alpha_k^{\gamma} + \alpha_j^{\gamma}\alpha_k^{\mu}\right) + \alpha_i^{\mu}\left(\alpha_j^{\beta}\alpha_k^{\gamma} + \alpha_j^{\gamma}\alpha_k^{\beta}\right) + \\ \alpha_i^{\gamma}\left(\alpha_j^{\beta}\alpha_k^{\mu} + \alpha_j^{\mu}\alpha_k^{\beta}\right) + \alpha_i^{\beta+\mu}\left(\alpha_j^{\gamma} + \alpha_k^{\gamma}\right) + \\ +\alpha_i^{\beta+\gamma}\left(\alpha_j^{\mu} + \alpha_k^{\mu}\right) + \alpha_i^{\mu+\gamma}\left(\alpha_j^{\beta} + \alpha_k^{\beta}\right) \end{bmatrix} \alpha_i^{2n}\alpha_j^n\alpha_k^n$$

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

Where no two indexes of *i, j, k,* and *l* are equals and (*j, k, l*) is the set of permutations of {*j, k, l*}.
Thus;
*P*1. Each term of the first sum is not equal zero.
*P*2. For one term of the second term is equal to zero to necessary and sufficient;

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

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

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

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

$$A^{\beta} + A^{\mu} + A^{\gamma} + 1 = 0 \tag{30}$$

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

$$\alpha_i^{\beta}\left(\alpha_j^{\mu}\alpha_k^{\gamma} + \alpha_j^{\gamma}\alpha_k^{\mu}\right) + \alpha_i^{\mu}\left(\alpha_j^{\beta}\alpha_k^{\gamma} + \alpha_j^{\gamma}\alpha_k^{\beta}\right) + \alpha_i^{\gamma}\left(\alpha_j^{\beta}\alpha_k^{\mu} + \alpha_j^{\mu}\alpha_k^{\beta}\right) + \alpha_i^{\beta+\mu}\left(\alpha_j^{\gamma} + \alpha_k^{\gamma}\right) + \alpha_i^{\beta+\gamma}\left(\alpha_j^{\mu} + \alpha_k^{\mu}\right) + \alpha_i^{\mu+\gamma}\left(\alpha_j^{\beta} + \alpha_k^{\beta}\right) = 0 \tag{31}$$

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

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

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

Suppose; $A=\frac{\alpha_j}{\alpha_i}$, $B=\frac{\alpha_k}{\alpha_i}$ then for one term from the third sum is equal to zero is necessary and sufficient;

$$A^{\beta}B^{\mu}+A^{\mu}B^{\beta}+A^{\beta}B^{\gamma}+A^{\gamma}B^{\beta}+A^{\mu}B^{\gamma}+A^{\gamma}B^{\mu}+(A^{\beta}+A^{\mu}+A^{\gamma})+(B^{\beta}+B^{\mu}+B^{\gamma})=0 \quad (32)$$

*P*4. One term of the forth sum is equal to zero is necessary and sufficient;

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

Or;

$$\left(\alpha_i^{\beta}+\alpha_l^{\beta}\right)\left(\alpha_j^{\mu}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\mu}\right)+\left(\alpha_i^{\mu}+\alpha_k^{\mu}\right)\left(\alpha_j^{\gamma}\alpha_l^{\beta}+\alpha_j^{\beta}\alpha_l^{\gamma}\right)+\left(\alpha_i^{\gamma}+\alpha_k^{\gamma}\right)\left(\alpha_k^{\beta}\alpha_l^{\mu}+\alpha_k^{\mu}\alpha_l^{\beta}\right)=0 \quad (33)$$

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

$$\left[1+\left(\frac{\alpha_l}{\alpha_i}\right)^{\beta}\right]\left[\left(\frac{\alpha_j}{\alpha_i}\right)^{\mu}\left(\frac{\alpha_k}{\alpha_i}\right)^{\gamma}+\left(\frac{\alpha^j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_k}{\alpha_i}\right)^{\mu}\right]+$$
$$\left[1+\left(\frac{\alpha_k}{\alpha_i}\right)^{\mu}\right]\left[\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\left(\frac{\alpha_l}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_j}{\alpha_i}\right)^{\beta}\left(\frac{\alpha_l}{\alpha_i}\right)^{\gamma}\right]+ \quad (34)$$
$$\left[1+\left(\frac{\alpha_j}{\alpha_i}\right)^{\gamma}\right]\left[\left(\frac{\alpha_k}{\alpha_i}\right)^{\beta}\left(\frac{\alpha_l}{\alpha_i}\right)^{\mu}+\left(\frac{\alpha_k}{\alpha_i}\right)^{\beta}+\left(\frac{\alpha_l}{\alpha_i}\right)^{\mu}\right]=0$$

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

$$(1+C^{\beta})(A^{\mu}B^{\gamma}+A^{\gamma}B^{\mu})+(1+B^{\mu})(A^{\gamma}C^{\beta}+A^{\beta}C^{\gamma})+(1+A^{\gamma})(B^{\beta}C^{\mu}++B^{\mu}C^{\beta})=0 \quad (35)$$

*P*5. 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) $\alpha_k^{4n}=\alpha_i^{3n}\alpha_j^{n}$ 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;

$$A_k^4B^{\beta+\mu+\gamma}+A_i^3A_j(A^{\beta}+A^{\mu}+A^{\gamma})=0 \quad (36)$$

*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;

$$1)\ \alpha_l^{4n}=\alpha_i^{2n}\alpha_j^{n}\alpha_k^{n} \quad (37)$$

Where *i*, *j*, *k*, and *l* are different.

$$2)\ A_l^4\alpha_l^{\beta+\mu+\gamma}+A_i^2A_jA_k\begin{bmatrix}\alpha_i^{\beta}\left(\alpha_j^{\mu}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\mu}\right)+\alpha_i^{\mu}\left(\alpha_j^{\beta}\alpha_k^{\gamma}+\alpha_j^{\gamma}\alpha_k^{\beta}\right)+\\ \alpha_i^{\gamma}\left(\alpha_j^{\beta}\alpha_k^{\mu}+\alpha_j^{\mu}\alpha_k^{\beta}\right)+\alpha_i^{\beta+\mu}\left(\alpha_j^{\gamma}+\alpha_k^{\gamma}\right)+\\ +\alpha_i^{\beta+\gamma}\left(\alpha_j^{\mu}+\alpha_k^{\mu}\right)+\alpha_i^{\mu+\gamma}\left(\alpha_j^{\beta}+\alpha_k^{\beta}\right)\end{bmatrix}=0 \quad (38)$$

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;

$$A_l^4C^{\beta+\mu+\gamma}+A_i^2A_jA_k\begin{bmatrix}A^{\mu}B^{\gamma}+A^{\gamma}B^{\mu}+A^{\beta}B^{\gamma}+A^{\gamma}B^{\beta}+A^{\beta}B^{\mu}+A^{\mu}B^{\beta}+\\ +(A^{\beta}+A^{\mu}+A^{\gamma})+(B^{\beta}+B^{\mu}+B^{\gamma})\end{bmatrix}=0 \quad (39)$$

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

*P*7. Sum one term of the second sum with one term of the third sum is equal to zero.

