Research Article **RJMCS (2018) 2:11**

Research Journal of Mathematics and Computer Science
(ISSN:2576-3989)

Generating New Orthogonal Binary Sequences Using Quotient Rings $Z/p^m Z$

Dr. Ahmad Hamza Al Cheikha

Dep. of Mathematical Science, College of Arts-science and Education, Ahlia Uni., Manama, Bahrain

ABSTRACT

Orthogonal Sequences (as M-Sequences, Walsh Sequences, ...) 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 a correct form, especially in the pilot channels, the Sync channels, and the Traffic channel. This research is useful to generate new sets of orthogonal 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) from quotient rings Z/pmZ, where Z is the integers and p is prime, replacing each event number by zero and replacing each odd number by one.

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

***Correspondence to Author:**
Dr. Ahmad Hamza Al Cheikha
Dep. of Mathematical Science, College of Arts-science and Education, Ahlia Uni., Manama, Bahrain

How to cite this article:
Ahmad Hamza Al Cheikha.Generating New Orthogonal Binary Sequences Using Quotient Rings Z/pm Z. Research Journal of Mathematics and Computer Science, 2018; 2:11. .

eSciencePublisher

eSciPub LLC, Houston, TX USA.
Website: http://escipub.com/

I. Introduction

Shannon's classic articles, 1948-1949, were followed by many research papers on the question of finding successful ways to encode a successful encoding of the media to allow it to be transmitted correctly through jammed channels. [16]

The main obstacle to encoding and decoding is the complexity of decoding and decoding. For this reason, efforts have been made to design cryptographic and decoding methods in an easy way. The works of Hocquenghem in 1959, Reed Solomon 1960, Chaudhuri and Bose in 1960, BCH codes or Bose–Chaudhuri–Hocquenghem codes and others as Goppa, and Petrson 1961 were a new starting point for solving this issue. [1-7]

In all stages of encoding and decoding the orthogonal sequences play the main role in these processes n all stages of encoding and decoding, the orthogonal sequences play the main role in these processes, including: the sequences with maximum period M-Sequences, the Walsh sequences, the Reed-Solomon sequences, and the other. [8-11]

Orthogonal Sequences are used widely at the forward links of communication channels to sift

through this information is transmitted to reach the receivers this information in a correct form,

especially in the pilot channels, the Sync channels, and the Traffic channel.[12-16]

II. Research method and Material

***Definition* 1.** The complement of the binary vector $X=(x_1,x_2,...,x_n),\ x_i\in F_2\{0,1\}$ is the vector

$\overline{X}=(\overline{x_1},\overline{x_2},...,\overline{x_n})$, where:

$$\overline{x_i}=\begin{cases}1 & if \quad x_i=0\\ 0 & if \quad x_i=1\end{cases}. \text{ [1,2]}$$

***Definition* 2.** Suppose $x=(x_0,x_1,...,x_{n-1})$ and $y=(y_0,y_1,...,y_{n-1})$ are binary vectors of

length n on *GF*(2)={0,1}. The coefficient of correlations function of x and y, denoted by $R_{x,y}$,

is:

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

Where $x_i + y_i$ is computed *mod* 2. It is equal to the number of agreements components minus

the number of disagreements corresponding to components or if $x_i, y_i\in\{1,-1\}$ (usually,

replacing in binary vectors x and y each "1" by "-1" and each "0" by "1") then

$$R_{x,y}=\sum_{i=0}^{n-1}x_i y_i \text{ , [1,2],[13-18]} \qquad (2)$$

[3-5] [8,9]

***Definition* 3.** Suppose $x=(x_0,x_1,...,x_{n-1})$ and $y=(y_0,y_1,...,y_{n-1})$ are binary vectors of

length n on *GF*(2)={0,1}, or components belong to {1, -1}, is said strictly orthogonal or

briefly orthogonal if $R_{x,y}=0$, (Usually, said orthogonal if $R_{x,y}\in\{-1,0,1\}$). [5-7],[11-13]

***Definition* 4.** Suppose G is a set of binary vectors of length n:

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

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

Satisfied:

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

(3)

$$2.\ \forall X,Y\in G(X\neq Y),\ \sum_{i=0}^{n-1}x_i^* y_i^*=0\, or\left|R_{x,y}\right|=0.$$

That is, the absolute value of "the number of agreements minus the number of disagreements"

is equal to zero. [2,6],[8-12]

III. Results and Discussion

The best method for getting binary representation of the multiplication table of quotient ring

$Z/(p^m Z)$, where Z is the integers and p is prime, is replacing each event number by "0" and replacing each odd number by "1', by this way each row of the table , except the multiplies

of p, contains $(p^m+1)/2$ of "0.s' and $(p^m-1)/2$ of "1.s" and Ri is the complement of R(p^m-i) or $Ri = \overline{R(11-i)}$ except the first entry . We searching between these rows about comfortable subset of rows which with the null row form an additional subgroups achieve the number of "0.s" and the number of "1.s" or orthogonal conditions in the vector space $2^{(p^m)}$, where the addition is performed by *mod* 2.

