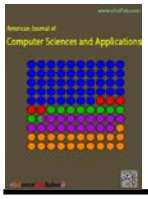
Research Article **AJCSA, 2017, 1:2**



American Journal of Computer Sciences and Applications
(ISSN:2575-775X)

Composed Reed Solomon Sequences Generated by i^{th} Partial Sum of Geometrical Sequences

Dr. Ahmad Hamza Al Cheikha

Math. Sci. Dep. Col. of Arts Sci. & Edu. Ahlia Uni. Manam, Bahrain

ABSTRACT

Reed–Solomon codes are an important group of error-correcting that were introduced by Irving S. Reed and Justine Solomon in 1960. They used in the error coding control, special in systems that have two way communication channels in two externally applications: deep telecommunications and the compact disc. They have many important applications, the most prominent of which include consumer technologies such as CDs, DVDs, Blue-ray Discs, QR Codes, data transmission, technologies such as DSL and Wi MAX, broadcast, systems such as DVB and ATSC, and storage systems such as RAID 6 . They are also used in satellite communication.

This research is useful to generate new Reed Solomon Codes and their composed sequences using the ith partial sum of geometrical 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.

Keywords: Minimal polynomial; Minimum distance; BCH Sequences; Reed-Solomon sequences; Quasi- orthogonal Sequences; Orthogonal sequences; Code; Span.

***Correspondence to Author:**
Dr. Ahmad Hamza Al Cheikha, Math. Sci. Dep. Col. of Arts Sci. & Edu. Ahlia Uni. Manam, Bahrain

How to cite this article:
Ahmad Hamza Al Cheikha. Composed Reed Solomon Sequences Generated by ith Partial Sum of Geometrical Sequences. American Journal of Computer Sciences and Applications, 2017; 1:2.

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

1. Introduction

1.1 Reed Solomon Sequences(Codes)

Reed-Solomon codes RS**:** The Reed-Solomon code RS over F_q is BCH code with length $N = q - 1$, $q \neq 2$, and: length, dimension and minimum distance of the code denoted by N, K, D. This code is a linear and cyclic. If $q = 2^m$ then we can represent each element in F_q in row with the length m and its components are

in F_2 according to basis in F_q and the new code will be of the form: $[n = mN, k = mK, d \geq D]$.

The binary representation maintains on the linearity (but not necessary on the cyclic).

The RS codes are very important because:

- They are preferred codes when the length of the code need to be less than the order of field.
- They are appropriate to construct other codes (as binary codes and concatenated codes likes Justine codes and MDS codes).
- They are useful for correct impulsivity errors. (Fraleigh, 1971; Yang, 1998).

2. Research Methods and Materials

- Definition 1**:** If F is a finite filed then any generator of a the cyclic group F^* is called primitive element in F (Fraleigh. 1971; Jong et al, 1998).
- Definition 2**:** The polynomial $f \in F(x)$, of degree $K \geq 1$ is called a primitive polynomial over F if it irreducible for some of its primitive elements of F (Jong at el, 1995; Lidl and Niederreiter, 1986).
- Definition 3**:** Suppose G is a set of binary vectors of the length n:

$$G = \{X;\ X = (x_0 x_2 \ldots x_{n-1}), x_i \in F_2 = \{0,1\}\}$$

and $1^* = -1$ *and* $0^* = 1$, then the set G is called Orthogonal set if it satisfies the two following conditions :

1. $\forall X \in G: \sum_{i=0}^{n-1} x_i^* \in \{-1,0,1\}$

That is the difference between the number of "1"s and the number of "0"s in X at most is one.

2. $\forall X, Y \in G \text{ and } X \neq Y: \sum_{i=0}^{n-1} x_i^* y_i^* \in \{-1,0,1\}$

(Lee and Miller, 1998; Al Cheikha, 2005)).

* Definition 4**:** The set G is called quasi orthogonal if it satisfies the two following conditions:

1. $\forall X, Y \in G: \left| \sum_{i=1}^{n-1} x_i^* \right| \leq k$

2 . $\forall X, Y \in G, X \neq Y : \left|\sum_{i=0}^{n-1} x_i^* y_i^*\right| \leq \ell$ Degree of similarity could be determined by $[k, \ell]$ (Yang Kim, Kumar, 2000; Yang, 1998).

- Definition 5. Minimum distance d: The minimum distance d of a set C of binary vectors is:

  $d = \min_{x,y \in C} d(x, y),\ x, y \in C$ (Mac William and Sloane, 1978).

