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

Ahmad Al Cheikha\textsuperscript{1*} Ebtisam Haj Omar\textsuperscript{2}
1. Department of Math Science, Ahlia University, Bahrain
2. Department of Electronic Energy, Tishreen University, Syria

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 \cite{[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?m \cite{[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, M\textsubscript{p}-Sequences \cite{[9-11]}.

2. Research Method and Materials

2.1 Mp-Sequences or M-Sequences over Fp

Mp\textsubscript{-}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, these 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.
\[ a_{n+k} = \gamma_{k-1}a_{n+k-1} + \gamma_{k-2}a_{n+k-2} + \ldots + \gamma_0a_n \cdot \]
\[ + \gamma \; \gamma \; \gamma \; \gamma \; \gamma \in F_p = \{0,1,2,\ldots, p-1\} \], \( i = 0,1,\ldots, k-1 \)
\[ \text{Or; } \]
\[ a_{n+k} = \sum_{i=0}^{k-1} \gamma_i a_{n+i} + \gamma \]
\[ \text{where, } \gamma, \gamma_0, \gamma_1, \ldots, \gamma_{k-1} \text{ are in the field } F_p \text{ and } k \text{ is positive integer, it is called a linear recurring sequence of complexity or order } k, \text{ for } \gamma = 0 \text{ the sequence is called homogeneous sequence (H.L.R.S), in other case the sequence is called non-homogeneous, the vector } \langle a_0, a_1, \ldots, a_{k-1} \rangle \text{ is called the initial vector and the characteristic equation of the sequence is; } \]
\[ f(x) = x^k + \gamma_{k-1}x^{k-1} + \ldots + \gamma_1x + \gamma_0 \]
\[ \text{(2)} \]

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 \( \bar{x} = (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n) \) is the complement of the vector \( \bar{x} = (a_1, a_2, \ldots, a_n) \in F_p \) where \( \bar{a}_i -= p-1 \) if \( a_i \neq 0 \) and \( \bar{a}_i = 0 \) if \( a_i = 0 \)

#### Definition 3

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

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

Where \( \frac{n+1}{p} \) is the nearest integer of the number \( \frac{n+1}{p} \), and we said the two vectors \( t \) and \( l \) are orthogonal if \( \sum_{i=0}^{n} l_i = 0, \sum_{i=0}^{n} t_i = 0 \mod p \), and \( R_{t,l} \leq 1 \).

#### Definition 4

The periodic sequence \( \{a_t\}_{t \in N} \) over \( F_p \), with the period \( r = p^k - 1 \) has the “Ideal Auto Correlation” property if and only its periodic auto Correlations \( R_a(t) \) of the form:

\[ a(t) = 0 \; \text{and } R_a(t) \leq 1 \]
\[ \text{(5)} \]

When;

\[ a(t) = \sum_{i=0}^{r-1} a_i(t + \tau) \mod p, \tau = 0,1,\ldots, r; R_a(t) = \]
\[ \frac{1}{r} \left[ \sum_{i=0}^{r-1} (-1)^{t_{i+\tau} + a(t)} \right] - \left( \frac{p^k - 1}{2} \right) \text{ for } \tau \neq 0 \]
\[ \text{(6)} \]

#### Definition 5

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

1. \( \forall t \in A; |R_{t,0}| \leq 1 \).
2. \( \forall t, l \in A, \; t \neq l; |R_{t,l}| \leq 1 \).

#### Definition 6

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

\[ g(x) = x^n f(1/x) \]
\[ \text{(9)} \]

#### 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 \( r \mod f(x) \) 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 \( F_p \).

#### Lemma 8. (Fermat’s theorem).

If the finite field \( F \) of order \( q \) then each element \( x \) of \( F \) satisfies the equation;

\[ x^q = x \]
\[ \text{(10)} \]

#### 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 \( x \) is a root of \( g(x) \) in any splitting field of \( F_p \) then the general term of the sequence \( \{a_n\} \) is;

\[ a_n = \sum_{i=1}^{k} C_i \left( a^{p^{-1}} \right)^n \]
\[ \text{(11)} \]

And the sequence \( \{a_n\} \) has the period \( p^k - 1 \).

