

ARTICLE

Study the Multiplication M-sequences and Its Reciprocal SequencesAhmad Al Cheikha^{1*} Ebtisam Haj Omar²

1. Math. Sci.Dep., Ahlia Uni., Bahrain

2. Elect. Energy Dep., Tishreen Univ, Syria

ARTICLE INFO

Article history

Received: 2 August 2021

Accepted: 15 August 2021

Published Online: 30 August 2021

Keywords:

Binary sequences

Finite fields

Shift register

Equivalent binary linear shift register

Degree of complexity

ABSTRACT

M-Sequences play a big important role, as the other binary orthogonal sequences, for collection the information on the input links and distribution these information on the output links of the communication channels and for building new systems with more complexity, larger period, and security, through multiplication these sequences. In our article we try to study the construction of the multiplication sequence $\{z_n\}$ and its linear equivalent, this multiplication sequence is as multiple two sequences, the first sequence $\{a_n\}$ is an arbitrary M-sequence and the second sequence $\{b_n\}$ is not completely different but is the reciprocal sequence of the first sequence $\{a_n\}$ that is the reciprocal sequence has characteristic polynomial $g(x)$ is reciprocal of $f(x)$, which is the characteristic polynomial of the first sequence $\{a_n\}$, also we will study the linear equivalent of the multiplication sequence $\{z_n\}$ and we will see that the length of the linear equivalent of $\{z_n\}$ is equal to $((deg f(x))^2 - deg(f(x)))$.

1. Introduction

Sloane, N.J.A., study the product or multiplication sequence $\{z_n\}$ on t degrees of $\{a_n\}$ which has the degree of complexity r and gave the answer that the degree of complexity

of $\{z_n\}$ can't be exceeded, $N_t = \binom{r}{1} + \binom{r}{2} + \dots + \binom{r}{t}$.

M-Sequences are used in the forward links for mixing the information on connection and as in the backward links of these channels to receivers get the information in a correct form, especially in the pilot channels and in the sync channels^[1-8].

Al Cheikha A. H., studied the construction of the multiplication binary M-Sequences and their complexities, periods, and the lengths of the linear equivalents of these multiplication sequences, where the multiplication will be on one M-Sequence or on more than one sequence and gave an Illustration of the answer of the question "why

the linear shift register don't be reached the maximum length N_t ", where the product or multiplication will be on h degrees of one M-Sequence, also, the length of the equivalent shift register of the multiplication sequence is equal to the product r by s , where, r and s are the length of the shift registers of the first and second sequences respectively and they are prime numbers^[9-14].

2. Research Method and Materials**2.1 M- Sequences**

The sequence $\{s_n\}$ of the form:

$$s_{n+k} = \gamma_{k-1}s_{n+k-1} + \gamma_{k-2}s_{n+k-2} + \dots + \gamma_0s_n +$$

$$\gamma; \gamma \& \gamma_i \in F_2, i = 0, 1, \dots, k-1$$

$$\text{or } s_{n+k} = \sum_{i=0}^{k-1} \gamma_i s_{n+i} + \gamma \quad (1)$$

*Corresponding Author:

Ahmad Al Cheikha,

Math. Sci.Dep., Ahlia Uni., Bahrain;

Email: alcheikhaa@yahoo.com

Where, $\gamma, \gamma_0, \gamma_1, \dots, \gamma_{k-1}$ are in the field F_2 and k is positive integer is called a binary linear recurring sequence of complexity or order k , if $\gamma = 0$ then the sequence is called homogeneous sequence (H.L.R.S), in other case the sequence is called non-homogeneous, the vector $(s_0, s_1, \dots, s_{k-1})$ is called the initial vector and the characteristic equation of the sequence is:

$$f(x) = x^k + \gamma_{k-1}x^{k-1} + \dots + \gamma_1x + \gamma_0 \tag{2}$$

We are limited in our article to $\gamma_0 = 1$.

2.2 Definitions and Theorems

Definition 1

The binary sequence $\{s_n\}$ satisfies the following condition;

$$s_{n+r} = s_n \quad ; \quad n = 0, 1, \dots$$

Is called a periodic sequence and the smallest natural number r which not equal to zero is called the period of the sequence [2,6].

Definition 2

The L.F.S.R is a linear feedback shift register which 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 3

The vector $\bar{X} = (\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n)$ is the complement of the vector $X = (s_1, s_2, \dots, s_n)$, $s_i \in F_2$ where

$$\bar{s}_i = 0 \text{ if } s_i = 1 \text{ and } \bar{s}_i = 1 \text{ if } s_i = 0 \tag{3} \text{ [2,6,7]}$$

Definition 4

The coefficient of correlations function of two binary vectors $t = (t_0, t_1, \dots, t_{n-1})$ and $l = (l_0, l_1, \dots, l_{n-1})$ is

$$R_{t,l} = \sum_{i=0}^{n-1} (-1)^{t_i+l_i} \tag{4}$$

Where $t_i + l_i$ is computed by *mod 2*.

If $x_i, y_i \in \{1, -1\}$ (usually, replacing in binary vectors t and l each "1" by "1* = -1" and each "0" by "0* = 1" then

$$R_{t,l} = \sum_{i=0}^{n-1} t_i^* l_i^* \tag{5} \text{ [2-9]}$$

Definition 5

If $|R_{t,l}| \leq 1$ of the two vectors t and l then we said the vectors t and l are orthogonal [8-10].

Definition 6

If A is a set of binary vectors as the following:

$$A = \{t; t = (t_0, t_1, \dots, t_{n-1}) \quad x_i \in F_2, i = 0, 1, \dots, n-1 \}$$

The set A is orthogonal if and only if satisfies the following two conditions:

$$1. \forall t \in A, \left| \sum_{i=0}^{n-1} t_i^* \right| \leq 1, \text{ or } |R_{t,0}| \leq 1. \tag{6}$$

$$2. \forall t, l \in A, \& t \neq l, \left| \sum_{i=0}^{n-1} t_i^* l_i^* \right| \leq 1 \text{ or } |R_{t,l}| \leq 1. \tag{7} \text{ [6,9]}$$

Definition 7

The maximum length of an equivalent binary linear feedback shift register is always less than or equal to the maximum length $r N_t$ [2,3,8].

Definition 8

The reciprocal function of the function $f(x)$ is the function:

$$g(x) = x^n f(1/x) \tag{8}$$

Where, n is the degree of $f(x)$ [7].

Theorem 9

If $\{s_n\}$ is a H.L.R.S binary sequence with the complexity k , period r and its characteristic polynomial is $f(x)$ then $r | \text{ord } f(x)$ and if the polynomial $f(x)$ is primitive then the period of the sequence $\{s_n\}$ is $2^k - 1$ and this sequence is called M-Sequence [6, 12-15].

