Compose Walsh's Sequences and M-Sequences

Dr. Ahmad Hamza Al Cheikha

Department of Mathematical Science, College of Arts-science and Education,
Ahlia University, Exhibition Street, Manama, Bahrain
alcheikhaa@yahoo.com

ABSTRACT

Walsh Sequences and M-Sequences 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 Traffic channel.This research is useful to generate new sets of sequences (which are also with the corresponding null sequence additive groups) by compose Walsh Sequences and 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 – Walsh Sequences, M-sequences, Additive group, Coefficient of Correlation, Orthogonal sequences, Code.

INTRODUCTION

***A.* Walsh's Sequences:** In 1923, J.L. Walsh defined a system of orthogonal functions that is complete over the normalized interval (0,1). Walsh sequences of order 2k , which are generated by the binary representation of Walsh functions of order N = 2k , form a group under 2 addition (addition group). The set of these sequences except W0 forms orthogonal closed set and the number of "1"s is equal the number of "0" and each of them is equal 2^{k-1}. [I-III].

The Walsh functions can be generated by any of the following methods:

1. Using Rademacher functions.
2. Using Hadamard matrices.
3. Exploiting the symmetry properties of Walsh functions.
4. Using division ring under 2k addition [IV-VII].

B. M-Sequences: M- Linear Recurring Sequences

Let k be a positive integer and $\lambda ,\lambda_0,\lambda_1,...,\lambda_{k-1}$ are elements in the field F_2 then the sequence $z_0,z_1,\dots$is called non homogeneous linear recurring sequence of order k iff :

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

$$or \qquad z_{n+k} = \sum_{i=0}^{k-1}\lambda_i z_{n+i} + \lambda \qquad\qquad (1)$$

The elements $z_0,z_1,\dots,z_{k-1}$ are called the **initial values** (or the vector $(z_0,z_1,\dots,z_{k-1})$ is called the initial vector). If $\lambda = 0$ then the sequence $a_0,a_1,\dots$ is called homogeneous linear recurring sequence (H. L. R. S.), except the zero initial vector, and the polynomial

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

is called the characteristic polynomial. In this study, we are limited to $\lambda_0 = 1$. [I]-[III]

II. RESEARCH METHODS AND MATERIALS

Definition1. The Ultimately Periodic Sequence $z_0, z_1, ...$with the smallest period *r* is called a periodic *iff*:

$$z_{n+r} = z_n \quad ; \quad n = 0, 1, ... \text{ [I]-[IV]}$$

Definition2. The complement of the binary vector $X = (x_1, x_2, ..., x_n)$ is the vector

$$\overline{X} = (\overline{x_1}, \overline{x_2}, ..., \overline{x_n}) \text{ , when } \overline{x_i} = \begin{cases} 1 & if \quad x_i = 0 \\ 0 & if \quad x_i = 1 \end{cases} \text{. [I]-[IV]}$$

Definition3. Any Periodic Sequence $z_0, z_1, ...$over F_2 with prime characteristic polynomial is an orthogonal cyclic code and ideal auto correlation [I]-[X].

Definition4. Suppose $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, ..., y_{n-1})$ 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: $R_{x,y} = \sum_{i=0}^{n-1} (-1)^{x_i + y_i}$

Definition5. Suppose G is a set of binary vectors of length *n*

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

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

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

$$\forall X, Y \in G \; and \; X \neq Y), \sum_{i=0}^{n-1} x_i^* y_i^* \in \{-1, 0, 1\}, \quad or \quad |R_{x,y}| \leq 1.$$

That is, the absolute value of "the number of agreements minus the number of disagreements" is equal to or less than 1. [I]

Definition6. *Hamming distance* $d(x, y)$: The Hamming distance between the binary vectors $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, ..., y_{n-1})$ is the number of the disagreements of the corresponding components of *x* and *y*.[IX]

Definition7. *Minimum distance d*: The minimum distance *d* of a set *C* of binary vectors is: $d = \min_{x, y \in C} d(x, y)$. [IX]

Definition8. 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*.[IX]

Definition9. 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 $\overline{\omega}$.[IX-X]

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 w : the number of"1"s and the number of "0"s are $n_1$and n_2 respectively then in the binary vector $x(w)$: the number of"1"s and the number of "0"s are $m_1 n_1 + m_2 n_2$ and $m_1 n_2 + m_2 n_1$ respectively.**[**XI**]-[**XV**]**

Theorem2.

i. If $a_0, a_1, ...$ 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 and $2^{k-1} - 1$ of "0"s .[6]

I. Results and Discussion

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

$$f(x) = x^m + \lambda_{m-1} x^{m-1} + \ldots + \lambda_1 x + \lambda_0$$

And the set $A = \{a_i . i = 1,2,\ldots 2^m - 1\}$ of all cyclic shift of the sequence a_1 and the set A form with the zero sequence an additive group, and the set $\tilde{A} = \{\tilde{a}_i . i = 1,2,\ldots 2^m - 1\}$ when $\tilde{a}_i = (a_i, 0)$ is the extending a_i by addition the “0” to the end of a_i .