#### Theorem 10

\[ \text{if } (q^m - 1) | (q^n - 1) \Leftrightarrow m | n \]
\[ \text{(12)} \]

It any subfield of the field \( F_{p^m} \) 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
the field $F_{p^m}$ contains a subfield of order $p^m$.  

*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 $a_1, a_2, \ldots, a_k$ are its independent different roots in the $F_p$, which is a splitting field of $F_p$, then the general term of the sequence $\{s_n\}$ is

$$s_n = A_1a_1^n + A_2a_2^n + \ldots + A_ka_k^n = \sum_{i=1}^{k} A_i a_i^n$$  

(13)

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

$$a_1 = a, a_2 = a^p, \ldots, a_k = a^{p^{k-1}}$$

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

$$s_n = A_1a^n + A_2(a^p)^n + \ldots + A_k(a^{p^{k-1}})^n = \sum_{i=1}^{k} A_i(a^{p^{i-1}})^n$$  

(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 $a_i$ is of the form $a^p$, and $\beta_i$ is reciprocal $a_i$ then $\beta_i = \alpha^{k-p} - p^{-1}$ and $\zeta_n$ can be written in the form;

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

(15)

Thus;

$$s_n \zeta_n = \left(\sum_{i=1}^{k} A_i(a^{p^{i-1}})^n\right) \left(\sum_{j=1}^{k} B_j(\alpha^{p^{j-1}})^n\right)$$

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

(16)

Example 1

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

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

\[ x^2 + x + 2 = 0 \]

If $\alpha$ 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 \}

\[ \alpha^2 \alpha = \alpha + 2, S_2 = 2\alpha + 1 \]

And the general solution of the characteristic equation is;

$$S_n = \alpha^6(\alpha^n) + \alpha^2(\alpha^3)^n$$

Or;

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

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

$$0 \ 1 \ 2 \ 2 \ 0 \ 1 \ 1 \ 0 \ 1 \ 2 \ 2 \ 1 \ 0 \ 2 \ 1 \ 1 \ \ldots$$

(20)

We can see the important properties;

$$\alpha^2(\alpha^3)^3 = (\alpha^7(\alpha^3))^3 = \alpha^2 \& (\alpha^3)^3 = \alpha^3$$

By the same way;

$$\alpha^2(\alpha^3)^3 = (\alpha^8(\alpha))^3 = \alpha^6 \& (\alpha^3)^3 = \alpha$$

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;

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

(23)

Is very easy looking that $\alpha^7, \alpha^5$, are roots of the characteristic polynomial $g(x)$ corresponding the roots...
\( \alpha, \alpha^3 \) of \( f(x) \) and the general term \( \zeta_n \) is:
\[
\zeta_n = B_1(\alpha^7)^n + B_2(\alpha^5)^n
\]

For the initial vector \( (\zeta_0 = 1, \zeta_1 = 1) \):
\[
\begin{align*}
  n = 0 & \rightarrow B_1 + B_2 = 1 \\
  n = 1 & \rightarrow \alpha^7 B_1 + \alpha^5 B_2 = 1
\end{align*}
\]
We have \( B_1 = \alpha^5, B_2 = \alpha^7 \) and the general term of the sequence \( \{\zeta_n\} \) is:
\[
\zeta_n = \alpha^5 (\alpha^7)^n + \alpha^7 (\alpha^5)^n 
\]
(24)

We can see the important properties;
\[
(\alpha^5 (\alpha^7))^3 = (\alpha^7 (\alpha^5))^3 = \alpha^7 & (\alpha^7)^3 = \alpha^5 
\]
(25)

By the same way;
\[
(\alpha^7 (\alpha^5))^3 = (\alpha^5 (\alpha^7))^3 = \alpha^5 & (\alpha^7)^3 = \alpha^7 
\]
(26)

The sequence \( \{\zeta_n\} \) is periodic with the period \( 2^3 - 1 = 8 \) and it is the flowing sequence;
\[
1120221011202210 \ldots 
\]
(27)

Figure 2 shows the shift register generating \( \{\zeta_n\} \)

![Figure 2. Shift register generating \( \{\zeta_n\} \)](image)