Lemma 10 (Fermat's theorem)

Each element x of the finite field F satisfies the equation:

$$x^q = x \tag{9}$$

Where q is the number of all elements in F [6,10].

Theorem 11

If $\{s_n\}$ is a homogeneous binary linear recurring sequence and $g(x)$ is its characteristic prime polynomial of degree k and λ is a root of $g(x)$ in any splitting field of F_2 then the general term of the sequence $\{s_n\}$ is:

$$s_n = \sum_{i=1}^k C_i \left(\lambda^{2^{i-1}} \right)^n \tag{11} \text{ [6,12]}$$

Theorem 12

$$i. (q^m - 1) | (q^n - 1) \Leftrightarrow m | n \tag{12}$$

ii. any subfield of the field F_{2^n} is a field of order 2^m where $m|n$ and if F_q is a field of order $q=2^n$ then any subfield of it has the order 2^m and $m|n$, and by inverse if $m|n$ then the field F_{2^n} contains a subfield of order 2^m [6,11-15].

*Our study is limited to the M-Sequence of the period $r=2^k-1$.

3. Results and Discussion

3.1 Multiplication Two Reciprocal Binary M-Sequences

If $\{a_n\}$ is a recurring M-Sequence of degree k and $f(x)$ is its characteristic prime polynomial (of degree k), which has the independent different roots $\alpha_1, \alpha_2, \dots$, then general term of sequence $\{a_n\}$ will be given through the relation:

$$a_n = A_1\alpha_1^n + A_2\alpha_2^n + \dots + A_k\alpha_k^n = \sum_{i=1}^k A_i\alpha_i^n \quad (13)$$

If the sequence $\{a_n\}$ in F_2 , its characteristic prime polynomial is $f(x)$, and α is a root of $f(x)$ then the general term of the sequence $\{a_n\}$ is

$$a_n = A_1\alpha^n + A_2(\alpha^{2^{2-1}})^n + \dots + A_k(\alpha^{2^{k-1}})^n = \sum_{i=1}^k A_i(\alpha^{2^{i-1}})^n \quad (14)$$

Suppose the recurring M-Sequence $\{b_n\}$ which has the characteristic prime polynomial $g(x)$, and $g(x)$ is the reciprocal of $f(x)$ and $\beta_1, \beta_2, \dots, \beta_k$ are the different linear independent roots of $g(x)$, which are reciprocal of $\alpha_1, \alpha_2, \dots, \alpha_k$, then $\{b_n\}$ is

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

The sequence $\{b_n\}$ is called the reciprocal sequence of the sequence $\{a_n\}$.

Thus, if α_i is of the form $\alpha^{2^{i-1}}$ and β_i is reciprocal α_i then $\beta_i = \alpha^{2^k-2^{i-1}-1}$ and b_n will be written in the form

$$b_n = B_1\alpha^{n(2^k-2)} + B_2\alpha^{n(2^k-3)} + \dots + B_k\alpha^{n(2^k-2^{k-1}-1)} = \sum_{i=1}^k B_i\alpha^{n(2^k-2^{i-1}-1)} \quad (15)$$

Thus

$$a_n b_n = \left(\sum_{i=1}^k A_i(\alpha^{2^{i-1}})^n \right) \left(\sum_{j=1}^k B_j(\alpha^{n(2^k-2^{j-1}-1)})^n \right) = \left(\sum_{i,j=1, i \neq j}^k A_i B_j (\alpha^{2^{i-1}})^n (\alpha^{n(2^k-2^{j-1}-1)})^n \right) + \left(\sum_{i=1}^k A_i B_i \right) \quad (16)$$

Example 1

Suppose the binary recurring sequence $\{a_n\}$ where

$$a_{n+3} + a_{n+1} + a_n = 0, \text{ or } a_{n+3} = a_{n+1} + a_n \quad (17)$$

The characteristic equation of sequence is $x^3 + x + 1 = 0$ and its characteristic polynomial $f(x) = x^3 + x + 1$, if α is a root of the characteristic equation then α generates the field

$$F_{2^3} = \{0, \alpha^7 = 1, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1\} \quad (18)$$

and a_n is given by the formula

$$a_n = A_1\alpha^n + A_2(\alpha^2)^n + A_3(\alpha^4)^n$$

For the initial vector $(a_0 = 0, a_1 = 1, a_2 = 0)$ we have

$$\begin{cases} A_1 + A_2 + A_3 = 0 \\ \alpha A_1 + \alpha^2 A_2 + \alpha^4 A_3 = 1 \\ \alpha^2 A_1 + \alpha^4 A_2 + \alpha A_3 = 0 \end{cases}$$

Solution this gives us that $A_1 = \alpha^2, A_2 = \alpha^4, A_3 = \alpha$ and a_n is

$$a_n = \alpha^2(\alpha)^n + \alpha^4(\alpha^2)^n + \alpha(\alpha^4)^n \quad (19)$$

The periodic of $\{a_n\}$ is $2^3 - 1 = 7$ and we have the following sequence

0 1 0 1 1 0, 0 1 0 1

The following Figure1, shows the shift register generating $\{a_n\}$

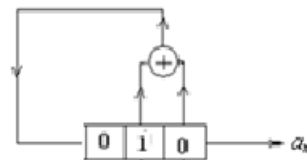


Figure 1. Shift register generating $\{a_n\}$

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

$$\beta_1 = \frac{\alpha^7}{\alpha} = \alpha^6, \beta_2 = \frac{\alpha^7}{\alpha^2} = \alpha^5, \beta_3 = \frac{\alpha^7}{\alpha^4} = \alpha^3 \quad (20)$$

Is very easy looking that $\alpha^6, \alpha^5, \alpha^3$ are roots of the characteristic polynomial $g(x)$ corresponding the roots $\alpha, \alpha^2, \alpha^4$ of $f(x)$ and b_n is

$$b_n = B_1(\alpha^6)^n + B_2(\alpha^5)^n + B_3(\alpha^3)^n$$

For the initial vector $(b_0 = 0, b_1 = 1, b_2 = 1)$

$$\begin{cases} B_1 + B_2 + B_3 = 0 \\ \alpha^6 B_1 + \alpha^5 B_2 + \alpha^3 B_3 = 1 \\ \alpha^5 B_1 + \alpha^3 B_2 + \alpha^6 B_3 = 1 \end{cases}$$

We have $B_1 = \alpha, B_2 = \alpha^2, B_3 = \alpha^4$ and the general term of the sequence $\{b_n\}$ is

$$b_n = \alpha(\alpha^6)^n + \alpha^2(\alpha^5)^n + \alpha^4(\alpha^3)^n \quad (21)$$

The sequence $\{b_n\}$ is periodic with the period $2^3 - 1 = 7$ and it is the following sequence
 0 1 1 1 0 1 0, 0 1 1 1 0

