International Journal of Theoretical and Applied Mathematics
2019; 5(1): 10-20
http://www.sciencepublishinggroup.com/j/ijtam
doi: 10.11648/j.ijtam.20190501.12
ISSN: 2575-5072 (Print); ISSN: 2575-5080 (Online)

Compose Quotient Ring Sequences with Walsh's Sequences and M-Sequences

Ahmad Hamza Al Cheikha

Department of Mathematical Science, College of Arts-Science and Education, Ahlia University, Manama, Bahrain

Email address:
alcheikhaa@yahoo.com

To cite this article:
Ahmad Hamza Al Cheikha. Compose Quotient Ring Sequences with Walsh's Sequences and M-Sequences. *International Journal of Theoretical and Applied Mathematics*. Vol. 5, No. 1, 2019, pp. 10-20. doi: 10.11648/j.ijtam.20190501.12

Received: December 7, 2018; **Accepted**: April 4, 2019; **Published**: May 6, 2019

Abstract: Quotient ring sequences are completely new orthogonal sets without coders and decoders to the moment but Walsh sequences of the order 2^k, k positive integer, and M-Sequences with zero sequence form additive groups, Except the zero sequences, Walsh sequences, and M-Sequences formed orthogonal sets and used widely in the forward links and inverse links of communication channels for mixing and sifting information as in the systems CDMA and other channels. The current paper studied the orthogonal sets (which are also with the corresponding null sequence additive groups) generated through compose quotient ring sequences with self, Compose quotient ring sequences with the best and very important sequences Walsh sequences and M-sequences and by inverse for getting these new orthogonal sets or sequences with longer lengths and longer minimum distances in order to increase the confidentiality of information and increase the possibility of correcting mistakes in the communication channels.

Keywords: Quotient ring Sequences, Walsh Sequences, M-sequences, Coefficient of Correlation, Code, Orthogonal Sequences, Additive group, Span

1. Introduction

1.1. Orthogonal Quotient Ring Sequences

We can get quotient ring sequences from the Multiplication table of quotient rings $Z_{p^m} = Z/(p^m Z)$, where Z is the Integers and p is a prime number, deleting the rows which have index multiple of p, replacing each event number by "0" and each odd number by "1", and choosing one of the subsets of binary rows which each row in it contains $(p^m+1)/2$ of "0.s' and $(p^m-1)/2$ of "1.s" (Length each row is p^m) and each subset has, without zero row, a biggest orthogonal span (its size is u, where $u=\sum_{i=1}^{m+1}\binom{m+1}{i}$). These biggest orthogonal span, we say, $Q=\{q_1, q_2, ..., q_u\}$,with zero row $q_0 = r_0$ forms an additive subgroup in the vector space $2^{(p^m)}$. The number of these subsets is at most $\binom{p^m - p^{m-1}}{m+1}$. [1,2]

For $p = 2$ we get Walsh sequences. [3]

1.2. Walsh Sequence

Walsh sequences are binary sets with 2^k of rows (or sequences), except the zero row, each set is orthogonal, the length of each row is 2^k and contains 2^{k-1} of "0.s" and the same number of "1.s", and forms an additive group with the zero row where the addition performed by *mod* 2, also they are known under the name *Walsh functions*.

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

(1) Using Rademacher functions.

(2) Using Hadamard matrices. [4]

(3) Exploiting the symmetry properties of Walsh functions. [5]:

(4) Using division ring under 2^k addition. [6, 7]

1.3. Binary 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 $z_0, z_1, ...$ is called non homogeneous linear recurring sequence of order k *iff*:

$$
\begin{aligned}
&z_{n+k} = \lambda_{k-1}z_{n+k-1} + \lambda_{k-2}z_{n+k-2} + \ldots \\
&+\lambda_0 z_n + \lambda,\ \lambda_i \in F_2\ , i = 0,1,\ldots,k-1; \\
&or \quad z_{n+k} = \sum_{i=0}^{k-1} \lambda_i z_{n+i} + \lambda
\end{aligned} \tag{1}
$$

The elements $z_0, z_1, \ldots, z_{k-1}$ are called the initial values (or the vector $(z_0, z_1, \ldots, z_{k-1})$ is called the initial vector).

If $\lambda = 0$ then the sequence $z_0, z_1, \ldots$ is called homogeneous linear recurring sequence (H. L. R. S.), except the zero initial vector, and the polynomial

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

Is called the characteristic polynomial. In this study, we are limited to $\lambda_0 = 1$. [8, 9].

Orthogonal quotient rings sequences are good and important sequences absolutely new, published one month ago, linear, suitable and sufficient lengths and minimum distances, to this moment there is no coders and decoders for them.

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.

2. Research Method and Materials

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

$$z_{n+r} = z_{n;} n = 0, 1, \ldots \ [10] \tag{3}$$

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

$$\overline{X} = (\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}) \tag{4}$$

When;

$$\overline{x_i} = \begin{cases} 1 & if \quad x_i = 0 \\ 0 & if \quad x_i = 1 \end{cases}. \ [11] \tag{5}$$

Definition 3. Suppose $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ are vectors of length *n* on *GF*(2) = F_2 = {0,1}. The coefficient of correlations function of *x* and *y*,

Denoted by $R_{x,y}$, is:

$$R_{x,y} = \sum_{i=0}^{n-1} (-1)^{x_i + y_i} \quad [12] \tag{6}$$

Definition 4. Any Periodic Sequence $z_0, z_1, \ldots$. over F_2 with prime characteristic polynomial is an orthogonal cyclic code and ideal auto correlation. [13,14]

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

$$G = \{X; X = (x_0, x_1, \ldots, x_{n-1}), x_i \in F_2, i = \{0, \ldots, n-1\}\} \tag{7}$$

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

$$\forall X \in G, \sum_{i=0}^{n-1} x_i^* \in \{-1,0,1\} \quad or \quad |R_{x,0}| \le 1 \tag{8}$$

$$\forall X, Y \in G \ and \ X \ne Y, \sum_{i=0}^{n-1} x_i^* y_i^* \in \{-1,0,1\}, \ or \ldots |R_{x,y}| \le 1 \tag{9}$$

That is, the absolute value of "the number of agreements minus the number of disagreements" is equal to or less than 1. [15]

Definition 6. *Hamming distance* $d(x, y)$: The Hamming distance between the binary vectors $x = (x_0, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ is the number of the disagreements of the corresponding components of *x* and *y*. [16]

Definition 7. 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 $\overline{\omega}$.