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;
\[
\begin{align*}
  z_n = s_n \zeta_n &= [\alpha^{6}(\alpha^6)^n + \alpha^2(\alpha^7)^n] \cdot \alpha^5 (\alpha^7)^n + \alpha^7 (\alpha^5)^n \\
  &= \alpha^{13}(\alpha^6)^n + \alpha^7 (\alpha^7)^n + \alpha^7 + \alpha^{11} \\
  &= \alpha^{13}\alpha^6 + \alpha^7 \alpha^{10} + \alpha^7 + \alpha^{11} 
\end{align*}
\]
(28)

Or,
\[
z_n = \alpha^5 \alpha^6 + \alpha^7 \alpha^{2n} + 2 
\]
(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 \( \deg f(x) = 2 \). 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 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 \( \{z_n\} \)](image)

xSuppose the linear homogeneous part of \( z_n \) is \( LHP(z_n) \);
\[
LHP(z_n) = z'_n = \alpha^5 \alpha^{6n} + \alpha^7 \alpha^{2n} 
\]
(30)

The sequence \( \{z'_n\} \) is;
\[
1 2 2 1 1 2 2 1 1 2 2 1 \ldots 
\]
(31)

The characteristic equation of the sequence \( \{z'_n\} \) is;
\[
(x - \alpha^2)(x - \alpha^6) = 0 
\]
\[
x^2 + 1 = 0 
\]
(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 \( \{z'_n\} \)](image)

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

![Figure 5. Shift register generating the sequence \( \{a_n\} \) on \( F_3 \)](image)
Thus, the sequence \( \{z_n\} \) is a linear nonhomogeneous sequence with the length of its linear 

Suppose the multiplication sequence \( \{z_n\} \), where \( z_n = 1 \).

And;

\[
F_j = 0, a_0, a_2, a_3, a_3 = a + 2a + a_3 = 2a^2 + a + 2a_0 = a + 1 + a_0,
\]

\[
a_1 = a + 2a + a_2 = 2a^2 + a + 2a = a + 2a_0 + a + 1 + a_0 = a + 2a_0 + a + 1,
\]

\[
a_2 = 2a + 1 + a_0 = 2a^2 + 2a + a_0 = a + 2 + a_0 = a + 1 + a_0 + 1,
\]

\[
a_3 = a^2 + 2a + a_2 = 2a^2 + a + 2a = a + 2a_0 + a + 1 + a_0 + 1 = a + 2a_0 + a + 1 + 1.
\]

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

\[
a_n = A_1a^n + A_2(2a_1 + A_2 + a_1) = 2a + a + a + a + 1.
\]

We can look that one period of the sequence \( \{a_n\} \) 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   …….

The reciprocal polynomial of \( g(x) \) and it's corresponding the roots \( \alpha, \alpha^2, \alpha^3 = \alpha^9 \) of \( \alpha \) and the general term \( b_n \) is;

\[
b_n = B_1(\alpha^{25})^n + B_2(\alpha^{23})^n + B_3(\alpha^7)^n
\]

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

\[
\begin{align*}
& n = 0 \rightarrow B_1 + B_2 + B_3 = 2 \\
& n = 1 \rightarrow \alpha^{25}B_1 + \alpha^{23}B_2 + \alpha^7B_3 = 1 \\
& n = 2 \rightarrow \alpha^{24}B_1 + \alpha^{20}B_2 + \alpha^8B_3 = 1
\end{align*}
\]

Thus, \( B_1 = \alpha^{25}, B_2 = \alpha^7, B_3 = \alpha^7 \)

We can see the properties;

\[
\begin{align*}
& (B_1)^3 = (\alpha^{25})^3 = \alpha^{25} = \beta_2 \\
& (B_2)^3 = (\alpha^{23})^3 = \alpha^{23} = \beta_3 \\
& (B_3)^3 = (\alpha^7)^3 = \alpha^7 = \beta_1
\end{align*}
\]

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

\[
b_n = \alpha^{21}(\alpha^{25})^n + \alpha^{11}(\alpha^{23})^n + \alpha^7(\alpha^7)^n
\]

The sequence \( \{b_n\} \) is periodic with the period 31-1=26 and it is the following sequence;

\[
2112101002201221202001110 211210100...
\]

Figure 6 shows register generating \( \{b_n\} \);

\[
\begin{align*}
\text{Figure 6. shift register generating } \{b_n\}
\end{align*}
\]