- Definition 6**.** The code C of the form [n, k, d] if each element (Code word) has the: length n, rank k (the number of information components, Message), minimum distance d (Gong and youssef, 2002).
- Definition 7**.** If C is a set of binary sequences and ω is any binary vector then: $C(\omega) = \{x_i(\omega);\ x_i \in C\}$, when , we replace each “1” in x_i by ω and each “0” in x_i by $\overline{\omega}$ (Al Cheikha and Ruchin, 2014; Al Cheikha, 2014).
- Definition 8. If $M = \{x_1, x_2, ..., x_n\}$, where: $x_i \in F^m$, $n \leq m$ and F is a field , then $Span\, M = \sum_{i=1}^{n} a_i x_i$ (Fraleigh. 1971).

3. Results and Discussion (Findings)

3.1.Generating RS codes using geometrical sequences

- 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 ω: the number of”1”s and the number of “0”s are n_1 and n_2 respectively, then in the binary vector $x(\omega)$: the number of”1”s and the number of “0”s are $n_1 m_1 + n_2 m_2$ and $n_1 m_2 + n_2 m_1$ respectively (Al Cheikha 2016; Al Cheikha 2016).
- Theorem 2. F_{2^n} is isomorphic to F_2^n and Elements set F_{2^n} have $n2^{n-1}$ of ones and $n2^{n-1}$ of zeros (Lee and Miller, 1998).
- Theorem 3. If (G,+) is a additive group, A is a subgroup of G and satisfies the following two conditions:

  1. $b_1, b_2 \notin A \Rightarrow b_1 - b_2 \in A$
  2. $a \in A, b \notin A \Rightarrow a - b \notin A$

For each $a, b, b_1, b_2 \in G$, then: $G = A \cup (b + A)$ (Mac William and Sloane, 1978).

If F_{2^n} is Galois field of order 2^n, $F_2 = \{0,1\}$, α is a prime element and we construct the geometrical sequence with the first element is 1 and the basis

α, thus, we have the sequence:

$$X = (1, \alpha, \alpha^2, \cdots, \alpha^{2^n-2}, 1, \alpha, \alpha^2, \cdots) \quad (1)$$

and it is a periodic sequence with the period $2^n - 1$ and contains all non zero elements of F_{2^n} Al Cheikha, 2016).

The set $A = \{ a_i, i = 0,1,2,...,2^n - 2 \}$, where $a_i = (\alpha^i, \alpha^{i+1}, ..., \alpha^{2^n-2+i}) = \alpha^i (1, \alpha, \alpha^2, ..., \alpha^{2^n-2})$ when the powers are computed by mod $2^n - 1$, is linear and closed under the addition and form Reed Solomon Code with: length N = $2^n - 1$, minimum distance D = $2^n - 1$ and dimension K= 1 and $\underline{A} = \{\underline{a_i}\}$ where $\underline{a_i} = (\underline{\alpha}^i, \underline{\alpha}^{i+1}, ..., \underline{\alpha}^{2^n-2+i})$ is the binary representation of a_i .

The set $\underline{A}$ is closed under the addition but not necessary linear with: length $\underline{N} = n(2^n - 1)$, minimum

distance $\underline{D} = n2^{n-1}$ and dimension $\underline{K} \geq 2$, Thus $\underline{A}$ is quasi-orthogonal set and each sequence in $\underline{A}$ contains $2^{n-1} - n$ of "0"s .

I. We extend a_i, $i = 0.1.2.\cdots, 2^n - 2$ to the sequence $\tilde{a}_i = (a_i.0) = (\alpha^i, \alpha^{i+1}, \cdots, \alpha^{2^n-2-i}, 0)$ by adding the zero of F_{2^n} , and $\tilde{\underline{A}} = \{\tilde{\underline{a}}_i\}$ where

II. $\tilde{\underline{a}}_i = (\underline{\alpha}^i, \underline{\alpha}^{i+1}, ..., \underline{\alpha}^{2^n-2+i}, \underline{0})$, is the binary representation of $\tilde{a}_i$.

The set $\tilde{A}$ is linear, closed under the addition and form code with: length $\tilde{N} = 2^n$, minimum Distance $\tilde{D} = 2^n - 1$ and dimension $\tilde{K}$ =1.

The set $\tilde{\underline{A}}$ is closed under the addition but not necessary linear with: length $\tilde{\underline{N}} = n2^n$, minimum Distance $\tilde{\underline{D}} = n2^{n-1}$ and dimension $\tilde{\underline{K}} \geq 2$.

Thus each of $\tilde{\underline{a}}_i, \tilde{\underline{a}}_j, \tilde{\underline{a}}_i + \tilde{\underline{a}}_j$ (if $i \neq j$) , has $n2^{n-1}$ of "1" and $n2^{n-1}$ of " 0 " and $\tilde{\underline{A}}$ is an orthogonal set**.**

III. Compose $\underline{A}$ with $\underline{A}$ or $\underline{A}(\underline{A})$ is quasi-orthogonal sets, $A(\underline{A})$, $\underline{A}(A)$ and $\underline{A}(\underline{A})$ are orthogonal sets (Al Cheikha 2016).