*P*8. Sum one term of the second sum with one term of the forth sum is equal to zero.

*P*9. Sum one term of the third sum with one term of the forth sum is equal to zero.

*P*10. Sum three terms of the different for sums is equal to zero.

*P*11. Sum four terms of the different for sums is equal to zero.

Example 3. Suppose the recurrent sequence $a_{n+4}+a_{n+1}+2a_n=0$ or $a_{n+4}=2a_{n+1}+a_n$ as showing in the following figure 5 where the sequence is a multiplication on four degrees of the sequence $\{a_n\}$;

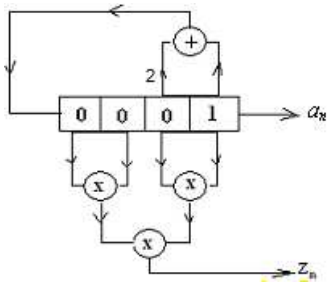

Figure 5. *The sequence $\{z_n\}$ is multiplication on four degrees of the sequence $\{a_n\}$.*

The characteristic polynomial of this sequence is; $f(x)=x^4+x+2$ and it is a prime polynomial on F_3 of degree 4, generates F_{3^4}, and its characteristic equation is $x^4+x+2=0$, if α is a root of the characteristic equation then the general solution of the characteristic equation or the general term of the sequence is $\{a_n\}$ of the form;

$$a_n=A_1(\alpha)^n+A_2(\alpha^3)^n+A_3(\alpha^9)^n+A_4(\alpha^{27})^n \text{ or}$$
$$a_n=A_1\alpha^n+A_2\alpha^{3n}+A_3\alpha^{9n}+A_4\alpha^{27n}$$

Solving the following system for consecutively values of *n*=0, 1, 2, 3;

$$\begin{cases}A_1+A_2+A_3+A_4=1\\ A_1\alpha+A_2\alpha^3+A_3\alpha^9+A_4\alpha^{27}=0\\ A_1\alpha^2+A_2\alpha^6+A_3\alpha^{18}+A_4\alpha^{54}=0\\ A_1\alpha^3+A_2\alpha^9+A_3\alpha^{27}+A_4\alpha=0\end{cases}$$

We have $A_1=A_2=A_3=A_4=1$ and the general solution is;

$$a_n=\alpha^n+\alpha^{3n}+\alpha^{9n}+\alpha^{27n}$$

The sequence $\{a_n\}$ is periodic and its period is 3^4-1=80, and is.

1000100210 11120 02201 0221101012 1221201222 2000200120 2221001102 011220202021

2112102111, 1000100210 1112002201 0221101012…

$$a_{n+1}=\alpha^{n+1}+\alpha^{3n+3}+\alpha^{9n+9}+\alpha^{27n+27}=\alpha\alpha^n+\alpha^3\alpha^{3n}+\alpha^9\alpha^{9n}+\alpha^{27}\alpha^{27n}$$

$$b_n=a_n.a_{n+1}=\alpha(\alpha^2)^n+\alpha^{25}(\alpha^4)^n+\alpha^3(\alpha^6)^n+\alpha^{55}(\alpha^{10})^n+\alpha^{54}(\alpha^{12})^n+\alpha^9(\alpha^{18})^n+$$
$$+\alpha^{46}(\alpha^{28})^n+\alpha^5(\alpha^{30})^n+\alpha^{65}(\alpha^{36})^n+\alpha^{27}(\alpha^{54})^n$$

$$a_{n+2}=\alpha^2(\alpha)^n+\alpha^6(\alpha^3)^n+\alpha^{18}(\alpha^9)^n+\alpha^{54}(\alpha^{27})^n$$

$$b_n.a_{n+2}=\alpha(\alpha)^n+\alpha^3(\alpha^3)^n+\alpha^{37}(\alpha^5)^n+\alpha^{39}(\alpha^7)^n+\alpha^9(\alpha^9)^n+\alpha^{34}(\alpha^{11})^n++\alpha^{68}(\alpha^{13})^n+$$
$$+\alpha^{64}(\alpha^{15})^n+\alpha^{49}(\alpha^{19})^n+\alpha^{79}(\alpha^{21})^n+\alpha^{27}(\alpha^{27})^n+\alpha^{73}(\alpha^{29})^n+\alpha^{44}(\alpha^{31})^n+$$
$$+\alpha^{22}(\alpha^{33})^n+\alpha^{74}(\alpha^{37})^n+\alpha^{25}(\alpha^{39})^n+\alpha^{13}(\alpha^{45})^n+\alpha^{17}(\alpha^{55})^n+\alpha^{67}(\alpha^{57})^n+\alpha^{31}(\alpha^{63})^n$$

$$a_{n+3} = \alpha^3(\alpha)^n + \alpha^9(\alpha^3)^n + \alpha^{27}(\alpha^9)^n + \alpha(\alpha^{27})^n$$

Suppose;

$$z_n = a_n.a_{n+1}.a_{n+2}.a_{n+3}$$

Thus;

$$\begin{aligned} z_n = {} & \alpha^4(\alpha^2)^n + \alpha^{19}(\alpha^4)^n + \alpha^{43}(\alpha^6)^n + \alpha^{35}(\alpha^8)^n + \alpha^{23}(\alpha^{10})^n + \alpha^{67}(\alpha^{12})^n + +\alpha^{34}(\alpha^{14})^n + \alpha^{54}(\alpha^{16})^n + \alpha^{45}(\alpha^{18})^n + \alpha^{49}(\alpha^{20})^n \\ & + \alpha^{25}(\alpha^{22})^n + \alpha^7(\alpha^{24})^n + \alpha^{41}(\alpha^{28})^n + \alpha^{26}(\alpha^{30})^n + \alpha^{28}(\alpha^{32})^n + \alpha^{56}(\alpha^{34})^n + \alpha^{38}(\alpha^{36})^n + \alpha^4(\alpha^{38})^n + \alpha^{52}(\alpha^{40})^n + \alpha^{16}(\alpha^{42})^n \\ & + \alpha^{10}(\alpha^{46})^n + \alpha^{72}(\alpha^{48})^n + \alpha^{40}(\alpha^{54})^n + \alpha^{20}(\alpha^{56})^n + \alpha^{27}(\alpha^{58})^n + \alpha^{76}(\alpha^{60})^n + \alpha^{24}(\alpha^{64})^n + \alpha^{48}(\alpha^{66})^n + \alpha^{58}(\alpha^{72})^n \end{aligned}$$

