Compose M-Sequences

Ahmad Hamza Al Cheikha

Department of Mathematical Science, College of Arts-science and Education, Ahlia University, Exhibition Street, Manama, Bahrain. Email : alcheikhaa@yahoo.com
His Research interest are Design Orthogonal sequences with variable length, Finite Fields, Linear and Non Linear codes, Copositive Matrices and Fuzzy Sets

ABSTRACT

M - Sequences (which formed a closed sets under the addition and with the corresponding null sequence formed additive groups and generated by feedback registers) are used widely at the forward links of communication channels to mix the information on connecting to and at the backward links of these channels to sift through this information is transmitted to reach the receivers this information in correct form, specially in the pilot channels, the Sync channels, and the Traffics channel. This research is useful to generate new sets of orthogonal sequences by compose M-sequences with the bigger lengths and the bigger minimum distance that assists to increase secrecy of these information and increase the possibility of correcting mistakes resulting in the channels of communication.

Index terms: Recurring Sequences, Characteristic Polynomial, M-sequences, Compose Sequences, Orthogonal Sequences, Code, Minimum Distance

INTRODUCTION

M-Sequences: M- Linear Recurring Sequences

Let k be a positive integer and λ, λ_0, λ_1, ..., λ_{k-1} are elements in the field F_2 then the sequence $z_0, z_1, ..$ is called non homogeneous linear recurring sequence of order k *iff*:

$$z_{n+k} = \lambda_{k-1} z_{n+k-1} + \lambda_{k-2} z_{n+k-2} + ... + \lambda_0 z_n + \lambda,\ \lambda_i \in F_2,\ i = 0,1,...,k-1$$

$$or \qquad z_{n+k} = \sum_{i=1}^{k-1} \lambda_i z_{n+i} + \lambda \tag{1}$$

The elements $z_0, z_1, .., z_{k-1}$ are called the initial values (or the vector $(z_0, z_1, .., z_{k-1})$ is called the initial vector). If $\lambda = 0$ then the sequence $z_0, z_1, ...$ is called homogeneous linear recurring sequence (H. L. R. S.), except the zero initial vector, and the polynomial

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

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

(Farleigh, 1971), (*Lee and Miller, 1998*), (*Thomson*, *2013*), (*Yang and Kumar*, *2000*).

Literature Review

- In the *The Theory Of Error- Correcting Codes.* (*Mac Williams and Sloane*, *2006*) it was explained about finite field, linear and no linear codes as: M-Sequences, Reed Solomon code, Goppa codes and Reed Muller codes, and the orthogonal sequences.
- In the Finite Fields and Their Application (*Lidl and Nidereiter*, *1994*) it was explained about finite field, recurring sequences and M-Sequences.
- In the Teoria Kodirovania (*Kacami and Tokora*, *1978*). it was explained about finite field, linear and no linear codes as: M-Sequences, Reed Solomon code, Goppa codes Reed Muller codes, and the orthogonal sequences.

- In the CDMA System Engineering Hand Book (*Lee and Miller*, *1998*) it was explained about Walsh Sequences, linear correlation and M-Sequences.
- In the Binary Pseudorandom Sequences For period 2^{n-1} with Ideal Autocorrelation. (*Jong, Solomon and Golomb*, *1998*) it was explained about recurring Sequences and special M-Sequences.
- In the Compose Walsh's Sequences and Reed Solomon Sequences (*Al Cheikha*, *2015*). it was explained about number of un "1.s" and "0.s" in compose two sequences and special Compose Walsh's Sequences and Reed Solomon Sequences.

RESEARCH METHODS AND MATERIALS

Definition 1. The Ultimately Periodic Sequence $z_0, z_1, ..,$ with the smallest period r is called a periodic *iff*:

$z_{n+r} = z_n;\ n = 0, 1...$(*Yang and Kumar*, *2000*), (*Yang*, *1998*)

Definition 2. The complement of the binary vector is the vector $X = (x_1, x_2, ..., x_n)$

$\overline{X} = (\overline{x_1}, \overline{x_2}, ..., \overline{x_n})$, when $\overline{x_i} = \begin{cases} 1 & if \quad x_i = 0 \\ 0 & if \quad x_i = 1 \end{cases}$. (*Yang and Kumar*, *2000*), (*Yang 1998*).