Thus: each of these sequences a_i contains 2^{m-1} of “1”s and $2^{m-1} - 1$ of “0”s, and each of these sequences a_i contains 2^{m-1} of “1”s and 2^{m-1} of “0”s.

Second: We suppose $W^*_{2^n} = \{w_i, i = 1,2,\ldots 2^n - 1\}$ the set of all Walsh sequences of order 2^n except the null sequence w_0 then each of these w_i contains 2^{n-1} of “1”s and the same number of “0” and $W^*_{2^n}$ is closed under the addition.

First Step

Compose *A* with $W^*_{2^n}$ or $A(W^*_{2^n})$

A		$W^*_{2^n}$	
Number of “1”s	Number of “0”s	Number of “1”s	Number of “0”s
2^{m-1}	$2^{m-1} - 1$	2^{n-1}	2^{n-1}

* For $w_i \in W_{2^n}$ we define the set: $B_k = A(w_k) = \{b_i = a_i(w_k), a_i \in A\}$ then:

a) The number of “1” in b_i is:

$$\left(2^{m-1}\right)\left(2^{n-1}\right) + \left(2^{m-1} - 1\right)\left(2^{n-1}\right)$$

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

b) The number of “0” in b_i is:

$$\left(2^{m-1}\right)\left(2^{n-1}\right) + \left(2^{m-1} - 1\right)\left(2^{n-1}\right)$$

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

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

d) for $b_i, b_j \in B_k$ and $i \neq j$ the $b_i + b_j = (a_i + a_j)(w_k)$ then:

* The number of “1”s in $b_i + b_j$ is: $2^{m+n-1} - 2^{n-1}$

* The number of “0”s in $b \quad + b_j$ is: $2^{m+n-1} - 2^{n-1}$

And the difference between the number of “1”s and the number of “0”s is zero..

Thus B_k is an orthogonal set.

Second Step

Compose $\widetilde{A}$ with $W_{2^n}^*$ or $\widetilde{A}\left(W_{2^n}^*\right)$

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

* For $w_k \in W_{2^n}$ we define the set: $\widetilde{B}_k = \widetilde{A}(w_k) = \{\widetilde{b}_i = \widetilde{a}_i(w_k), a_i \in A\}$ then:

a) The number of "1" in $\widetilde{b}_i$ is: $\left(2^{m-1}\right)\left(2^{n-1}\right) + \left(2^{m-1}-1\right)\left(2^{n-1}\right)$

b) The number of "0" in $\widetilde{b}_i$ is: $\left(2^{m-1}\right)\left(2^{n-1}\right) + \left(2^{m-1}\right)\left(2^{n-1}\right) = 2^{m+n-1}$

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

d) for $b_i, b_j \in B_k$ and $i \neq j$ the $\widetilde{b}_i + \widetilde{b}_j = (\widetilde{a}_i + \widetilde{a}_j)(w_k)$ then:

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

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

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

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

Third step

Compose $W_{2^n}^*$ with A with or $W_{2^n}^*(A)$

$W_{2^n}^*$		A	
Number of "1"s	Number of "0"s	Number of "1"s	Number of "0"s
2^{n-1}	2^{n-1}	2^{m-1}	$2^{m-1}-1$

* For $a_k \in A$ we define the set: $C_k = w_i(a_k) = \{c_i = w_i(a_k), w_i \in W_{2^n}\}$ then:

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

$$\left(2^{n-1}\right)\left(2^{m-1}\right) + \left(2^{n-1}\right)\left(2^{m-1}-1\right)$$

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

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

$$\left(2^{n-1}\right)\left(2^{m-1}\right) + \left(2^{n-1}\right)\left(2^{m-1}-1\right)$$

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

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

d) for $c_i, c_j \in C_k$ and $i \neq j$ the $c_i + c_j = (w_i + w_j)(a_k)$ then:

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

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

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

Thus C_k is an orthogonal set.