The sequence $\{z_n\}$ has the complexity 29 and;

$$\alpha^2.\alpha^4.\alpha^6.\ldots.\alpha^{64}.\alpha^{66}.\alpha^{72} = 1$$

The sequence is periodic with the period 40;
0000000000 2000000000 0100000012 1200002100, 0000000000 2000000000 0100000012 1200002100, ….
In other side for one period of the sequence;
w_0=(0000000000 2000000000 0100000012 1200002100)
and the all its permutations are;
w_1=(0000000000 0200000000 0010000001 2120000210)
w_2=(0000000000 0020000000 0001000000 1212000021)
w_3=(1000000000 0002000000 0000100000 0121200002)
w_4=(2100000000 0000200000 0000010000 0012120000)
w_5=(0210000000 0000020000 0000001000 0001212000)
⋮
From equations (4) and (5);

$$w_i(\tau) = 0 \; and \; R_{w_i}(\tau) = 19 \; ; i = 0,1,...,12$$

And*;*
w_{0+1}=(0000000000 2200000000 0110000010 0020002010)
thus;

$$w_{0+1} \notin S, \sum_{w_{0+2}} = 0, \; and \; R_{w_0, w_1} = 19$$

And*;*
w_{1+2}=(0000000000 0220000000 0011000001 0002000201)
Thus;

$$w_{1+2} \notin S, \sum_{w_{1+2}} = 0, \; and \; R_{w_2, w_3} = 19$$

Thus; the set S is not an orthogonal set.
We have;

$$\left.\begin{aligned} & A_1 = A_2 = A_3 = A_4 = 1 \\ & \alpha_1 = \alpha, \alpha_2 = \alpha^3, \alpha_3 = \alpha^9, \alpha_4 = \alpha^{27} \end{aligned}\right\} and \; \beta = 1, \mu = 2, \gamma = 3$$

*P*1. First property, no term in the first sum is equal to zero.
*P*2. Second property, one term in the second sum is equal to zero necessary and sufficient the following corresponding condition (30);

$$A^\beta + A^\mu + A^\gamma + 1 = 0, \text{ where } A = \frac{\alpha_j}{\alpha_i}$$

a. For i=1, j=2 $\Rightarrow A=\frac{\alpha^3}{\alpha}=\alpha^2$ and $A^1+A^2+A^3+1=\alpha^{37}\neq 0$

b. For i=1, j=3 $\Rightarrow A=\frac{\alpha^9}{\alpha}=\alpha^8$ and $A^1+A^2+A^3+1=\alpha^{37}\neq 0$

c. For i=1, j=4 $\Rightarrow A=\frac{\alpha^{27}}{\alpha}=\alpha^{26}$ and $A^1+A^2+A^3+1=\alpha^{18}\neq 0$

d. For i=2, j=3 $\Rightarrow A=\frac{\alpha^9}{\alpha^3}=\alpha^6$ and $A^1+A^2+A^3+1=\alpha^{65}\neq 0$

e. For i=2, j=4 $\Rightarrow A=\frac{\alpha^{27}}{\alpha^3}=\alpha^{24}$ and $A^1+A^2+A^3+1=\alpha^{37}\neq 0$

f. For i=2, j=1 $\Rightarrow A=\frac{\alpha}{\alpha^3}=\alpha^{78}$ and $A^1+A^2+A^3+1=\alpha^{50}\neq 0$

g. For i=3, j=4 $\Rightarrow A=\frac{\alpha^{27}}{\alpha^9}=\alpha^{18}$ and $A^1+A^2+A^3+1=\alpha^{13}\neq 0$

h. For i=3, j=1 $\Rightarrow A=\frac{\alpha}{\alpha^9}=\alpha^{72}$ and $A^1+A^2+A^3+1=\alpha^{13}\neq 0$

i. For i=3, j=2 $\Rightarrow A=\frac{\alpha^3}{\alpha^9}=\alpha^{74}$ and $A^1+A^2+A^3+1=\alpha^{31}\neq 0$

j. For i=4, j=1 $\Rightarrow A=\frac{\alpha}{\alpha^{27}}=\alpha^{54}$ and $A^1+A^2+A^3+1=\alpha^{56}\neq 0$

k. For i=4, j=2 $\Rightarrow A=\frac{\alpha^3}{\alpha^{27}}=\alpha^{56}$ and $A^1+A^2+A^3+1=\alpha^{12}\neq 0$

l. For i=4, j=3 $\Rightarrow A=\frac{\alpha^9}{\alpha^{27}}=\alpha^{62}$ and $A^1+A^2+A^3+1=\alpha^{39}\neq 0$

Thus, no term of the second sum is equal to zero.

*P*3. Third property, one term in the third sum is equal to zero necessary and sufficient the following corresponding condition (32);

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

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

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

We can see that S is symmetric for A and B then;

a. For i=1, j=2, k=3 $\Rightarrow A=\alpha^2, B=\alpha^8$ and $S=\alpha^{48}\neq 0$

b. For i=1, j=2, k=4 $\Rightarrow A=\alpha^2, B=\alpha^{26}$ and $S=\alpha^{57}\neq 0$

c. For i=1, j=3, k=4 $\Rightarrow A=\alpha^8, B=\alpha^{26}$ and $S=\alpha^{71}\neq 0$

d. For i=2, j=3, k=4 $\Rightarrow A=\alpha^5, B=\alpha^{23}$ and $S=\alpha^{27}\neq 0$

e. For i=2, j=3, k=1 $\Rightarrow A=\alpha^6, B=\alpha^{78}$ and $S=\alpha^{60}\neq 0$

f. For i=2, j=4, k=1 $\Rightarrow A=\alpha^{23}, B=\alpha^{78}$ and $S=\alpha^{71}\neq 0$