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;

\[
z_n = a_n b_n = \left[ \alpha^{22}(\alpha^n + \alpha^{14}(\alpha^3)^n + \alpha^{16}(\alpha^9)^n \right]
\]

\[
\alpha^{21}(\alpha^{25})^n + \alpha^{11}(\alpha^{23})^n + \alpha^7(\alpha^7)^n
\]

\[
z_n = \alpha^9(\alpha^2)^n + \alpha(\alpha^6)^n + \alpha^{11}(\alpha^8)^n + \alpha^{18}(\alpha^2)^n + \alpha^{21}(\alpha^5)^n + \alpha^7(\alpha^4)^n + 1
\]

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 \( \{z_n\} \)
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](image)

Figure 8. Linear Equivalent of \( \{ z'_n \} \) with 6 complexity on \( F_3 \)

The sequence \( \{ z'_n \} \) is:

\[
2001221221002 2001221221002 \ldots
\] (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](image)

Figure 10 shows the shift register generating sequence \( \{ t_n \} \)

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

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

If \( \beta \) is a root of the characteristic equation then the general term of the sequence \( \{ t_n \} \) is of the form;

\[t_n = \mu_1 \beta^n + \mu_2 \beta^{n+1} + \mu_3 \beta^{n+2} + \mu_4 \beta^{n+3}, \quad n = 0, 1, 2, 3, 4, \ldots\]

Solving the following system (see appendix);

\[
\begin{align*}
(\mu_1)^3 &= (\beta^{10})^3 = \mu_2 \\
(\mu_2)^3 &= (\beta^{30})^3 = \mu_3 \\
(\mu_3)^3 &= (\beta^{30})^3 = \mu_4 \\
\end{align*}
\] (45)

The sequence \( \{ t_n \} \) is periodic and its period is \( 3^4 - 1 = 80 \).
The unitary polynomial \( g(x) = x^4 + 2x^3 + 2 \) is the reciprocal polynomial of \( f(x) \) and the roots of \( g(x) \) are:

\[
(\beta_1)^3 = (\beta_2)^3 = (\beta_7)^3 = \beta_3, \quad (\beta_3)^3 = (\beta_5)^3 = \beta_1
\]

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

\[
\tau_n = \lambda_1(\beta_7)^n + \lambda_2(\beta_7)^n + \lambda_3(\beta_7)^n + \lambda_4(\beta_5)^n
\]

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

\[
\begin{align*}
&n = 0 \Rightarrow \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 0 \\
&n = 1 \Rightarrow (\beta_7)^n \lambda_1 + (\beta_7^3)^n \lambda_2 + (\beta_7^4)^n \lambda_3 + (\beta_7^5)^n \lambda_4 = 1 \\
&n = 2 \Rightarrow (\beta_7^2)^n \lambda_1 + (\beta_7^6)^n \lambda_2 + (\beta_7^8)^n \lambda_3 + (\beta_7^9)^n \lambda_4 = 2 \\
&n = 3 \Rightarrow (\beta_7^3)^n \lambda_1 + (\beta_7^5)^n \lambda_2 + (\beta_7^3)^n \lambda_3 + (\beta_7^6)^n \lambda_4 = 0
\end{align*}
\]

We have \( \lambda_1 = \beta^0, \lambda_2 = \beta^{27}, \lambda_3 = \beta, \lambda_4 = \beta^3 \), and \( \tau_n \) is:

\[
\tau_n = \beta^9(\beta_7)^n + \beta^{27}(\beta_7)^n + (\beta_7^3)^n + (\beta_5^3)^n
\]

We can see that:

\[
(\lambda_1)^3 = (\beta^9)^3 = \lambda_2; \quad (\lambda_2)^3 = (\beta^2)^3 = \lambda_3
\]

\[
(\lambda_3)^3 = (\beta^5)^3 = \lambda_4; \quad (\lambda_4)^3 = \lambda_1
\]

The period of \( \{\tau_n\} \) is \( 3^4 - 1 = 80 \) and the sequence is:

\[
0120000001 \quad 0222002011 \quad 1102002220 \quad 1000000210 \quad 0120000001 \quad 0222002011 \quad 1102002220 \quad 1000000210 \quad \ldots
\]

We can check that the set of all periodic permutations of one period of \( \{\tau_n\} \) is not orthogonal set.