Corollary 1. 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. [17]

Theorem2.

If $a_0, a_1, \ldots$. is a homogeneous linear recurring sequence of order *k* in F_2, satisfies (1) then this sequence is periodic.

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. [18, 19]

3. Results and Discussions (Findings)

3.1. Compose Quotient Ring Sequences with Other Quotient Ring Sequences

Suppose $Q_1 = \{q_1, q_2, \ldots, q_{u_1}\}$ and $Q_2 = \{q_1^{'}, q_2^{'}, \ldots, q_{u_2}^{'}\}$ are two orthogonal quotient rings sequences generated from binary representation of $Z_{p_1^m}, Z_{p_2^n}$ respectively, then in $Q_1(Q_2)$:

Table 1. *The numbers of "1.s" and "0.s" in each sequence of* Q_1 *and* Q_2 *.*

Q_1		Q_2	
Number of "1.s"	**Number of "0.s"**	**Number of "1.s"**	**Number of "0.s"**
$\frac{p_1^m-1}{2}$	$\frac{p_1^m+1}{2}$	$\frac{p_2^n-1}{2}$	$\frac{p_2^n+1}{2}$

A) For $q_k^{'} \in Q_2$ we define the set:

$A_k = Q_1\left(q_k^{'}\right) = \{a_i = q_i\left(q_k^{'}\right), q_i \in Q_1\}$ then:

(1) The number of "1.s" in a_i is:

$$\left(\frac{p_1^m-1}{2}\right)\left(\frac{p_2^n-1}{2}\right)+\left(\frac{p_1^m+1}{2}\right)\left(\frac{p_2^n+1}{2}\right)=\frac{p_1^m p_2^n+1}{2}$$

(2) The number of "0.s" in a_i is:

$$\left(\frac{p_1^m-1}{2}\right)\left(\frac{p_2^n+1}{2}\right)+\left(\frac{p_1^m+1}{2}\right)\left(\frac{p_2^n-1}{2}\right)=\frac{p_1^m p_2^n-1}{2}$$

(3) The difference between the number of "1"s and the number of "0"s is one

b) For $a_i, a_j \in A_k$ and $i \neq j$, $a_i + a_j = q_i(q_k^{'}) + q_j(q_k^{'})$

$a_i + a_j = (q_i + q_j)(11...1)_{p_2^n}$ and $a_i + a_j \neq (q_i + q_j)(q_k^{'})$

(4) The number of "1.s" in $a_i + a_j$ is $\frac{p_1^m-1}{2}(p_2^n)$, the number of "0.s" in $a_i + a_j$ is $\frac{p_1^m+1}{2}(p_2^n)$

(5) The difference between the number of "0.s" and the number of "1.s" is p_2^n

Thus, A_k is not an orthogonal set and $Q_1\left(Q_2\right)$ are not orthogonal sets.

c) By symmetric property $Q_2\left(Q_1\right)$ are not orthogonal sets.

d) By the same way for $q_i, q_j \in Q_1$ and $i \neq j$, then $\overline{q}_i, \overline{q}_j$ satisfies the first orthogonal condition but: $\overline{q}_i(q_k^{'}) + \overline{q}_j(q_k^{'}) = (\overline{q}_i + \overline{q}_j)(00...0)_{p_2^n}$ and

(6) The number of "0"s in $\overline{q}_i(q_k^{'}) + \overline{q}_j(q_k^{'})$ is $\frac{p_1^m+1}{2}(p_2^n)$

The number of "1"s in $\overline{q}_i(q_k^{'}) + \overline{q}_j(q_k^{'})$ is $\frac{p_1^m-1}{2}(p_2^n)$.

(7) The difference between the number of "0.s" and the number of "1.s" is p_2^n. Thus, $\overline{Q}_1\left(Q_2\right)$ are not orthogonal sets also $\overline{Q}_1\left(Q_2\right)$, $Q_1\left(\overline{Q}_2\right)$, and $\overline{Q}_1\left(\overline{Q}_2\right)$ are not orthogonal sets.

e) If we redefine the addition on $A_k = Q_1(q_k^{'})$ as following:

For $a_i, a_j \in A_k$, $a_i \oplus a_j = (q_i + q_j)(q_k^{'})$ then the number of "1.s" in $a_i \oplus a_j$ is $\frac{p_1^m p_2^n+1}{2}$, the number of "0.s" is $\frac{p_1^m p_2^n-1}{2}$, and the difference between the number of "1.s" and the number of "0.s" is one in this cause $(Q_1(Q_2),\oplus)$ and $Q_2(Q_1),\oplus)$ are orthogonal sets.

f) Extending Q_1, Q_2 to $\tilde{Q}_1$, $\tilde{Q}_2$ respectively by adding "1" or "0" to the end (or starting) of each sequence in Q_1, Q_2, then $\tilde{Q}_1(\tilde{q}_1^{'})$, $\bar{\tilde{Q}}_1(\tilde{q}_1^{'})$, $\bar{\tilde{Q}}_1(\bar{\tilde{q}}_1)$ are not orthogonal sets.