3.2. Generating RS codes using partial sum of geometrical sequences

First Step: We suppose s_i the i[th] partial sum of the Series (2):

$$S = 1 + \alpha + \alpha^2 + \ldots + \alpha^{2^n-2} + 1 + \ldots \quad (2)$$

and $(s_i)_{i \in N^*}$ the sequence of the i[th] partial sums of the sequence. Thus:

$$s_i = 1+\alpha+\ldots+\alpha^{i-1} = \frac{1+\alpha^i}{1+\alpha},\ i = 1, 2, 3,...$$

From $\alpha^{2^n-1} = 1$, the sequence (s_i) is periodic with period $2^n - 1$, and:

$$(s_i) = (\frac{1+\alpha}{1+\alpha}, \frac{1+\alpha^2}{1+\alpha}, \ldots, \frac{1+\alpha^{2^n-1}}{1+\alpha} = 0, \frac{1+\alpha}{1+\alpha}, \frac{1+\alpha^2}{1+\alpha}, \ldots),\ i \geq 1$$

Assuming that $C = \{c_i, i = 0, \ldots, 2^n - 2\}$ where:

$$c_i = (\frac{1+\alpha^{i+1}}{1+\alpha}, \frac{1+\alpha^{i+2}}{1+\alpha}, \ldots, \frac{1+\alpha^{2^n-1}}{1+\alpha}, \frac{1+\alpha}{1+\alpha}, \ldots, \frac{1+\alpha^i}{1+\alpha}),\ i \geq 0$$

When the power computed by mod $2^n - 1$ and $\underline{C} = \{\underline{c_i}\}$ where $\underline{c_i}$ is binary representation of c_i, we can find:

$$c_0 = \left(\frac{1+\alpha}{1+\alpha}\ ,\ \frac{1+\alpha^2}{1+\alpha},\ \ldots\ ,\ \frac{1+\alpha^{2^n-1}}{1+\alpha} = 0 \right)$$

$$c_1 = \left(\frac{1+\alpha^2}{1+\alpha}\ ,\frac{1+\alpha^3}{1+\alpha},\ \ldots\ ,\frac{1+\alpha^{2^n-1}}{1+\alpha}, \frac{1+\alpha}{1+\alpha} \right)$$

.....

$$c_i = \left(\frac{1+\alpha^{i+1}}{1+\alpha}, \ldots, \frac{1+\alpha^{2^n-1}}{1+\alpha}, \frac{1+\alpha}{1+\alpha}, \ldots, \frac{1+\alpha^i}{1+\alpha} \right)$$

.....

$$c_{2^n-2} = \left(\frac{1+\alpha^{2n-1}}{1+\alpha}\ ,\ \frac{1+\alpha}{1+\alpha},\ \ldots\ ,\ \frac{1+\alpha^{2^n-2}}{1+\alpha} \right)$$

Thus each of $c_i, i = 0, \ldots, 2^n - 2$ contains all the field elements F_{2^n} except $\left(\frac{1}{1+\alpha}\right)$. computing $c_i + c_j$ for $j > i$, we can find:

$$c_i = \left(\frac{1+\alpha^{i+1}}{1+\alpha}, \frac{1+\alpha^{i+2}}{1+\alpha}, \ldots, \frac{1+\alpha^{2^n-1-(j-i)}}{1+\alpha}, \ldots, \frac{1+\alpha^{2^n-1}}{1+\alpha}, \frac{1+\alpha}{1+\alpha}, \ldots, \frac{1+\alpha^i}{1+\alpha} \right)$$

$$c_j = \left(\frac{1+\alpha^{j+1}}{1+\alpha}, \frac{1+\alpha^{j+2}}{1+\alpha}, \ldots, \frac{1+\alpha^{2^n-1}}{1+\alpha}, \ldots, \frac{1+\alpha^{2^n-1+(j-i)}}{1+\alpha}, \frac{1+\alpha^{1+(j-i)}}{1+\alpha}, \ldots, \frac{1+\alpha^{j}}{1+\alpha} \right)$$

$$c_i + c_j = \left(\frac{\alpha^{i+1}+\alpha^{j+1}}{1+\alpha}, \frac{\alpha^{i+2}+\alpha^{j+2}}{1+\alpha}, \ldots, \frac{1+\alpha^{-(j-i)}}{1+\alpha}, \ldots, \frac{1+\alpha^{j-i}}{1+\alpha}, \frac{\alpha+\alpha^{1+(j-i)}}{1+\alpha}, \ldots, \frac{\alpha^{i}+\alpha^{j}}{1+\alpha} \right)$$