Figure 11 illustrated the nonlinear feedback shift register generating \( \{z_n\}\):

\[
z_n = t_n \tau_n = \left[ \beta^{16} \beta^n + \beta^{16} \beta^n + \beta^{16} \beta^n + \beta^{37} \right] + \\
\left[ \beta^{4} \beta^n \beta^n + \beta^{37} \beta^n + \beta^{4} \beta^n + \beta^n \right]
\]

\[
z_n = \beta^{49} \beta^{37} \beta^n + \beta^{49} \beta^{37} \beta^n + \beta^{49} \beta^{37} \beta^n + \beta^{37} \beta^n
\]

Thus, the sequence \( \{z_n\} \) is a linear homogeneous sequence with the length 12 and equal to \( \{\deg f(x)\} \), periodic with the period 40 and this sequence is:

\[
0120000001 \quad 0222002011 \quad 1102002220 \quad 1000000210 \quad 0120000001 \quad 0222002011 \quad 1102002220 \quad 1000000210 \quad \ldots
\]

We can see that:

\[
\beta^2 \beta^6 \beta^8 \beta^18, \beta^{24}, \beta^{26}, \beta^{54}, \beta^{56}, \beta^{62}, \beta^{72}, \beta^{74}, \beta^{78} = \beta^{80} = 1
\]

Thus, \( \{z_n\} = \{z_n'\} \) where \( \{z_n'\} \) the linear part of \( \{z_n\} \), the characteristic equation of \( \{z_n\} \) is of the form:

\[
x^{12} + 2 \alpha_1 x^{11} + \alpha_2 x^{10} + \alpha_3 x^9 + \alpha_4 x^8 + \alpha_5 x^7 + \alpha_6 x^6 + \alpha_7 x^5 + \alpha_8 x^4 + \alpha_9 x^3 + \alpha_2 x^2 + \alpha_1 x + 1 = 0
\]

Or:

\[
z_{n+2} + \alpha_1 z_{n+1} + \alpha_2 z_{n} + \alpha_3 z_{n+1} + \alpha_4 z_{n+2} + \alpha_5 z_{n+3} + \alpha_6 z_{n+4} + \alpha_7 z_{n+5} + \alpha_8 z_{n+6} + \alpha_9 z_{n+7} + 1 = 0
\]
Thus, for \( n = 0,1,2,3,\ldots,10 \) and adding for \( n = 11 \) if it is need we can find the coefficients of the characteristic equation of \( \{ s_n \} \) as following;

\[
\begin{align*}
2a_{11} + a_0 + 2a_2 + a_1 &= 0 \\
2a_{11} + a_{10} + a_4 + 2a_2 &= 0 \\
2a_{11} + 2a_{10} + 2a_2 + a_1 &= 0 \\
2a_{11} + 2a_{10} + 2a_8 + a_6 &= 0 \\
2a_{11} + 2a_8 + 2a_2 &= 0 \\
2a_{11} + 2a_{10} + 2a_4 + a_2 &= 0 \\
2a_{11} + a_{10} + a_4 + 2a_2 &= 0 \\
2a_{11} + a_{10} + a_4 + 2a_2 &= 0 \\
2a_{11} + a_{10} + a_4 + 2a_2 &= 0 \\
2a_{11} + a_{10} + a_4 + 2a_2 &= 0 \\
\end{align*}
\]

Thus;

\[
\begin{align*}
\alpha_1 &= a_1 = 0; \\
\alpha_2 &= a_4 = a_3 = a_5 = 0; \\
\alpha_3 &= a_{10} = a_2 = 0; \\
\alpha_4 &= a_6 = 1;
\end{align*}
\]

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

\[
x^3 + 2x^2 + 2x + 1 = 0
\]

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

\[
z_{n+2} + 2z_{n+1} + 2z_{n+3} + z_{n+5} + z_{n+7} = 0
\]

Or;

\[
z_{n+2} + z_{n+3} + z_{n} = 0
\]

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 \( F_{2^3} \) with two degree where;

\[
v_{n+2} + v_{n+1} + 2v_n = 0 \quad v_{n+2} = 4v_{n+1} + 3v_n
\]

Figure 13 shows the shift register generating it;