3.2. Compose Quotient Ring Sequences with Walsh Sequences and Increase

3.2.1. Compose Quotient Ring Sequences with Walsh Sequences

Suppose $Q = \{q_1, q_2, ..., q_u\}$ is an orthogonal quotient ring sequences generated from binary representation of Z_{p^m} and $W = \{w_1, w_2, ..., w_{2^n-1}\}$ is a Walsh sequences of order 2^n without zero sequences w_0 sequences, then in $Q(W)$.

Table 2. *The numbers of "1.s" and "0.s" in each sequence of Q and W.*

Q		***W***	
Number of "1.s"	Number of "0.s"	Number of "1.s"	Number of "0.s"
$\frac{p^m-1}{2}$	$\frac{p^m+1}{2}$	2^{n-1}	2^{n-1}

a) For $w_k \in W$ we define the set $B_k = Q\left(w_k\right) = \{b_i = q_i\left(w_k\right), q_i \in Q\}$ then:

(1) The number of "1.s" in b_i is

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

(2) The number of "0.s" in b_i is

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

(3) The difference between the number of "1.s" and the number of "0.s" is zero

b) For $b_i, b_j \in B_k$ and $i \neq j$, $b_i + b_j = (q_i)(w_k) + (q_j)(w_k) = (q_i + q_j)(11...1)_{2^n}$ and the difference between the number of "1.s" and the number of "0.s" is 2^n.

Thus B_k is not orthogonal set and $(Q)(W)$ are not orthogonal sets.

c) if redefining on $Q(W)$ the operation $\oplus$ as following for $b_i, b_j \in B_k$ and $i \neq j$, $b_i \oplus b_j = (q_i + q_j)(w_k)$ in this cause.

The number of "1.s" and the number of "0.s" in $\tilde{b}_i$ is $2^{n-1}p^m$, the difference between them is zero.

The number of "1.s" in $b_i \oplus b_j$ is $2^{n-1}p^m$, the number of "0.s" in $b_i \oplus b_j$ is $2^{n-1}p^m$.

The difference between the number of "1.s" and the number of "0.s" in b_i and $b_i \oplus b_j$ is zero.

Thus $(B_k, \oplus)$ is an orthogonal set and $Q(W), \oplus)$ are orthogonal sets.

3.2.2. Compose Walsh Sequences with Quotient Ring Sequence

Suppose $Q = \{q_1, q_2, ..., q_u\}$ is an orthogonal quotient ring sequences generated from binary representation of Z_{p^m} and $W = \{w_1, w_2, ..., w_{2^n-1}\}$ is a Walsh sequences of order 2^n without zero sequences w_0 sequences, then in $W(Q)$

Table 3. The numbers of "1.s" and "0.s" in each sequence of W and Q

W		**Q**	
Number of "1.s"	Number of "0.s"	Number of "1.s"	Number of "0.s"
2^{n-1}	2^{n-1}	$(p^m$-1)/2	$(p^m$+1)/2

a) For $q_k \in Q$ we define the set $\tilde{B}_k = W(q_k) = \{\tilde{b}_i = w_i(q_k), w_i \in W\}$ then

* The number of "1.s" and the number of "0.s" in $\tilde{b}_i$ is $2^{n-1}p^m$, the difference between them is zero.

For $\tilde{b}_i, \tilde{b}_j \in \tilde{B}_k$ and $i \neq j$, $\tilde{b}_i + \tilde{b}_j = (w_i)(q_k) + (w_j)(q_k) = (w_i + w_j)(11..1)_{p^m}$, the number of "1.s" and the number of "0.s" in $\tilde{b}_i + \tilde{b}_j$ is $2^{n-1}p^m$, and the difference between the number of "1.s" and the number of "0.s" is zero.

Thus $\tilde{B}_k$ is an orthogonal set and $W(Q)$ are orthogonal sets.

b) If redefining on $W(Q)$ the operation $\oplus$ as following for $\tilde{b}_i, \tilde{b}_j \in \tilde{B}_k$ and $i \neq j$, $\tilde{b}_i \oplus \tilde{b}_j = (w_i + w_j)(q_k)$ in this case.

In $\tilde{b}_i \oplus \tilde{b}_j$, the number of "1.s" is $2^{n-1}p^m$, the number of "0.s" is $2^{n-1}p^m$, the difference between them is zero, $(\tilde{B}_k, \oplus)$ is an orthogonal set, and $(W(Q), \oplus)$ are orthogonal sets.

3.3. Compose Quotient Ring Sequences and M-Sequences and Inverse

3.3.1. Compose Quotient Ring Sequences and M-Sequences

Suppose $Q = \{q_1, q_2, ..., q_u\}$ is an orthogonal quotient ring sequences generated from binary representation of Z_{p^m} and a_1 is a non zero M-Sequence generated by the non homogeneous linear recurring sequence (1) of order n with the prime characteristic polynomial.

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

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

Table 4. The numbers of "1.s" and "0.s" in each sequence of Q and A.

Q		**A**	
Number of "1.s"	Number of "0.s"	Number of "1.s"	Number of "0.s"
$\frac{p^m - 1}{2}$	$\frac{p^m + 1}{2}$	2^{n-1}	$2^{n-1} - 1$

a) For $a_k \in A$ we define the set $C_k = Q(a_k) = \{c_i = q_i(a_k), q_i \in Q\}$ then.