Figure 2 showing register generating $\{b_n\}$

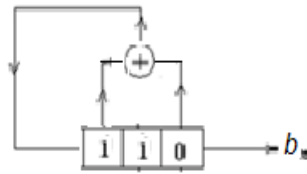


Figure 2. shift register generating $\{b_n\}$

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 $z_n = a_n \cdot b_n$, we have

$$z_n = a_n \cdot b_n = [\alpha^2(\alpha)^n + \alpha^4(\alpha^2)^n + \alpha(\alpha^4)^n] [\alpha(\alpha^6)^n + \alpha^2(\alpha^5)^n + \alpha^4(\alpha^3)^n] \quad (22)$$

$$z_n = a_n \cdot b_n = \alpha^5 \alpha^n + \alpha^3 \alpha^{2n} + \alpha^2 \alpha^{3n} + \alpha^6 \alpha^{4n} + \alpha \alpha^{5n} + \alpha^4 \alpha^{6n} + 1$$

Thus, the sequence $\{z_n\}$ is a linear nonhomogeneous sequence with the length of its linear equivalent is equals 6 that is equal to $(\deg f(x))^2 - \deg f(x) = 6$. The period of $\{z_n\}$ is 7, and the sequence $\{a_n\}$ is
 0101010, 0101010

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: 0101010 is: 0010101 and the sum of the two vectors is 0111111.

Suppose the linear homogeneous part of z_n is $LHP(z_n) = \{z'_n\}$;

$$LHP(z_n) = z'_n = \alpha^5 \alpha^n + \alpha^3 \alpha^{2n} + \alpha^2 \alpha^{3n} + \alpha^6 \alpha^{4n} + \alpha \alpha^{5n} + \alpha^4 \alpha^{6n} \quad (23)$$

The sequence $\{z'_n\}$ is

1 0 1 0 1 0 1, 1 0 1 0 1 0 1 ...

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

Figure 3, illustrates the linear feedback shift registers generating the sequence $\{z_n\}$.

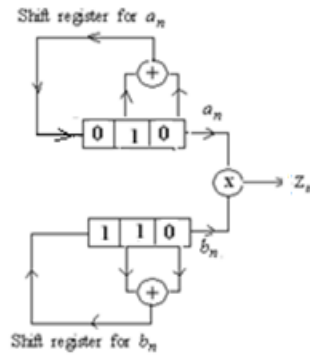


Figure 3. Illustrated the multiplication sequence $\{z_n\}$

We can look that $\alpha^n \cdot \alpha^{2n} \cdot \alpha^{3n} \cdot \alpha^{4n} \cdot \alpha^{5n} \cdot \alpha^{6n} = \alpha^{21n} = 1$, and the characteristic equation of the sequence $\{z'_n\}$ is of the form

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

Or

$$z'_{n+6} + \mu_5 z'_{n+5} + \mu_4 z'_{n+4} + \mu_3 z'_{n+3} + \mu_2 z'_{n+2} + \mu_1 z'_{n+1} + z'_n = 0$$

Thus, for $n = 0, 1, 2, 3, 4, 5$ we have the following system of equations

$$\begin{cases} 1 + \mu_4 + \mu_2 + 1 = 0 \\ 1 + \mu_5 + \mu_3 + \mu_1 = 0 \\ \mu_5 + \mu_4 + \mu_2 + 1 = 0 \\ 1 + \mu_4 + \mu_3 + \mu_1 = 0 \\ \mu_5 + \mu_3 + \mu_2 + 1 = 0 \end{cases}$$

Solving this system we have: $\mu_5 = \mu_4 = \mu_3 = \mu_2 = \mu_1 = 1$ and the characteristic equation of the sequence $\{z'_n\}$ is

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0 \quad (24)$$

Or

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

And the recurring formula of the sequence $\{z'_n\}$ is

$$z'_{n+6} + z'_{n+5} + z'_{n+4} + z'_{n+3} + z'_{n+2} + z'_{n+1} + z'_n = 0 \quad (25)$$

Figure4 showing the linear equivalent of the $\{z'_n\}$:

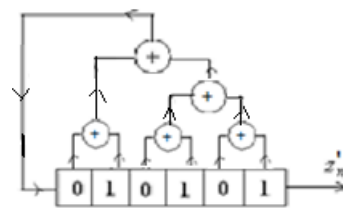


Figure 4. the linear feedback shift register generating the sequence $\{z'_n\}$

We can get $\{z_n\}$ from $\{z'_n\}$ by adding complement gate at the output of $\{z'_n\}$.

Example 2

Giving the sequence $\{a_n\}$ generating by shift register as in Figure 5.

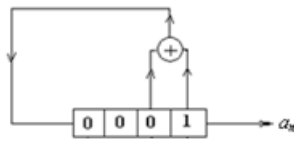


Figure 5. Linear feedback shift register generating sequence $\{a_n\}$

Where

$$a_{n+4} + a_{n+1} + a_n = 0 \text{ or } a_{n+4} = a_{n+1} + a_n \quad (26)$$

And $f(x) = x^4 + x + 1$ is its prime characteristic polynomial with the roots $\beta, \beta^2, \beta^4 = \beta + 1, \beta^8 = \beta^2 + 1$ which are in the field F_{2^4} where

$$\begin{aligned} F_{2^4} = \{0, \beta, \beta^2, \beta^3, \beta^4 = \beta + 1, \beta^5 = \beta^2 + \beta, \beta^6 = \beta^3 + \beta^2, \\ \beta^7 = \beta^3 + \beta + 1, \beta^8 = \beta^2 + 1, \beta^9 = \beta^3 + \beta, \\ \beta^{10} = \beta^2 + \beta + 1, \beta^{11} = \beta^3 + \beta^2 + \beta, \beta^{12} = \beta^3 + \beta^2 + \\ \beta + 1, \beta^{13} = \beta^3 + \beta^2 + 1, \beta^{14} = \beta^3 + 1, \beta^{15} = 1\} \end{aligned} \quad (27)$$

And a_n is of the form

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

Or

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

The period of the sequence $\{a_n\}$ is $2^4 - 1 = 15$ and

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

Or

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

Solution this system gives us

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

And

$$a_n = \beta^{14}(\beta^n) + \beta^{13}(\beta^2)^n + \beta^{11}(\beta^4)^n + \beta^7(\beta^8)^n \quad (28)$$

And $\{a_n\}$ is a M-Sequence with period $2^4 - 1 = 15$.

$$100010011010111 \ 100010011010111 \dots \dots \quad (29)$$

The cyclic permutations of one period form an orthog-

onal set.