First step: For p = 3

1. For the quotient ring $Z/(3^2)$: The following table 1 showing the multiple in the ring $Z/3^2 Z$:

Table 1: Multiplication Table of $Z/3^2 Z$

	*	0	1	2	3	4	5	6	7	8
R0	0	0	0	0	0	0	0	0	0	0
R1	1	0	1	2	3	4	5	6	7	8
R2	2	0	2	4	6	8	1	3	5	7
R3	3	0	3	6	0	3	6	0	3	6
R4	4	0	4	8	3	7	2	6	1	5
R5	5	0	5	1	6	2	7	3	8	4
R6	6	0	6	3	0	6	3	0	6	3
R7	7	0	7	5	3	1	8	6	4	2
R8	8	0	8	7	6	5	4	3	2	1

Table 2 showing the binary representation of table1, when in table 1 each even num-ber replaced by "0" and each odd number replaced by "1":

Table 2: Binary Representation of $Z/3^2 Z$

	*	0	1	2	3	4	5	6	7	8
R0	0	0	0	0	0	0	0	0	0	0
R1	1	0	1	0	1	0	1	0	1	0
R2	2	0	0	0	0	0	1	1	1	1
R3	3	0	1	0	0	1	0	0	1	0
R4	4	0	0	0	1	1	0	0	1	1
R5	5	0	1	1	0	0	1	1	0	0
R6	6	0	0	1	0	0	1	0	0	1
R7	7	0	1	1	1	1	0	0	0	0
R8	8	0	0	1	0	1	0	1	0	1

From the table 2:

- All entries in the R0 are "0" And does not meet the conditions of orthogonal.
- Each row of R3, R6 contains six of "0.s", three of "1.s" and does not meet the conditions of orthogonal.

- Each of the rows of the set $\{R1, R2, R4, R5, R7, R8\}$ contains $(3^2+1)/2$ of "0.s" , (3^2-1) of "1.s" and the first condition of orthogonal is verified and: R1+R8 = R2+R7=…=R4+R5= [011111111].
- The following table 3 showing the addition between some of the rows in the set where R*i* + R*j* denoted by R*i*+*j*.

Table 3: Addition between some of the rows{R1, R2, …,R8}

R1+2	0	1	0	1	0	0	1	0	1
R1+4	0	1	0	0	1	1	0	0	1
R2+4	0	0	0	1	1	1	1	0	0
R1+5	0	0	1	1	0	0	1	1	0
R2+5	0	1	1	0	0	0	0	1	1
R4+5	0	1	1	1	1	1	1	1	1
R1+7	0	0	1	0	1	1	0	1	0
R2+7	0	1	1	1	1	1	1	1	1
R1+8	0	1	1	1	1	1	1	1	1

We can see that ***Span***{R1, R2, R4}= {R1, R2, R4, R1+2,R1+4, R2+4} is a maximum closed orthogonal set contained in F_{3^2} and the number of these maximum closed orthogonal sets is at most $\binom{6}{3} = 20$ sets. 2. For the quotient ring $Z/3^3Z$: The multiplication table of $Z/3^3Z$ is the following:

Table 4: Multiplication Table of $Z/3^3Z$

	*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
R0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
R1	1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
R2	2	0	2	4	6	8	10	12	14	16	18	20	22	24	26	1	3	5	7	9	11	13	15	17	19	21	23	25
R3	3	0	3	6	9	12	15	18	21	24	0	3	6	9	12	15	18	21	24	0	3	6	9	12	15	18	21	24
R4	4	0	4	8	12	16	20	24	1	5	9	13	17	21	25	2	6	10	14	18	22	26	3	7	11	15	19	23
R5	5	0	5	10	15	20	25	3	8	13	18	23	1	6	11	16	21	26	4	9	14	19	24	2	7	12	17	22
R6	6	0	6	12	18	24	3	9	15	21	0	6	12	18	24	3	9	15	21	0	6	12	18	24	3	9	15	21
R7	7	0	7	14	21	1	8	15	22	2	9	16	23	3	10	17	24	4	11	18	25	5	12	19	26	6	13	20
R8	8	0	8	16	24	5	13	21	2	10	18	26	7	15	23	4	12	20	1	9	17	25	6	14	22	3	11	19
R9	9	0	9	18	0	9	18	0	9	18	0	9	18	0	9	18	0	9	18	0	9	18	0	9	18	0	9	18
R10	10	0	10	20	3	13	23	6	16	26	9	19	2	12	22	5	15	25	8	18	1	11	21	4	14	24	7	17
R11	11	0	11	22	6	17	1	12	23	7	18	2	13	24	8	19	3	14	25	9	20	4	15	26	10	21	5	16
R12	12	0	12	24	9	21	6	18	3	15	0	12	24	9	21	6	18	3	15	0	12	24	9	21	6	18	3	15
R13	13	0	13	26	12	25	11	24	10	23	9	22	8	21	7	20	6	19	5	18	4	17	3	16	2	15	1	14
R14	14	0	14	1	15	2	16	3	17	4	18	5	19	6	20	7	21	8	22	9	23	10	24	11	25	12	26	13
R15	15	0	15	3	18	6	21	9	24	12	0	15	3	18	6	21	9	24	12	0	15	3	18	6	21	9	24	12
R16	16	0	16	5	21	10	26	15	4	20	9	25	14	3	19	8	24	13	2	18	7	23	12	1	17	6	22	11
R17	17	0	17	7	24	14	4	21	11	1	18	8	25	15	5	22	12	2	19	9	26	16	6	23	13	3	20	10
R18	18	0	18	9	0	18	9	0	18	9	0	18	9	0	18	9	0	18	9	0	18	9	0	18	9	0	18	9
R19	19	0	19	11	3	22	14	6	25	17	9	1	20	12	4	23	15	7	26	18	10	2	21	13	5	24	16	8
R20	20	0	20	13	6	26	19	12	5	25	18	11	4	24	17	10	3	23	16	9	2	22	15	8	1	21	14	7
R21	21	0	21	15	9	3	24	18	12	6	0	21	15	9	3	24	18	12	6	0	21	15	9	3	24	18	12	6
R22	22	0	22	17	12	7	2	24	19	14	9	4	26	21	16	11	6	1	23	18	13	8	3	25	20	15	10	5
R23	23	0	23	19	15	11	7	3	26	22	18	14	10	6	2	25	21	17	13	9	5	1	24	20	16	12	8	4
R24	24	0	24	21	18	15	12	9	6	3	0	24	21	18	15	12	9	6	3	0	24	21	18	15	12	9	6	3
R25	25	0	25	23	21	19	17	15	13	11	9	7	5	3	1	26	24	22	20	18	16	14	12	10	8	6	4	2
R26	26	0	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

The binary representation of the table 5 is:

Table 5: Binary Representation of Multiplication table of $Z/3^3 Z$

	*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
R0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
R1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
R2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1
R3	3	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0
R4	4	0	0	0	0	0	0	0	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1	1
R5	5	0	1	0	1	0	1	1	0	1	0	1	1	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0
R6	6	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	1	1
R7	7	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0
R8	8	0	0	0	0	1	1	1	0	0	0	0	1	1	1	0	0	0	1	1	1	1	0	0	0	1	1	1
R9	9	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0
R10	10	0	0	0	1	1	1	0	0	0	1	1	0	0	0	1	1	1	0	0	1	1	1	0	0	0	1	1
R11	11	0	1	0	0	1	1	0	1	1	0	0	1	0	0	1	1	0	1	1	0	0	1	0	0	1	1	0
R12	12	0	0	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1
R13	13	0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
R14	14	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	1	0	1
R15	15	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1	0	0
R16	16	0	0	1	1	0	0	1	0	0	1	1	0	1	1	0	0	1	0	0	1	1	0	1	1	0	0	1
R17	17	0	1	1	0	0	0	1	1	1	0	0	1	1	1	0	0	0	1	1	0	0	0	1	1	1	0	0
R18	18	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1
R19	19	0	1	1	1	0	0	0	1	1	1	1	0	0	0	1	1	1	0	0	0	0	1	1	1	0	0	0
R20	20	0	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1
R21	21	0	1	1	1	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	0	1	1	0	0	0	0
R22	22	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0	1	1	0	1	0	1	1	0	1	0	1
R23	23	0	1	1	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	0	0	0	0	0	0
R24	24	0	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1
R25	25	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
R26	26	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

We can see: R1+R26 = R2+R25= … = R13+R14= [01 1 1 1 1…1]27

$R1+R2$, Contains 13 of "0.s" and 14 of "1.s".

$R1+R4$, Contains 15 of "0.s" and 12 of "1.s".

$R1+R5$, Contains 16 of "0.s" and 11 of "1.s".

- $R1+R7$, Contains 14 of "0.s" and 13 of "1.s".

$R1+R8$, Contains 13 of "0.s" and 14 of "1.s".

$R1+R10$, Contains 15 of "0.s" and 12 of "1.s".