Definition 3. Any Periodic Sequence $z_0, z_1, ...,$ over F_2 with prime characteristic polynomial is an orthogonal cyclic code and ideal auto correlation.

(*Al Cheikha and Ruchin*, *2014)*, (*Byrnes and Swick*, *1970*), (*Jong, Solomon and Golomb*, *1998*), (*Lidl and Pilz*, *1984*), (*Sloane*, *1076*).

Definition 4. Suppose $x = (x_0, x_1., x_{n-1})$ and $x = (y_0, y_1., y_{n-1})$ are vectors of length n on $GF(2)= \{0, 1\}$. The coefficient of correlations function of x and y, denoted by $R_{x,y}$ is:

$$R_{x,y} = \sum_{i=0}^{n-1} (-1)^{x_i + y_i}$$

Definition 5. Suppose G is a set of binary vectors of length n

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

Let 1*= -1 and 0*=1. The set G is said to be orthogonal if the following two conditions are satisfied:

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

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

That is, the absolute value of "the number of agreements minus the number of disagreements" is equal to or less than 1. (Yang and Kumar, *2000*)

Definition 6. *Hamming distanced* (x, y): The Hamming distance between the binary vectors $x = (x_0, x_1, ..., x_{n-1})$ and $y = (y_0, y_1, .., y_{n-1})$ is the number of the disagreements of the corresponding components of x and y. (*Mac Williams and Sloane*, *2006*).

Definition 7. *Minimum distance d*: The minimum distance d of a set C of binary vectors is: $d = \min_{x,y \in C} d(x, y)$. (*Mac Williams and Sloane*, *2006*).

Definition 8. The code C of the form $[n, k, d]$ if each element (Codeword) has the: length n, the rank k is the number of information components (Message), minimum distance d (*Mac Williams and Sloane*, *2006*).

Definition 9. If C is a set of binary sequences and ω is any binary vector then:

$C(\omega)= \{x_i(\omega): x_i \in C\}$, We replace each "1" in x_i by ω and each "0" in x_i by $\bar{\omega}$.

(*Al Cheikha*, *2015*), (*David, 2008*).

Corollary1. If in the binary vector x: the number of "1"s and the number of "0"s are m_1 and m_2 respectively, and in the binary vector ω: the number of"1"s n_1 and n_2 the number of "0"s are and respectively then in the binary vector $x(\omega)$: the number of"1"s and the number of "0"s are $m_1n_1+ m_2n_2$ and $m_1n_2+ m_2n_1$ respectively**.** (*Al Cheikha*, *2015*).

Theorem 2.

i. If $z_0, z_1, ...,$ is a homogeneous linear recurring sequence of order k in F_2, satisfies (1) then this sequence is periodic.
ii. If the characteristic polynomial $f(x)$ of the sequence is primitive then the period of the sequence is 2^{k-1}, and this sequence is called M – sequence and each of these sequences contains 2^{k-1} of "1"s and2^{k-1} - 1 of "0"s. (*Kacami and Tokora*, *1997*), (*Lee and Miller, 1998*), (*Lidl and Nidereiter*, *1994*).

Theorem 2.

The number of irreducible polynomials in $F_q(x)$ of degree m and order e is φ (e)/m, if $e \geq 2$, When φ is the Euler function and m is the order of q by mod e, and equal to 2 if

$m = e = 1$, and equal to zero elsewhere. (*Lidl and Nidereiter*, *1994*). (*Mac Williams and Sloane, 2006*).

RESULTS AND DISCUSSION (FINDINGS)

We suppose $a_1$is a non zero M-Sequence generated by the non homogeneous linear recurring sequence (1) of order k with the prime characteristic polynomial:

$f(x)= x^k + \beta_{k-1}x^{k-1} +..... + \beta_1 x + \beta_0$

And the set $A = \{a_i, i = 1, 2, ..., 2^{k-1}\}$ of all cyclic shift of the sequence $a_1$and the set A form with the zero sequence an additive group, and the set and

$\widetilde{A} = \{\widetilde{a_i}, i = 1, 2, ..., 2^{k-1}\}$, and b_1 is a non zero M-Sequence generated by the non homogeneous linear recurring sequence (1) of order m with the prime characteristic polynomial: $g(x)= x^m + \lambda^{m-1} x^{m-1} +... + \lambda_1 x + \lambda_0$

