BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Electronic & Information Systems
https://ojs.bilpublishing.com/index.php/jeis

ARTICLE

Generalization of Multiplication M-Sequences over Fp and Its Reciprocal Sequences

Ahmad Al Cheikha[1*] Ebtisam Haj Omar[2]

1. Department of Math Science, Ahlia University, Bahrain
2. Department of Electronic Energy, Tishreen University, Syria

ARTICLE INFO

Article history
Received: 23 September 2021
Accepted: 8 October 2021
Published Online: 2 November 2021

Keywords:
Mp-Sequences
Finite fields
Shift register
Orthogonal
Complexity
Characteristic polynomial
Reciprocal polynomial

ABSTRACT

M_p-Sequences or M-Sequence over F_p not used so much in current time as binary M-Sequences and it is pending with the difficult to construct there coders and decoders of Mp-Sequences further these reasons there is expensive values to construct them but the progress in the technical methods will be lead to fast using these sequences in different life's ways, and these sequences give more collection of information and distribution them on the input and output links of the communication channels, building new systems with more complexity, larger period, and security. In current article we will study the construction of the multiplication Mp-Sequence $\{z_n\}$ and its linear equivalent, this sequences are as multiple two sequences, the first sequence $\{S_n\}$ is an arbitrary Mp-Sequence and the second sequence $\{\zeta_n\}$ reciprocal sequence of the first sequence $\{S_n\}$, length of the sequence $\{z_n\}$, period, orthogonal and the relations between the coefficients and roots of the characteristic polynomial of $f(x)$ and it's reciprocal polynomial $g(x)$ and compare these properties with corresponding properties in M-Sequences.

1. Introduction

Sloane, N.J.A., studied the product or multiplication sequence $\{z_n\}$ on t degrees of the sequence $\{a_n\}$ which has the degree of complexity r and gave the answer that the degree of complexity of $\{z_n\}$ can't be exceeded [1,2].

Mokayes D. Al Cheikha A. H., studied the construction of the multiplication binary M-Sequences where the multiplication on one M-Sequence or on more than one sequence and gave an illustrated about the question "why the length of the linear equivalent shift register don't reached the maximum length?" [3-8].

Al Cheikha A. H., Omar E H.., studied the construction of the multiplication binary M-Sequences with it's reciprocal sequences, they studied the length of the result multiplication sequence $\{z_n\}$ which is equals $[(\deg f(x))^2 - \deg(f(x))]$, linear equivalent, properties of the coefficients of the roots of the characteristic polynomial $f(x)$ and it's reciprocal sequence. Current article and showing the agreement and disagreement between these coefficients and corresponding roots, in the first side, in binary M-Sequences, and in the second side, Mp-Sequences [9-11].

2. Research Method and Materials

2.1 Mp-Sequences or M-Sequences over Fp

Mp- Sequences or M-Sequences over Fp $\{a_n\}$ is of the form;

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

Distributed under creative commons license 4.0 DOI: https://doi.org/10.30564/jeisr.v3i2.3740

$$a_{n+k} = \gamma_{k-1}a_{n+k-1} + \gamma_{k-2}a_{n+k-2} + ... + \gamma_0 a_n$$

$$+\gamma; \gamma \,\&\, \gamma_i \in F_p = \{0,1,2,..., p-1\}, i = 0,1,...,k-1$$

Or;

$$a_{n+k} = \sum_{i=0}^{k-1} \gamma_i a_{n+i} + \gamma \tag{1}$$

where, $\gamma, \gamma_0, \gamma_1, ..., \gamma_{k-1}$ are in the field *Fp* and *k* is positive integer is called a linear recurring sequence of complexity or order *k*, *for* $\gamma = 0$ the sequence is called homogeneous sequence (H.L.R.S), in other case the sequence is called non-homogeneous, the vector $(a_0, a_1, ..., a_{k-1})$ is called the initial vector and the characteristic equation of the sequence is;

$$f(x) = x^k + \gamma_{k-1}x^{k-1} + ... + \gamma_1 x + \gamma_0 \tag{2}$$ [12-14]

We are limited in our article to $p > 2$.

2.2 Definitions and Theorems

Definition 1

The L.F.S.R is a linear feedback shift register if contains only addition circuits and the general term of the sequence $\{s_n\}$ generated through the shift register is the term of the output of the register [3].

Definition 2

The vector $\overline{X} = (\overline{a_1}, \overline{a_2}, ..., \overline{a_n})$ is the complement of the vector $X = (a_1, a_2, ..., a_n,)\, a_i \in F_p$ where

$$\overline{a_i} == p-1 \; if \; a_i \neq 0 \; and \; \overline{a_i} = 0 \; if \; a = 0 \tag{3}$$ [12-14]

Definition 3

The coefficient of correlation function of the two vectors $t = (t_0, t_1, ..., t_{n-1})$ and $l = (l_0, l_1, ..., l_{n-1})$ on F_p which denoted by $R_{t,l}$, is:

$$R_{t,l} = \left| \left(\sum_{i=0}^{n-1} (-1)^{t_i + l_i} \right) - \left(\left[\frac{n+1}{p} \right] - 1 \right) \right| \tag{4}$$

Where $\left[\frac{n+1}{p} \right]$ is the nearest integer of the number $\frac{n+1}{p}$, and we said the two vectors *t* and *l* are orthogonal if $\sum l = \sum_{i=0}^{n} l_i = 0, \sum t = \sum_{i=0}^{n} t_i = 0 \; mod \; p$, and $R_{t,l} \leq 1$ [8-10,13].

Definition 4

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

$$a(\tau) = 0 \;\; and \;\; R_a(\tau) \leq 1 \tag{5}$$

When;

$$a(\tau) = \sum_{t=0}^{r-1} a_i (t+\tau) \; mod \; p, \tau = 0,1,...,r; \; R_a(\tau) =$$

$$\left| \sum_{t=0}^{r-1} (-1)^{a(t+\tau)+a(t)} - \left(p^{k-1} - 1\right) \right|, \;\; for \; \tau \neq \frac{p^k - 1}{2} \tag{6}$$

Definition 5

The set $A = \left\{ t; t = (t_0, t_1, ..., t_{n-1}) \; t_i \in F_p, i = 0,1,...,n-1 \right\}$ is called an orthogonal set if and only if the set *A* satisfies the following two conditions;

$$1. \; \forall t \in A; \left| R_{t,0} \right| \leq 1. \tag{7}$$

$$2. \; \forall t, l \in A, \& \; t \neq l, \left| R_{t,l} \right| \leq 1. \tag{8}$$ [15,16]

Definition 6

If the function *f*(*x*) has the degree *n* then the reciprocal function of *f*(*x*) is the function;

$$g(x) = x^n f(1/x) \tag{9}$$

Theorem 7

If $\{s_n\}$ is a H.L.R.S sequence with the complexity *k*, period *r* and its characteristic polynomial is $f(x)$ then $r \,|\, ord\, f(x)$ and if the polynomial $f(x)$ is primitive and it's coefficients are in F_p then the period of the sequence $\{s_n\}$ is $p^k - 1$ and this sequence is called M_p-Sequence or M-Sequence over F_p [2,15-17].

Lemma 8. (Fermat's theorem).

If the finite field F of order *q* then each element *x* of *F* satisfies the equation;

$$x^q = x \tag{10}$$ [2,15-18]

Theorem 9

If $\{a_n\}$ is a H.L.R.S in F_p and $g(x)$ is its characteristic prime polynomial of degree *k* and α is a root of $g(x)$ in any splitting field of F_p then the general term of the sequence $\{a_n\}$ is;

$$a_n = \sum_{i=1}^{k} C_i \left(\alpha^{p^{i-1}} \right)^n \tag{11}$$

And the sequence $\{a_n\}$ has the period p^{k-1} [2,18].