$R1+R11$, Contains 16 of "0.s" and 11 of "1.s".

- $R1+R13$, Contains 14 of "0.s" and 13 of "1.s".

$R1+R14$, Contains 12 of "0.s" and 15 of "1.s".

$R1+R16$, Contains 11 of "0.s" and 16 of "1.s".

$R1+R17$, Contains 12 of "0.s" and 15 of "1.s".

- $R1+R19$, Contains 14 of "0.s" and 13 of "1.s".

$R1+R20$, Contains 13 of "0.s" and 14 of "1.s".

$R1+R22$, Contains 11 of "0.s" and 16 of "1.s".

$R1+R23$, Contains 12 of "0.s" and 15 of "1.s".

- $R1+R25$, Contains 14 of "0.s" and 13 of "1.s".

$R1+R26$, Contains 1 of "0.s" and 26 of "1.s".

Such any two rows from the set {R1, R7, R13,R19,R25} are orthogonal:

R1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
R7	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1
R13	0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
R19	0	1	1	1	0	0	0	1	1	1	1	0	0	0	1	1	1	0	0	0	0	1	1	1	0	0
R25	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0

But:

- $R7+R13$, Contains 14 of "0.s" and 13 of "1.s".

$R7+R19$, Contains 10 of "0.s" and 17 of "1.s".

- $R7+R25$, Contains 14 of "0.s" and 13 of "1.s".
- $R13+R25$, Contains 14 of "0.s" and 13 of "1.s".

We have the set of four rows {R1, R7, R13, R25} and any two rows of them are orthogonal.

R1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
R7	7	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1
R13	13	0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
R25	25	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0

Thus we can find the following table 6 is the Span of these rows{R1, R7, R13, R25}:

Table 6: Span of { R1, R7, R13, R25}

R1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
R7	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1
R1+7	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0
R13	0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
R1+13	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
R7+13	0	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0
R1+7+13	0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
R25	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
R1+25	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	1	0	1
R7+25	0	0	1	0	0	1	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	1	0	0	1
R13+25	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0	1	1	0	0	1	1	0	0	1	1
R1+7+25	0	1	1	1	0	0	0	0	1	1	1	1	0	0	1	1	0	0	0	0	1	1	1	1	0	0
R1+13+25	0	1	1	0	0	1	1	0	0	1	1	0	0	1	0	1	1	0	0	1	1	0	0	1	1	0
R7+13+25	0	1	1	0	1	0	0	1	0	1	1	0	1	0	1	0	1	0	0	1	0	1	1	0	1	0
R1+7+13+25	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	1	0	1	1

From this table we can see the following:

- Any two rows of { R1, R7, R13, R25} are orthogonal.
- Sum any three rows of { R1, R7, R13, R25} contains 13 of "0.s" and 14 of "1.s".
- Sum all rows of { R1, R7, R13, R25}

contains 11 of "0.s" and 16 of "1.s", this means: if

there are four people sent their messages m_1, m_2, m_3, m_4 according to the lines R1, R7, R13, R25 respectively then then the decoder may not be able to specify each of these Messages separately but for any three of them, the decoder can identify each one of them.

- Thus, ***B*** = ***Span***{R1, R7, R13} is a closed orthogonal set and the number of as theses sets

is at most $\binom{18}{3} = 816$ sets.

Second step: For *p* = 5

1. For the quotient ring $Z/5Z$: The following table 7 showing the multiple in the quotient ring $Z/5Z$:

Table7: Multiplication table of Z/5Z with binary representation

*	0	1	2	3	4		*	C0	C1	C2	C3	C4		*	C0	C1	C2	C3	C4
0	0	0	0	0	0		R0	0	0	0	0	0		R0	0	0	0	0	0
1	0	1	2	3	4	$\Rightarrow$	R1	0	1	0	1	0	$\Rightarrow$	R1	0	1	0	1	0
2	0	2	4	1	3		R2	0	0	0	1	1		R2	0	0	0	1	1
3	0	3	1	4	2		R3	0	1	1	0	0		R1+2	0	1	0	0	1
4	0	4	3	2	1		R4	0	0	1	0	1		R4	0	0	1	0	1

From this table we can see that $Span\{R1, R2\}$ is $\{R1, R2, R_{1+2}\}$, where $R_{1+2} = R1 + R2$, and $R_{1+2} = (0\ 1\ 0\ 0\ 1)$ don't belong to the rows set of table and each of the rows contains three of "0.s" and two of the "1.s" but $R_{1+2+3} = (0\ 0\ 0\ 0)$ and: R1+R4 = R2+R3 = [0 1 1 1 1].