(1) The number of "1.s" in c_i is

$$\left(\frac{p^m - 1}{2}\right)\left(2^{n-1}\right) + \left(\frac{p^m + 1}{2}\right)\left(2^{n-1} - 1\right) = \left(\frac{2^n p^m - p^m - 1}{2}\right).$$

(2) The number of "0.s" in c_i is

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

(3) The difference between the number of "0.s" and the number of "1.s" is one

(4) For $c_i, c_j \in C_k$ and $i \neq j$, $c_i + c_j = (q_i + q_j)(11...1)_{2^n-1}$,

the number of "1.s" in $c_i + c_j$ is;

$\frac{(2^n-1)(p^m-1)}{2}$, the number of "0.s" in $c_i + c_j$ is $\frac{(2^n-1)(p^m+1)}{2}$, and the difference between the number of "0.s" and the number of "1.s" is $2^n - 1$.

Thus C_k is not orthogonal set and $Q(A)$ are not orthogonal sets.

b) Redefining on $Q(A)$ the operation $\oplus$ as following for $c_i, c_j \in C_k$ and $i \neq j$, $c_i \oplus c_j = (q_i + q_j)(a_k)$, in $c_i \oplus c_j$ the number of "1.s" is $\frac{2^n p^m - p^m - 1}{2}$, the number of "0.s" is $\frac{2^n p^m - p^m + 1}{2}$, and the difference between the number of "0.s" and the number of "1.s" is one.

Thus $(C_k, \oplus)$ is an orthogonal set and $(Q(A), \oplus)$ are orthogonal sets.

3.3.2. Compose M-Sequences and Quotient Ring Sequences and Finding $A(Q)$

Table 5. *The numbers of "1.s" and "0.s" in each sequence of A and Q.*

A		***Q***	
Number of "1.s"	Number of "0.s"	Number of "1.s"	Number of "0.s"
2^{n-1}	$2^{n-1}-1$	$(p^m$-1)/2	$(p^m$+1)/2

a) For $q_k \in Q$ we define the set $\tilde{C}_k = A(q_k) = \{\tilde{c}_i = a_i(q_k), a_i \in A\}$ then.

(1) The number of "1.s" in c_i is $\left(\frac{2^n p^m - p^m - 1}{2}\right)$, the number of "0.s" in c_i is $\left(\frac{2^n p^m - p^m + 1}{2}\right)$.

(2) The difference between the number of "0.s" and the number of "1.s" is one

b) For $\tilde{c}_i, \tilde{c}_j \in \tilde{C}_k$ and $i \neq j$, $\tilde{c}_i + \tilde{c}_j = (a_i + a_j)(11...1)_{p^m}$, in $\tilde{c}_i + \tilde{c}_j$ the number of "1.s" is

$2^{n-1} p^m$, the number of "0.s" is $(2^{n-1}-1)p^m$, and the difference between the number of "1.s" and the number of "0.s" is p^m.

Thus $\tilde{C}_k$ is not orthogonal set and $A(Q)$ are not orthogonal sets.

c) Redefining on $A(Q)$ the operation $\oplus$ as following for $q_k \in Q$ and $i \neq j$, $\tilde{c}_i \oplus \tilde{c}_j = (a_i + a_j)(q_k)$, in $\tilde{c}_i \oplus \tilde{c}_j$ the number of "1.s" is $\frac{2^n p^m - p^m - 1}{2}$, the number of "0.s" is $\frac{2^n p^m - p^m + 1}{2}$, and the difference between the number of "0.s"and the number of "1.s" is one.

Thus $(\tilde{C}_k, \oplus)$ is an orthogonal set and $A(Q), \oplus)$ are orthogonal sets.

Example 1. For p =5, Table 1. Contains the multiplication on Z_5 and their binary representation.

Table 6. *.Multiplication on Z_5 and their binary representation.*

	*	0	1	2	3	4			*	0	1	2	3	4
R0	0	0	0	0	0	0		r_0	0	0	0	0	0	0
R1	1	0	1	2	3	4		r_1	1	0	1	0	1	0
R2	2	0	2	4	1	3	$\Rightarrow$	r_2	2	0	0	0	1	1
R3	3	0	3	1	4	2		r_3	3	0	1	1	0	0
R4	4	0	4	3	2	1		r_4	4	0	0	1	0	1

Each of r_1 and r_2 contains $3 = \frac{5+1}{2}$ of "0.s" and $2 = \frac{5-1}{2}$ of "1.s" and $r_1 + r_2$ contains also 3 of "0.s" and 2 of "1.s", but $r_1 + r_4 = r_2 + r_3 =$ [0 1 1 1 1], where "+" is the ordinary addition and performed by *mod* 2, $span\{r_1, r_2\}$, without

$r_0 = q_0$, is $Q_1 = \{q_1 = r_1, q_2 = r_2, q_3 = r_1 + r_2\}$ is a biggest orthogonal set, where $q_1 = (01010)$, $q_2 = (00011)$,

$q_3 = (01001)$, and $Span\{r_1, r_2\} = \{q_0, q_1, q_2, q_3\}$ is a subgroup in the binary vector space of order 2^5 for addition and $q_2 = (00011)$, $q_3 = (01001)$, and $Span\{r_1, r_2\} = \{q_0, q_1, q_2, q_3\}$ is a subgroup in the binary vector space of order 2^5 for addition and.