Theorem 10

i. $(q^m - 1) \,|\, (q^n - 1) \Leftrightarrow m \,|\, n$ **(12)**

ii. any subfield of the field F_{p^n} is a field of order p^m where $m \,|\, n$ and if F_q is a field of order $q = p^n$ then any subfield of it is has the order p^m and $m \,|\, n$, and by inverse if $m \,|\, n$ then

Distributed under creative commons license 4.0
DOI: https://doi.org/10.30564/jeisr.v3i2.3740

the field F_{p2^n} contains a subfield of order p^m [2,15-18].

*Our study is limited to the M_p-Sequence or M-Sequence over F_p and it's period is: $r = p^k - 1$.

3. Results and Discussion

Multiplication Two Reciprocal Mp-Sequences

If $f(x)$ is the characteristic prime polynomial of the M_p-Sequence $\{s_n\}$ of degree k in the field F_p, and $\alpha_1, \alpha_2, \ldots \alpha_k$ are it's independent different roots in the F_p^k, which is a splitting field of F_p then the general term of the sequence $\{s_n\}$ is

$$s_n = A_1\alpha_1^n + A_2\alpha_2^n + \ldots + A_k\alpha_k^n = \sum_{i=1}^{k} A_i\alpha_i^n \tag{13}$$

And if α is a root of $f(x)$ then we can find;

$$\alpha_1 = \alpha, \alpha_2 = \alpha^{p^{2-1}}, \ldots, \alpha_k = \alpha^{p^{k-1}}$$

And the general term of the sequence $\{s_n\}$ becomes;

$$s_n = A_1\alpha^n + A_2(\alpha^{p^{2-1}})^n + \ldots + A_k(\alpha^{p^{k-1}})^n = \sum_{i=1}^{k} A_i(\alpha^{p^{i-1}})^n \tag{14}$$

Suppose $g(x)$ is the reciprocal of $f(x)$, $\beta_1, \beta_2, \ldots, \beta_k$ are the different linear independent roots of $g(x)$, and $g(x)$ characteristic polynomial of the M_p-Sequence $\{\zeta_n\}$ reciprocal sequence of $\{s_n\}$ then the general term of the sequence $\{\zeta_n\}$ is

$$\zeta_n = B_1\beta_1^n + B_2\beta_2^n + \ldots + B_k\beta_k^n = \sum_{i=1}^{k} B_i\beta_i^n$$

Thus, if α_i is of the form $\alpha^{p^{i-1}}$ and β_i is reciprocal α_i then $\beta_i = \alpha^{p^k - p^{i-1} - 1}$ and ζ_n can be written in the form;

$$\zeta_n = B_1\alpha^{n(p^k-2)} + B_2\alpha^{n(p^k-3)} + \ldots + B_k\alpha^{n(p^k-p^{k-1}-1)} = \sum_{i=1}^{k} B_i\alpha^{n(p^k-p^{i-1}-1)} \tag{15}$$

Thus;

$$s_n\zeta_n = \left(\sum_{i=1}^{k} A_i(\alpha^{p^{i-1}})^n\right)\left(\sum_{j=1}^{k} B_j(\alpha^{(p^k-p^{j-1}-1)})^n\right) = \left(\sum_{i,j=1,i\neq j}^{k} A_iB_j(\alpha^{p^{i-1}})^n(\alpha^{(p^k-p^{j-1}-1)})^n\right) + \left(\sum_{i=1}^{k} A_iB_i\right) \tag{16}$$

Example 1

Suppose the polynomial $f(x) = x^2 + x + 2$ which is a prime characteristic polynomial the sequence $\{s_n\}$, $\forall n \in N; s_n \in F_3$ s_n satisfies;

$$s_{n+2} + s_{n+1} + 2s_n = 0; or\ s_{n+2} = 2s_{n+1} + s_n; s_0 = 0, s_1 = 1$$

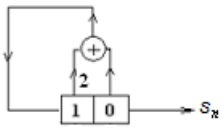

Figure 1. *Shift register generating the sequence $\{s_n\}$ on F_3*

The characteristic equation of the sequence $\{s_n\}$ is;

$$x^2 + x + 2 = 0 \tag{17}$$

If α is a root of the equation then;

$$\alpha^2 + \alpha + 2 = 0$$

And;

$$F_{3^2} = \{0, \alpha^8 = 1, \alpha, \alpha^2 = 2\alpha + 1, \alpha^3 = 2\alpha + 2, \alpha^4 = 2, \alpha^5 = 2\alpha, \alpha^6 = \alpha + 2, \alpha^7 = \alpha + 1 \tag{18}$$

The general term of the sequence $\{s_n\}$ is of the form;

$$S_n = S_1\alpha^n + S_2(\alpha^3)^n$$

Solving the following equations;

$$\begin{cases} n = 0 \rightarrow S_1 + S_2 = 0 \\ n = 1 \rightarrow \alpha S_1 + \alpha^3 S_2 = 1 \end{cases}$$

We have;

$$S_1 = \alpha^6 = \alpha + 2, S_2 = \alpha^2 = 2\alpha + 1$$

And the general solution of the characteristic equation is;

$$S_n = \alpha^6(\alpha)^n + \alpha^2(\alpha^3)^n \tag{19}$$

Or;

$$S_n = (\alpha + 2)\alpha^n + (2\alpha + 1)(2\alpha + 2)^n$$

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 1 0 2 1 1 ….. (20)

We can see the important properties;

$$\left(\alpha^6(\alpha)\right)^3 = \left(\alpha^2(\alpha^3)\right) or\ (\alpha^6)^3 = \alpha^2\ \&\ (\alpha)^3 = \alpha^3 \tag{21}$$

By the same way;

$$\left(\alpha^2(\alpha^3)\right)^3 = \left(\alpha^6(\alpha)\right) or\ (\alpha^2)^3 = \alpha^6\ \&\ (\alpha^3)^3 = \alpha \tag{22}$$

The unitary reciprocal polynomial of the prime $f(x)$ is the prime polynomial $g(x) = x^2 + 2x^2 + 2$ and it is the characteristic polynomial of the recurring sequence $\{\zeta_n\}$ where $\zeta_{n+2} + 2\zeta_{n+1} + 2\zeta_n = 0$ or $\zeta_{n+2} = \zeta_{n+1} + \zeta_n$, the roots of $g(x)$ are;

$$\beta_1 = \frac{\alpha^8}{\alpha} = \alpha^7, \beta_2 = \frac{\alpha^8}{\alpha^3} = \alpha^5 \tag{23}$$

Is very easy looking that α^7, α^5, are roots of the characteristic polynomial $g(x)$ corresponding the roots

Distributed under creative commons license 4.0 DOI: https://doi.org/10.30564/jeisr.v3i2.3740

α, α^3 of $f(x)$ and the general term ζ_n is;

$$\zeta_n = B_1(\alpha^7)^n + B_2(\alpha^5)^n$$

For the initial vector ($\zeta_0 = 1, \zeta_1 = 1$);

$$\begin{cases} n = 0 \rightarrow B_1 + B_2 = 1 \\ n = 1 \rightarrow \alpha^7 B_1 + \alpha^5 B_2 = 1 \end{cases}$$

We have $B_1 = \alpha^5, B_2 = \alpha^7$ and the general term of the sequence $\{\zeta_n\}$ is;

$$\zeta_n = \alpha^5(\alpha^7)^n + \alpha^7(\alpha^5)^n \quad (24)$$

We can see the important properties;

$$\left(\alpha^5(\alpha^7)\right)^3 = \left(\alpha^7(\alpha^5)\right) or\ (\alpha^5)^3 = \alpha^7\ \&\ (\alpha^7)^3 = \alpha^5 \quad (25)$$