g. For i=3, j=4, k=1 $\Rightarrow A=\alpha^{18}, B=\alpha^{72}$ and $S=\alpha^{28}\neq 0$

h. For i=3, j=4, k=2 $\Rightarrow A=\alpha^{18}, B=\alpha^{74}$ and $S=\alpha^{73}\neq 0$

i. For i=3, j=1, k=2 $\Rightarrow A=\alpha^{72}, B=\alpha^{74}$ and $S=\alpha^{73}\neq 0$

j. For i=4, j=1, k=2 $\Rightarrow A=\alpha^{54}, B=\alpha^{56}$ and $S=\alpha^{53}\neq 0$

k. For i=4, j=1, k=3 $\Rightarrow A=\alpha^{54}, B=\alpha^{62}$ and $S=\alpha^{13}\neq 0$

l. For i=4, j=2, k=3 $\Rightarrow$ $A=\alpha^{56}, B=\alpha^{72}$ and $S=\alpha^{66}\neq 0$

Thus, no term of the third sum is equal to zero.

*P*4. Forth property, one term in the forth sum is equal to zero necessary and sufficient the following corresponding condition (35);

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

Where, $A=\frac{\alpha_j}{\alpha_i}$, $B=\frac{\alpha_k}{\alpha_i}$, and $C=\frac{\alpha_l}{\alpha_i}$ Suppose;

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

a. For i=1, j=2, k=3, l=4; $A=\alpha^2, B=\alpha^8, C=\alpha^{26}\Rightarrow$ S=$\alpha^{50}\neq 0$

b. For i=1, j=2, k=4, l=3; $A=\alpha^2, B=\alpha^{26}, C=\alpha^8\Rightarrow$ S=$\alpha^{52}\neq 0$

c. For i=1, j=3, k=2, l=4; $A=\alpha^8, B=\alpha^2, C=\alpha^{26}\Rightarrow$ S=$\alpha^{36}\neq 0$

d. For i=1, j=3, k=4, l=2; $A=\alpha^8, B=\alpha^{26}, C=\alpha^2\Rightarrow$ S=$\alpha^{18}\neq 0$

e. For i=1, j=4, k=2, l=3; $A=\alpha^{26}, B=\alpha^2, C=\alpha^8\Rightarrow$ S=$\alpha^{36}\neq 0$

f. For i=1, j=4, k=3, l=2; $A=\alpha^{26}, B=\alpha^8, C=\alpha^2\Rightarrow$ S=$\alpha^{73}\neq 0$

g. For i=2, j=3, k=4, l=1; $A=\alpha^6, B=\alpha^{23}, C=\alpha^{78}\Rightarrow$ S=$\alpha^{48}\neq 0$

h. For i=3, j=4, k=1, l=2; $A=\alpha^{18}, B=\alpha^{72}, C=\alpha^{74}\Rightarrow$ S=$\alpha^{19}\neq 0$

i. For i=4, j=1, k=2, l=3; $A=\alpha^{54}, B=\alpha^{56}, C=\alpha^{62}\Rightarrow$ S=$\alpha^{43}\neq 0$

And we have the same result for other combination of i, j, k and l, and no term of the forth sum is equal to zero.

*P*5. Fifths property, 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) $\alpha_k^{4n}=\alpha_i^{3n}\alpha_j^n$; Where i, j, k are different.

(2) $A_k^4\alpha_k^{\beta+\mu+\gamma}+A_i^3A_j(\alpha_i^{\beta+\mu}\alpha_j^{\gamma}+\alpha_i^{\beta+\gamma}\alpha_j^{\mu}+\alpha_i^{\mu+\gamma}\alpha_j^{\beta}+\alpha^{\beta+\mu+\gamma})=0$

By division on $\alpha_i^{\beta+\mu+\gamma}$ and suppose $A=\frac{\alpha_j}{\alpha_i}$ and $B=\frac{\alpha_k}{\alpha_i}$ the condition (2) becomes;

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

For our paragraph the second condition becomes;

$$B^6+(A^3+A^2+A^1+1)=0$$

Suppose $S=B^6+(A^3+A^2+A^1+1)$

a. For i=1, j=2, k=3; $(\alpha^9)^4=\alpha^{36}, (\alpha)^3(\alpha^3)=\alpha^6\neq\alpha^{36}$ and the first condition is not satisfied.

b. For i=1, j=2, k=4; $(\alpha^{27})^4=\alpha^{28}, (\alpha)^3(\alpha^3)=\alpha^6\neq\alpha^{28}$ and the first condition is not satisfied.

c. For i=1, j=3, k=4; $(\alpha^{27})^4=\alpha^{28}, (\alpha)^3(\alpha^9)=\alpha^{12}\neq\alpha^{28}$ and the first condition is not satisfied.

d. For i=1, j=3, k=2; $(\alpha^3)^4=\alpha^{12}, (\alpha)^3(\alpha^9)=\alpha^{12}$ thus, the first condition is satisfied and for the second condition we have; $A=\alpha^8$, $B=\alpha^2$, $S=\alpha^3+2\alpha^2+2\alpha=\alpha^{35}\neq 0$ thus, the sum of these two terms is not equal to zero.

e. For i=1, j=4, k=2; $(\alpha^3)^4=\alpha^{12}, (\alpha)^3(\alpha^{27})=\alpha^{30}\neq\alpha^{12}$ and the first condition is not satisfied.

f. For i=1, j=4, k=3; $(\alpha^9)^4=\alpha^{36}, (\alpha)^3(\alpha^{27})=\alpha^{30}\neq\alpha^{36}$ and the first condition is not satisfied.

g. For i=2, j=3, k=4; $(\alpha^{27})^4=\alpha^{28}, (\alpha^3)^3(\alpha^9)=\alpha^{18}\neq\alpha^{28}$ and the first condition is not satisfied.

h. For i=2, j=3, k=1; $(\alpha)^4=\alpha^4, (\alpha^3)^3(\alpha^9)=\alpha^{18}\neq\alpha^4$ and the first condition is not satisfied.

i. For i=2, j=4, k=3; $(\alpha^9)^4=\alpha^{36}, (\alpha^3)^3(\alpha^{27})=\alpha^{36}$ thus, the first condition is satisfied and for the second condition we

have; $A=\alpha^{24}$, $B=\alpha^{6}$, $S=\alpha^{3}+\alpha=\alpha^{25}\neq 0$ thus, the sum of these two terms is not equal to zero.