From this simple example we can see, there are only four closed orthogonal sets are: $Span\{R1, R2\}$, $Span\{R1, R3\}$, $Span\{R2, R4\}$, and $Span\{R3, R4\}$, and $4 \le \binom{4}{2} = 6$.

2. Multiplication table of $Z/5^2 Z$

Table 8: Multiplication Table of $Z/5^2 Z$

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	0	2	4	6	8	10	12	14	16	18	20	22	24	1	3	5	7	9	11	13	15	17	19	21	23
3	0	3	6	9	12	15	18	21	24	2	5	8	11	14	17	20	23	1	4	7	10	13	16	19	22
4	0	4	8	12	16	20	24	3	7	11	15	19	23	2	6	10	14	18	22	1	5	9	13	17	21
5	0	5	10	15	20	0	5	10	15	20	0	5	10	15	20	0	5	10	15	20	0	5	10	15	20
6	0	6	12	18	24	5	11	17	23	4	10	16	22	3	9	15	21	2	8	14	20	1	7	13	19
7	0	7	14	21	3	10	17	24	6	13	20	2	9	16	23	5	12	19	1	8	15	22	4	11	18
8	0	8	16	24	7	15	23	6	14	22	5	13	21	4	12	20	3	11	19	2	10	18	1	9	17
9	0	9	18	2	11	20	4	13	22	6	15	24	8	17	1	10	19	3	12	21	5	14	23	7	16
10	0	10	20	5	15	0	10	20	5	15	0	10	20	5	15	0	10	20	5	15	0	10	20	5	15
11	0	11	22	8	19	5	16	2	13	24	10	21	7	18	4	15	1	12	23	9	20	6	17	3	14
12	0	12	24	11	23	10	22	9	21	8	20	7	19	6	18	5	17	4	16	3	15	2	14	1	13
13	0	13	1	14	2	15	3	16	4	17	5	18	6	19	7	20	8	21	9	22	10	23	11	24	12
14	0	14	3	17	6	20	9	23	12	1	15	4	18	7	21	10	24	13	2	16	5	19	8	22	11
15	0	15	5	20	10	0	15	5	20	10	0	15	5	20	10	0	15	5	20	10	0	15	5	20	10
16	0	16	7	23	14	5	21	12	3	19	10	1	17	8	24	15	6	22	13	4	20	11	2	18	9
17	0	17	9	1	18	10	2	19	11	3	20	12	4	21	13	5	22	14	6	23	15	7	24	16	8
18	0	18	11	4	22	15	8	1	19	12	5	23	16	9	2	20	13	6	24	17	10	3	21	14	7
19	0	19	13	7	1	20	14	8	2	21	15	9	3	22	16	10	4	23	17	11	5	24	18	12	6
20	0	20	15	10	5	0	20	15	10	5	0	20	15	10	5	0	20	15	10	5	0	20	15	10	5
21	0	21	17	13	9	5	1	22	18	14	10	6	2	23	19	15	11	7	3	24	20	16	12	8	4
22	0	22	19	16	13	10	7	4	1	23	20	17	14	11	8	5	2	24	21	18	15	12	9	6	3
23	0	23	21	19	17	15	13	11	9	7	5	3	1	24	22	20	18	16	14	12	10	8	6	4	2
24	0	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

The binary representation of the table 8 is the table 9:

Table 9: Binary Representation of Multiplication table of $Z/5^2Z$

*	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	C21	C22	C23	C24
R0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
R1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
R2	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
R3	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0
R4	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
R5	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0
R6	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
R7	0	1	0	1	1	0	1	0	0	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1	0
R8	0	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1
R9	0	1	0	0	1	0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1	0	1	1	0
R10	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1
R11	0	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1	1	0	1	1	0	0	1	1	0
R12	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
R13	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
R14	0	0	1	1	0	0	1	1	0	1	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1
R15	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0
R16	0	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1
R17	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0
R18	0	0	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1	0	0	1	0	1	1	0	1
R19	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
R20	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1
R21	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0
R22	0	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1
R23	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
R24	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

From this table we can see that each row in the table contains 13 of "0.s" and 12 of "1.s" except the rows R0, R5, R10, R15, and R20 and each row of R5, R10, R15, and R20 contains 15 of "0.s" and 10 of "1.s" and: R1+R24 = R2+R23 =…. = R12+R13 = [0 1 1 1 1…1]$_{25}$.

a. Using the rows of the set A = {R1, R2, R4} as a basis, we can find *Span* {A} as an orthogonal closed set of rows which with the R0 form an additional subgroup in the vector space $2^{(2^m)}$. Table 10 showing elements Span {A} as an orthogonal closed set and each row contains 13 of "0.s" and 12 of "1.s". Elements Span {A} don't belong to the table 3.