By the same way;

$$\left(\alpha^7(\alpha^5)\right)^3 = \left(\alpha^5(\alpha^7)\right) or\ (\alpha^7)^3 = \alpha^5\ \&\ (\alpha^5)^3 = \alpha^7 \quad (26)$$

The sequence $\{\zeta_n\}$ is periodic with the period $2^3 - 1 = 8$ and it is the flowing sequence;

1 1 2 0 2 2 1 0 1 1 2 0 2 2 1 0 …. (27)

Figure 2 shows the shift register generating $\{\zeta_n\}$

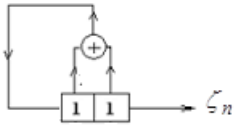

Figure 2. *shift register generating* $\{\zeta_n\}$

We can look that one period of the sequence $\{\zeta_n\}$ is one period of the sequence $\{s_n\}$but through reading it by inverse from the right to the left.

The multiplication sequence $\{z_n\}$, where $z_n = s_n . \zeta_n$ is;

$$\begin{aligned} z_n = s_n.\zeta_n &= \left[\alpha^6(\alpha)^n + \alpha^2(\alpha^3)^n\right]\left[\alpha^5(\alpha^7)^n + \alpha^7(\alpha^5)^n\right] \\ &= \alpha^{13}\alpha^{6n} + \alpha^7\alpha^{10n} + \alpha^9 + \alpha^{11} \\ &= \alpha^{13}\alpha^{6n} + \alpha^7\alpha^{10n} + 2 \end{aligned} \quad (28)$$

Or;

$$z_n = \alpha^5\alpha^{6n} + \alpha^7\alpha^{2n} + 2 \quad (29)$$

Thus, the sequence $\{z_n\}$ is a linear nonhomogeneous sequence with the length of its linear homogeneous equivalent is equals 2 that is equal to $(\deg f(x))^2 - \deg f(x) = 2$, The period of $\{z_n\}$is 4 and it's the half period of the sequence$\{s_n\}$and the sequence $\{z_n\}$ is: 0110 0110 0110 0110 …….

We can check that the set of the all periodic permutation of one period is not an orthogonal set for example , for one permutation of the period: 0110 is: 0011 and the sum of the two vectors is 0121 and is not belong to the set of permutations.

Figure 3 illustrates the feedback shift registers generating the sequence $\{z_n\}$;

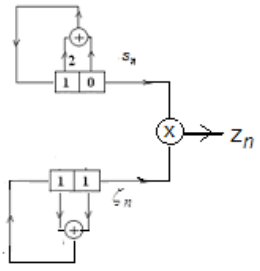

Figure 3. *Illustrated the multiplication sequence* $\{z_n\}$

xSuppose the linear homogeneous part of z_n is $LHP(z_n)$ $=\{z_n^{'}\}$;

$$LHP(z_n) = z_n^{'} = \alpha^5\alpha^{6n} + \alpha^7\alpha^{2n} \quad (30)$$

The sequence $\{z_n^{'}\}$ is;

1 2 2 1 1 2 2 1 1 2 2 1 … (31)

The characteristic equation of the sequence $\{z_n^{'}\}$is;

$$(x - \alpha^2)(x - \alpha^6) = 0$$

$$x^2 + 1 = 0 \quad (32)$$

And the recurring formula is $z_n^{'} + z_n^{'} = 0$ or $z_n^{'} = 2z_n^{'}$. Figure 4 illustrate the linear shift register generating sequence $\{z_n^{'}\}$.

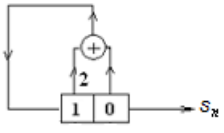

Figure 4. *shift register generating the sequence* $\{z_n^{'}\}$

As the sequence $\{z_n\}$ the set of all periodic permutations of one period of the sequence $\{z_n^{'}\}$ is not an orthogonal set.

Example 2

Suppose the polynomial $f(x) = x^3 + 2x + 1$ which is a prime characteristic polynomial the sequence $\{a_n\}$ as in figure5, $\forall n \in N; a_n \in F_3$ a_n satisfies;

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

$$a_1 = 1, a_2 = 1$$

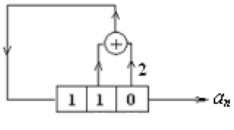

Figure 5. *Shift register generating the sequence* $\{a_n\}$*on* F_3

Distributed under creative commons license 4.0
DOI: https://doi.org/10.30564/jeisr.v3i2.3740

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

$$x^3 + 2x + 1 = 0 \tag{33}$$

If α is a root of the equation then;

$$\alpha^3 + 2\alpha + 1 = 0 \tag{34}$$

And;

$$\begin{aligned} F_{3^3} = \{0, \alpha^{26} = 1, \alpha, \alpha^2, \alpha^3 = \alpha + 2, \alpha^4 = \alpha^2 + 2\alpha, \alpha^5 = 2\alpha^2 + \alpha + 2, \alpha^6 = \alpha^2 + \alpha + 1, \\ \alpha^7 = \alpha^2 + 2\alpha + 2, \alpha^8 = 2\alpha^2 + 2, \alpha^9 = \alpha + 1, \alpha^{10} = \alpha^2 + \alpha, \alpha^{11} = \alpha^2 + \alpha + 2 \\ \alpha^{12} = \alpha^2 + 2, \alpha^{13} = 2, \alpha^{14} = 2\alpha, \alpha^{15} = 2\alpha^2, \alpha^{16} = 2\alpha + 1, \alpha^{17} = 2\alpha^2 + \alpha, \\ \alpha^{18} = \alpha^2 + 2\alpha + 1, \alpha^{19} = 2\alpha^2 + 2\alpha + 2, \alpha^{20} = 2\alpha^2 + \alpha + 1, \alpha^{21} = \alpha^2 + 1, \\ \alpha^{22} = 2\alpha + 2, \alpha^{23} = 2\alpha^2 + 2\alpha, \alpha^{24} = 2\alpha^2 + 2\alpha + 1, \alpha^{25} = 2\alpha^2 + 1\} \end{aligned} \tag{35}$$

The general term of the sequence $\{a_n\}$ is of the form;

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

Solving the following equations ;

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

We have;

$$A_1 = \alpha^{22} = 2\alpha + 2, A_2 = \alpha^{14} = 2\alpha, A_3 = \alpha^{16} = 2\alpha + 1$$

We can see the properties;

$$(A_1)^3 = (\alpha^{22})^3 = \alpha^{14} = A_2$$
$$(A_2)^3 = (\alpha^{14})^3 = \alpha^{16} = A_3$$
$$(A_3)^3 = (\alpha^{16})^3 = \alpha^{22} = A_1$$

And the general solution of the characteristic equation is;

$$a_n = \alpha^{22}(\alpha)^n + \alpha^{14}(\alpha^3)^n + \alpha^{16}(\alpha^9)^n \tag{36}$$

Or;

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

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

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 01110…. (37)

The reciprocal polynomial of the prime $f(x)$ is the prime polynomial $g(x) = x^3 + 2x^2 + 1$ and it is the characteristic polynomial of the recurring sequence $b_{n+3} + 2b_{n+2} + b_n = 0$ or $b_{n+3} = b_{n+2} + 2b_n$, the roots of $g(x)$ are;

$$\beta_1 = \frac{\alpha^{26}}{\alpha} = \alpha^{25}, \beta_2 = \frac{\alpha^{26}}{\alpha^3} = \alpha^{23}, \beta_3 = \frac{\alpha^{26}}{\alpha^9} = \alpha^{17} \tag{38}$$