The sequence $b_{n+4} + b_{n+3} + b_n = 0$ or $b_{n+4} = b_{n+3} + b_n$ is recurring and $g(x) = x^4 + x^3 + 1$ is its characteristic polynomial is prime and reciprocal $f(x)$, and

$$\beta_1 = \frac{\beta^{15}}{\beta} = \beta^{14}, \beta_2 = \frac{\beta^{15}}{\beta^2} = \beta^{13}, \beta_3 = \frac{\beta^{15}}{\beta^4} = \beta^{11}, \beta_4 = \frac{\beta^{15}}{\beta^8} = \beta^7$$

Are roots of $g(x)$ and b_n is

$$b_n = B_1(\beta^{14})^n + B_2(\beta^{13})^n + B_3(\beta^{11})^n + B_4(\beta^7)^n$$

For the initial vector $(b_n = 0, b_1 = 1, b_2 = 1, b_3 = 1)$

$$\begin{cases} n = 0 \Rightarrow B_1 + B_2 + B_3 + B_4 = 0 \\ n = 1 \Rightarrow \beta^{14}B_1 + \beta^{13}B_2 + \beta^{11}B_3 + \beta^7B_4 = 1 \\ n = 2 \Rightarrow \beta^{13}B_1 + \beta^{11}B_2 + \beta^7B_3 + \beta^{14}B_4 = 1 \\ n = 3 \Rightarrow \beta^{12}B_1 + \beta^9B_2 + \beta^3B_3 + \beta^6B_4 = 1 \end{cases}$$

We have $B_1 = B_2 = B_3 = B_4 = 1$, and b_n is

$$b_n = (\beta^{14})^n + (\beta^{13})^n + (\beta^{11})^n + (\beta^7)^n \quad (30)$$

The period of $\{b_n\}$ is $2^4 - 1 = 15$ and the sequence is 011110101100100, 011110101100100... (31)

For the initial vector (1 1 1 0) we have the sequence $\{b'_n\}$ where, we can get the general term of $\{b'_n\}$ from b_n through shifting n by 2 and b'_n is

$$b'_n = \beta^{13}(\beta^{14})^n + \beta^{11}(\beta^{13})^n + \beta^7(\beta^{11})^n + \beta^{14}(\beta^7)^n \quad (32)$$

And the sequence $\{b'_n\}$ is

$$111010110010001, 111010110010001, 111\dots(33)$$

Figure 6 showing the linear feedback shift register generating $\{b_n\}$

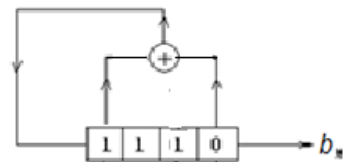


Figure 6. Shift register generating $\{b_n\}$

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

Suppose the multiplication sequence $\{z_n\}$ where $z_n = a_n \cdot b_n$ we have

$$z_n = a_n \cdot b_n = [\beta^{14} \cdot \beta^n + \beta^{13} \cdot \beta^{2n} + \beta^{11} \cdot \beta^{4n} + \beta^7 \cdot \beta^{8n}] \cdot [(\beta^{14})^n + (\beta^{13})^n + (\beta^{11})^n + (\beta^7)^n] \quad (34)$$

$$z_n = \beta^{14}\beta^{14n} + \beta^{13}\beta^{13n} + \beta^{14}\beta^{12n} + \beta^{12}\beta^{11n} + \beta^{13}\beta^{9n} + \beta^{14}\beta^{8n} + \beta^7\beta^{7n} + \beta^7\beta^{6n} + \beta^7\beta^{4n} + \beta^{12}\beta^{3n} + \beta^{12}\beta^{2n} + \beta^{13}\beta^n$$

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 15 and this sequence is

100010010010001, 100010010010001, 10001 ...

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

Figure 7 illustrated the nonlinear feedback shift register generating $\{z_n\}$.

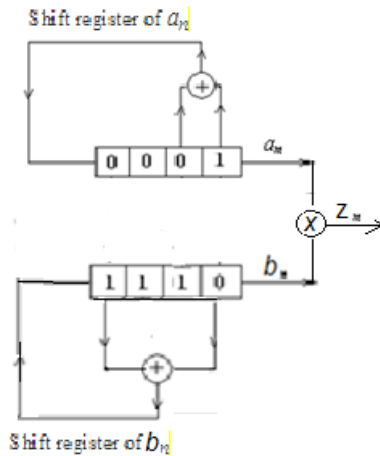


Figure 7. Illustrated the multiplication sequence $\{z_n\}$

We can look that $\beta^{14n} \cdot \beta^{13n} \cdot \beta^{12n} \cdot \beta^{11n} \cdot \beta^{9n} \cdot \beta^{8n} \cdot \beta^{7n} \cdot \beta^{6n} \cdot \beta^{4n} \cdot \beta^{3n} \cdot \beta^{2n} \cdot \beta^n = \beta^{90n} = 1$.

Thus, the characteristic equation of $\{z_n\}$ is of the form; $x^{12} + \mu_{11}x^{11} + \mu_{10}x^{10} + \mu_9x^9 + \mu_8x^8 + \mu_7x^7 + \mu_6x^6 + \mu_5x^5 + \mu_4x^4 + \mu_3x^3 + \mu_2x^2 + \mu_1x + 1 = 0$

Or

$$z_{n+16} + \mu_{11}z_{n+11} + \mu_{10}z_{n+10} + \mu_9z_{n+9} + \mu_8z_{n+8} + \mu_7z_{n+7} + \mu_6z_{n+6} + \mu_5z_{n+5} + \mu_4z_{n+4} + \mu_3z_{n+3} + \mu_2z_{n+2} + \mu_1z_{n+1} + z_n = 0$$

Thus, for $n = 0, 1, 2, 3, \dots, 10$ and adding for $n = 11$ because the equation for $n = 10$ is linearly pending with the equations for $n = 0$ to $n = 9$ we have the following system of 12 equations:

$$\begin{cases} \mu_{10} + \mu_7 + \mu_4 = 1 \\ \mu_9 + \mu_6 + \mu_3 = 0 \\ \mu_8 + \mu_5 + \mu_2 = 1 \\ \mu_{11} + \mu_7 + \mu_4 + \mu_1 = 1 \end{cases}$$

$$\begin{cases} \mu_{11} + \mu_{10} + \mu_6 + \mu_3 = 1 \\ \mu_{10} + \mu_9 + \mu_5 + \mu_2 = 0 \\ \mu_9 + \mu_8 + \mu_4 + \mu_1 = 0 \\ \mu_8 + \mu_7 + \mu_3 = 0 \end{cases}$$

$$\begin{cases} \mu_{11} + \mu_7 + \mu_6 + \mu_2 = 0 \\ \mu_{10} + \mu_6 + \mu_5 + \mu_1 = 0 \\ \mu_9 + \mu_5 + \mu_4 = 0 \\ \mu_{11} + \mu_8 + \mu_4 + \mu_3 = 0 \end{cases}$$