Table 10: Span {A} as orthogonal closed set

*	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	C21	C22	C23	C24
R1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
R2	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
R1+2	0	1	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	1	0	1
R4	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
R1+4	0	1	0	1	0	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	1	0	1
R2+4	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
R1+2+4	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	0	1	0

Thus we can think about basis of the biggest orthogonal closed set.

- From the following representation of rows R1, R3 and R1+R3 showing:

R1	6	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
R3	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0
+	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	1	1	0	0	0	0	0	0	0	0

Thus R1+R3 contains 18 of “0.s” and 7 of “1.s” then these rows R1 and R3 can’t be in one basis.

- For the same reason R2, R6 as showing in the following representation:

R2	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
R6	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
+	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0

R2 = R6 contains 18 of “0.s” and 7 of “1.s” and R6 can’t be in one basis with R2.

- The following representation of R4, R7 and R4+R7:

R4	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
R7	0	1	0	1	1	0	1	0	0	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1	0
+	0	1	0	1	1	0	1	1	1	0	1	1	0	0	1	1	0	1	1	1	0	1	1	0	1

Showing: R4+R7 contains 9 of “0.s” and 16 of “1.s” and R4,R7 can’t be in one basis.

- By the same ways the sets $\{R1, R2, R4, R8\}$, $\{R1, R2, R4, R9\}$ can’t find biggest orthogonal set of rows.

The result study of $Span\{B\}$, where $B = \{R1, R2, R4, R11\}$, showing in the table 11, the all rows of $Span\{B\}$ satisfies the orthogonal conditions except $R_{1+2+4+11}$ Which contains 17 of “0.s” and 8 of “1.s” as showing in table 11

.

Table 11: Showing rows of *Span* {*B*}

*	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	C21	C22	C23	C24
R1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
R2	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
R1+2	0	1	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	1	0	1
R4	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
R1+4	0	1	0	1	0	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	1	0	1
R2+4	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
R1+2+4	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	0	1	0
R11	0	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1	1	0	1	1	0	0	1	1	0
R1+11	0	0	0	1	1	0	0	1	1	1	0	0	1	1	0	0	1	1	1	0	0	1	1	0	0
R2+11	0	1	0	0	1	1	0	0	1	0	0	1	1	1	1	0	0	1	0	0	1	1	0	0	1
R4+11	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	1	0	1	0	1	1	0	0	1
R 1+2+11	0	0	0	1	1	0	0	1	1	1	0	0	1	0	1	1	0	0	0	1	1	0	0	1	1
R1+4+11	0	0	0	1	1	0	0	0	0	0	1	1	0	1	0	0	1	1	1	1	1	0	0	1	1
R2+4+11	0	1	0	0	1	1	0	1	0	1	1	0	0	1	1	0	0	1	0	1	0	0	1	1	0
R1+2+4+ +11	0	0	0	1	1	0	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	1	1	0	0

- The following representation of R4, R12 and R4+R12:

R4	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
R12	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
+	0	0	0	1	1	0	0	0	0	1	1	0	0	0	0	1	1	0	0	0	0	1	1	0	0

Showing: R4+R12 contains 17 of “0.s” and 8 of “1.s” and R4,R7 can’t be in one basis.

• The following representation of R4, R13 and R4+R13:

R4	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
R13	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
+	0	1	1	0	0	1	1	1	1	0	0	1	1	1	1	0	0	1	1	1	1	0	0	1	1

Showing: R4+R12 contains 9 of “0.s” and 16 of “1.s” and R4,R13 can’t be in one basis.

• The following representation of $R_{1+2+4+14}$

R2+4	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
R1+14	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1
+	0	1	1	0	0	1	1	1	1	1	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1

Showing: $R_{1+2+4+14}$ contains 9 of “0.s” and 16 of “1.s” and R1, R2, R4, R14 can’t be in one basis.

• The following representation of R_{2+4+16}

R2+4	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
R16	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	1
+	0	1	1	0	0	1	1	1	1	1	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1

Showing: R_{2+4+16} contains 9 of “0.s” and 16 of “1.s” and R2, R4, R16 can’t be in one basis.

• The following representation of R1, R17 and R1+R17:

R1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
R17	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0
+	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	0

Showing: R1+R17 contains 19 of “0.s” and 6 of “1.s” and R1,R17 can’t be in one basis.

• The following representation of R4, R18 and R4+R18:

R4	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
R18	0	0	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1	0	0	1	0	1	1	0	1
+	0	0	1	0	0	1	0	0	0	1	0	0	1	1	0	0	1	0	0	0	1	0	0	1	0

Showing: R4+R18 contains 17 of “0.s” and 8 of “1.s” and R4,R18 can’t be in one basis.