We can see the properties;

$$(\beta_1)^3 = (\alpha^{25})^3 = \alpha^{23} = \beta_2$$
$$(\beta_2)^3 = (\alpha^{23})^3 = \alpha^{17} = \beta_3$$
$$(\beta_3)^3 = (\alpha^{17})^3 = \alpha^{25} = \beta_1$$

Is very easy looking that $\alpha^{25}, \alpha^{23}, \alpha^{17}$ are roots of the characteristic polynomial $g(x)$ corresponding the roots $\alpha, \alpha^3, \alpha^{3^2} = \alpha^9$ of $f(x)$ and the general term b_n is;

$$b_n = B_1(\alpha^{25})^n + B_2(\alpha^{23})^n + B_3(\alpha^{17})^n$$

For the initial vector ($b_0 = 2$, $b_1 = 1$, $b_2 = 1$);

$$\begin{cases} n = 0 \to B_1 + B_2 + B_3 = 2 \\ n = 1 \to \alpha^{25}B_1 + \alpha^{23}B_2 + \alpha^{17}B_3 = 1 \\ n = 2 \to \alpha^{24}B_1 + \alpha^{20}B_2 + \alpha^8 B_3 = 1 \end{cases}$$

Thus, $B_1 = \alpha^{21}, B_2 = \alpha^{11}, B_3 = \alpha^7$

We can see the properties;

$$(B_1)^3 = (\alpha^{21})^3 = \alpha^{11} = B_2$$
$$(B_2)^3 = (\alpha^{11})^3 = \alpha^7 = B_3$$
$$(B_3)^3 = (\alpha^7)^3 = \alpha^{21} = B_1$$

And the general term of the sequence $\{b_n\}$ is;

$$b_n = \alpha^{21}(\alpha^{25})^n + \alpha^{11}(\alpha^{23})^n + \alpha^7(\alpha^{17})^n \tag{39}$$

The sequence $\{b_n\}$ is periodic with the period 3^3-1=26 and it is the following sequence;

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

Figure 6 shows register generating $\{b_n\}$;

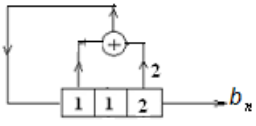

Figure 6. *shift register generating* $\{b_n\}$

We can look that one period of the sequence $\{b_n\}$ is one period of the sequence $\{a_n\}$ but through reading it by inverse from the right to the left.

Suppose the multiplication sequence $\{z_n\}$, where $z_n = a_n.b_n$, we have;

$$\begin{aligned} z_n = a_n.b_n = \left[\alpha^{22}(\alpha)^n + \alpha^{14}(\alpha^3)^n + \alpha^{16}(\alpha^9)^n\right] \\ \alpha^{21}(\alpha^{25})^n + \alpha^{11}(\alpha^{23})^n + \alpha^7(\alpha^{17})^n \\ z_n = \alpha^9(\alpha^2)^n + \alpha(\alpha^6)^n + \alpha^{11}(\alpha^8)^n + \\ \alpha^3(\alpha^{18})^n + \alpha^{21}(\alpha^{20})^n + \alpha^7(\alpha^{24})^n + 1 \end{aligned} \tag{40}$$

Thus, the sequence $\{z_n\}$ is a linear nonhomogeneous sequence with the length of its linear homogeneous equivalent is equals 6 that is equal to $(\deg f(x))^2 - \deg f(x) = 6$, The period of $\{z_n\}$ is 13, and the sequence $\{z_n\}$

Distributed under creative commons license 4.0 DOI: https://doi.org/10.30564/jeisr.v3i2.3740

is: 0 1 1 2 0 0 2 0 0 2 1 1 0 0 1 1 2 0 0 2 0 0 2 1 1 0 …….

Figure 7 illustrates the linear feedback shift registers generating the sequence $\{z_n\}$;

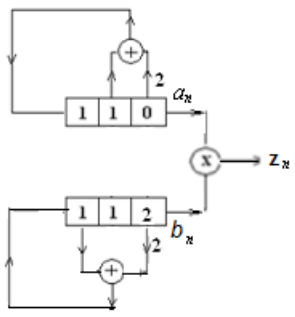

Figure 7. *Illustrated the multiplication sequence* $\{z_n\}$

We can check that the set of the all periodic permutation of one period is not an orthogonal set for example, for one permutation of the period: 0 1 1 2 0 0 2 0 0 2 1 1 0 is: 0 0 1 1 2 0 0 2 0 0 2 1 1and the sum of the two vectors is 0 1 2 0 2 0 2 2 0 2 0 2 1 and is don't belong to the set of all permutations of the first period.

The linear homogeneous part of z_n is $LHP(z_n)=\{z_n'\}$;

$$z_n' = \alpha^9(\alpha^2)^n + \alpha(\alpha^6)^n + \alpha^{11}(\alpha^8)^n + \alpha^3(\alpha^{18})^n + \alpha^{21}(\alpha^{20})^n + \alpha^7(\alpha^{24})^n \quad (41)$$

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

$$(x-\alpha^2)(x-\alpha^6)(x-\alpha^8)(x-\alpha^{18})(x-\alpha^{20})(x-\alpha^{24})=0$$

We can see that;

$$(-\alpha^2)(-\alpha^6)(-\alpha^8)(-\alpha^{18})(-\alpha^{20})(-\alpha^{24})=1$$

And the characteristic equation is of the form;

$$x^6+\beta_1x^5+\beta_2x^4+\beta_3x^3+\beta_4x^2+\beta_5x+1=0$$

Calculated the coefficients we have;

$$\beta_1=0,\beta_2=1,\beta_3=2,\beta_4=0,\beta_5=1$$

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

$$x^6+x^4+2x^3+x+1=0 \quad (42)$$

Or;

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

Thus, the recurring sequence $\{z_n'\}$is;

$$z_{n+6}'+z_{n+4}'+2z_{n+3}'+z_{n+1}'+z_n'=0 \quad (43)$$

Or;

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

Figure 8 shows its feedback linear shift register of the sequence $\{z_n'\}$.

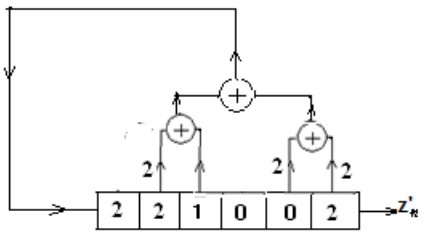

Figure 8. *Linear Equivalent of* $\{z_n'\}$ *with 6 complexity on* F_3

The sequence $\{z_n'\}$ is;

2 0 0 1 2 2 1 2 2 1 0 0 2 2 0 0 1 2 2 1 2 2 1 0 0 2 ….. (44)

As the sequence $\{z_n\}$ the set of all periodic permutations of one period of the sequence $\{z_n'\}$is not an orthogonal set.