Solving this system we have: $\mu_{11} = \mu_9 = \mu_8 = \mu_2 = 0$; $\mu_{10} = \mu_7 = \mu_6 = \mu_5 = \mu_4 = \mu_3 = \mu_1 = 1$ and the characteristic

equation of the sequence $\{z_n\}$ is

$$x^{12} + x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1 = 0 \tag{35}$$

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

$$z_{n+12} + z_{n+10} + z_{n+7} + z_{n+6} + z_{n+5} + z_{n+4} + z_{n+3} + z_{n+1} + z_n = 0 \tag{36}$$

Figure 8 showing the linear equivalent of the $\{z_n\}$:

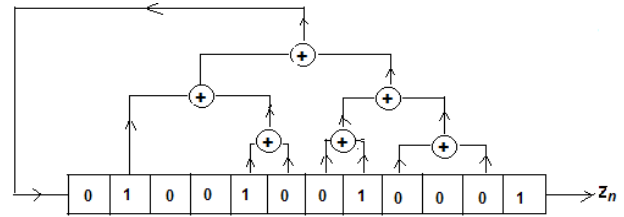


Figure 8. Shift register generating sequence $\{z_n\}$

Example 3

Given in Figure 9 the shift register generating the recurring sequence $\{a_n\}$ with five degrees:

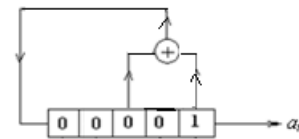


Figure 9. Shift register generating the sequence $\{a_n\}$

Where

$$a_{n+5} + a_{n+2} + a_n = 0 \text{ or } a_{n+5} = a_{n+2} + a_n \tag{37}$$

And $\{a_n\}$ has the polynomial $f(x) = x^5 + x^2 + 1$ as a prime characteristic polynomial, the roots $f(x)$ are; $\gamma, \gamma^2, \gamma^4, \gamma^8 = \gamma^3 + \gamma^2 + 1, \gamma^{16} = \gamma^4 + \gamma^3 + \gamma + 1$ which are lie in the field F_{2^5} and

$$\begin{aligned} F_{2^5} = \{ & 0, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5 = \gamma^2 + 1, \gamma^6 = \gamma^3 + \gamma, \gamma^7 = \gamma^4 + \gamma^2, \gamma^8 \\ & = \gamma^3 + \gamma^2 + 1, \gamma^9 = \gamma^4 + \gamma^3 + \gamma, \gamma^{10} = \gamma^4 + 1, \gamma^{11} = \gamma^2 + \gamma + 1, \gamma^{12} \\ & = \gamma^3 + \gamma^2 + \gamma, \gamma^{13} = \gamma^4 + \gamma^3 + \gamma^2, \gamma^{14} = \gamma^4 + \gamma^3 + \gamma^2 + 1, \gamma^{15} \\ & = \gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1, \gamma^{16} = \gamma^4 + \gamma^3 + \gamma + 1, \gamma^{17} = \gamma^4 + \gamma + 1, \gamma^{18} \\ & = \gamma + 1, \gamma^{19} = \gamma^2 + \gamma, \gamma^{20} = \gamma^3 + \gamma^2, \gamma^{21} = \gamma^4 + \gamma^3, \gamma^{22} = \gamma^4 + \\ & \gamma^2 + 1, \gamma^{23} = \gamma^3 + \gamma^2 + \gamma + 1, \gamma^{24} = \gamma^4 + \gamma^3 + \gamma^2 + \gamma, \gamma^{25} = \gamma^4 + \\ & \gamma^3 + 1, \gamma^{26} = \gamma^4 + \gamma^2 + \gamma + 1, \gamma^{27} = \gamma^3 + \gamma + 1, \gamma^{28} = \gamma^4 + \gamma^2 + \gamma, \\ & \gamma^{29} = \gamma^3 + 1, \gamma^{30} = \gamma^4 + \gamma, \gamma^{31} = 1 \} \end{aligned}$$

And a_n of the form

$$a_n = A_1\gamma^n + A_2\gamma^{2n} + A_3\gamma^{4n} + A_4\gamma^{8n} + A_5\gamma^{16n}$$

Or

$$a_n = A_1\beta^n + A_2(\gamma^2)^n + A_3(\gamma^4)^n + A_4(\gamma^3 + \gamma^2 + 1)^n + A_5(\gamma^4 + \gamma^3 + \gamma + 1)^n$$

And

$$\begin{aligned}
 n = 0 &\Rightarrow A_1 + A_2 + A_3 + A_4 + A_5 = 1 \\
 n = 1 &\Rightarrow A_1\gamma + A_2\gamma^2 + A_3\gamma^4 + A_4\gamma^8 + A_5\gamma^{16} = 0 \\
 n = 2 &\Rightarrow A_1\gamma^2 + A_2\gamma^4 + A_3\gamma^8 + A_4\gamma^{16} + A_5\gamma = 0 \\
 n = 3 &\Rightarrow A_1\gamma^3 + A_2\gamma^6 + A_3\gamma^{12} + A_4\gamma^{24} + A_5\gamma^{17} = 0 \\
 n = 4 &\Rightarrow A_1\gamma^4 + A_2\gamma^8 + A_3\gamma^{16} + A_4\gamma + A_5\gamma^2 = 0
 \end{aligned}$$

From the previously system of equation we have

$$A_1 = \gamma^{26}, A_2 = \gamma^{21}, A_3 = \gamma^{11}, A_4 = \gamma^{22}, A_5 = \gamma^{13}$$

Thus, a_n is equals

$$\begin{aligned}
 a_n &= \gamma^{26} \cdot (\gamma)^n + \gamma^{21} \cdot (\gamma^2)^n + \gamma^{11} \cdot (\gamma^4)^n + \gamma^{22} \cdot (\gamma^8)^n \\
 &+ \gamma^{13} (\gamma^{16})^n
 \end{aligned} \tag{39}$$

The period of $\{a_n\}$ is $2^5 - 1 = 31$, and the all cyclic permutations of one period is an orthogonal set.

$$\begin{aligned}
 &1000010010110011111000110111010 \\
 &1000010 \dots\dots
 \end{aligned} \tag{40}$$

Suppose the binary recurring sequence $b_{n+5} + b_{n+3} + b_n = 0$ or $b_{n+5} = b_{n+3} + b_n$ with the prime characteristic polynomial $g(x) = x^5 + x^3 + 1$ which is the reciprocal $f(x)$, thus the roots of $g(x)$ are

$$\begin{aligned}
 \gamma_1 &= \frac{\gamma^{31}}{\gamma} = \gamma^{30}, \gamma_2 = \frac{\gamma^{31}}{\gamma^2} = \gamma^{29}, \gamma_3 = \frac{\gamma^{31}}{\gamma^4} = \gamma^{27}, \\
 \gamma_4 &= \frac{\gamma^{31}}{\gamma^8} = \gamma^{23}, \gamma_5 = \frac{\gamma^{31}}{\gamma^{16}} = \gamma^{15}
 \end{aligned}$$