And the set of all cyclic shift of the sequence and the set A form with the zero

sequence an additive group the $\widetilde{B} = \{\widetilde{b_i}, i = 1, 2, ..., 2^{m-1}\}$

First Step

Compose A with B or $A(B)$

$\widetilde{A}$		$\widetilde{B}$	
Number of "1"s	**Number of "0"s**	**Number of "1"s**	**Number of "0"s**
2^{k-1}	$2^{k-1}-1$	2^{m-1}	$2^{m-1}-1$

* For $b \in B$ we define the set: $C_k = A(b_k)= c_i = a_i(b_k)$, $a_i \in \widetilde{A}$ then:

a) The number of "1" in $\widetilde{c_i}$is:

$(2^{k-1})(2^m-1)+ (2^{k-1} - 1)(2^{m-1} - 1)$

$= 2^{k + m-1} - 2^{k-1} - 2^{m-1} + 1$

b) The number of "0" in c_i is:

$(2^{k-1})(2^{m-1} - 1) + (2^{k-1} - 1)(2^{m-1})$

$= 2^{k + m-1} - 2^{k-1} - 2^{m-1}$

c) The difference between the number of "1"s and the number of "0"s is: one

d) for $c_i, c_j \in C_k$ and $i \neq j$ the $c_i + c_j = (a_i + a_j)(b_k)$ then:

* The number of "1"s in $c_i + c_j$ is: $= 2^{k+m-1} - 2^{k-1} - 2^{m-1} + 1$

* The number of "0"s in $c_i + c_j$ is: $= 2^{k+m-1} - 2^{k-1} - 2^{m-1}$

And the difference between the number of "1"s and the number of "0"s is one

Thus C_k is an orthogonal set.

Second Step

Compose $\widetilde{A}$ with B or $\widetilde{A}(B)$

$\widetilde{A}$		$\widetilde{B}$	
Number of "1"s	**Number of "0"s**	**Number of "1"s**	**Number of "0"s**
2^{k-1}	2^{k-1}	2^{m-1}	$2^{m-1}-1$

* For $b \in B$ we define the set: $\widetilde{C}_k = \widetilde{A}(b_k) = \{\widetilde{c}_i = a_i(b_k),\ a_i \in A\}$ then:

a) The number of "1" in $\widetilde{c}_i$ is:

$(2^{k-1})(2^{m-1}) + (2^{k-1})(2^{m-1} - 1)$

$= 2^{k} + {}^{m-1} - 2^{k-1}$

b) The number of "0" in $\widetilde{c}_i$ is:

$(2^{k-1})(2^{m-1} - 1) + (2^{k-1})(2^{m-1})$

$= 2^{k} + {}^{m-1} - 2^{k-1}$

c) The difference between the number of "1"s and the number of "0"s is: zero

d) for $\widetilde{c}_i, \widetilde{c}_j \in \widetilde{c}_k$ and $i \pm j$ the $\widetilde{c}_i + \widetilde{c}_j = (\widetilde{a}_i + \widetilde{a}_j)(b_k)$ then:

* The number of "1"s in $\widetilde{c}_i + \widetilde{c}_j$ is: $= 2^{k + m-1} - 2^{k-1}$

* The number of "0"s in $\widetilde{c}_i + \widetilde{c}_j$ is: $= 2^{k + m-1} - 2^{k-1}$

And the difference between the number of "1"s and the number of "0"s is zero

Thus $\widetilde{c}_k$ is an orthogonal set.

Third Step

Compose B with A with or $B(A)$

$\widetilde{B}$		$\widetilde{A}$	
Number of "1"s	**Number of "0"s**	**Number of "1"s**	**Number of "0"s**
2^{m-1}	$2^{m-1}-1$	2^{k-1}	$2^{k-1}-1$

* For $a_k \in A$ we define the set: $D_k = b_i(a_k) = \widetilde{d}_i = b_i(a_k)$, ;$b_i \in B$ then:

a) The number of "1" in d_i is:

$(2^{m-1})(2^{k-1}) + (2^{m-1} - 1)(2^{k-1} - 1)$

$= 2^{m} + {}^{k-1} - 2^{m-1} - 2^{k-1} + 1$

b) The number of "0" in d_i is:

$(2^{m-1})(2^{k-1} - 1) + (2^{m-1} - 1)(2^{k-1})$

$= 2^{m} + {}^{k-1} - 2^{m-1} - 2^{k-1}$

c) The difference between the number of "1"s and the number of "0"s is: one

d) for $d_i, d_j \in D_k$ and $i \pm j$ the $d_i + d_j = (b_i + b_j)(a_k)$ then:

* The number of "1"s in $d_i + d_j$ is: $= 2^{m} + {}^{k-1} - 2^{m-1} - 2^{k-1} + 1$

* The number of "0"s in $d_i + d_j$ is: $= 2^{m} + {}^{k-1} - 2^{m-1} - 2^{k-1}$

And the difference between the number of "1"s and the number of "0"s is one

Thus D_k is an orthogonal set.

Forth Step

Compose $\widetilde{B}$ with A or $B(A)$

$\widetilde{B}$		$\widetilde{A}$	
Number of "1"s	**Number of "0"s**	**Number of "1"s**	**Number of "0"s**
2^{m-1}	2^{m-1}	2^{k-1}	$2^{k-1}-1$

* For $a_k \in A$ we define the set: $\widetilde{D}_k = \widetilde{b}_i(a_k) = \widetilde{d}_i = \widetilde{b}_i(a_k)$, ;$b_i \in B$ then:

a) The number of "1" in $\widetilde{d}_i$ is:

$(2^{m-1})(2^{k-1}) + (2^{m-1})(2^{k-1} - 1)$

$= 2^{m} + {}^{k-1} - 2^{m-1}$

b) The number of "0" in $\widetilde{d}_i$ is:

$(2^{m-1})(2^{k-1} - 1) + (2^{m-1})(2^{k-1})$

$= 2^{m + k-1} - 2^{m-1}$

c) The difference between the number of "1"s and the number of "0"s is: zero

d) for $\widetilde{d}_i, \widetilde{d}_j \in \widetilde{D}_k$ and $i \pm j$ the $\widetilde{d}_i + \widetilde{d}_j = (\widetilde{b}_i + \widetilde{b}_j)(a_k)$ then:

* The number of "1"s in $\widetilde{d}_i + \widetilde{d}_j$ is: $= 2^{m} + ^{k-1} - 2^{m-1}$

* The number of "0"s in $\widetilde{d}_i + \widetilde{d}_j$ is: $= 2^{m} + ^{k-1} - 2^{m-1}$

And the difference between the number of "1"s and the number of "0"s is zero

Thus $\widetilde{D}_k$ is an orthogonal set.

Fifth Step

Compose $\widetilde{A}$ with $\widetilde{B}$ or $\widetilde{A}(\widetilde{B})$

$\widetilde{A}$		$\widetilde{B}$	
Number of "1"s	**Number of "0"s**	**Number of "1"s**	**Number of "0"s**
2^{k-1}	2^{k-1}	2^{m-1}	2^{m-1}

* For $b \in B$ we define the set: $\widetilde{E}_k = \widetilde{A}(\widetilde{b}_k) = \{ \widetilde{e}_i = \widetilde{a}_i(\widetilde{b}_k), a_i \in A\}$ then:

a) The number of "1" in $\widetilde{e}_i$ is:

$(2^{k-1})\ (2^{m-1}) + (2^{k-1})\ (2^{m-1})$

$= 2^{k + m-1}$

b) The number of "0" in $\widetilde{e}_i$ is:

$(2^{k-1})\ (2^{m-1}) + (2^{k-1})\ (2^{m-1})$

$= 2^{k + m-1}$

c) The difference between the number of "1"s and the number of "0"s is: zero

d) for $\widetilde{e}_i, \widetilde{e}_j \in \widetilde{E}_k$ and $i \pm j$ the $\widetilde{e}_i + \widetilde{e}_j = (\widetilde{a}_i + \widetilde{a}_j)(\widetilde{b}_k)$ then:

* The number of "1"s in $\widetilde{e}_i + \widetilde{e}_j$ is: $= 2^{k + m-1}$

* The number of "0"s in $\widetilde{e}_i + \widetilde{e}_j$ is: $= 2^{k + m-1}$

And the difference between the number of "1"s and the number of "0"s is zero

Thus $\widetilde{E}_k$ is an orthogonal set.