• The following representation of R2, R19 and R2+R19:

R2	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
R19	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
+	0	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1

Showing: R2+R19 contains 9 of “0.s” and 16 of “1.s” and R2,R19 can’t be in one basis.

• The following representation of R4, R21 and R4+R21:

R4	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1
R21	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0
+	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Showing: R4+R21 contains only one “0.” and 24 of “1.s” and R4,R21 can’t be in one basis.

• The following representation of R1, R22 and R1+R22:

R1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
R22	0	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1
+	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

Showing: R1+R22 contains only 9 of “0.s” and 16 of “1.s” and R1,R22 can’t be in one basis.

• The following representation of R2, R23 and R2+R23:

R2	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
R23	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
+	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Showing: R2+R23 contains only one of “0.s” and 24 of “1.s” and R2,R23 can’t be in one basis.

- The following representation of R1, R24 and R1+R24:

R1	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**
R24	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**
+	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Showing: R1+R24 contains only one “0.” and 24 of “1.s” and R1, R24 can’t be in one basis. Thus the biggest orthogonal closed set contains at most 3 rows and the number of these sets is at most $\binom{20}{3} = 1140$.

Third Step: Table 11 showing the multiplication in the quotient ring Z/11Z:

Table 12: Multiplication in the ring $Z/11Z$

	*	0	1	2	3	4	5	6	7	8	9	10
R0	0	0	0	0	0	0	0	0	0	0	0	0
R1	1	0	1	2	3	4	5	6	7	8	9	10
R2	2	0	2	4	6	8	10	1	3	5	7	9
R3	3	0	3	6	9	1	4	7	10	2	5	8
R4	4	0	4	8	1	5	9	2	6	10	3	7
R5	5	0	5	10	4	9	3	8	2	7	1	6
R6	6	0	6	1	7	2	8	3	9	4	10	5
R7	7	0	7	3	10	6	2	9	5	1	8	4
R8	8	0	8	5	2	10	7	4	1	9	6	3
R9	9	0	9	7	5	3	1	10	8	6	4	2
R10	10	0	10	9	8	7	6	5	4	3	2	1

The binary representation of table 12 is the following table 13:

Table 12: The binary representation of the multiplication in $Z/11Z$

	*	0	1	2	3	4	5	6	7	8	9	10
R0	0	0	0	0	0	0	0	0	0	0	0	0
R1	1	0	1	0	1	0	1	0	1	0	1	0
R2	2	0	0	0	0	0	0	1	1	1	1	1
R3	3	0	1	0	1	1	0	1	0	0	1	0
R4	4	0	0	0	1	1	1	0	0	0	1	1
R5	5	0	1	0	0	1	1	0	0	1	1	0
R6	6	0	0	1	1	0	0	1	1	0	0	1
R7	7	0	1	1	0	0	0	1	1	1	0	0
R8	8	0	0	1	0	0	1	0	1	1	0	1
R9	9	0	1	1	1	1	1	0	0	0	0	0
R10	10	0	0	1	0	1	0	1	0	1	0	1

Each row in the table 12 except R0 contains 6 of the “0.s” and 5 of the “1” and R*i* is the complement of R(11-i) or $Ri = \overline{R(11-i)}$ except the first entry. We searching about the big orthogonal closed sets.

First we will search about this big orthogonal closed set which contains R1.

R1	0	1	0	1	0	1	0	1	0	1	0
R2	0	0	0	0	0	0	1	1	1	1	1
R1+2	0	1	0	1	0	1	1	0	1	0	1

- R1+R2 contains 5 of “0.s” and 6 of “1.s” and satisfies the orthogonal condition.

R1+R3 contains 7 of “0.s” and 4 of “1.s” and don’t satisfies the orthogonal condition and R3 can’t be with R1 in one basis.

R1+R4 contains 7 of “0.s” and 4 of “1.s” and don’t satisfies the orthogonal condition and R4 can’t be with R1 in one basis.

R1+R5 contains 7 of “0.s” and 4 of “1.s” and don’t satisfies the orthogonal condition and R5 can’t be with R1 in one basis.

- R1+R6 contains 5 of “0.s” and 6 of “1.s” and satisfies the orthogonal condition but R2+R6 contains 7 of “0.s” and 4 of “1.s” thus R2 and R6 can’t be in one basis.
- R1+R7 contains 5 of “0.s” and 6 of “1.s” and satisfies the orthogonal condition but R2+R7 contains 7 of “0.s” and 4 of “1.s” thus R2 and R7 can’t be in one basis.
- R1+R8 contains 5 of “0.s” and 6 of “1.s” and satisfies the orthogonal condition thus R8 can be with R1 in one basis.