Table 7. *Span $\{r_1, r_2\}$ without $q_0 = r_0$.*

q_1	0	1	0	1	0
q_2	0	0	0	1	1
q_3	0	1	0	0	1

Example 2. For $p = 3$, Table 2 showing binary representation of Z_{3^2}

Table 8. *Binary Representation of Z_{3^2} .*

	*	0	1	2	3	4	5	6	7	8
r_0'	0	0	0	0	0	0	0	0	0	0
r_1'	1	0	1	0	1	0	1	0	1	0
r_2'	2	0	0	0	0	0	1	1	1	1
r_3'	3	0	1	0	0	1	0	0	1	0
r_4'	4	0	0	0	1	1	0	0	1	1
r_5'	5	0	1	1	0	0	1	1	0	0
r_6'	6	0	0	1	0	0	1	0	0	1
r_7'	7	0	1	1	1	1	0	0	0	0
r_8'	8	0	0	1	0	1	0	1	0	1

We can see that $Span\{r_1', r_2', r_4'\} = \{r_1', r_2', r_4', r_1' + r_2', r_1' + r_4', r_2' + r_4'\}$ is a maximum closed orthogonal set contained in F_{2^9}.

Thus $Q_2 = \{q_1', q_2', q_3', q_4', q_5', q_6'\}$ where $q_1' = r_1' = (010101010)$, $q_2' = r_2' = (000001111)$, $q_3' = r_3' = (000110011)$, $q_4' = (010100101)$, $q_5' = (010011001)$, $q_6' = (000111100)$.

a) Finding $Q_1(q_1')$, where $q_1' = (010101010)$, $\overline{q_1'} = (101010101)$.

Table 9. *Compose Q_1 with q_1' from Q_2 .*

$q_1(q_1')$	101010101	010101010	101010101	010101010	101010101
$q_2(q_1')$	101010101	101010101	101010101	010101010	010101010
$q_3(q_1')$	101010101	010101010	101010101	101010101	010101010
$a_1 + a_2 = q_1(q_1') + q_2(q_1')$	000000000	111111111	000000000	000000000	111111111

Thus $p_1 = 5, m_1 = 1, p_2 = 3, m_2 = 2$ and.

Each row contains $\frac{p_1^m p_2^n + 1}{2} = \frac{5(3^2)+1}{2} = 23$ of "1.s", and $\frac{p_1^m p_2^n - 1}{2} = \frac{5(3^2)-1}{2} = 22$ of "0.s".

The difference between the number of "1.s" and the number of "0.s is one but $q_1(q_1') + q_2(q_1')$ contains 18 of "0.s", 27 of "0.s" and the difference between the number of "0.s" and the number of "1.s" is $3^2 = 9$ and $A_k = Q_1(q_k')$ not orthogonal set or $Q_1(Q_2)$ are not orthogonal sets.

b) If we redefine the addition on $A_k = Q_1(q_k')$ as following, For $a_i, a_j \in A_k$, $a_i \oplus a_j = (q_i + q_j)(q_k)$ then, the number of "1.s" in $a_i \oplus a_j$ is $\frac{p_1^m p_2^n + 1}{2}$, the number of "0.s" is $\frac{p_1^m p_2^n - 1}{2}$ and the difference between the number of "1.s" and the number of "0"s is one.

Table 10. *Compose q_1 and q_2 from Q_1 .*

$a_1 \oplus a_2 = (q_1 + q_2)(q_1') = q_3(q_1')$	101010101	010101010	101010101	101010101	010101010

$a_1 \oplus a_2$ Contains 23 of "1.s", 22 of "0.s" thus, $A_k = Q_1(q_k')$ is an orthogonal set and $Q_1(Q_2)$ with the operation ⊕ in this case are orthogonal sets.

c) Also $\overline{q}_i(q_k)+\overline{q}_j(q_k)$ is not orthogonal set, For example, calculate $\overline{q}_1(q_1)+\overline{q}_2(q_1)$ we have.

Table 11. *Complements of q_1 and q_2 from Q_1.*

$\overline{q}_1$	1	0	1	0	1
$\overline{q}_2$	1	1	1	0	0

Table 12. *Span*{ $\overline{q}_1(q_1^{'})$, $\overline{q}_2(q_1^{'})$ }.*

$\overline{q}_1(q_1^{'})$	010101010	101010101	010101010	101010101	011010101
$\overline{q}_2(q_1^{'})$	010101010	010101010	010101010	101010101	101010101
$\overline{q}_1(q_1^{'})+\overline{q}_2(q_1^{'})$	000000000	111111111	000000000	000000000	111111111

Thus, $\overline{q}_1(q_1^{'})+\overline{q}_2(q_1^{'}) = (\overline{q}_1+\overline{q}_2)(111111111)$ and $\overline{Q}_1(q_1)$ is not orthogonal set or $\overline{Q}_1(Q_2)$ are not orthogonal sets.

d) Extending Q_1 , Q_2 to $\tilde{Q}_1, \tilde{Q}_2$ respectively by adding "1" or "0"to the end (or starting) of each sequence in Q_1 , Q_2 , then $\tilde{Q}_1(q_1^{'}), \tilde{Q}_1(\tilde{q}_1^{'}), \bar{\tilde{Q}}_1(\tilde{q}_1^{'}), \bar{\tilde{Q}}_1(\bar{\tilde{q}}_1)$ are not orthogonal sets, for example:

Table 13. *Extending q_1 and q_2 from Q_1.*

$\tilde{q}_1$	0	1	0	1	0	0
$\tilde{q}_2$	0	0	0	1	1	0

Table 14. *Span*{ $\tilde{q}_1(q_1')$, $\tilde{q}_2(q_1')$ }.*

$\tilde{q}_1(q_1')$	101010101	010101010	101010101	010101010	101010101	101010101
$\tilde{q}_2(q_1')$	101010101	101010101	101010101	010101010	010101010	101010101
$\tilde{q}_1(q_1')+\tilde{q}_2(q_1')$	000000000	111111111	000000000	000000000	111111111	000000000

Thus, $\tilde{q}_1(q_1')$ + $\tilde{q}_2(q_1')$ = $(\tilde{q}_1+\tilde{q}_2)(000000000)$ and $\tilde{Q}_1(q_1)$ is not orthogonal set or $\tilde{Q}_1(Q_2)$ are not orthogonal sets.