$$= \left(\alpha^{i+1}\frac{1+\alpha^{j-i}}{1+\alpha}, \alpha^{i+2}\frac{1+\alpha^{j-i}}{1+\alpha}, \ldots, \alpha^{i-j}\frac{1+\alpha^{j-i}}{1+\alpha}, \ldots, \frac{1+\alpha^{j-i}}{1+\alpha} \ldots, \alpha\frac{1+\alpha^{j-i}}{1+\alpha}, \ldots, \alpha^{i}\frac{1+\alpha^{j-i}}{1+\alpha} \right)$$

$$c_i + c_j = \frac{1+\alpha^{j-i}}{1+\alpha}\left(\alpha^{i+1}, \alpha^{i+2}, \ldots, \alpha^{j-i}, \ldots, 1 = \alpha^{2^n-1}, \alpha, \ldots, \alpha^{i} \right)$$

And $c_i + c_j$ contains all elements field F_{2^n} except "0"

Where

$\frac{1+\alpha^{j-i}}{1+\alpha} \neq 0$, for $j > i$, $j = 1,...2^n - 2, i = 0,.....2^n - 3$ and:

a. For $c_i \in C$, the number of "1"s in $\underline{c_i}$ is $\left(n2^{n-1} - w\left(\frac{1}{\underline{1+\alpha}} \right) \right)$ and the number of "0"s is $\left(n2^{n-1} - \left(n - w\left(\frac{1}{\underline{1+\alpha}} \right) \right) \right)$ and the difference between the number of "1"s and the number of "0"s

b. is $\left(n - 2w\left(\frac{1}{\underline{1+\alpha}} \right) \right)$.

c. For $c_i, c_j \in C$ and $i \neq j$, then $\underline{c_i} + \underline{c_j}$ contains $n2^{n-1}$ of "1"s (i.e: the number of disagreement elements of $\underline{c_i}$, $\underline{c_j}$) and ($n.2^{n-1} - n$) of "0" s (i.e: the number of agreement elements of $\underline{c_i}$ $\underline{c_j}$) and the difference between the number of "1"s and the number of '0"s is also n.

- Thus: $\underline{C}$ form a quasi-orthogonal set of degree $\left[\left(n - 2w\left(\frac{1}{\underline{1+\alpha}} \right) \right), n \right]$ and C, $\underline{C}$ are nonlinear.
- The set C is a cyclic code but nonlinear over F_q (when $q = 2^n$) with the length $N = q - 1$ and minimum distance D = N – 1.

We can assume that C is a Reed Solomon Code after closing eyes to the linear property.

Compose $\underline{C}$ with $\underline{C}$ or $\underline{C}(\underline{C})$

$\underline{C}$		$\underline{C}$	
Number of “1”s	Number of “0”s	Number of “1”s	Number of “0”s
$\left(n2^{n-1}-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)$	$\left(n2^{n-1}-\left(n-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)$	$\left(n2^{n-1}-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)$	$\left(n2^{n-1}-\left(n-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)$

* For $c_k \in C$ we define the set: $\underline{P_k}=\underline{C}(\underline{c_k})=\{\underline{p_i}=\underline{c_i}(\underline{c_k}), c_i \in C\}$ then:

a. The number of “1”s in $\underline{p_i}$ is:

$$\left(n2^{n-1}-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\left(n2^{n-1}-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)+\left[n2^{n-1}-\left(n-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right]\left[n2^{n-1}-\left(n-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right]$$

$$=2n^2 2^{2(n-1)}+2\left(w\left(\frac{1}{\underline{1+\alpha}}\right)\right)^2+n^2(1-2^n)-2nw\left(\frac{1}{\underline{1+\alpha}}\right)$$

b. The number of “0”s in $\underline{p_i}$ is:

$$2\left(n2^{n-1}-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\left(n2^{n-1}-\left(n-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)$$

$$=2n^2 2^{2(n-1)}-n^2 2^n+2n\,w\left(\frac{1}{\underline{1+\alpha}}\right)-2\left(w\left(\frac{1}{\underline{1+\alpha}}\right)\right)^2$$

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

$$=4\left(w\left(\frac{1}{\underline{1+\alpha}}\right)\right)^2-4n\,w\left(\frac{1}{\underline{1+\alpha}}\right)+n^2$$

$$=\left(n-2w\left(\frac{1}{\underline{1+\alpha}}\right)\right)^2$$

d. for $\underline{p_i},\underline{p_j} \in \underline{P_k}$ and $i \neq j$ the $\underline{p_i}+\underline{p_j}=(\underline{c_i}+\underline{c_j})(\underline{c_k})$ then:

* The number of “1”s in $\underline{p_i}+\underline{p_j}$ is:

$$n2^{n-1}\left(n2^{n-1}-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)+\left(n2^{n-1}-n\right)\left(n2^{n-1}-\left(n-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)$$

$$=2n^2 2^{2(n-1)}+n^2\left(1-2^n\right)-n\,w\left(\frac{1}{\underline{1+\alpha}}\right).$$

- The number of "0" s in $\underline{p_i}+\underline{p_j}$ is:

$$n2^{n-1}\left(n2^{n-1}-\left(n-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)+\left(n2^{n-1}-n\right)\left(n2^{n-1}-w\left(\frac{1}{\underline{1+\alpha}}\right)\right)$$

$$=2n^2 2^{2(n-1)}-n^2 2^n+n\,w\left(\frac{1}{\underline{1+\alpha}}\right) \text{ of "0"s.}$$

And the difference between the number of "1"s and the number of "0"s is: $n^2-2n\,w\left(\frac{1}{\underline{1+\alpha}}\right)$.

Thus $\underline{P_k}$ is a quasi-orthogonal set of degree $\left[\left(n-2w\left(\frac{1}{\underline{1+\alpha}}\right)\right)^2,\left[n^2-2n\,w\left(\frac{1}{\underline{1+\alpha}}\right)\right]\right]$.

Second Step: Extending C

By extending the sequences ($c_i \in C$) to the sequences $\tilde{c}_i=\left(c_i,\frac{1}{1+\alpha}\right)$ by adding the term $\frac{1}{1+\alpha}\in F_{2^n}^*$, and assuming $\tilde{C}=\{\tilde{c}_i\}$ and $\underline{\tilde{C}}=\{\underline{\tilde{c}_i}\}$ where $\underline{\tilde{c}}$ is the binary representation of $\tilde{c}$.

For ($i\neq j$), each of $\tilde{c}_i,\tilde{c}_j,\tilde{c}_i+\tilde{c}_j$ contains all the field elements of F_{2^n} , also each of $\underline{\tilde{c}_i},\underline{\tilde{c}_j},\underline{\tilde{c}_i+\tilde{c}_j}$ contain $n2^{n-1}$ of "1"s and the same number of "0"s , and $\underline{\tilde{C}}$ form orthogonal set .

The sum of two different elements of $\tilde{C}$ does not belong to $\tilde{C}$, i.e: $\tilde{C}$ and $\underline{\tilde{C}}$ are nonlinear.

Compose $\underline{\tilde{C}}$ with $\underline{\tilde{C}}$ or $\underline{\tilde{C}}(\underline{\tilde{C}})$

$\underline{\tilde{C}}$		$\underline{\tilde{C}}$	
Number of "1"s	Number of "0"s	Number of "1"s	Number of "0"s
$n2^{n-1}$	$n2^{n-1}$	$n2^{n-1}$	$n2^{n-1}$

* For $c_k \in C$ we define the set: $\underline{\tilde{P}_k} = \underline{\tilde{C}}(\underline{\tilde{c}_k}) = \{\underline{\tilde{p}_i} = \underline{\tilde{c}_i}(\underline{\tilde{c}_k}), c_i \in C\}$ then:

a. The number of "1"s in $\underline{\tilde{p}_i}$ is: $2n^2 2^{2(n-1)}$ of " 1"s.

b. The number of "0"s in $\underline{\tilde{p}_i}$ is: $2n^2 2^{2(n-1)}$ of " 0"s.

c. The difference between the number of " 1 "s and the number of " 0 "s in $\underline{\tilde{p}_i}$ is zero.

d. For $\underline{\tilde{p}_i}, \underline{\tilde{p}_j} \in \underline{\tilde{P}_k}$ and $i \neq j$ thus $\underline{\tilde{p}_i} + \underline{\tilde{p}_j} = (\underline{\tilde{c}_i} + \underline{\tilde{c}_j})(\underline{\tilde{c}_k})$ has the same number of "1"s and the same number of "0"s and the same difference.

Thus: $\underline{\tilde{P}_k}$ is an orthogonal set.