j. For *i*=2, *j*=4, *k*=1; $(\alpha)^4=\alpha^4,(\alpha^3)^3(\alpha^{27})=\alpha^{36}\neq\alpha^4$ and the first condition is not satisfied

k. For *i*=2, *j*=1, *k*=4; $(\alpha^{27})^4=\alpha^{28},(\alpha^3)^3(\alpha)=\alpha^{10}\neq\alpha^{28}$ and the first condition is not satisfied.

l. For *i*=2, *j*=1, *k*=3; $(\alpha^9)^3=\alpha^{27},(\alpha^3)^3(\alpha)=\alpha^{10}\neq\alpha^{27}$ and the first condition is not satisfied.

m. For *i*=3, *j*=1, *k*=4; $(\alpha^{27})^4=\alpha^{28},(\alpha^9)^3(\alpha)=\alpha^{28}$ thus, the first condition is satisfied and for the second condition we have; $A=\alpha^{72}$, $B=\alpha^{18}$, $S=2\alpha^2+\alpha+1=\alpha^{74}\neq 0$ thus, the sum of these two terms is not equal to zero. By the same way, the combinations for *i*=3 and other values of *j* and *k* are not satisfy the first condition.

n. For *i*=4, *j*=2, *k*=1; $(\alpha)^4=\alpha^4,(\alpha^{27})^3(\alpha^3)=\alpha^4$ thus, the first condition is satisfied and for the second condition we have; $A=\alpha^{56}$, $B=\alpha^{54}$, $S=2\alpha=\alpha^{41}\neq 0$ thus, the sum of these two terms is not equal to zero.

By the same way, the combinations for *i*=4 and other values of *j* and *k* are not satisfy the first condition.

*P*6. Sixth property, sum one term of the first sum with one term of the third sum is equal to zero necessary and sufficient the two condition;

(1) $\alpha_l^{4n}=\alpha_i^{2n}\alpha_j^n\alpha_k^n$; Where *i, j, k, l*, are different.

(2) $A_l^4\alpha_l^{\beta+\mu+\gamma}+A_i^2A_jA_k[A^\mu B^\gamma+A^\gamma B^\mu+A^\beta B^\gamma+A^\gamma B^\beta+A^\beta B^\mu+A^\mu B^\beta++(A^\beta+A^\mu+A^\gamma)+$

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

Where, $A=\dfrac{\alpha_j}{\alpha_i}$, $B=\dfrac{\alpha_k}{\alpha_i}$, and $C=\dfrac{\alpha_l}{\alpha_i}$.

For our paragraph the second condition becomes;

$C^6+[A^2B^3+A^3B^2+A^1B^3+A^3B^1+A^1B^2+A^2B^1+(A^1+A^2+A^3)+(B^1+B^2+B^3)]=0$

Suppose; $S=C^6+[A^2B^3+A^3B^2+A^1B^3+A^3B^1+A^1B^2+A^2B^1+(A^1+A^2+A^3)+(B^1+B^2+B^3)]$

a. For *i*=1, *j*=2, *k*=3, *l*=4; $(\alpha^{27})^4=\alpha^{28},(\alpha)^2(\alpha^3)(\alpha^9)=\alpha^{14}\neq\alpha^{28}$ and the first condition is not satisfied.

b. For *i*=1, *j*=2, *k*=4, *l*=3; $(\alpha^9)^4=\alpha^{36},(\alpha)^2(\alpha^3)(\alpha^{27})=\alpha^{32}\neq\alpha^{36}$ and the first condition is not satisfied

c. For *i*=1, *j*=3, *k*=2, *l*=4; $(\alpha^{27})^4=\alpha^{28},(\alpha)^2(\alpha^9)(\alpha^3)=\alpha^{14}\neq\alpha^{28}$ and the first condition is not satisfied

d. For *i*=1, *j*=3, *k*=4, *l*=2; $(\alpha^3)^4=\alpha^{12},(\alpha)^2(\alpha^9)(\alpha^{27})=\alpha^{38}\neq\alpha^{12}$ and the first condition is not satisfied.

e. For *i*=1, *j*=4, *k*=2, *l*=3; $(\alpha^9)^4=\alpha^{36},(\alpha)^2(\alpha^{27})(\alpha^3)=\alpha^{32}\neq\alpha^{36}$ and the first condition is not satisfied.

f. For *i*=1, *j*=4, *k*=3, *l*=2; $(\alpha^3)^4=\alpha^{12},(\alpha)^2(\alpha^{27})(\alpha^9)=\alpha^{38}\neq\alpha^{12}$ and the first condition is not satisfied.

By the same way for other values of *i*=2, 3, 4 and their corresponding values of *j*, *k*, *l* the first condition is not satisfied.

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

Suppose $\alpha\in F_{p^r}$ & $\beta\in F_{p^s}$ and α & β are not in F_p then $\alpha.\beta$ is in F_{p^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 sequence $\{a_n\}$ on F_p which has the complexity *r* and α is a primitive root of its characteristic equation then this sequence is periodic and its period is p^r -1, $\{b_n\}$ is other sequence on F_p which has the complexity *s* and β is a primitive root of its characteristic equation then this sequence is periodic and its period is p^s -1, and suppose for easily, *r* and *s* are relatively prime then the roots of the characteristic equation of the sequence $\{z_n\}=\{a_n.b_n\}$ are in the field $F_{p^{r.s}}$ and this sequence has the period *lcm* $((p^r-1),(p^s-1))$.

Example 4. Suppose, the linearly recurring sequence $\{a_n\}$ defining through the recurring formula $a_{n+2}+a_{n+1}+2a_n=0$ or $a_{n+2}=2a_{n+1}+a_n$ *and* the linearly recurring sequence $\{b_n\}$ on F_p defined through the recurring formula $b_{n+3}+2b_{n+1}+b_n=0$ or $b_{n+3}=b_{n+1}+2b_n$ 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 $\{z_n\}$.