Example 3

The recurring sequence $\{t_n\}$is giving by the shift register as in Figure 9;

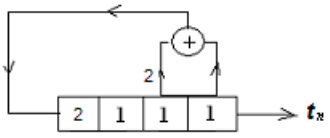

Figure 9. *Shift register generating sequence* $\{t_n\}$

The prime polynomial $f(x)=x^4+x+2$ is he characteristic polynomial of the sequence $\{t_n\}$in the field F_3, and it's characteristic equation is $x^4+x+2=0$, the recurring formula of the sequence is;

$$t_{n+4}+t_{n+1}+2t_n=0 \quad or \quad t_{n+4}=2t_{n+1}+t_n \quad (44)$$

If β is a root of the characteristic equation then the general term of the sequence $\{t_n\}$ is of the form;

$t_n=\mu_1(\beta)^n+\mu_2(\beta^3)^n+\mu_3(\beta^9)^n+\mu_4(\beta^{27})^n$ or $t_n=\mu_1\beta^n+\mu_2\beta^{3n}+\mu_3\beta^{9n}+\mu_4\beta^{27n}$

Solving the following system (see appendix);

$$\begin{cases} n=0\rightarrow \mu_1+\mu_2+\mu_3+\mu_4=1 \\ n=1\rightarrow \mu_1\beta+\mu_2\beta^3+\mu_3\beta^9+\mu_4\beta^{27}=1 \\ n=2\rightarrow \mu_1\beta^2+\mu_2\beta^6+\mu_3\beta^{18}+\mu_4\beta^{54}=1 \\ n=3\rightarrow \mu_1\beta^3+\mu_2\beta^9+\mu_3\beta^{27}+\mu_4\beta=2 \end{cases}$$

Thus, $\mu_1=\beta^{10},\mu_2=\beta^{30},\mu_3=\beta^{90},\mu_4=\beta^{270}$ or $\mu_1=\beta^{10},\mu_2=\beta^{30},\mu_3=\beta^{10},\mu_4=\beta^{30}$

We can see that;

$$(\mu_1)^3=(\beta^{10})^3=\mu_2\Rightarrow(\mu_3)^3=\mu_4$$
$$(\mu_2)^3=(\beta^{30})^3=\mu_3,\Rightarrow(\mu_4)^3=\mu_1$$

And t_n is;

$$t_n=\beta^{10}(\beta)^n+\beta^{30}(\beta^3)^n+\beta^{10}(\beta^9)^n+\beta^{30}(\beta^{27})^n \quad (45)$$

The sequence $\{t_n\}$ is periodic and its period is 3^4-1 =

Distributed under creative commons license 4.0
DOI: https://doi.org/10.30564/jeisr.v3i2.3740

80, and it is;

1112002201 0221101012 1221201222 2000200120 2221001102 0112202021

2112102111 1000100210, 1112002201 0221101012 … (46)

The unitary polynomial $g(x) = x^4 + 2x^3 + 2$ is the reciprocal polynomial of $f(x)$ and the roots of $g(x)$ are;

$(\beta_1)^3 = (\beta^{79})^3, = \beta_2, (\beta_2)^3 = (\beta^{77})^3 \beta_3, , (\beta_3)^3 = (\beta^{71})^3 = \beta_4, (\beta_4)^3 = (\beta^{53})^3 = \beta_1$

Figure 10 shows the shift register generating sequence $\{\tau_n\}$ for the initial vector (0,1,2,0);

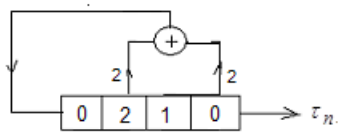

Figure 10. *Shift register generating sequence* $\{\tau_n\}$

The reciprocal sequence of $\{t_n\}$ is the sequence $\{\tau_n\}$ where;

$$\tau_n = \lambda_1(\beta^{79})^n + \lambda_2(\beta^{77})^n + \lambda_3(\beta^{71})^n + \lambda_4(\beta^{53})^n \quad (47)$$

For the initial vector ($\tau_0 = 0, \tau_1 = 1, \tau_2 = 2, \tau_3 = 0$);

$$\begin{cases} n = 0 \Rightarrow \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0 \\ n = 1 \Rightarrow \beta^{79}\lambda_1 + \beta^{77}\lambda_2 + \beta^{71}\lambda_3 + \beta^{53}\lambda_4 = 1 \\ n = 2 \Rightarrow \beta^{78}\lambda_1 + \beta^{74}\lambda_2 + \beta^{62}\lambda_3 + \beta^{26}\lambda_4 = 2 \\ n = 3 \Rightarrow \beta^{77}\lambda_1 + \beta^{71}\lambda_2 + \beta^{53}\lambda_3 + \beta^{79}\lambda_4 = 0 \end{cases}$$

We have $\lambda_1 = \beta^9, \lambda_2 = \beta^{27}, \lambda_3 = \beta, \lambda_4 = \beta^3$, and τ_n is;

$$\tau_n = \beta^9(\beta^{79})^n + \beta^{27}(\beta^{77})^n + \beta(\beta^{71})^n + \beta^3(\beta^{53})^n \quad (48)$$

We can see that;

$(\lambda_1)^3 = (\beta^9)^3 = \lambda_2; (\lambda_2)^3 = (\beta^{\mathbf{2}}) = \lambda_3$

$(\lambda_3)^3 = (\beta^3)^3 = \lambda_4; \Rightarrow (\lambda_4)^3 = \lambda_1$

The period of $\{\tau_n\}$ is $3^4 - 1 = 80$ and the sequence is;

0120010001 1112012112 1202022110 2011001222 0210020002 2221021221

2101011220 1022002111, 0120010001 1112012112 …. (49)

We can see that one period of the sequence $\{\tau_n\}$ is one period of the sequence $\{t_n\}$ but by reading it by inverse from the right to the left.

Suppose the multiplication sequence $\{z_n\}$ where $z_n = t_n . \tau_n$ we have;

$$z_n = t_n.\tau_n = \left[\beta^{10}\beta^n + \beta^{30}\beta^{3n} + \beta^{10}\beta^{9n} + \beta^{30}\beta^{27n}\right] \left[\beta^9(\beta^{79})^n + \beta^{27}(\beta^{77})^n + \beta(\beta^{71})^n + \beta^3(\beta^{53})\right]$$

$$\begin{aligned} z_n = {} & \beta^{39}\beta^{2n} + \beta^{37}\beta^{6n} + \beta^{19}\beta^{8n} + \beta\ \beta^n \\ & + \beta^{31}\beta^{18n} + \beta^{57}\beta^{24n} + \beta^{39}\beta^{26n} + \beta^{13}\beta^{54n} \\ & + \beta^{33}\beta^{56n} + \beta^{13}\beta^{62n} + \beta^{11}\beta^{72n} + \beta^{31}\beta^{74n} \\ & + \beta^{37}(\beta^{78})^n + \beta^{11} + \beta^{19} + \beta^{57} + \beta^{33} \end{aligned} \quad (50)$$

Or;

$$\begin{aligned} z_n = {} & \beta^{39}\beta^{2n} + \beta^{37}\beta^{6n} + \beta^{19}\beta^{8n} + \beta\beta^n \\ & + \beta^{31}\beta^{18n} + \beta^{57}\beta^{24n} + \beta^{39}\beta^{26n} + \beta^{13}\beta^{54n} \\ & + \beta^{33}\beta^{56n} + \beta^{13}\beta^{62n} + \beta^{11}\beta^{72n} + \beta^{31}\beta^{74n} \\ & + \beta^{37}\beta^{78n} \end{aligned} \quad (51)$$

Thus, the sequence $\{z_n\}$ is a linear homogeneous sequence with the length 12 and equal to $(\deg f(x))^2 -$ $\deg f(x) = 12$, periodic with the period 40 and this sequence is;

0120000001 0222002011 1102002220 1000000210, 0120000001 0222002011

1102002220 1000000210, ……. (52)

We can check that the set of the all periodic permutations of one period of $\{z_n\}$ is not orthogonal set.