Step Sixth

Compose $\widetilde{B}$ with $\widetilde{A}$ or $\widetilde{B}(\widetilde{A})$

By the same way as I step fifth step we can se that $\widetilde{F}_k = \widetilde{B}(\widetilde{a}_k) = \widetilde{f}_i = \widetilde{b}_i(\widetilde{a}_k), b_i \in B\}$

Also is an orthogonal set.

Example 1: If α is a root of the prime polynomial $f(x)= x^2 + x + 1$ and generates $GF(2^2)$ and Suppose the Linear Binary Recurring Sequence be

$$z_{n+2} = z_{n+1} + z_n \text{ or } z_{n+2} + z_{n+1} + z_n = 0 \quad (4)$$

With the characteristic equation $x^2 + x + 1 = 0$ and the characteristic polynomial $f(x)= x^2 + x + 1$, which is a prime then the general solution of equation (1) For the initial position: $y_1 = 1$, $y_2 = 0$ is given by: $y_n = \alpha \cdot \alpha^n + \alpha^2 \cdot \alpha^{2n}$, and the sequence is periodic with the period $2^2 - 1 = 3$

and a_1= (101), by the cyclic permutations on a_1 we have $A = \{a_1, a_2, a_3\}$ where:

a_1= (101), a_2 = (110), a_3=(011), The first two digits in each sequence are the initial position of the feedback register, and the set A is an orthogonal set and a cyclic code of the form [n =3, k=2, d = 2].

Extend each sequence addition of 0 to the end of each, such we have $\widetilde{A} = \{\widetilde{a_1}, \widetilde{a_2}, \widetilde{a_3}\}$ where:

$\widetilde{a_1}$= (1010), $\widetilde{a_2}$ = (1100), $\widetilde{a_3}$=(0110)

The sets $\widetilde{A}$ and is an orthogonal set and a codes of the form [n =4, k=2, d = 2].

There is only one prime polynomial of order 2 that is $f(x)= x^2 + x + 1$.

Example 2: If α is a root of the prime polynomial $f(x)= x^3 + x + 1$ and generates $GF(2^3)$ and Suppose the Linear Recurring Sequence be:

$$z_{n+3} = z_{n+1} + z_n \text{ or } z_{n+3} + z_{n+1} + z_n = 0 \quad (5)$$

With the characteristic equation $x^3 + x + 1 = 0$ and the characteristic polynomial $f(x)= x^3 + x + 1$, which is a prime and generates F_2^3 and if $x = \beta \in GF\ (2^3)$ is a root of $f(x)$ and For the initial position: $z_1 = 1$, $z_2 = 0$, $z_3 = 0$ then the general solutions of equation (2) is given by$z_n = \beta^2 \cdot \beta^n + \beta^4 \cdot \alpha^{2n} + \beta \cdot \beta^{4n}$, and the sequence is periodic with the period $2^3 - 1 = 7$ and b_1 = (1001011), by the cyclic permutations on b_1 we have $B = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7\}$ where: b_2=(1100101), b_3=(1110010), b_4=(0111001),

b_5=(1011100), b_6=(0101110), b_7=(0010111), and the first three digits in each sequence are the initial position of the feedback register, and the set M_7 is an orthogonal set and a cyclic code of the form [n =7, k=3, d = 4].

Extend each sequence addition of 0 to the end B of each, such we have: $\widetilde{B} = \{\widetilde{b_1}, \widetilde{b_2}, \widetilde{b_3}, \widetilde{b_4}, \widetilde{b_5}, \widetilde{b_6}, \widetilde{b_7}\}$

where:

$\widetilde{b_1}$ = (10010110), $\widetilde{b_2}$=(11001010), $\widetilde{b_3}$=(11100100), $\widetilde{b_4}$=(01110010), $\widetilde{b_5}$=(10111000),

$\widetilde{b_6}$=(01011100), $\widetilde{b_7}$=(00101110).

The set $\widetilde{B}$ is an orthogonal set and a code of the form [n =8, k=3, d = 4].

There are only two prime polynomial of order 3 that are $f(x)= x^3 + x + 1$ and its conjugate $g(x)= x3 + x^2 + 1$.