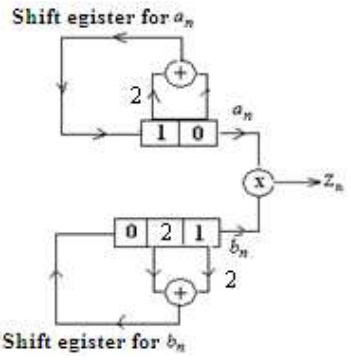

Figure 6. *Feedback shift registers for the sequences $\{a_n\}$ and $\{b_n\}$.*

The characteristic equation of the sequence $\{a_n\}$ is

$x^2+x+2=0$ and its characteristic polynomial is the prime polynomial $f(x)=x^2+x+$. If α is a root of $f(x)$, where $\alpha^2+\alpha+2=0$ then α generate the field F_{3^2} and;

$$F_{3^2}=\{0,\alpha^8=1,\alpha,\alpha^2=2\alpha+1,\alpha^3=2\alpha+2,\alpha^4=2,\alpha^5=2\alpha,\alpha^6=\alpha+2,\alpha^7=\alpha+1\} \quad (40)$$

The general term of the sequence $\{a_n\}$ is of the form $a_n=c_1(\alpha)^n+c_2(\alpha^3)^n$, solving the following system for n=0 and 1 we have;

$$\begin{cases}c_1+c_2=0\\ c_1\alpha+c_2\alpha^3=1\end{cases}\Rightarrow\begin{cases}c_1=2\alpha^2=\alpha+2\\ c_2=\alpha^2=2\alpha+1\end{cases}$$

And the general term of the sequence is;

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

And the sequence is periodic with the period: 3^2-1=8 and the sequence is;

0 1 2 2 0 2 1 1 0 1 2 2 0 2 1 1 0 1 2 2 0 2 1 1 ….

The characteristic equation of the sequence $\{b_n\}$ is $x^3+2x+1=0$ and its characteristic polynomial is the prime polynomial $f(x)=x^3+2x+1$. If β is a root of $f(x)$, where $\beta^3+2\beta+1=0$ then β generate the field F_{3^3} and from *example* 1 and equation 9 we have the general term of the sequence $\{b_n\}$ is of the form $b_n=c_1(\beta)^n+c_2(\beta^3)^n+c_3(\beta^9)^n$, solving the following system for n=0, 1, and 2 we have;

$$\begin{cases}c_1+c_2+c_3=1\\ c_1\beta+c_2\beta^3+c_3\beta^9=2\\ c_1\beta^2+c_2\beta^6+c_3\beta^{18}=0\end{cases}\Rightarrow\begin{cases}c_1=\beta^{20}=2\beta^2+\beta+1\\ c_2=\beta^8=2\beta^2+2\\ c_3=\beta^{24}=2\beta^2+2\beta+1\end{cases}$$

And the general solution of the characteristic equation is;

$$b_n=\beta^{20}(\beta)^n+\beta^8(\beta^3)^n+\beta^{24}(\beta^9)^n$$

Or;

$$b_n=(2\beta^2+\beta+1)\beta^n+(2\beta^2+2)(\beta+2)^n+(2\beta^2+2\beta+1)(\beta+1)^n$$

And the sequence is periodic with the period: 3^3-1=26 and the sequence is;

1 2 0 1 1 1 0 0 2 0 2 1 2 2 1 0 2 2 2 0 0 1 0 1 2 1 1 2 0 1 1 1 0 ….

From the relation $z_n=a_n.b_n$ we have;

$$z_n=2\alpha^2\beta^{20}(\alpha\beta)^n+2\alpha^2\beta^8(\alpha\beta^3)^n+2\alpha^2\beta^{24}(\alpha\beta^9)^n+\alpha^2\beta^{20}(\alpha^3\beta)^n+\alpha^2\beta^8(\alpha^3\beta^3)^n+\alpha^2\beta^{24}(\alpha^3\beta^9)^n \quad (41)$$

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

$$(\alpha\beta)(\alpha\beta^3)(\alpha\beta^9)(\alpha^3\beta)(\alpha^3\beta^3)(\alpha^3\beta^9)=\alpha^{12}\beta^{26}=\alpha^4=2$$

And its characteristic equation is of the form;

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

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

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

Thus, we have; $c_1=c_2=1, c_3=2; c_4=c_5=0$ and, in result, the recurring equation of $\{z_n\}$ is;

$$z_{n+6}+2z_{n+3}+z_{n+2}+z_{n+1}+2z_n=0 \quad (42)$$

Or;

$$z_{n+6}=z_{n+3}+2z_{n+2}+2z_{n+1}+z_n$$

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

$$f(x)=x^6+2x^3+x^2+x+2$$

This polynomial is not irreducible polynomial and;

$$f(x)=x^6+2x^3+x^2+x+2=(x+2)^2(x^2+1)(x^2+2x+2)$$

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

The linear feedback shift register of the sequence $\{z_n\}$ is showing in the following figure 7;

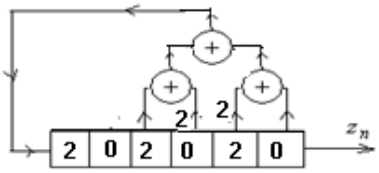

Figure 7. *The linear feedback register of the sequence $\{z_n\}$.*

Thus, the sequence $\{z_n\}$is periodic with the period *lcm*(8, 26))=104 and the sequence is;

02020200001201100210020101
21021100100222001100010112
01010100002102200120010202
12012220020011002200020221,
02020200001201100210020101 …..

Thus for one period we say w_0 where;

w_0=(02020200001201100210020101
21021100100222001100010112
01010100002102200120010202
12012220020011002200020221)

From equations (4) and (5);

$$w_i(\tau) = 0 \text{ and } R_{w_i}(\tau) = 16 ; i = 0,1,...,104$$

And; $w_{0+1}=w_0 + w_1=$
(12222220001021210201022111
00120210110211201210011120
21111110002012120102011222
00210120220122102120022210)
Thus;

$$w_{0+1} \notin S, \sum_{w_{0+1}} = 0, \text{ and } R_{w_0,w_1} = 2$$

Thus; S is not an orthogonal set

In other hand the polynomial $h(x) = x^6 + x + 2$ is a prime polynomial in F_2^6 and if γ is a root of $h(x)$ in F_2^6 then γ generates F_2^6 and;

For written z_n through elements in F_2^6 we need search in F_2^6 about first element e_1 which satisfies the characteristic equation $x^2 + x + 2 = 0$ and will be equal to α, and we search about second element e_2 which satisfies the characteristic equation $x^3 + 2x + 1 = 0$ and will be equal to β then after w replacing in formula of z_n each α by first element e_1 and each β by the second element e_2 we have z_n written through elements from the field F_3^6, and this step is not very need in our current study.

Thus the nonlinearly Property allows us construct new sequences with largest periods.