---

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

\( x \)And \( \{ v_n \} \) has the polynomial \( f(x) = x^2 + x + 2 \) as a prime characteristic polynomial, the roots \( f(x) \) are;

\[
y, y^2 = 4y + 4 \quad \text{which are in the field } F_{2^3}\text{ and;}
\]

\[
F_{2^3} = \{0, y, y^2 = 4y + 3, y^3 = 4y + 2, y^4 = 3y + 2, y^5 = 4y + 4, y^6 = 2, y^7 = 2y, y^8 = 5y + 1, y^9 = 3y + 4, y^{10} = y^4 + 4, y^{11} = 3y + 3, y^{12} = 4, y^{13} = 4y, y^{14} = y^2 + y, y^{15} = y + 3, y^{16} = 2y + 3, y^{17} = y + 1, y^{18} = 3, y^{19} = 3y, y^{20} = 2y + 4, y^{21} = 2y + 1, y^{22} = 4y + 1, y^{23} = 2y + 2 \}
\]

And \( v_n \) is of the form;

\[
v_n = A_1y^n + A_2y^{5n}
\]

Or;

\[
\begin{align*}
n = 0 &\Rightarrow A_1 + A_2 = 1 \\
n = 1 &\Rightarrow A_1y + A_2y^5 = 2
\end{align*}
\]

Solving this system we have;

\[
A_1 = 3, A_2 = y^{18}
\]

But \( (A_1)^5 = (3)^5 \neq A_1 = y^{18} \) and \( (A_1)^{21} = (y^{18})^{21} = y^{18} \neq A_1 \)

Thus, \( v_n \) is equals;

\[
v_n = 3(y)^n + y^{18}(y^5)^n
\]

The sequence \( \{ v_n \} \) is period with the period \( 5^2 = 25 \), and all cyclic permutations of one period is an orthogonal set;

\[
1 2 1 0 3 2 4 2 0 1 4 4 3 4 0 2 3 3 1 3 0 4 1, 1 2 1 0 3 2 2 4 0 1 4 4 3 4 0 2 3 3 1 3 0 4 1
\]

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;

\[
y_1 = \frac{24}{y}, y_2 = \frac{24}{y} = y^{19}
\]

Is very easy looking that \( y^{23}, y^{19} \) are roots of the
characteristic polynomial $g(x), (y^{23})^3 = y^{19}$, $(y^{19})^4 = y^{23}$ and $v_n$ is of the form;

$$w_n = B_1(y^{23})^n + B_2(y^{19})^n$$

(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 $n = 0, n = 1$;

$$\begin{align*}
B_1 + B_2 &= 1 \\
y^{23}B_1 + y^{19}B_2 &= 4
\end{align*}$$

Solving this system of equations we have:

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

$$(B_1)^3 = (y^{17})^3 = y^{51} = B_2 \text{ and } (B_2)^3 = (y^{13})^3 = y^{39} = B_1$$

Thus;

$$w_n = y^{17}(y^{23})^n + y^{13}(y^{19})^n$$

(61)

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

$$1 4 0 3 1 3 \ 2 0 4 3 4 4 1 0 2 4 2 2 3 0 1 2 1, 1 4 0 3 1 3 3 \ 2 0$$

(62)

Figure 14 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 $\{z_n\}$ is of the form;

$$z_n = v_nw_n$$

$$z_n = 3(y^{17} + 3y^{13}y^{20} + y^{15}y^{4} + y^7)$$

(63)

$$z_n = 3y^{13}y^{20} + y^{17}y^4 + 3$$

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

$$1 3 0 0 3 1, 1 3 0 0 3 1, \ldots$$

(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;

$$3 0 0 0 0 3, 3 0 0 0 0 3, \ldots$$

(65)

And the set of 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;

$$\begin{align*}
s_n &= a^6(\alpha^n) + a^2(\alpha^3)^n \\
\zeta_n &= a^5(\alpha^n) + a^7(\alpha^5)^n
\end{align*}$$

(66)

In example 2:

$$\begin{align*}
s_n &= a^n(\alpha^2) + a(\alpha^4)^n + a^n(\alpha^6)^n \\
b_n &= a^{21}(\alpha^{25})^n + a^{11}(\alpha^{13})^n + a^{17}(\alpha^7)^n
\end{align*}$$