Figure 11 illustrated the nonlinear feedback shift register generating $\{z_n\}$;

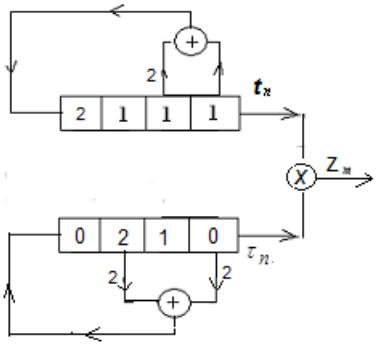

Figure 11. *Illustrated the multiplication sequence* $\{z_n\}$

We can see that $\beta^2.\beta^6.\beta^8.\beta.\beta^{18}.\beta^{24}.\beta^{26}.\beta^{54}.\beta^{56}.\beta^{62}.\beta^{72}.\beta^{74}.\beta^{78} = \beta^{480} = 1.$

Thus, $\{z_{n\}} = \{z_n^{'}\}$ where $\{z_n^{'}\}$ the linear part of $\{z_n\}$, the characteristic equation of $\{z_n\}$ is of the form;

$$x^{12} + \alpha_{11}x^{11} + \alpha_{10}x^{10} + \alpha_9x^9 + \alpha_8x^8 + \alpha_7x^7 + \alpha_6x^6 + \alpha_5x^5 + \alpha_4x^4 + \alpha_3x^3 + \alpha_2x^2 + \alpha_1x + 1 = 0$$

Or;

$$z_{n+12} + \alpha_{11}z_{n+11} + \alpha_{10}z_{n+10} + \alpha_9z_{n+9} + \alpha_8z_{n+8} + \alpha_7z_{n+7} + \alpha_6z_{n+6} + \alpha_5z_{n+5} + \alpha_4z_{n+4} + \alpha_3z_{n+3} + \alpha_2z_{n+2} + \alpha_1z_{n+1} + z_n = 0$$

Distributed under creative commons license 4.0
DOI: https://doi.org/10.30564/jeisr.v3i2.3740

Thus, for n = 0,1,2,3,…,10 and adding for n = 11 if it is need we can find the coefficients of the characteristic equation of $\{s_n\}$ as following;

$$\begin{cases} 2\alpha_{11}+\alpha_9+2\alpha_2+\alpha_1=1 \\ 2\alpha_{11}+\alpha_{10}+\alpha_8+2\alpha_1=0 \\ 2\alpha_{11}+2\alpha_{10}+2\alpha_9+\alpha_7=1 \\ 2\alpha_{10}+2\alpha_9+2\alpha_8+\alpha_6=0 \end{cases}$$

$$\begin{cases} 2\alpha_9+2\alpha_8+2\alpha_7+\alpha_5=1 \\ 2\alpha_{11}+2\alpha_8+2\alpha_7+2\alpha^6+\alpha_4=0 \\ 2\alpha_{10}+2\alpha_7+2\alpha_6+2\alpha_5+\alpha_3=2 \\ \alpha_{11}+2\alpha_9+2\alpha_6+2\alpha_5+2\alpha_4+\alpha_2=2 \end{cases}$$

$$\begin{cases} \alpha_{11}+\alpha_{10}+2\alpha_8+2\alpha_5+2\alpha_4+2\alpha_3+\alpha_1=2 \\ \alpha_{11}+\alpha_{10}+\alpha_9+2\alpha_7+2\alpha_4+2\alpha_3+2\alpha_2=1 \\ \alpha_{11}+\alpha_{10}+\alpha_9+\alpha_8+2\alpha_6+2\alpha_3+2\alpha_2+2\alpha_1=0 \end{cases}$$

Thus;

$\alpha_1=\alpha_3=0;\quad \alpha_2=\alpha_4=\alpha_5=\alpha_6=$
$\alpha_9=\alpha_{10}=\alpha_{11}=2;\quad \alpha_7=\alpha_8=1$

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

$$x^{12}+2x^{11}+2x^{10}+2x^9+x^8+x^7+ 2x^6+2x^5+2x^4+2x^2+1=0 \quad (53)$$

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

$$z_{n+12}+2z_{n+11}+2z_{n+10}+2z_{n+9}+z_{n+8}+z_{n+7} +2z_{n+6}+2z_{n+5}+2z_{n+4}+2z_{n+2}+z_n=0 \quad (54)$$

Or;

$$z_{n+12}=z_{n+11}+z_{n+10}+z_{n+9}+2z_{n+8}+2z_{n+7} +z_{n+6}+z_{n+5}+z_{n+4}+z_{n+2}+2z_n \quad (55)$$

Figure 12 shows the linear equivalent of the $\{z_n\}$;

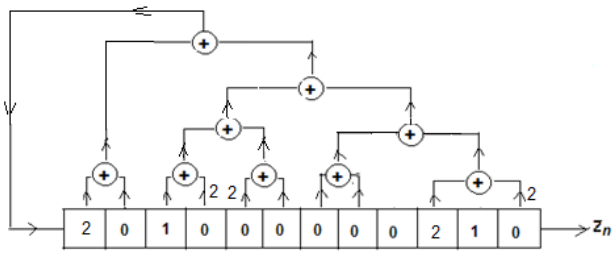

Figure 12. *Shift register generating sequence* $\{z_n\}$

Example 4

Given the recurring sequence $\{v_n\}$ over F_{5^2} with two degree where;

$$v_{n+2}+v_{n+1}+2v_n=0 \text{ or } v_{n+2}=4v_{n+1}+3v_n \quad (56)$$

Figure 13 shows the shift register generating it;

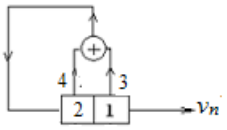

Figure 13. *Shift register generating the sequence* $\{v_n\}$

xAnd $\{v_n\}$ has the polynomial $f(x)=x^2+x+2$ as a prime characteristic polynomial, the roots $f(x)$ are; $\gamma, \gamma^5=4\gamma+4$ which are lie in the field F_{5^2} and;

$$\begin{aligned} &F_{5^2}=\{0,\gamma^{24}=1,\gamma,\gamma^2=4\gamma+3,\gamma^3=4\gamma+2,\gamma^4= \\ &3\gamma+2,\gamma^5=4\gamma+4,\gamma^6=2,\gamma^7=2\gamma,\gamma^8=5\gamma+1, \\ &\gamma^9=3\gamma+4,\gamma^{10}=\gamma+4,\gamma^{11}=3\gamma+3,\gamma^{12}= \\ &4,\gamma^{13}=4\gamma,\gamma^{14}=\gamma+2,\gamma^{15}=\gamma+3,\gamma^{16}=2\gamma+3, \\ &\gamma^{17}=\gamma+1,\gamma^{18}=3,\gamma^{19}=3\gamma,\gamma^{20}=2\gamma+4,\gamma^{21}= \\ &2\gamma+1,\gamma^{22}=4\gamma+1,\gamma^{23}=2\gamma+2\} \end{aligned} \quad (57)$$

And v_n is of the form;

$$v_n=A_1\gamma^n+A_2\gamma^{5n}$$

Or;

$$\begin{cases} n=0\Rightarrow A_1+A_2=1 \\ n=1\Rightarrow A_1\gamma+A_2\gamma^5=2 \end{cases}$$

Solving this system we have;

$$A_1=3, A_2=\gamma^{18}$$

But $(A_1)^5=(3)^5\neq A_2=\gamma^{18}$ and $(A_2)^5=(\gamma^{18})^5=\gamma^{18}\neq A_1$
Thus, v_n is equals;

$$v_n=3(\gamma)^n+\gamma^{18}(\gamma^5)^n \quad (58)$$

The sequence $\{v_n\}$ is period with the period 5^2-1 = 24, and the all cyclic permutations of one period is an orthogonal set;