Is very easy looking that $\gamma^{30}, \gamma^{29}, \gamma^{27}, \gamma^{23}, \gamma^{15}$ are roots of the characteristic polynomial $g(x)$ and the b_n is of the form

$$b_n = B_1(\gamma^{30})^n + B_2(\gamma^{29})^n + B_3(\gamma^{27})^n + B_4(\gamma^{23})^n + B_5(\gamma^{15})^n$$

For the initial vector ($b_n = 0, b_1 = 1, b_2 = 0, b_3 = 1, b_4 = 1$, are the latest 5th values of one period of the sequence $\{a_n\}$ but by inverse we read them from the right to the left) and by solving the following system for $n = 0, n = 1, n = 2, 3$ and $n = 4$)

$$\begin{cases}
 B_1 + B_2 + B_3 + B_4 + B_5 = 0 \\
 \gamma^{30} B_1 + \gamma^{29} B_2 + \gamma^{27} B_3 + \gamma^{23} B_4 + \gamma^{15} B_5 = 1 \\
 \gamma^{29} B_1 + \gamma^{27} B_2 + \gamma^{23} B_3 + \gamma^{15} B_4 + \gamma^{30} B_5 = 0 \\
 \gamma^{28} B_1 + \gamma^{25} B_2 + \gamma^{19} B_3 + \gamma^7 B_4 + \gamma^{14} B_5 = 1 \\
 \gamma^{27} B_1 + \gamma^{23} B_2 + \gamma^{15} B_3 + \gamma^{30} B_4 + \gamma^{29} B_5 = 1
 \end{cases}$$

Solving this system of equations we have: $B_1 = \gamma^{25}, B_2 = \gamma^{19}, B_3 = \gamma^7, B_4 = \gamma^{14}, B_5 = \gamma^{28}$, and b_n is

$$\begin{aligned}
 b_n &= \gamma^{25} (\gamma^{30})^n + \gamma^{19} (\gamma^{29})^n + \gamma^7 (\gamma^{27})^n + \gamma^{14} (\gamma^{23})^n + \\
 &\gamma^{28} (\gamma^{15})^n
 \end{aligned} \tag{41}$$

The sequence $\{b_n\}$ is periodic with the period $2^5 - 1 = 31$ and it is the flowing sequence:

$$\begin{aligned}
 &0101110110001111100110100100001, \\
 &0101110 \dots
 \end{aligned} \tag{42}$$

Figure 10 illustrated shift register generating $\{b_n\}$.

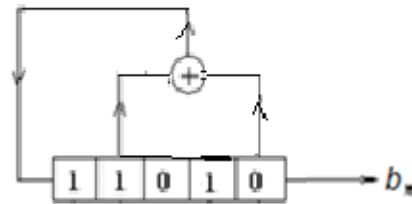


Figure 10. Shift register generating sequence $\{b_n\}$

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

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

$$\begin{aligned}
 z_n &= a_n \cdot b_n \\
 &= \left[\gamma^{26} \cdot (\gamma)^n + \gamma^{21} \cdot (\gamma^2)^n + \gamma^{11} \cdot (\gamma^4)^n + \gamma^{22} \cdot (\gamma^8)^n \right. \\
 &\quad \left. + \gamma^{13} (\gamma^{16})^n \right] \left[\gamma^{25} (\gamma^{30})^n + \gamma^{19} (\gamma^{29})^n + \gamma^7 (\gamma^{27})^n + \right. \\
 &\quad \left. \gamma^{14} (\gamma^{23})^n + \gamma^{28} (\gamma^{15})^n \right] \\
 z_n &= \gamma^{15} \gamma^n + \gamma^{30} \gamma^{2n} + \gamma^5 \gamma^{3n} + \gamma^{29} \gamma^{4n} + \gamma^{10} \gamma^{6n} + \\
 &\quad \gamma^{16} \gamma^{7n} + \gamma^{27} \gamma^{8n} + \gamma^{20} \gamma^{12n} + \gamma \gamma^{14n} + \gamma^7 \gamma^{15n} + \\
 &\quad \gamma^{23} \gamma^{16n} + \gamma^{18} \gamma^{17n} + \gamma^8 \gamma^{19n} + \gamma^{19} \gamma^{23n} + \gamma^9 \gamma^{24n} + \\
 &\quad \gamma^4 \gamma^{25n} + \gamma^{25} \gamma^{27n} + \gamma^2 \gamma^{28n} + \gamma^{28} \gamma^{29n} + \gamma^{14} \gamma^{30n} + \\
 &\quad (\gamma^{20} + \gamma^9 + \gamma^{18} + \gamma^5 + \gamma^{10}) \\
 z_n &= \gamma^{15} \gamma^n + \gamma^{30} \gamma^{2n} + \gamma^5 \gamma^{3n} + \gamma^{29} \gamma^{4n} + \gamma^{10} \gamma^{6n} + \\
 &\quad \gamma^{16} \gamma^{7n} + \gamma^{27} \gamma^{8n} + \gamma^{20} \gamma^{12n} + \gamma \gamma^{14n} + \gamma^7 \gamma^{15n} + \\
 &\quad \gamma^{23} \gamma^{16n} + \gamma^{18} \gamma^{17n} + \gamma^8 \gamma^{19n} + \gamma^{19} \gamma^{23n} + \gamma^9 \gamma^{24n} + \\
 &\quad \gamma^4 \gamma^{25n} + \gamma^{25} \gamma^{27n} + \gamma^2 \gamma^{28n} + \gamma^{28} \gamma^{29n} + \gamma^{14} \gamma^{30n} + 1
 \end{aligned} \tag{43}$$

Thus, the sequence $\{z_n\}$ is a linear nonhomogeneous sequence and it is:

$$\begin{aligned}
 &00000100100000111100000100100000, \\
 &0000010 \dots\dots
 \end{aligned} \tag{44}$$

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 $(\deg f(x))^2 - \deg f(x) = 20$, and the period of $\{z'_n\}$ is 31 and $\{z'_n\}$ is the complement of $e \{z_n\}$, thus, $\{z_n\}$ is

$$\begin{aligned}
 &1111101101111100011111101101111 \\
 &1, 1111101 \dots\dots
 \end{aligned} \tag{45}$$

And the set of the all cyclic permutations of one period of $\{z_n\}$ is not an orthogonal set. Figure 11 shows the non-linear shift register generating the sequence $\{z_n\}$.