(67)

In example 3:

$$\begin{align*}
t_n &= \beta^{10} + \beta^{6} \beta^3 + \beta^{10} \beta^{10} + \beta^{30} \beta^{27} \\
\tau_n &= \beta^2(\beta^2)^n + \beta^7(\beta^7)^n + \beta(\beta^1)^n + \beta^3(\beta^3)^n
\end{align*}$$

(68)

In example 4;

$$\begin{align*}
v_n &= 3(y^{17} + y^{13}(y^7)^n) \\
w_n &= y^{17}(y^{19})^n
\end{align*}$$

(69)

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

$$s_n = A_1(\alpha^n) + A_2(\alpha^{n-2})^n + \ldots + A_k(\alpha^{n-k})^n$$

$$= \sum_{i=1}^{k} A_i(\alpha^{n-i})^n$$

(70)

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

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

(71)

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

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

(72)

Or;

$$z_n = \left( \sum_{i=1}^{k} A_i B_j(\alpha^{n-i})(\alpha(\alpha^{p^k-1}-1))^n \right) + \left( \sum_{i=1}^{k} A_i B_1 \right)$$

(73)

We can see the following conclusions.
4. Conclusions

P1. For one period of the sequence \(\{S_i\}\) the corresponding period of its reciprocal sequence \(\{\zeta_n\}\) is the same but by inverse from the right to the left.

P2. In the both form of the general term we have of each of them; \((A_j)^p = (A_{j+1})\) and \((B_i)^p = (B_{i+1})\) except example 4 that is, \((A_j)^p = 3\) = 3 \(\mod 5\) \(\neq\) \(A_j\) also \((A_j)^p = 3\) = 3 \(\mod 5\) \(A_j\) but \((B_i)^5 = B_2\) \& \((B_2)^5 = B_1\).

P3. In the both form of the general term we have of each of them; \((\alpha^p)^{r-1})^p = (\alpha^{p^r})\) and \((\alpha^p)^{r-1} - 1)\)\( = (\alpha^p)^{r-1} - 1)\).

P4. The exponent of the coefficient of the first term in the general term in the sequence \(\{S_i\}\) is larger than the corresponding coefficient in the sequence \(\{\zeta_n\}\) by one except example 4.

P5. The length of the linear homogeneous part of the sequence \(\{z_i\}\) is equal to ((deg \(f(x)) = \deg f(x)\)) Where \(f(x)\) is the characteristic polynomial of the sequence \(\{S_i\}\).

P6. The period of the sequence \(\{\zeta_n\}\) equals the period of the sequence \(\{z_i\}\) and equals \((p^r - 1)\) but the period of the sequence \(\{z_i\}\) in the examples 1 to 3 is equal to half of this value but in example 4 equals the quarter of this value.

P7. The set of all cyclic permutations of one period of the multiplication sequence \(\{z_i\}\) is not orthogonal set.

P8. There is important difference between the properties of multiplication M-Sequences and M2-Sequences.

P9. We did not come across one term in the basic M2-Sequenced \(\{S_1\}\) as the sum of Exp.\((A)\) and Exp. \((\alpha^p)^{r-1}\) in formula of \(S_1\) are complement that is; Exp.\((A)\) + Exp. \((\alpha^p)^{r-1}\) \(= p^k\) - 1 consequently the same for the \(\zeta_n\) and furthermore it the permutations between the "coefficients and roots which are in formula of \(\zeta_n\)" will not be in the formula of \(\zeta_n\) as in the binary M-Sequences.

References

[1] Sloane, N.J.A., (1976), “An Analysis Of The Strucure 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 \(F_p\) 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. IJICT. ISSN 0976-6367(Print),ISSN 0976 - 6375(Online),Vol.5, Issue 9. Pp. 61-72.

[5] 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, Vol. 4, Issue 2, PP 118-125.

[6] Al Cheikha A. H. (2018).Generation New Binary Sequences using Quotient Ring Z/\(p^n\)Z. 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 \(F_p\) in the Space \(R_n\), 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, IJISE, 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, IJISE, 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. (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 Faulutexts, 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), "Finite Fields and Their Applications, " Springer – Verlage New York, 1984.

[16] Lidl, R. & Niederreiter, 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.
# Appendix

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