1 2 1 0 3 2 2 4 2 0 1 4 4 3 4 0 2 3 3 1 3 0 4 1, 1 2 1 0 3 2 2 ……. (59)

The unitary reciprocal polynomial of $f(x)$ is the polynomial $g(x)=x^2+3x^3+3$ and the reciprocal sequence of $\{v_n\}$ is the sequence $\{w_n\}$ with the recurring formula;

$$w_{n+2}+3w_{n+1}+3w_n=0$$

Or;

$$w_{n+2}=2w_{n+1}+2w_n$$

The roots of $g(x)$ are;

$$\gamma_1=\frac{\gamma^{24}}{\gamma}=\gamma^{23}, \gamma_2=\frac{\gamma^{24}}{\gamma^5}=\gamma^{19}$$

Is very easy looking that γ^{23}, γ^{19} are roots of the

Distributed under creative commons license 4.0
DOI: https://doi.org/10.30564/jeisr.v3i2.3740

characteristic polynomial $g(x), (\gamma^{23})^5 = \gamma^{19}$, $(\gamma^{19})^5 = \gamma^{23}$ and v_n is of the form;

$$w_n = B_1(\gamma^{23})^n + B_2(\gamma^{19})^n \tag{60}$$

For the initial vector ($w_0 = 1$, $w_1 = 4$ are the latest two values of one period of the sequence $\{w_n\}$ but by inverse we read them from the right to the left) and by solving the following system for $n = 0$, $n = 1$;

$$\begin{cases} B_1 + B_2 = 1 \\ \gamma^{23}B_1 + \gamma^{19}B_2 = 4 \end{cases}$$

Solving this system of equations we have:

$B_1 = \gamma^{17}, B_2 = \gamma^{13}$ and;

$(B_1)^5 = (\gamma^{17})^5 = \gamma^{13} = B_2$ and $(B_2)^5 = (\gamma^{13})^5 = \gamma^{17} = B_1$

Thus;

$$w_n = \gamma^{17}(\gamma^{23})^n + \gamma^{13}(\gamma^{19})^n \tag{61}$$

The sequence $\{w_n\}$ is periodic with the period $5^2 - 1 = 24$ and it is;

1 4 0 3 1 3 3 2 0 4 3 4 4 1 0 2 4 2 2 3 0 1 2 1, 1 4 0 3 1 3 3 2 0 … (62)

Figure14 illustrated shift register generating $\{w_n\}$;

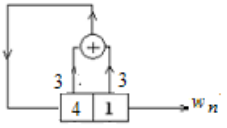

Figure 14. *Shift register generating sequence* $\{w_n\}$

One period of $\{v_n\}$ is an one period of the sequence $\{w_n\}$ but by inverse from the right to the left.

The multiplication sequence $\{z_n\}$ where $z_n = v_n.w_n$ is;

$$\begin{aligned} z_n &= v_n.w_n \\ &= \left[3(\gamma)^n + \gamma^{18}(\gamma^5)^n\right]\left[\gamma^{17}(\gamma^{23})^n + \gamma^{13}(\gamma^{19})^n\right] \\ z_n &= 3\gamma^{17} + 3\gamma^{13}\gamma^{20n} + \gamma^{11}\gamma^{4n} + \gamma^7 \\ z_n &= 3\gamma^{13}\gamma^{20n} + \gamma^{11}\gamma^{4n} + 3 \end{aligned} \tag{63}$$

Thus, the sequence $\{z_n\}$ is a linear nonhomogeneous sequence and periodic with the period 6 and it is;

1 3 0 0 3 1, 1 3 0 0 3 1 ……. (64)

The set of all cyclic permutations of one period is not orthogonal set.

Suppose the linear homogeneous part with the sequence is $\{z'_n\}$, which it's linear equivalent has the length $(\deg f(x))^2 - \deg f(x) = 2$, and the period of $\{z'_n\}$ is also 6 and $\{z'_n\}$ is;

3 0 0 0 0 3, 3 0 0 0 0 3, ….. (65)

And the set of the all cyclic permutations of one period of $\{z_n\}$ is not an orthogonal set.

Figure 15 Shows the nonlinear shift register generating sequence $\{z_n\}$;

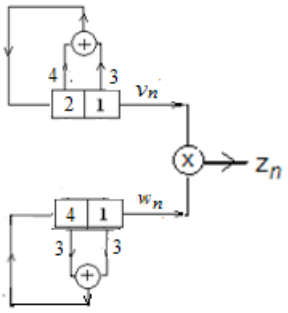

Figure 15. *Illustrated the multiplication sequence* $\{z_n\}$

According with the sequences $\{s_n\}$, its reciprocal sequence $\{\zeta_n\}$ and their multiplication sequence $\{z_n\}$ in the examples 1, 2, 3,4, we have;

In example 1:
$$\begin{cases} S_n = \alpha^6(\alpha)^n + \alpha^2(\alpha^3)^n \\ \zeta_n = \alpha^5(\alpha^7)^n + \alpha^7(\alpha^5)^n \end{cases} \tag{66}$$

In example 2:
$$\begin{cases} a_n = \alpha^{22}(\alpha)^n + \alpha^{14}(\alpha^3)^n + \alpha^{16}(\alpha^9)^n \\ b_n = \alpha^{21}(\alpha^{25})^n + \alpha^{11}(\alpha^{23})^n + \alpha^7(\alpha^{17})^n \end{cases} \tag{67}$$

In example 3:

$$\begin{cases} t_n = \beta^{10}\beta^n + \beta^{30}\beta^{3n} + \beta^{10}\beta^{9n} + \beta^{30}\beta^{27n} \\ \tau_n = \beta^9(\beta^{79})^n + \beta^{27}(\beta^{77})^n + \beta(\beta^{71})^n + \beta^3(\beta^{53})^n \end{cases} \tag{68}$$

In example 4.
$$\begin{cases} v_n = 3(\gamma)^n + \gamma^{18}(\gamma^5)^n \\ w_n = \gamma^{17}(\gamma^{23})^n + \gamma^{13}(\gamma^{19})^n \end{cases} \tag{69}$$

Suppose, the basic sequence is $\{S_n\}$ and it's of the form;

$$\begin{aligned} s_n &= A_1\alpha^n + A_2(\alpha^{p^{2-1}})^n + \ldots + A_k(\alpha^{p^{k-1}})^n \\ &= \sum_{i=1}^{k} A_i(\alpha^{p^{i-1}})^n \end{aligned} \tag{70}$$

And it's reciprocal sequence is $\{\zeta_n\}$ and it's of the form;

$$\begin{aligned} \zeta_n &= B_1\alpha^{n(p^k-2)} + B_2\alpha^{n(p^k-3)} + \ldots + B_k\alpha^{n(p^k-p^{k-1}-1)} \\ &= \sum_{i=1}^{k} B_i\alpha^{n(p^k-p^{i-1}-1)} \end{aligned} \tag{71}$$

And the product sequence is $\{z_n\}$ where $z_n = S_n\zeta_n$ and it's of the form;

$$z_n = \left(\sum_{i=1}^{k} A_i(\alpha^{p^{i-1}})^n\right)\left(\sum_{j=1}^{k} B_j(\alpha^{(p^k-p^{j-1}-1)})^n\right) \tag{72}$$

Or;

$$z_n = \left(\sum_{i,j=1,i\neq j}^{k} A_iB_j(\alpha^{p^{i-1}})^n(\alpha^{(p^k-p^{j-1}-1)})^n\right) + \left(\sum_{i=1}^{k} A_iB_i\right) \tag{73}$$

We can see the following conclusions.