Forth step

Compose $W^{*}_{2^n}$ with $\widetilde{A}$ or $W^{*}_{2^n}(\widetilde{A})$

$W^{*}_{2^n}$		$\widetilde{A}$	
Number of “1”s	Number of “0”s	Number of “1”s	Number of “0”s
2^{n-1}	2^{n-1}	2^{m-1}	2^{m-1}

* For $a_k \in A$ we define the set: $\widetilde{C}_k = w_i(\widetilde{a}_k) = \{\widetilde{c}_i = w_i(\widetilde{a}_k), w_i \in W_{2^n}\}$ then:

a) The number of “1” in $\widetilde{c}_i$ is: $(2^{n-1})(2^{m-1}) + (2^{n-1})(2^{m-1}) = 2^{n+m-1}$

b) The number of “0” in $\widetilde{c}_i$ is: $(2^{n-1})(2^{m-1}) + (2^{n-1})(2^{m-1}) = 2^{n+m-1}$

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 $i \neq j$ the $\widetilde{c}_i + \widetilde{c}_j = (w_i + w_j)(\widetilde{a}_k)$ then:

* The number of “1”s in $\widetilde{c}_i + \widetilde{c}_j$ is: 2^{n+m-1}

* The number of “0”s in $\widetilde{c}_i + \widetilde{c}_j$ is: 2^{n+m-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.

Example1. There are only one set of M-Sequences of order 3 that is:

$$z_{n+2} = z_{n+1} + z_n \text{ or } z_{n+2} + z_{n+1} + z_n = 0 \qquad (3)$$

With the characteristic equation $x^2 + x + 1 = 0$ and the characteristic polynomial $f(x) = x^2 + x + 1$ the set $A = \{a_1, a_2, a_3\}$ where: a_1 = (101), a_2 =(110), a_3 =(011), and 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].

Extending each sequence a_i addition of 0 to the end of each a_i (or to the beginning a_i)

Thus: $\widetilde{A} = \{\widetilde{a}_1, \widetilde{a}_2, \widetilde{a}_3\}$ where: $\widetilde{a}_1$ = (1010), $\widetilde{a}_2$ =(1100), $\widetilde{a}_3$ =(0110).

We suppose $W^{*}_{2^3}$ Walsh Sequences, that are:

Walsh Sequences of order 8=2^3
w_1 = 0 0 0 0 1 1 1 1
w_2 = 0 0 1 1 1 1 0 0
w_3 = 0 0 1 1 0 0 1 1
w_4 = 0 1 1 0 0 1 1 0
w_5 = 0 1 1 0 1 0 0 1
w_6 = 0 1 0 1 1 0 1 0
w_7 = 0 1 0 1 0 1 0 1

Thus:

a. For w_1 = 0 0 0 0 1 1 1 1 and $\overline{w}_1$ = 1 1 1 1 0 0 0 0 and we can see that $A(w_1)$ is:

$a_1(w_1) = 00001111 \quad 11110000 \quad 00001111$

$a_2(w_1) = 00001111 \quad 00001111 \quad 11110000$

$a_3(w_1) = 11110000 \quad 00001111 \quad 00001111$

And each of them contains $2^{2+3-1} - 2^{3-1} = 12$ of "1"s and the same number of "0"s and the difference between of them is zero.

And sum each two of them contains the same number of '1's and the same number of "0"s and the same difference.

Thus $A(w_1)$ is an orthogonal set.

b. For w_1 = 0 0 0 0 1 1 1 1 and $\overline{w}_1$ = 1 1 1 1 0 0 0 0 and we can see that $\widetilde{A}(w_1)$ is:

$\tilde{a}_1(w_1) = 00001111 \quad 11110000 \quad 00001111 \quad 11110000$

$\tilde{a}_2(w_1) = 00001111 \quad 00001111 \quad 11110000 \quad 11110000$

$\tilde{a}_3(w_1) = 11110000 \quad 00001111 \quad 00001111 \quad 11110000$

And each of them contains $2^{2+3-1} = 16$ of "1"s and the same number of "0"s and the difference between of them is zero.

And sum each two of them contains the same number of '1's and the same number of "0"s and the same difference.

Thus $\widetilde{A}(w_1)$ is an orthogonal set.

c. For a_1 = 1 0 1 and $\overline{a}_1$ = 0 1 0 and we can see that $W^{*}_{2^3}(a_1)$ is:

$w_1(a_1)$ = 010 010 010 010 101 101 101 101

$w_2(a_1)$ = 010 010 101 101 101 101 010 010

$w_3(a_1)$ = 010 010 101 101 010 010 101 101

$w_4(a_1)$ = 010 101 101 010 010 101 101 010

$w_5(a_1)$ = 010 101 101 010 101 010 010 101

$w_6(a_1)$ = 010 101 010 101 101 010 101 010

$w_7(a_1)$ = 010 101 010 101 010 101 010 101

And each of them contains $2^{3+2-1} - 2^{3-1} = 12$ of "1"s and the same number of "0"s and the difference between of them is zero.

And sum each two of them contains the same number of '1's and the same number of "0"s and the same difference.