Example 3. The following table showing Walsh sequences of order $8=2^3$ without null sequence.

Table 15. *Walsh Sequences of order 8=2^3.*

w_1 = 0 0 0 0 1 1 1 1
w_1 = 0 0 0 0 1 1 1 1
w_1 = 0 0 0 0 1 1 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

Suppose Q is as in example1, W is a set of Walsh Sequences of order 2^n,

a) Compose Q with W or $Q(W)$ and $B_k = Q(w_k) = \{b_i = q_i(w_k), q_i \in Q\}$, (for example $Q(W_{2^3})$ and B_1) then.

The number of "1.s" of each b_i is $2^{n-1}p^m$ **, (**in the example = $2^2(5)=20$ **).**

The number of "0.s" of each b_i is $2^{n-1}p^m$ **, (**in the example = $2^2(5)=20$ **).**

The difference between the number of "1.s" and the number of "0.s" is zero. For w_1 = (01010101), w_2 = (10101010).

Table 16. *Compose Q_1 with w_1 from W.*

$q_1(w_1)$	10101010	01010101	10101010	01010101	10101010
$q_2(w_1)$	10101010	10101010	10101010	01010101	01010101
$q_3(w_1)$	10101010	01010101	10101010	10101010	01010101
$q_1(w_1)+q_2(w_1)$	00000000	11111111	00000000	00000000	11111111

Thus, $q_1(w_1) + q_2(w_1)$ contains 16 of "1.s" and 24 of "0.s" and the difference between the number of "1.s" and the number of "0.s" is $2^n = 2^3 = 8$, and $Q(W_{2^3})$ or $Q(W)$ are not orthogonal sets.

Redefining on $Q(W)$ the operation $\oplus$ as following for $b_i, b_j \in B_k$ and $i \neq j$ as $b_i \oplus b_j = (q_i + q_j)(w_k)$ in this case (in the example $b_1 \oplus b_2 = (q_1 + q_2)(w_1) = q_3(w_1)$) and.

Table 17. *Compose q_1+q_2 = q_3 with w_1 from W.*

$q_1 \oplus q_2 = q_3(w_1)$	10101010	01010101	10101010	10101010	01010101

The number of "1"s in $b_i \oplus b_j$ is $2^{n-1}p^m$, (In the example =20)

The number of "0"s in $b_i \oplus b_j$ is. $2^{n-1}p^m$, (In the example =20)

The difference between the number of "1.s" and the number of "0.s" in b_i and $b_i \oplus b_j$ is zero.

Thus B_k is an orthogonal set and $(Q)(W)$ are orthogonal sets.

Example 4. Compose Walsh sequences with quotient ring sequences.

a) Compose W with Q or $W(Q)$ and $\tilde{B}_k = W(q_k) = \{\tilde{b}_i = w_i(q_i), w_i \in W\}$ (for example $W_{2^3}(Q)$ and $\tilde{B}_1$) then.

The number of "1.s" of each $\tilde{b}_i$ is $2^{n-1}p^m$, (in the example = $2^2(5) = 20$).

The number of "0.s" of each $\tilde{b}_i$ is $2^{n-1}p^m$, (in the example = $2^2(5) = 20$).

The difference between the number of "1.s" and the number of "0.s" is zero, $q_1 = (01010)$, $\overline{q_1} = (10101)$ and.

Table 18. *Compose W with q_1 from Q_1.*

$w_1(q_1)$	10101	10101	10101	10101	01010	01010	01010	01010
$w_2(q_1)$	10101	10101	01010	01010	01010	01010	10101	10101
$w_3(q_1)$	10101	10101	01010	01010	10101	10101	01010	01010
$w_4(q_1)$	10101	01010	01010	10101	10101	01010	01010	10101
$w_5(q_1)$	10101	01010	01010	10101	01010	10101	10101	01010
$w_6(q_1)$	10101	01010	10101	01010	01010	10101	01010	10101
$w_7(q_1)$	10101	01010	10101	01010	10101	01010	10101	01010
$w_1(q_1)+w_2(q_1)=w_3(q_1)$	00000	00000	11111	11111	00000	00000	11111	11111

For $i \neq j$ in $\tilde{b}_i + \tilde{b}_j$, the number of "1.s" and the number of "0.s" is $2^{n-1}p^m = 20$, and the difference between the number of "1.s" and the number of "0.s" is zero.

Thus $(\tilde{B}_k,+)$ is an orthogonal set and $(W(Q),+)$ are orthogonal sets.

b) Redefining on $W(Q)$ the operation $\oplus$ as following for $\tilde{b}_i, \tilde{b}_j \in \tilde{B}_k$ and $i \neq j$ as $\tilde{b}_i \oplus \tilde{b}_j = (w_i + w_j)(q_k)$ in this case (in the example $\tilde{b}_1 \oplus \tilde{b}_2 = (w_1 + w_2)(q_1) = w_3(q_1)$).

Table 19. *Compose w_1 + w_2 = w_3 from W with q_1 from Q_1 .*

$\tilde{b}_1 \oplus \tilde{b}_2 = w_3(q_1)$	10101	10101	01010	01010	10101	10101	01010	01010

(4) The number of "1.s" in $\tilde{b}_i \oplus \tilde{b}_j$ is $2^{n-1}p^m$, (In example =20)

(5) The number of "0.s" in $\tilde{b}_i \oplus \tilde{b}_j$ is $2^{n-1}p^m$, (In example =20)·

(6) The difference between the number of "1.s" and the number of "0.s" in b_i and $\tilde{b}_i \oplus \tilde{b}_j$ is zero.