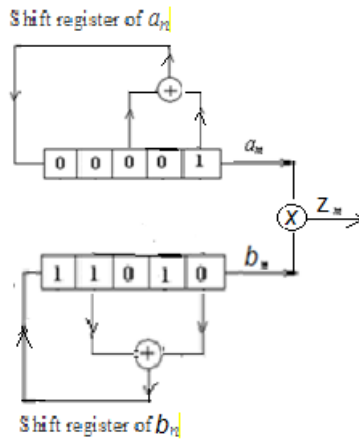


Figure 11. Illustrated the multiplication sequence $\{z_n\}$

According with the sequences $\{a_n\}$, its reciprocal sequence $\{b_n\}$ and their multiplication sequence $\{z_n\}$ in the examples 1, 2, 3 we have

In example 1:
$$\begin{cases} a_n = \alpha^2(\alpha)^n + \alpha^4(\alpha^2)^n + \alpha(\alpha^4)^n \\ b_n = \alpha(\alpha^6)^n + \alpha^2(\alpha^5)^n + \alpha^4(\alpha^3)^n \end{cases} \quad (46)$$

In example 2:

$$\begin{cases} a_n = \beta^{14} \cdot (\beta)^n + \beta^{13} \cdot (\beta^2)^n + \beta^{11} \cdot (\beta^4)^n + \beta^7 \cdot (\beta^8)^n \\ b_n = \beta^{13} (\beta^{14})^n + \beta^{11} (\beta^{13})^n + \beta^7 (\beta^{11})^n + \beta^{14} (\beta^7)^n \end{cases} \quad (47)$$

In example 3:

$$\begin{cases} a_n = \gamma^{26} \cdot (\gamma)^n + \gamma^{21} \cdot (\gamma^2)^n + \gamma^{11} \cdot (\gamma^4)^n + \gamma^{22} \cdot (\gamma^8)^n \\ \quad + \gamma^{13} (\gamma^{16})^n \\ b_n = \gamma^{25} (\gamma^{30})^n + \gamma^{19} (\gamma^{29})^n + \gamma^7 (\gamma^{27})^n + \gamma^{14} (\gamma^{23})^n \\ \quad + \gamma^{28} (\gamma^{15})^n \end{cases} \quad (48)$$

We can look the following properties

P1. For one period of the sequence $\{a_n\}$ the period of its reciprocal sequence $\{b_n\}$ is the same but must read or write it by inverse from the right to the left.

P2. In the both form of the general term of each of them and for two consecutive coefficients in each of them the square of the first coefficient equals the second coefficient, namely; $(A_i)^2 = A_{i+1}$, $(B_i)^2 = B_{i+1}$ and the square of the first term equals the second term .

P3. The exponent of the coefficient of the first term in the general term in the sequence $\{a_n\}$ is larger than the corresponding coefficient in the sequence $\{b_n\}$ by one.

P4. 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 $\{a_n\}$.

we will check these four properties by studying the case when the degree of the prime characteristic function of the sequence $\{a_n\}$ is six where

$$a_{n+6} + a_{n+1} + a_n = 0 \dots \text{or } a_{n+6} = a_{n+1} + a_n \quad (49)$$

Where

$$f(x) = x^6 + x + 1 \quad (50)$$

The characteristic equation is

$$x^6 + x + 1 = 0 \quad (51)$$

If α is a root of the characteristic equation then α generates the field $F2^6$, where Appendix 1 showing the elements of this field.

The term a_n is

$$a_n = A_1\alpha^n + A_2\alpha^{2n} + A_3\alpha^{4n} + A_4\alpha^{8n} + A_5\alpha^{16n} + A_6\alpha^{32n}$$

And

$$\begin{aligned} n=0 &\Rightarrow A_1 + A_2 + A_3 + A_4 + A_5 + A_6 = 1 \\ n=1 &\Rightarrow A_1\alpha + A_2\alpha^2 + A_3\alpha^4 + A_4\alpha^8 + A_5\alpha^{16} + A_6\alpha^{32} = 0 \\ n=2 &\Rightarrow A_1\alpha^2 + A_2\alpha^4 + A_3\alpha^8 + A_4\alpha^{16} + A_5\alpha^{32} + A_6\alpha = 0 \\ n=3 &\Rightarrow A_1\alpha^3 + A_2\alpha^6 + A_3\alpha^{12} + A_4\alpha^{24} + A_5\alpha^{48} + A_6\alpha^{33} = 0 \\ n=4 &\Rightarrow A_1\alpha^4 + A_2\alpha^8 + A_3\alpha^{16} + A_4\alpha^{32} + A_5\alpha + A_6\alpha^2 = 0 \\ n=5 &\Rightarrow A_1\alpha^5 + A_2\alpha^{10} + A_3\alpha^{20} + A_4\alpha^{40} + A_5\alpha^{17} + A_6\alpha^{34} = 0 \end{aligned}$$

Or, using Gaussian methods

$$\begin{aligned} A_1 + A_2 + A_3 + A_4 + A_5 + A_6 &= 1 \\ A_2 + A_3\alpha^{26} + A_4\alpha^{20} + A_5\alpha^{17} + A_6\alpha^{28} &= \alpha^{57} \\ A_3 + A_4\alpha^{46} + A_5\alpha^{31} + A_6\alpha^{36} &= \alpha^{19} \\ A_4 + A_5\alpha^{26} + A_6\alpha^7 &= \alpha^{12} \\ A_5 + A_6 &= \alpha \\ A_6\alpha^{17} &= \alpha^{48} \end{aligned}$$

Thus

$$A_6 = \alpha^{31}$$

According with the property P_2 we can guess A_1, \dots, A_5 , as the following

$$\begin{aligned} A_5 &= (A_6)^{1/2} = (\alpha^{31})^{1/2} = (\alpha^{31+63})^{1/2} = \alpha^{47} \\ A_4 &= (A_5)^{1/2} = (\alpha^{47})^{1/2} = (\alpha^{47+63})^{1/2} = \alpha^{55} \\ A_3 &= (A_4)^{1/2} = (\alpha^{55})^{1/2} = (\alpha^{55+63})^{1/2} = \alpha^{59} \\ A_2 &= (A_3)^{1/2} = (\alpha^{59})^{1/2} = (\alpha^{59+63})^{1/2} = \alpha^{61} \\ A_1 &= (A_2)^{1/2} = (\alpha^{61})^{1/2} = (\alpha^{61+63})^{1/2} = \alpha^{62} \end{aligned}$$

We can check these results through solving the above system of equations and we have the same results.

Thus, the term a_n is

$$a_n = \alpha^{62} \alpha^n + \alpha^{61} \alpha^{2n} + \alpha^{59} \alpha^{4n} + \alpha^{55} \alpha^{8n} + \alpha^{47} \alpha^{16n} + \alpha^{31} \alpha^{32n} \quad (52)$$

The sequence $\{a_n\}$ is M-Sequence, periodic with the period $2^6 - 1 = 63$, and the all cyclic permutations of one period is an orthogonal set and the sequence is

$$1000001000. 0110001010. 0111101000. 1110010010. 1101110110. 0110101011.111, 1000 \dots \quad (53)$$

The reciprocal polynomial of $f(x)$ is $g(x) = x^6 + x^5 + 1$ and for the initial vector $(b_0b_1b_2b_3b_4b_5) = (111110)$ we have the following reciprocal sequence $\{b_n\}$

$$111.1101010110.0110111011.0100100111.0001011110.0101000110. 0001000001, 111110 \dots \quad (54)$$

By checking the general terms of the sequence $\{s_n\}$ where $s_n = B_1\alpha^{62n} + B_2\alpha^{61n} + B_3\alpha^{59n} + B_4\alpha^{55n} + B_5\alpha^{47n} + B_6\alpha^{31n}$

Where α^{62} is reciprocal α , α^{61} is reciprocal α^2 , ..., α^{31} is reciprocal α^{32} .