Thus $W^{*}_{2^3}(a_1)$ is an orthogonal set.

d. For $\tilde{a}_1$ = 1 0 1 0 and $\overline{\tilde{a}}_1$ = 0 1 0 1 and we can see that $W^{*}_{2^3}(a_1)$ is:

$w_1(\tilde{a}_1)$ = 0101 0101 0101 0101 1010 1010 1010 1010

$w_2(\tilde{a}_1)$ = 0101 0101 1010 1010 1010 1010 0101 0101

$w_3(\tilde{a}_1)$ = 0101 0101 1010 1010 0101 0101 1010 1010

$w_4(\tilde{a}_1)$ = 0101 1010 1010 0101 0101 1010 1010 0101

$w_5(\tilde{a}_1)$ = 0101 1010 1010 0101 1010 0101 0101 1010

$w_6(\tilde{a}_1)$ = 0101 1010 0101 1010 1010 0101 1010 0101

$w_7(\tilde{a}_1)$ = 0101 1010 0101 1010 0101 1010 0101 1010

And each of them contains $2^{3+2-1} = 16$ of "1"s and the same number of "0"s and the difference between of them is zero.

And sum each two of them contains the same number of '1's and the same number of "0"s and the same difference.

Thus $W^{*}_{2^3}(\tilde{a}_1)$ is an orthogonal set.

V. CONCLUSION

1) The sets $A(W^*_{2^n})$ are linear not cyclic orthogonal sequences and form codes of: length *N* = $2^{m+n}-2^n$, minimum distance *d* = $2^{m+n-1}-2^{n-1}$, and dimension $k \ge m$.

2) The sets $\tilde{A}(W^*_{2^n})$ are linear not cyclic orthogonal sequences and form codes of: length N = 2^{m+n}, minimum distance *d* = 2^{m+n-1}, and dimension $k \ge m$.

3) The sets of $W^*_{2^n}(A)$ are linear not cyclic orthogonal sequences and form codes of: length N = $2^{m+n-1}-2^{n-1}$ minimum distance *d* = $2^{m+n-1}-2^{n-1}$, and dimension $k \ge n$.

4) The sets of $W^*_{2^n}(\tilde{A})$ are linear not cyclic orthogonal sequences and form codes of: length

N = 2^{m+n}, minimum distance d = 2^{m+n-1}, and dimension $k \ge n$.

Thus, sequence generated showed increased secrecy and increased possibility of correcting error in communication channel because it exhibited bigger length and the bigger minimum distance.

IV. ACKNOWLEDGMENTS

The authors express their gratitude to Prof. Abdulla Y Al Hawaj, Founder of Ahlia University for all the support provided.

VI. REFERENCE

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

II. Jong-Seon No, Solomon W. & Golomb," Binary Pseudorandom Sequences For period 2^n-1 with Ideal Autocorrelation*,* "IEEE Trans. Information Theory, Vol. 44 No 2, 1998, PP 814-817

III. Lee J.S &Miller L.E, "CDMA System Engineering Hand Book*,* "Artech House. Boston, London,Yang S.C,"*CDMA RF, 1998.* System Engineering, *"*ArtechHouse.Boston-London.

IV. Lidl, R.& Pilz,G., 1984. "Applied Abstract Algebra," Springer–VerlageNew York.

V. Lidl, R.& Niedereiter, H., 1994 "Introduction to Finite Fields and Their Application," Cambridge University USA.

VI. Thomson W. Judson, "2013 Abstract Algebra: Theory and Applications , " Free Software Foundation,2013.

VII. Fraleigh, J.B., 1971 "A First course In Abstract Algebra, Fourth printing. Addison- Wesley publishing compan*y* USA.

VIII. Mac Wiliams, F.G& Sloane, N.G.A., 2006 *"The Theory of Error- Correcting Codes,"* North-Holland, Amsterdam.

IX. Kacami,T. & Tokora, H., "1978Teoria Kodirovania, " Mir(MOSCOW). David, J.,2008 "Introductory Modern Algebra, "Clark University USA.

X. Sloane, N.J.A., "An Analysis Of The Stricture and Complexity Of Nonlinear Binary Sequence Generators," IEEE Trans. Information Theory Vol. It 22 No 6,1976,PP 732-736.

XI. Byrnes, J.S.; Swick."*Instant Walsh Functions"* , SIAM Review., Vol. 12 1970, pp.131.

XII. Al Cheikha A. H., Ruchin J., "Generation of Orthogonal Sequences by Walsh Sequences" International Journal of Soft Computing and Engineering . Vol.–4, Issue-1, March 2014, pp 182-184.

XIII. Al Cheikha A. H., "*Compose Walsh's Sequences and Reed Solomon Sequences*", ISERD International Conference, Cairo, Egypt, 30th December 2015, ISBN: 978-93-85832-90-1, pp 23-26.

Dr Ahmad Hamza Al Cheikha.

His Research interest

are Design Orthogonal sequences with variable length, Finite Fields, Linear and Non Linear codes, Copositive Matrices and Fuzzy Sets.