Thus $\tilde{B}_k$ is an orthogonal set and $W(Q)$ are orthogonal sets.

Example 5. Given $Q = \{q_1, q_2, q_3\}$ orthogonal quotient ring sequences generated from binary representation of Z_5 (as in the example1., p = 5 and m = 1) and a_1 is a non zero M-Sequence generated by the non homogeneous linear recurring sequence.

$$z_{n+2} = z_{n+1} + z_n \text{ or } z_{n+2} = z_{n+1} + z_n$$

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.

Table 20. *A = M-Sequences of order 3.*

a_1	1	0	1
a_2	1	1	0
a_3	0	1	1

Compos Q and A or finding $Q(A)$ $a_1 = (101)$, $\overline{a_1} = (010)$

Table 21. Elements Q_1 .

q_1	0	1	0	1	0
q_2	0	0	0	1	1
q_3	0	1	0	0	1

Table 22. Compose Q_1 with a_1 from A .

$q_1(a_1)$	010	101	010	101	010
$q_2(a_1)$	010	010	010	101	101
$q_3(a_1)$	010	101	010	010	101
$q_1(a_1)+q_2(a_1)=q_3(a_1)$	000	111	000	000	111

a) For $a_k \in A$ we define the set $C_k = Q\left(a_k\right) = c_i = q_i\left(a_k\right), q_i \in Q\}$ then.

(1) The number of "1.s" in c_i is $\left(\dfrac{2^n p^m - p^m - 1}{2}\right) = \dfrac{4(5)-5-1}{2} = 7$

(2) The number of "0.s" in c_i is $\left(\dfrac{2^n p^m - p^m - 1}{2}\right) = \dfrac{4(5)-5+1}{2} = 8$

(3) The difference between the number of "0.s" and the number of "1.s" is one.

b) For $c_i, c_j \in C_k$ and $i \neq j$ the $c_i + c_j = (q_i + q_j)(111)$ and the number of "1.s" in $c_i + c_j$ is $\dfrac{(2^n-1)(p^m-1)}{2} = 6$ the number of "0.s" in $c_i + c_j$ is $\dfrac{(2^n-1)(p^m+1)}{2} = 9$ and the difference between the number of "0.s" and the number of "1.s" is $2^n - 1 = 3$.

Thus C_k is not orthogonal set and $Q(A)$ are not orthogonal sets.

c) Redefining on $Q(A)$ the operation $\oplus$ as following for $c_i, c_j \in C_k$ and $i \neq j$ as $c_i \oplus c_j = (q_i + q_j)(a_k)$ in this case (in the example $c_1 \oplus c_2 = (q_1 + q_2)(a_1) = q_3(a_1)$) and.

Table 23. *Compose $q_1 + q_2 = q_3$ from Q_1 with a_1 from A.*

$c_1 \oplus c_2 = q_3(a_1)$	010	101	010	101	010

The number of "1.s" in $c_i \oplus c_j$ is $\dfrac{2^n p^m - p^m - 1}{2}$, (In example =7)

The number of "0.s" in $c_i \oplus c_j$ is $\dfrac{2^n p^m - p^m + 1}{2}$, (In example = 8)

The difference between the number of "0.s" and the number of "1.s" in $c_i \oplus c_j$ is one.

Thus $(C_k, \oplus)$ is an orthogonal set and $(Q(A), \oplus)$ are orthogonal sets.

d) For $\tilde{C}_k = A\left(q_k\right) = \tilde{c}_i = a_i\left(q_k\right), a_i \in A\}$

(7) The number of "1.s" in $\tilde{c}_i$ is $\left(\dfrac{2^n p^m - p^m - 1}{2}\right) = \dfrac{4(5)-5-1}{2} = 7$

(8) The number of "0.s" in $\tilde{c}_i$ is $\left(\dfrac{2^n p^m - p^m - 1}{2}\right) = \dfrac{4(5)-5+1}{2} = 8$

(9) The difference between the number of "0.s" and the number of "1.s" is one.

e) For $\tilde{c}_i, \tilde{c}_j \in \tilde{C}_k$ and $i \neq j$ the $\tilde{c}_i + \tilde{c}_j = (a_i + a_j)(11...1)_{p^m}$ in $\tilde{c}_i + \tilde{c}_j$ the number of "1.s" is $\dfrac{(2^n-1)(p^m-1)}{2} = 6$ the number of "0.s" is $\dfrac{(2^n-1)(p^m+1)}{2} = 9$ and the difference between the number of "0.s" and the number of "1.s" is $p^m = 3^1 = 3$.

Thus $\tilde{C}_k$ is not orthogonal set and $A(Q)$ are not orthogonal sets.

f) Redefining on $A(Q)$ the operation $\oplus$ as following for $\tilde{c}_i, \tilde{c}_j \in \tilde{C}_k$ and $i \neq j$ as $\tilde{c}_i \oplus \tilde{c}_j = (a_i + a_j)(q_k)$ in this case (in the example $\tilde{c}_1 \oplus \tilde{c}_2 = (a_1 + a_2)(q_1) = a_3(q_1)$)

Table 24. *Compose $a_1 + a_2 = a_3$ from A with q_1 from Q_1.*

$\tilde{c}_1 \oplus \tilde{c}_2 = a_3(q_1)$	10101	01010	01010

The number of "1"s in $\tilde{c}_i \oplus \tilde{c}_j$ is $\frac{2^n p^m - p^m - 1}{2}$, (In example =7)

The number of "0"s in $\tilde{c}_i \oplus \tilde{c}_j$ is $\frac{2^n p^m - p^m + 1}{2}$, (In example = 8)

The difference between the number of "0.s" and the number of "1.s" in $\tilde{c}_i \oplus \tilde{c}_j$ is one.