Distributed under creative commons license 4.0
DOI: https://doi.org/10.30564/jeisr.v3i2.3740

4. Conclusions

*P*1. For one period of the sequence $\{S_n\}$ the corresponding period of its reciprocal sequence $\{\zeta_n\}$ is the same but by inverse from the right to the left.

*P*2. In the both form of the general term we have of each of them; $(A_i)^p = (A_{i+1})$ and $(B_i)^p = (B_{i+1})$ except example 4 that is, $(A_1)^p = (3)^5 = 3 \bmod 5 \neq \gamma^{18} = A_2$ also $(A_2)^5 = (\gamma^{18})^5 = \gamma^{18} \neq 3 = A_1$ but $(B_1)^5 = B_2$ & $(B_2)^5 = B_1$.

*P*3. In the both form of the general term we have of each of them; $(\alpha^{p^{i-1}})^p = (\alpha^{p^i})$ and $(\alpha^{(p^k - p^{j-1}-1)})^p = (\alpha^{(p^k - p^j - 1)})$.

*P*4. The exponent of the coefficient of the first term in the general term in the sequence $\{S_n\}$ is larger than the corresponding coefficient in the sequence $\{\zeta_n\}$ by one except example 4.

*P*5. The length of the linear homogeneous part of the sequence $\{z_n\}$ is equal to $((\deg f(x))^2 - \deg f(x))$ Where the $f(x)$ is the characteristic polynomial of the sequence $\{S_n\}$.

P6. The period of the sequence $\{S_n\}$ equals the period of the sequence $\{\zeta_n\}$ and equals (p^k-1) but the period of the sequence $\{z_n\}$ in the examples1 to 3 is equal to half of this value but in example 4 is equals the quarter of this value.

P_7. The set of all cyclic permutations of one period of the multiplication sequence $\{z_n\}$ is not orthogonal set.

P_8. There is important difference between the properties of multiplication M-Sequences and M_p-Sequences.

P_9 – We did not come across one term in the basic M_p-Sequene $\{S_n\}$ as the sum of Exp.(A_i) and Exp. ($\alpha^{p^{i-1}}$) in formula of S_n are complement that is; (Exp.(A_i) + Exp. ($\alpha^{p^{i-1}}$) = p^k -1 consequently the same for the ζ_n and furthermore it the permutations between the "coefficients and roots which are in formula of S_n" will not be in the formula of ζ_n as in the binary M-Sequences.

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[15] Lidl, R.& Pilz, G., (1984), "*Applied Abstract Algebra*," Springer – Verlage New York, 1984.

[16] Lidl, R. & Niderreiter, H., (1994), "Introduction to Finite Fields and Their Application, " *Cambridge university* USA.

[17] Thomson W. Judson, (2013), "*Abstract Algebra: Theory and Applications*," Free Software Foundation.

[18] Fraleigh, J.B., (1971), "A First course In Abstract Algebra, *Fourth printing. Addison-Wesley publishing company* USA.

Distributed under creative commons license 4.0
DOI: https://doi.org/10.30564/jeisr.v3i2.3740

Appendix

F_{3^4}		
0	$\beta^{26}=\beta^2+2\beta+1$	$\beta^{53}=\beta+1$
$\beta^{80}=1$	$\beta^{27}=\beta^3+2\beta^2+\beta$	$\beta^{54}=\beta^2+\beta$
β	$\beta^{28}=2\beta^3+\beta^2+2\beta+1$	$\beta^{55}=\beta^3+\beta^2$
β^2	$\beta^{29}=\beta^3+2\beta^2+2\beta+2$	$\beta^{56}=\beta^3+2\beta+1$
β^3	$\beta^{30}=2\beta^3+2\beta^2+\beta+1$	$\beta^{57}=2\beta^2+1$
$\beta^4=2\beta+1$	$\beta^{31}=2\beta^3+\beta^2+2\beta+2$	$\beta^{58}=2\beta^3+\beta$
$\beta^5=2\beta^2+\beta$	$\beta^{32}=\beta^3+2\beta^2+2$	$\beta^{59}=\beta^2+\beta+2$
$\beta^6=2\beta^3+\beta^2$	$\beta^{33}=2\beta^3+\beta\alpha+1$	$\beta^{60}=\beta^3+\beta^2+2\beta$
$\beta^7=\beta^3+\beta+2$	$\beta^{34}=\beta^2+2\beta+2$	$\beta^{61}=\beta^3+2\beta^2+2\beta+1$
$\beta^8=\beta^2+\beta+1$	$\beta^{35}=\beta^3+2\beta^2+2\beta$	$\beta^{62}=2\beta\alpha^3+2\beta^2+1$
$\beta^9=\beta^3+\beta^2+\beta$	$\beta^{36}=2\beta^3+2\beta^2+2\beta+1$	$\beta^{63}=2\beta^3+2\beta+2$
$\beta^{10}=\beta^3+\beta^2+2\beta+1$	$\beta^{37}=2\beta^3+2\beta^2+2\alpha+2$	$\beta^{64}=2\beta^2+2$
$\beta^{11}=\beta^3+2\beta^2+1$	$\beta^{38}=2\beta^3+2\beta^2+2$	$\beta^{65}=2\beta^3+2\beta$
$\beta^{12}=2\beta^3+1$	$\beta^{39}=2\beta^3+2$	$\beta^{66}=2\beta^2+\beta+2$
$\beta^{13}=2\beta+2$	$\beta^{40}=2$	$\beta^{67}=2\beta^3+\beta^2+2\beta$
$\beta^{14}=2\beta^2+2\beta$	$\beta^{41}=2\beta$	$\beta^{68}=\beta^3+2\beta^2+\beta+2$
$\beta^{15}=2\beta^3+2\beta^2$	$\beta^{42}=2\beta^2$	$\beta^{69}=2\beta^3+\beta^2+\beta+1$
$\beta^{16}=2\beta^3+\beta+2$	$\beta^{43}=2\beta^3$	$\beta^{70}=\beta^3+\beta^2+2\beta+2$
$\beta^{17}=\beta^2+2$	$\beta^{44}=\beta+2$	$\beta^{71}=\beta^3+2\beta^2+\beta+1$
$\beta^{18}=\beta^3+2\beta$	$\beta^{45}=\beta^2+2\beta$	$\beta^{72}=2\beta^3+\beta^2+1$
$\beta^{19}=2\beta^2+2\beta+1$	$\beta^{46}=\beta^3+2\beta^2$	$\beta^{73}=\beta^3+2\beta+2$
$\beta^{20}=2\beta^3+2\beta^2+\beta$	$\beta^{47}=2\beta^3+2\beta+1$	$\beta^{74}=2\beta^2+\beta+1$
$\beta^{21}=2\beta^3+\beta^2+\beta\alpha+2\beta$	$\beta^{48}=2\beta^3+2\beta+2$	$\beta^{75}=2\beta^3+\beta^2+\beta$
$\beta^{22}=\beta^3+\beta^2+2$	$\beta^{49}=2\beta^3+2\beta^2+2\beta$	$\beta^{76}=\beta^3+\beta^2+\beta+2$
$\beta^{23}=\beta^3+\beta+1$	$\beta^{50}=2\beta^3+2\beta^2+\beta+2$	$\beta^{77}=\beta^3+\beta^2+\beta+1$
$\beta^{24}=\beta^2+1$	$\beta^{51}=2\beta^3+\beta^2+2$	$\beta^{78}=\beta^3+\beta^2+1$
$\beta^{25}=\beta^3+\beta$	$\beta^{52}=\beta^3+2$	$\beta^{79}=\beta^3+1$

Distributed under creative commons license 4.0 DOI: https://doi.org/10.30564/jeisr.v3i2.3740