1. Finding $A(b_1)$:

b_1 = (1001011), b_1 = (0110100):

$a_1(b_1)$= **(**1001011 0110100 1001011**)**

$a_2(b_1)$= **(**1001011 1001011 0110100**)**

$a_3(b_1)$= **(**0110100 1001011 1001011**)**

$A(b_1)$ is an orthogonal set with the length $n = 2^{2+3} - {}^{22} - 2^3 + 1 = 21$ dimension

k = 2 minimum distance $d = 2^{2+3-1} - 2^{2-1} - 2^{3-1} + 1 = 11$.

2. Finding $\widetilde{A}(b_1)$:

$\widetilde{a}_1(b_1)$= **(**1001011 0110100 1001011 0110100**)**

$\widetilde{a}_2(b_1)$= **(**1001011 1001011 0110100 0110100**)**

$\widetilde{a}_3(b_1)$= **(**0110100 1001011 1001011 0110100**)**

$\widetilde{A}(b_1)$ is an orthogonal set with the length $n = 22 + {}^{3} - {}^{22} = 28$, dimension

k = 2 minimum distance $d = 2^{2+3-1} - 2^2 - 1 = 14$.

3. Finding B(a_1)

a_1 = (1 0 1), a_1 = (0 1 0)

$b_1(a_1)$= (1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 1 0 1)

$b_2(a_1)$= (1 0 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1)

$b_3(a_1)$= (1 0 1 1 0 1 1 0 1 0 1 0 0 1 0 1 0 1 0)

$b_4(a_1)$= (0 1 0 1 0 1 1 0 1 1 0 1 0 1 0 0 1 0 1)

$b_5(a_1)$= (1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 0 1 0 0)

$b_6(a_1)$= (0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 0)

$b_7(a_1)$= (0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 1)

$B(a_1)$ is an orthogonal set with the length $n = 2^{3+2} - 2^3 = 21$, dimension

k = 3 minimum distance $d = 2^3 + 2 - 1 - 2^3 - 1 - 2^2 - 1 + 1 = 11$.

4. FINDING $\widetilde{B}(a_1)$

a_1 = (1 0 1), *bar* a_1 = (0 1 0)

$\widetilde{b}_1(a_1)$= (1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0)

$\widetilde{b}_2(a_1)$= (1 0 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0)

$\widetilde{b}_3(a_1)$= (1 0 1 1 0 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 0 1 0)

$\widetilde{b}_4(a_1)$= (0 1 0 1 0 1 1 0 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0)

$\widetilde{b}_5(a_1)$= (1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 0 1 0 0 1 0 0 1 0)

$\widetilde{b}_6(a_1)$= (0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 0 1 0 0 1 0)

$\widetilde{b}_7(a_1)$= (0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 0 1 0)

$\widetilde{B}(a_1)$ is an orthogonal set with the length $n = 2^{3+2} - {}^{23} = 24$, dimension

k = 3 minimum distance $d = 2^{3+2-1} - 2^3 - 1 = 12$.

5. Finding $\widetilde{A}(\widetilde{b}_1)$

$\widetilde{b}_1 = (10010110)$, $\widetilde{\widetilde{b}}_1 = (01101001)$:

$\widetilde{a}_1(\widetilde{b}_1)$= (10010110 01101001 10010110 01101001)

$\widetilde{a}_2(\widetilde{b}_1)$= (10010110 10010110 01101001 01101001)

$\widetilde{a}_3(\widetilde{b}_1)$= (01101001 10010110 10010110 01101001)

$\widetilde{A}(\widetilde{b}_1)$ is an orthogonal set with the length $n = 2^{2+3} = 32$, dimension k = 3

minimum distance $d = 2^{2+3-1} = 16$.

6. Finding $\widetilde{B}(\widetilde{a}_1)$

$\widetilde{a}_1 = (1\ 0\ 1\ 0)$, $\widetilde{a}_1 = (0\ 1\ 0\ 1)$

$\widetilde{b}_1(\widetilde{a}_1)$= (1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1)

$\widetilde{b}_2(\widetilde{a}^1)$= (1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1)

$\widetilde{b}_3(\widetilde{a}_1)$= (1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1)

$\widetilde{b}_4(\widetilde{a}_1)$= (0 1 0 1 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1)

$\widetilde{b}_5(\widetilde{a}_1)$= (1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1)

$\widetilde{b}_6(\widetilde{a}_1)$= (0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1)

$\widetilde{b}_7(\widetilde{a}_1)$= (0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 1 0 0 1 0 1)

$\widetilde{B}(\widetilde{a}_1)$ is an orthogonal set with the length $n = 2^{3+2} = 32$, dimension k = 3

minimum distance $d = 2^{3+2} - 1 = 16$.