Thus $(\tilde{C}_k, \oplus)$ is an orthogonal set and $(A(Q), \oplus)$ are orthogonal sets.

4. Conclusion

Suppose Q is an orthogonal quotient ring obtained from binary representation of Z_{p^m}, W is a Walsh sequences of order 2^n, and A is a M-Sequences, + is the ordinary addition *mod* 2, and $\oplus$ is a special addition *mod* 2 then

4.1. For Compose Quotient Ring Sequences with Other Quotient Ring Sequences

The $(Q_1(Q_2),+)$ and $(Q_2(Q_1),+)$ are not orthogonal sets, $(Q_1(Q_2),\oplus)$ and $(Q_2(Q_1),\oplus)$ are orthogonal sets with the length $N = p_1^m p_2^n$, minimum distance $d = \frac{p_1^m p_2^n + 1}{2}$, not linear, not cyclic, and dimension $k \geq m$, $k \geq n$ respectively.

For compose quotient ring sequences with other Walsh's Sequences or in inverse

(a) The $(Q(W),+)$ are not orthogonal sets, $(Q(W),\oplus)$ are orthogonal sets with the length $N = 2^n p^m$, minimum distance $d = 2^{n-1} p^m$, not linear, not cyclic, and dimension $k \geq m$

(b) The $(W(Q),+)$ and $(W(Q),\oplus)$ are orthogonal sets with the length $N = 2^n p^m$, minimum distance $d = 2^{n-1} p^m$, not linear, not cyclic, and dimension $k \geq n$.

4.2. For Compose Quotient Ring Sequences with Other M-Sequences or in Inverse

(c) The $(Q(A),+)$ are not orthogonal sets, $(Q(A),\oplus)$ are orthogonal sets with the length $N = (2^n - 1)p^m$, minimum distance $d = \frac{2^n p^m - p^m - 1}{2}$, not linear, not cyclic, and dimension $k \geq m$.

(d) The $(A(Q),+)$ are not orthogonal sets, $(A(Q),\oplus)$ are orthogonal sets with the length $N = (2^n - 1)p^m$, minimum distance $d = \frac{2^n p^m - p^m - 1}{2}$, not linear, not cyclic, and dimension $k \geq n$.

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.

Limitation

This method of compose sequences is useful for only binary sequences and the addition on the sequences computed by "*mod* 2" also used Microsoft Word 2010 and the Microsoft equation 3.0 for written the math equations.

The method for reading a page which has a block will be according to the following direction as in figure1.

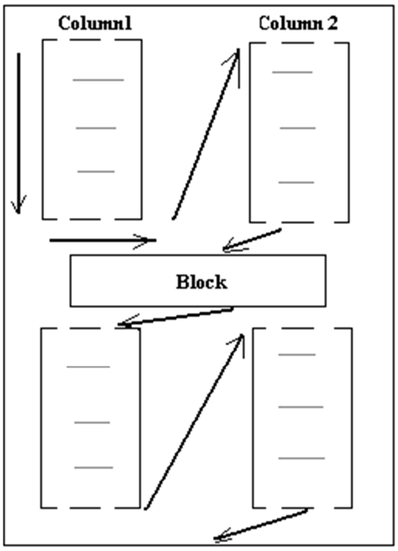

Figure 1. *Method reading page with block.*

Acknowledgements

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

References

[1] Al Cheikha A. H. (2018; 2, 11), "Generating new binary orthogonal sequences using quotient rings Z/p^mZ", Research Journal of Mathematics and Computer Science (RJMCS), pp 1-13.

[2] Al Cheikha A. H. (2016), "Compose Walsh's Sequences and M-Sequences", International journal of computer and technology (IJCT), Vol. 15, No. 7, 2016. pp. 6933- 6939.

[3] Byrnes, J. S., Swick, D. A. (1970*), "Instant Walsh Functions"*, (SIAM Review., Vol. 12, pp.131.

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

[5] Thomson, J. T. (2013), "Abstract Algebra Theory and Applications," Free Software Foundation.

[6] Al Cheikha A. H. (2005), "Isomorphic Sequences Sets Generation of the Walsh Sequences", Qatar University Science Journal Vol. 25, 2005. pp. 16-30.

[7] Lidl, R., Pilz, G. (1984), "Applied Abstract Algebra", New York Springer-Verlage New York.

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

[9] Lidl, R., Nidereiter, H. (1994), "Introduction to Finite Fields and Their Application," *Cambridge University* USA,.

[10] Sloane, N. J. A. (1076), "An Analysis Of The Stricture and Complexity Of Nonlinear Binary Sequence Generators," IEEE Trans. Information Theory Vol. It 22, No 6, PP 732- 736.

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

[12] Jong, N. S., Golomb, S. W., Gong, G., Lee, H. K., Gaal, P. (1998), "Binary Pseudorandom Sequences For period 2^n-1 with Ideal Autocorrelation*,*" IEEE Trans. Information Theor*y*, Vol. 44 No 2, PP. 814-817.

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

[14] Yang, K., Kim, Y. K., Kumar, P. V. (2000), "Quasi–orthogonal Sequences for code – Division Multiple Access Systems," *IEEE Trans. information theory*, Vol. 46 No3, Pp. 982- 993,.

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

[16] Kacami, T., Tokora, H. (1978), "Teoria Kodirovania", MOSCOW: Mir.

[17] Al Cheikha A. H. (July, 2017). Compose M-Sequences. Australian Journal of Business, Social Science and Information Technology. AJBSSIT. Vol. 3, Issue 3. Pp. 119-126. (Australia and New Zealand Business and Social Science Research Conference (ANZBSRC) 2016).

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

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