Third Step: Compose $\underline{C}$ with $\underline{\tilde{C}}$ or $\underline{C}(\underline{\tilde{C}})$

$\underline{C}$		$\underline{\tilde{C}}$	
Number of "1"s	Number of "0"s	Number of "1"s	Number of "0"s
$\left(n2^{n-1} - w\left(\frac{1}{\underline{1+\alpha}}\right)\right)$	$\left(n2^{n-1} - \left(n - w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)$	$n2^{n-1}$	$n2^{n-1}$

* For $c_k \in C$ we define the set: $\underline{Z_k} = \underline{C}(\underline{\tilde{c}_k}) = \{\underline{z_i} = \underline{c_i}(\underline{\tilde{c}_k}), c_i \in C\}$ then:

a. The number of "1"s in $\underline{z_i}$ is:

$$= n2^{n-1}\left(\left(n2^{n-1} - w\left(\frac{1}{\underline{1+\alpha}}\right)\right) + \left(n2^{n-1} - \left(n - w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)\right)$$

$$= 2n^2 2^{2(n-1)} - n^2 2^{n-1}$$

b. The number of "0"s in $\underline{z_i}$ is:

$$= n2^{n-1}\left(\left(n2^{n-1} - w\left(\frac{1}{\underline{1+\alpha}}\right)\right) + \left(n2^{n-1} - \left(n - w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)\right)$$

$$= 2n^2 2^{2(n-1)} - n^2 2^{n-1}$$

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

d. for $\underline{z_i}, \underline{z_j} \in \underline{Z_k}$ the $\underline{z_i} + \underline{z_j} = (\underline{c_i} + \underline{c_j})(\underline{\tilde{c}_k})$ contains: $2n^2 2^{2(n-1)} - n^2 2^{n-1}$ of "1"s and the same number of "0" and the difference between the number of "1"s and the number of "0"s is zero.

Thus: $\underline{Z_k}$ is an orthogonal set**.**

Forth Step: Compos $\underline{\tilde{C}}$ with $\underline{C}$ or $\underline{\tilde{C}}(\underline{C})$

$\underline{\tilde{C}}$		$\underline{C}$	
Number of "1"s	Number of "0"s	Number of "1"s	Number of "0"s
$n2^{n-1}$	$n2^{n-1}$	$\left(n2^{n-1} - w\left(\frac{1}{\underline{1+\alpha}}\right)\right)$	$\left(n2^{n-1} - \left(n - w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)$

* For $c_k \in C$ we define the set: $\underline{\tilde{Z}_k} = \underline{\tilde{C}}(\underline{c_k}) = \{\underline{\tilde{z}_i} = \underline{\tilde{c}_i}(\underline{c_k}), c_i \in C\}$ then:

a. The number of "1"s in $\underline{\tilde{z}_i}$ is:

$$= n2^{n-1}\left(\left(n2^{n-1} - w\left(\frac{1}{\underline{1+\alpha}}\right)\right) + \left(n2^{n-1} - \left(n - w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)\right)$$

$$= 2n^2 2^{2(n-1)} - n^2 2^{n-1}$$

b. The number of "0"s in $\underline{\tilde{z}_i}$ is:

$$= n2^{n-1}\left(\left(n2^{n-1} - w\left(\frac{1}{\underline{1+\alpha}}\right)\right) + \left(n2^{n-1} - \left(n - w\left(\frac{1}{\underline{1+\alpha}}\right)\right)\right)\right)$$

$$= 2n^2 2^{2(n-1)} - n^2 2^{n-1}$$

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

d. for $\underline{\tilde{z}_i}, \underline{\tilde{z}_j} \in \underline{Z_k}$ the $\underline{\tilde{z}_i} + \underline{\tilde{z}_j} = (\underline{\tilde{c}_i} + \underline{\tilde{c}_j})(\underline{c_k})$ contains the same number of "1"s, the same number of "0"s and the same difference between the number of "1"s and the number of "0"s.

Thus $\underline{\tilde{Z}_k}$ is an orthogonal set**.**

Example 1. Using the prime polynomial $f(x) = x^3 + x + 1$ over F_2, extending F_2 to F_{2^3} and if α is a root of f(x) and prime element in F_{2^3} then $\{1, \alpha, \alpha^2\}$ is a basis of F_{2^3} and the following

Table 1: A binary representation of F_{2^3}

F_{2^3}	**Binary Representation**	F_{2^3}	**Binary Representation**
0	000	$\alpha^3 = \alpha + 1$	011
1	001	$\alpha^4 = \alpha^2 + \alpha$	110
α	010	$\alpha^5 = \alpha^2 + \alpha + 1$	111
α^2	100	$\alpha^6 = \alpha^2 + 1$	101