3.3. Using Shift Feedback Register LFSR as Monitor Register

Suppose there is a set S of p linear feedback shift registers that is; S={LFSR(0), LFSR(1), ….., LFSR(p-1)} and the shift feedback shift register LFSR and we will use it as an monitor register as following:

a) If the output of the register LFSR is 0 then the output of the system S is the output of LFSR(0).

b) If the output of the register LFSR is 1 then the output of the system S is the output of LFSR(1).

……..

c) If the output of the register LFSR is p-1 then the output of the system S is the output of LFSR(p-1).

Suppose, output of LFSR(0) is I_0, output of LFSR(1) is I_1, …, output of LFSR(p-1) is Ip-1, and through

Solving the system of equations for $0 \le x \le p-1$;

$$s = a_{p-1}x^{p-1} + a_{p-2}x^{p-2} + ... + a_1 x + a_0 \qquad (43)$$

We can find the coefficients a_0, a_1, …, a_{p-1}, where "x" is the output of the monitor register LFSR and "s" is the output of the system S which is equal to the output of the register LFSR(x) for $0 \le x \le p-1$ and x^k computed by mod p, thus we get the solution of our problem.

Exampe 5.

1) For p=2 that is the all registers are binary registers and the all arithmetic operations are the operation on F_2, we can find the coefficients a_0, a_1 in the equation (49) as following;

The formula (49) will be; $s = a_1 x + a_0$

a) For x=0, then; $I_0 = a_0$ and $s = a_1 x + I_0$

b) For x=1, then; $I_1 = a_1 + I_0$

c) From b) and c) we have; $a_1 = I_1 + I_0$, and;

$$s = (I_1 + I_0)x + I_0$$

2) For p=3, the all arithmetic operations are the operations on F_3, we can find the coefficients a_0, a_1, a_2 in the equation (43) as following;

The formula (43) will be; $s = a_2 x^2 + a_1 x + a_0$

d) For x=0, then; $I_0 = a_0$ and $s = a_2 x^2 + a_1 x + I_0$

e) For x=1, then; $I_1 = a_2 + a_1 + I_0$

f) For x=2, then; $I_2 = a_2 + 2a_1 + I_0$

g) From b) and c) we have; $a_1 = 2I_1 + I_2$, $a_2 = 2I_2 + 2I_1 + 2I_0$ and;

$$s = (2I_0 + 2I_1 + 2I_2)x^2 + (2I_1 + I_2)x + I_0$$

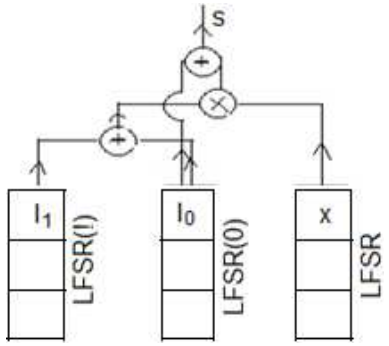

Figure 8. *System of three registers where LFSR is a monitor register to the other two registers.*

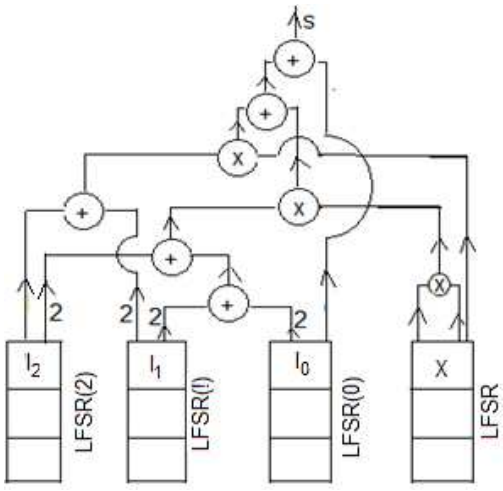

Figure 9. *System of four registers where LFSR is monitor register of the other three registers.*

4. Conclusion

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

$$ {}_rN_2 = \binom{r}{1} + \binom{r}{2} = r + \frac{r(r-1)}{2} \tag{44} $$

For example, for *r*=3 and *h*=2 the length of the linear equivalent of $\{z_n\}$ is 6.

2) If the sequence $\{z_n\}$ is multiplication on only two degrees of the recurring sequence $\{a_n\}$ over *Fp* and the characteristic polynomial of the sequence $\{a_n\}$ is prime of degree *r* then the sequence $\{z_n\}$ is also periodic and its period is equal to $\frac{p^r-1}{2}$ that is the half period of $\{a_n\}$ but the set of the cyclic permutations of one period of $\{z_n\}$is don't form an orthogonal set as the sequence $\{a_n\}$.

3) If the sequence $\{z_n\}$ is multiplication on *h* degrees of the recurring sequence $\{a_n\}$over *Fp* and the characteristic polynomial of the sequence $\{a_n\}$is prime of degree *r* and h >2 then the length of equivalent LFSR of $\{z_n\}$ is larger than of the maximum length in the binary sequences ${}_rN_h$, where;

$$ {}_rN_h = \binom{r}{1} + \ldots + \binom{r}{h} = r + \frac{r(r-1)}{2} + \ldots + \frac{r!}{h!(r-h)!} \tag{45} $$

For example, for *r*=3 and *h*=3 the length of the linear equivalent is 9 and larger than ${}_3N_3 = 7$ and for *r*=4, *h*=4 the length of the linear equivalent of $\{z_n\}$ is 29

4) Length of the linear equivalent of a multiplication sequence $\{z_n\}$ on *h* degrees of the linear recurring sequence $\{a_n\}$ over *Fp* 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 and any where is larger than (or equal for *h*=2) the maximum length ${}_rN_h$ in the binary sequences.

5) we suggestion that the maximum length of the linearly shift register equivalent of multiplication sequence $\{z_n\}$ on *h* degrees of a linear sequence $\{a_n\}$over *Fp* which has the complexity *r* is ${}_rM_h = \binom{r}{1} + p\binom{r}{2} + \ldots + p\binom{r}{h}$ for h >2 and thus for *p*=3; if *r*=3 and *h*=3 then ${}_3M_3 = 3 = 9 + 3 = 15$ and if *r*=4 and *h*=4 then $4M_4 = 4 + 18 + 12 + 3 = 37$.

6) If the sequence $\{z_n\}$ is a multiplication on two different 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 *lcm* $((p^r-1),(p^s-1))$, and has the complexity *r.s*. If *r* and *s* are not relatively prime then the period of the sequence $\{z_n\}$is $(p^{lcm(r,s)}-1)$ and its complexity is *lcm*(*r*,*s*).