According with property P_3 and P_2 we can guess B_1, \dots, B_6 , as the following

$$\begin{aligned} B_1 &= \alpha^{62-1} = \alpha^{61} \\ B_2 &= (B_1)^2 = (\alpha^{61})^2 = \alpha^{122} = \alpha^{59} \\ B_3 &= (B_2)^2 = (\alpha^{59})^2 = \alpha^{118} = \alpha^{55} \\ B_4 &= (B_3)^2 = (\alpha^{55})^2 = \alpha^{110} = \alpha^{37} \\ B_5 &= (B_4)^2 = (\alpha^{37})^2 = \alpha^{74} = \alpha^{11} \\ B_6 &= (B_5)^2 = (\alpha^{11})^2 = \alpha^{22} = \alpha^{22} \end{aligned}$$

And thus; the suggested general term of the sequence $\{s_n\}$ is

$$s_n = \alpha^{61}\alpha^{62n} + \alpha^{59}\alpha^{61n} + \alpha^{55}\alpha^{59n} + \alpha^{37}\alpha^{55n} + \alpha^{11}\alpha^{47n} + \alpha^{22}\alpha^{31n}$$

We can check that the sequence $\{s_n\}$ is the same reciprocal sequence $\{b_n\}$ and thus

$$b_n = \alpha^{61}\alpha^{62n} + \alpha^{59}\alpha^{61n} + \alpha^{55}\alpha^{59n} + \alpha^{37}\alpha^{55n} + \alpha^{11}\alpha^{47n} + \alpha^{22}\alpha^{31n} \quad (55)$$

Thus

$$\begin{cases} a_n = \alpha^{62}\alpha^n + \alpha^{61}\alpha^{2n} + \alpha^{59}\alpha^{4n} + \alpha^{55}\alpha^{8n} + \alpha^{47}\alpha^{16n} + \alpha^{31}\alpha^{32n} \\ b_n = \alpha^{61}\alpha^{62n} + \alpha^{59}\alpha^{61n} + \alpha^{55}\alpha^{59n} + \alpha^{37}\alpha^{55n} + \alpha^{11}\alpha^{47n} + \alpha^{22}\alpha^{31n} \end{cases}$$

Also we can check that

$$\begin{aligned} a_n.b_n &= \left(\sum_{i=1}^6 A_i(\alpha^{2^{i-1}})^n \right) \left(\sum_{j=1}^6 B_j(\alpha^{2^k - 2^{j-1} - 1})^n \right) \\ &= \left(\sum_{i,j=1, i \neq j}^6 A_i B_j (\alpha^{2^{i-1}} \alpha^{2^k - 2^{j-1} - 1})^n \right) + \sum_{i=1}^6 A_i B_i \end{aligned}$$

The first bracket contains 30 terms and

$$\begin{aligned} \sum_{i=1}^6 A_i B_i &= \alpha^{62}\alpha^{61} + \alpha^{61}\alpha^{59} + \alpha^{59}\alpha^{55} + \alpha^{55}\alpha^{37} \\ &\quad + \alpha^{47}\alpha^{11} + \alpha^{31}\alpha^{22} \\ &= \alpha^{123} + \alpha^{120} + \alpha^{114} + \alpha^{92} + \alpha^{58} + \alpha^{53} \\ &= \alpha^{60} + \alpha^{57} + \alpha^{51} + \alpha^{39} + \alpha^{58} + \alpha^{53} = 1 \end{aligned}$$

Thus,

$$a_n.b_n = \left(\sum_{i,j=1, i \neq j}^6 A_i B_j (\alpha^{2^{i-1}} \alpha^{2^k - 2^{j-1} - 1})^n \right) + 1$$

And the length of the linear equivalent of the linear homogeneous part of $a_n.b_n$ is equal to 30 that is equal to $((\deg f(x))^2 - \deg f(x))$.

4. Conclusions

For one period of the sequence $\{a_n\}$ the period of its reciprocal sequence $\{b_n\}$ is the same but we must read or write it by inverse from the right to the left.

In the both forms of the general term of the sequences $\{a_n\}$ and $\{b_n\}$ and for two consecutive coefficients in each of them the square of the first coefficient equals the second coefficient, namely; $(A_i)^2 = A_{i+1}$, $(B_i)^2 = B_{i+1}$ and the square of the first term is equals the second term.

The exponent of the coefficient of the first term in the general term in the sequence $\{a_n\}$ is larger than the corresponding coefficient in the first term of the sequence $\{b_n\}$ by one.

If each coefficient and its corresponding root (of the characteristic equation) in the general term of a sequence are reciprocal then these coefficients will be roots in the reciprocal sequence.

The length of the linear homogeneous part of the multiplication sequence $\{z_n\}$ is equals to $(\deg f(x))^2 - \deg f(x)$, where $f(x)$ is the prime characteristic polynomial of the sequence $\{a_n\}$.

The set of all cyclic permutations of one period of the reciprocal sequence $\{b_n\}$ is an orthogonal set but this set of the multiplication sequence $\{z_n\}$ is not an orthogonal set.

Each of the sequences $\{b_n\}$ and $\{z_n\}$ is a periodic sequence and has the same period of the sequence $\{a_n\}$.

References

[1] Sloane, N.J.A., (1976), "An Analysis Of The Structure And Complexity of Nonlinear Binary Sequence Generators," *IEEE Trans. Information Theory* Vol. It 22 No 6, PP 732-736.
 [2] Jong-Seon No, Solomon W. & Golomb, (1998), "Binary Pseudorandom Sequences For period $2^n - 1$ with Ideal Autocorrelation," *IEEE Trans. Information*

Theory, Vol. 44 No 2, PP 814-817.

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

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

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

[6] Yang K, Kg Kim y Kumar I. d, (2000), "Quasi-orthogonal Sequences for code-Division Multiple Access Systems," IEEE Trans .information theory, Vol. 46, No3, PP 982-993.

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

[8] Kasami, T. & Tokora, H., (1978), "Teoria Kodirovania," Mir(Moscow).

[9] 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.

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

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

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

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

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

[15] David, J., (2008), "Introductory Modern Algebra," Clark University USA.

Appendix

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