Table 2: Elements A and $\tilde{A}$ after adding the null column

$\tilde{a}_i$					a_i		0
$\tilde{a}_0$	1	α	α^2	α^3	α^4	α^5	α^6	0
$\tilde{a}_1$	α	α^2	α^3	α^4	α^5	α^6	1	0
$\tilde{a}_2$	α^2	α^3	α^4	α^5	α^6	1	α	0
$\tilde{a}_3$	α^3	α^4	α^5	α^6	1	α	α^2	0
$\tilde{a}_4$	α^4	α^5	α^6	1	α	α^2	α^3	0
$\tilde{a}_5$	α^5	α^6	1	α	α^2	α^3	α^4	0
$\tilde{a}_6$	α^6	1	α	α^2	α^3	α^4	α^5	0

$$S = 1 + \alpha + \alpha^2 + \alpha^3 + \ldots + \alpha^6 + 1 + \alpha + \ldots$$

$$s_1 = 1 \quad ; \quad s_2 = 1 + \alpha = \alpha^3 \quad ;$$

$$s_3 = 1 + \alpha + \alpha^2 = \alpha^5; \; s_4 = \alpha^5 + \alpha^3 = \alpha^2$$

$$s_5 = \alpha^2 + \alpha^4 = \alpha \; ; \; s_6 = \alpha + \alpha^5 = \alpha^2 + 1 \; ;$$

$$s_7 = \alpha^2 + 1 + \alpha^6 = 0 \; ; \; s_8 = 1$$

Noting that $\frac{1}{1+\alpha} = \alpha^{-3} = \alpha^4$.

Table 3: Elements C and $\tilde{C}$ in F_{2^3}

$\tilde{c}_i$					c_i			α^4
$\tilde{c}_0$	1	α^3	α^5	α^2	α	α^6	0	α^4
$\tilde{c}_1$	α^3	α^5	α^2	α	α^6	0	1	α^4
$\tilde{c}_2$	α^5	α^2	α	α^6	0	1	α^3	α^4
$\tilde{c}_3$	α^2	α	α^6	0	1	α^3	α^5	α^4
$\tilde{c}_4$	α	α^6	0	1	α^3	α^5	α^2	α^4
$\tilde{c}_5$	α^6	0	1	α^3	α^5	α^2	α	α^4
$\tilde{c}_6$	0	1	α^3	α^5	α^2	α	α^6	α^4

Table 4: Elements $\underline{C}$ and $\underline{\tilde{C}}$ in F_{2^3}

$\underline{\tilde{c}}_i$					c_i			110
$\underline{\tilde{c}}_0$	001	011	111	100	010	101	000	110
$\underline{\tilde{c}}_1$	011	111	100	010	101	000	001	110
$\underline{\tilde{c}}_2$	111	100	010	101	000	001	011	110
$\underline{\tilde{c}}_3$	100	010	101	000	001	011	111	110
$\underline{\tilde{c}}_4$	010	101	000	001	011	111	100	110
$\underline{\tilde{c}}_5$	101	000	001	011	111	100	010	110
$\underline{\tilde{c}}_6$	000	001	011	111	100	010	101	110

Noting that $w\left(\frac{1}{1+\alpha}\right) = w\left(\alpha^4\right) = 2$, we can find:

1. For $c_i \in C$, the number of ones is $3(2^{3-1}) - 2 = 10$ and the number of zeros i $3(2^{3-1}) - (3-2) = 11$ and $\underline{\tilde{c}}_i \in \underline{\tilde{C}}$, contains $3(2^{3-1})$ of ones and the same number of zeros .
2. For $c_i, c_j \in C, i \neq j$ then $\underline{c}_i + \underline{c}_j$ contains $3(2^{3-1}) = 12$ of ones (which is the number of
3. disagreement numbers between $\underline{c}_i, \underline{c}_j$) and $3(2^{3-1}) - 3 = 9$ of zeros (which is the
4. number of agreement numbers between $\underline{c}_i, \underline{c}_j$) , also $\underline{\tilde{C}}$ form a nonlinear orthogonal set.
5. Compose $\underline{\tilde{C}}$ with c_0 or $\underline{\tilde{C}}(c_0)$

$\underline{c}_0 = 00101111111000101010000, \quad \underline{\bar{c}}_0 = 11010000011101010111$

$\underline{\tilde{c}}_0(c_0) = 11010000011101010111\ 11010000011101010111\ 00101111111000101010000$

11010000011101010111 00101111111000101010000 00101111111000101010000

00101111111000101010000 00101111111000101010000 00101111111000101010000

00101111111000101010000 11010000011101010111 11010000011101010111

11010000011101010111 00101111111000101010000 11010000011101010111

00101111111000101010000 11010000011101010111 00101111111000101010000

11010000011101010111 11010000011101010111 11010000011101010111

00101111111000101010000 00101111111000101010000 11010000011101010111

$\underline{\tilde{c}}_1(c_0) = 11010000011101010111\ 00101111111000101010000\ 00101111111000101010000$