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

8) We can use one shift feedback register LFSR over *Fp* as monitor register for other *p* registers over *Fp*.

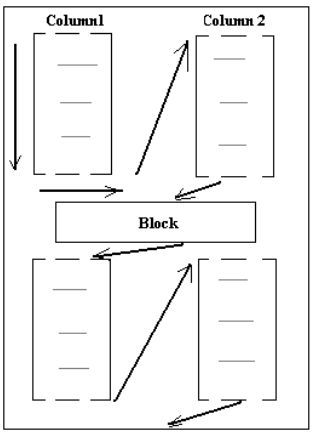

Figure 10. *Method reading page with block.*

Limitation: The method for reading a page which has a block will be according to the following direction as in figure 10.

Appendix

Table 1. *Elements* F_{3^4}.

F_{3^4}		
0	$\alpha^{26} = \alpha^2 + 2\alpha + 1$	$\alpha^{53} = \alpha + 1$
$\alpha^{80} = 1$	$\alpha^{27} = \alpha^3 + 2\alpha^2 + \alpha$	$\alpha^{54} = \alpha^2 + \alpha$
α	$\alpha^{28} = 2\alpha^3 + \alpha^2 + 2\alpha + 1$	$\alpha^{55} = \alpha^3 + \alpha^2$
α^2	$\alpha^{29} = \alpha^3 + 2\alpha^2 + 2\alpha + 2$	$\alpha^{56} = \alpha^3 + 2\alpha + 1$
α^3	$\alpha^{30} = 2\alpha^3 + 2\alpha^2 + \alpha + 1$	$\alpha^{57} = 2\alpha^2 + 1$
$\alpha^4 = 2\alpha + 1$	$\alpha^{31} = 2\alpha^3 + \alpha^2 + 2\alpha + 2$	$\alpha^{58} = 2\alpha^3 + \alpha$
$\alpha^5 = 2\alpha^2 + \alpha$	$\alpha^{32} = \alpha^3 + 2\alpha^2 + 2$	$\alpha^{59} = \alpha^2 + \alpha + 2$
$\alpha^6 = 2\alpha^3 + \alpha^2$	$\alpha^{33} = 2\alpha^3 + \alpha + 1$	$\alpha^{60} = \alpha^3 + \alpha^2 + 2\alpha$

$\alpha^7 = \alpha^3 + \alpha + 2$	$\alpha^{34} = \alpha^2 + 2\alpha + 2$	$\alpha^{61} = \alpha^3 + 2\alpha^2 + 2\alpha + 1$
$\alpha^8 = \alpha^2 + \alpha + 1$	$\alpha^{35} = \alpha^3 + 2\alpha^2 + 2\alpha$	$\alpha^{62} = 2\alpha^3 + 2\alpha^2 + 1$
$\alpha^9 = \alpha^3 + \alpha^2 + \alpha$	$\alpha^{36} = 2\alpha^3 + 2\alpha^2 + 2\alpha + 1$	$\alpha^{63} = 2\alpha^3 + 2\alpha + 2$
$\alpha^{10} = \alpha^3 + \alpha^2 + 2\alpha + 1$	$\alpha^{37} = 2\alpha^3 + 2\alpha^2 + 2\alpha + 2$	$\alpha^{64} = 2\alpha^2 + 2$
$\alpha^{11} = \alpha^3 + 2\alpha^2 + 1$	$\alpha^{38} = 2\alpha^3 + 2\alpha^2 + 2$	$\alpha^{65} = 2\alpha^3 + 2\alpha$
$\alpha^{12} = 2\alpha^3 + 1$	$\alpha^{39} = 2\alpha^3 + 2$	$\alpha^{66} = 2\alpha^2 + \alpha + 2$
$\alpha^{13} = 2\alpha + 2$	$\alpha^{40} = 2$	$\alpha^{67} = 2\alpha^3 + \alpha^2 + 2\alpha$
$\alpha^{14} = 2\alpha^2 + 2\alpha$	$\alpha^{41} = 2\alpha$	$\alpha^{68} = \alpha^3 + 2\alpha^2 + \alpha + 2$
$\alpha^{15} = 2\alpha^3 + 2\alpha^2$	$\alpha^{42} = 2\alpha^2$	$\alpha^{69} = 2\alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^{16} = 2\alpha^3 + \alpha + 2$	$\alpha^{43} = 2\alpha^3$	$\alpha^{70} = \alpha^3 + \alpha^2 + 2\alpha + 2$
$\alpha^{17} = \alpha^2 + 2$	$\alpha^{44} = \alpha + 2$	$\alpha^{71} = \alpha^3 + 2\alpha^2 + \alpha + 1$
$\alpha^{18} = \alpha^3 + 2\alpha$	$\alpha^{45} = \alpha^2 + 2\alpha$	$\alpha^{72} = 2\alpha^3 + \alpha^2 + 1$
$\alpha^{19} = 2\alpha^2 + 2\alpha + 1$	$\alpha^{46} = \alpha^3 + 2\alpha^2$	$\alpha^{73} = \alpha^3 + 2\alpha^2 + 2$
$\alpha^{20} = 2\alpha^3 + 2\alpha^2 + \alpha$	$\alpha^{47} = 2\alpha^3 + 2\alpha + 1$	$\alpha^{74} = 2\alpha^2 + \alpha + 1$
$\alpha^{21} = 2\alpha^3 + \alpha^2 + 2\alpha + 2$	$\alpha^{48} = 2\alpha^3 + 2\alpha + 2$	$\alpha^{75} = 2\alpha^3 + \alpha^2 + \alpha$
$\alpha^{22} = \alpha^3 + \alpha^2 + 2$	$\alpha^{49} = 2\alpha^3 + 2\alpha^2 + 2\alpha$	$\alpha^{76} = \alpha^3 + \alpha^2 + \alpha + 2$
$\alpha^{23} = \alpha^3 + \alpha + 1$	$\alpha^{50} = 2\alpha^3 + 2\alpha^2 + \alpha + 2$	$\alpha^{77} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^{24} = \alpha^2 + 1$	$\alpha^{51} = 2\alpha^3 + \alpha^2 + 2$	$\alpha^{78} = \alpha^3 + \alpha^2 + 1$
$\alpha^{25} = \alpha^3 + \alpha$	$\alpha^{52} = \alpha^3 + 2$	$\alpha^{79} = \alpha^3 + 1$

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, No 3, 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] 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.

[15] Al Cheikha. A. H., (2020), "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.ijics.20200503.11.