CONCLUSION

1. $A(B)$ are orthogonal sets with lengths $n = 2^{k+m} - 2^k - 2^{m+1}$ and minimum distance $d = 2^{k+m-1} - 2^{k-1} - 2^{m-1} + 1]$.

2. $\widetilde{A}(B)$ are orthogonal sets with lengths $n = 2^{k+m} - {}^{2k}$ and minimum distance $d = 2^{k+m-1} - 2^{k-1}]$.

3. $B(A)$ are orthogonal sets with lengths $n = 2^{m+k} - 2^m - 2^k$ and minimum distance $d = 2^{m+k-1} - 2^{m-1}]$.

4. $\widetilde{B}(A)$ are orthogonal sets with lengths $n = 2^{m+k} - 2^{mk}$ and minimum distance $d = 2^{m+k-1} - 2^{m-1}]$.

5. $\widetilde{A}(\widetilde{B})$ are orthogonal sets with lengths $n = 2^{k+m}$ and minimum distance $d = 2^{k+m-1}]$.

6. $\widetilde{B(A)}$ are orthogonal sets with lengths $n = 2^{m+k}$ and minimum distance $d = 2^{m+k-1}$].

Implications

This research is useful to generate new sets of orthogonal sequences by compose M-sequences with the bigger lengths and the bigger minimum distance that assists to increase secrecy of these information and increase the possibility of correcting mistakes resulting in the channels of communication.

Limitation

This method of compose sequences is useful for only binary sequences and the addition on the sequences computed by "*mod* 2 "

REFERENCES

[1] Al Cheikha A. H. (2015). Compose Walsh's Sequences and Reed Solomon Sequences. *Paper presented at the ISERD International Conference, Cairo, Egypt*, 30th December 2015, ISBN: 978-93-85832-90-1: 23-26.
[2] Al Cheikha A. H., Ruchin J. (March 2014), Generation of Orthogonal Sequences by Walsh Sequences. *International Journal of Soft Computing and Engineering.*4(1): 182-184.
[3] Byrnes, J.S. Swick (1970). Instant Walsh Functions, *SIAM Rever*.12: 131.
[4] David, J. (2008). Introductory Modern Algebra. *Clark University.* USA, 2008.
[5] Farleigh, J. B. (1971). A First course In Abstract Algebra. *Fourth printing. Addison-Wesley publishing company* USA.
[6] Jong-Seon No, Solomon W & Golomb. (1998). Binary Pseudorandom Sequences For period 2_{n-1} with Ideal Autocorrelation. *IEEE Trans. Information Theory.* 44(2): 814-817.
[7] Kacami, T.&Tokora, H. (1978). Teoria Kodirovania. *Mir*(*MOSCOW*).
[8] Lee J.S &Miller L.E. (1998). *CDMA System Engineering Hand Book.* Artech House. Boston, London.
[9] Lidl, R.& Nidereiter, H. (1994). *Introduction to Finite Fields and Their Application*. Cambridge university USA.
[10] Lidl, R.& Pilz, G. (1984). *Applied Abstract Algebra.* Springer – Verlage New York.
[11] Mac Wiliams, F.G& Sloane.G.A. (2006). *The Theory Of Error- Correcting Codes.* North-Holland, Amsterdam.
[12] Sloane, N. J. A. (1076), "An Analysis Of The Stricture and Complexity Of Nonlinear Binary Sequence Generators. *IEEE Trans. Information Theory.* 22(6): 732-736.
[13] Thomson W. Judson. (2013). *Abstract Algebra: Theory and Applications.* Free Software Foundation.
[14] Yang K, Kg Kim y Kumar l. d. (2000). Quasi – orthogonal Sequences for code - Division Multiple Access Systems. *IEEE Trans. information theor.* 46(3): 982-993.
[15] Yang S.C. (1998). *CDMA RF System Engineering.* Artech House.Boston-London.