R2+R8 contains 7 of “0.s” and 4 of “1.s” and don’t satisfies the orthogonal condition thus R8 can’t be with R1 in one basis.

R1+R9 contains 7 of “0.s” and 4 of “1.s” and don’t satisfies the orthogonal condition thus R9 can’t be with R1 in one basis.

R1+R10 contains 10 of “0.s” and only one of “1.s”and don’t satisfies the orthogonal condition thus R9 can’t be with R1 in one basis.

There are *Span* {R1, R2}, *Span* {R1, R6}, *Span* {R1, R7}, and *Span* {R1, R8} are orthogonal closed sets in the space 2^{11}.

Thus in the quotient ring Z/11Z there are at most 4(10) = 40 (and $4(10) = 40 \le \binom{10}{2} = 45$) orthogonal closed sets as *Span*{R1,R2}.

R1 + R10 = R2 + R8 = … = R5 + R6 = [0 1 1 1 1 1 1 1 1 1 1].

Conclusions

1. In binary representation of Z/p^mZ, the length of each row is p^m, started by zero, and has $(p^m+1)/2$ of “0.s”, $(p^m-1)/2$ of “1.s” except the rows that are multiple of *p*.
2. In each rows R1, R2, … , R(p^m-1) is satisfies the relation: $Ri = \overline{R(p^m - i)}$ except the first entry is zero or: R1+ R(p^m-1) = R2+ R(p^m-2) = … = R((p^m-1)/2)+ R((p^m+1)/2) = $[0\ 1\ 1\ 1 \ldots 1]_{P^m}$.
3. Number of the biggest orthogonal closed sets (in the space 2^p) which we can get them from the quotient ring Z/pZ is less than or equal $\binom{p-1}{2}$.
4. Number of the biggest orthogonal closed sets (in the space 2^p) which we can get them from the quotient ring Z/p^2Z is less than or equal $\binom{p^2-p}{3}$.
5. Number of the biggest orthogonal closed sets (in the space $2^{(p^2)}$) which we can get them from the quotient ring Z/p^3Z is less than or equal $\binom{p^3-p^2}{3}$.
6. In the First Step, Table 6, The row R(1+7+13+25) contains 11 of “0.s” and 16 of “1.s” this means: if there are four people sent their messages m_1, m_2, m_3, m_4 according to the lines R1,

R7, R13, R25 respectively then then the decoder may not be able to specify each of these

Messages separately but for any three of them, the decoder can identify each one of them.

7. From 4 to 6 we can guess that number of the biggest orthogonal closed sets (in the space

$2^{(p^m)}$) is less than or equal $\binom{p^m - p^{m-1}}{m+1}$

Acknowledgment: The author express their gratitude to Prof. Abdulla Y Al Hawaj, President of Ahlia University for all the support

Reference

[1] 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.

[2] Al Cheikha A. H. (2017). Compose Binary Matrices. *American Journal of Computer*

sciences and Applications. AJCSA. Vol.1, Issue 2. Pp. 0001- 0017.

[3] Al Cheikha A. H. (September,2014). Some Properties of M-Sequences Over Finite Field

Fp. *International Journal of Computer Engineering & Technology*. IJCER. Vol.5, Issue 9.

Pp. 61- 72.

[4] Al Cheikha A. H. (September,2014). Composed Walsh Sequences and M-Sequences.

International Journal of Computers & Technology. IJCT. Vol.15, Issue 7. Pp. 6933- 6939.

[5] Al Cheikha A. H. (2017). Composed Reed Solomon Sequences Generated by *ith* Partial

Sum of Geometrical Sequences. *American Journal of Computer sciences and Applications.*

AJCSA. Vol.1, Issue 1. Pp. 0001- 000116.

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

[7] David, J., "Introductory Modern Algebra, "*Clark University* USA, 2008.

[8] 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.

[9] Lee J.S &Miller L.E, "*CDMA System Engineering Hand Book, "*Artech House.

Boston, London,1998.

[10] Lidl, R.& Pilz,G., "*Applied Abstract Algebra*," Springer–Verlage New York, 1984.

[11] Lidl, R.& Nidereiter, H., "Introduction to Finite Fields and Their Application,"

Cambridge University USA, 1994.

[12] Mac Wiliams, F.G& Sloane, N.G.A., "*The Theory of Error- Correcting Codes,"*

North-Holland, Amsterdam, 2006.

[13] 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.

[14] Thomson W. Judson, "*Abstract Algebra: Theory and Applications* , " Free

Software Foundation,2013.

[15] Yang S.C,"*CDMA RF System Engineering,* "ArtechHouse.Boston-London,1998.

[16] Sakrison D.J. Communication Theory: Transmission of Waveforms and Digital

information, Publisher: John Wiley & Sons Inc, 1968