00101111111000101010000 00101111111000101010000 00101111111000101010000

00101111111000101010000 11010000011101010111 11010000011101010111

11010000011101010111 00101111111000101010000 11010000011101010111

00101111111000101010000 11010000011101010111 00101111111000101010000

11010000011101010111 11010000011101010111 11010000011101010111

11010000011101010111 11010000011101010111 00101111111000101010000

00101111111000101010000 00101111111000101010000 11010000011101010111

$\underline{\tilde{c}}_2(c_0) = 00101111111000101010000\ 00101111111000101010000\ 00101111111000101010000$

00101111111000101010000 11010000011101010111 11010000011101010111

11010000011101010111 00101111111000101010000 11010000011101010111

0010111111000010101000 1101000000111010101111 0010111111000010101000

1101000000111010101111 1101000000111010101111 1101000000111010101111

1101000000111010101111 1101000000111010101111 0010111111000010101000

1101000000111010101111 0010111111000010101000 0010111111000010101000

0010111111000010101000 0010111111000010101000 1101000000111010101111

$\tilde{\underline{c}}_3(c_0) =$0010111111000010101000 1101000000111010101111 1101000000111010101111

1101000000111010101111 0010111111000010101000 1101000000111010101111

0010111111000010101000 1101000000111010101111 0010111111000010101000

1101000000111010101111 1101000000111010101111 1101000000111010101111

1101000000111010101111 1101000000111010101111 0010111111000010101000

1101000000111010101111 0010111111000010101000 0010111111000010101000

0010111111000010101000 0010111111000010101000 0010111111000010101000

0010111111000010101000 0010111111000010101000 1101000000111010101111

$\tilde{\underline{c}}_4(c_0) =$1101000000111010101111 0010111111000010101000 1101000000111010101111

0010111111000010101000 1101000000111010101111 0010111111000010101000

1101000000111010101111 1101000000111010101111 1101000000111010101111

1101000000111010101111 1101000000111010101111 0010111111000010101000

1101000000111010101111 0010111111000010101000 0010111111000010101000

0010111111000010101000 0010111111000010101000 0010111111000010101000

0010111111000010101000 1101000000111010101111 1101000000111010101111

0010111111000010101000 0010111111000010101000 1101000000111010101111

$\tilde{\underline{c}}_5(c_0) =$0010111111000010101000 1101000000111010101111 0010111111000010101000

1101000000111010101111 1101000000111010101111 1101000000111010101111

1101000000111010101111 1101000000111010101111 0010111111000010101000

1101000000111010101111 0010111111000010101000 0010111111000010101000

0010111111000010101000 0010111111000010101000 0010111111000010101000

0010111111000010101000 1101000000111010101111 1101000000111010101111

1101000000111010101111 0010111111000010101000 1101000000111010101111

00101111110001010100 00101111110001010100 11010000011101010111

$\tilde{\underline{c}}_6(c_0)$ = 11010000011101010111 11010000011101010111 11010000011101010111

11010000011101010111 11010000011101010111 00101111100010101000

11010000011101010111 00101111100010101000 00101111100010101000

00101111100010101000 00101111100010101000 00101111100010101000

00101111100010101000 11010000011101010111 11010000011101010111

11010000011101010111 00101111100010101000 11010000011101010111

00101111100010101000 11010000011101010111 00101111100010101000

00101111100010101000 00101111100010101000 11010000011101010111

We can look that: Length $\tilde{\underline{C}}(\underline{c}_0)$ is $N_{\tilde{\underline{z}}} = n^2 2^n \left(2^n - 1\right)$ = $3(2^3)(2^3 - 1) = 168$,

Minimum distance is $d_{\tilde{\underline{z}}} = 2n^2 2^{2(n-1)} - n^2 2^{n-1}$ = $2(3^2)2^{2(3-1)} - 3^2 2^{3-1} = 252$.

Dimension ≥ 2

4. Conclusion

If α is a primitive element in the field F_{2^n} then the geometrical sequence $X = (1, \alpha, \alpha^2 ..., \alpha^n, ...)$ and S , where S is the sequence of i^{th} partial sum of X , are periodic with period $2^n - 1$, and: if C is the all permutations of one period of S, $\tilde{C}$ is extending of C by adding $\frac{1}{1+\alpha}$ to the end of each period in C and $\tilde{\underline{C}} \& \tilde{\underline{C}}$ the binary representation of $C \& \tilde{C}$ respectively, then:

1. The set C is cyclic sequences and form Reed Solomon code of: length $N = 2^n - 1$, minimum distance $D = 2^n - 2$ and dimension of *Span* C, $K \geq 2$.
2. The set $\underline{C}$ is nonlinear, not cyclic and *Span* $\underline{C}$ is Quasi-Orthogonal set (code) of order $\left[\left(n - 2w\left(\frac{1}{1+\alpha}\right)\right), n\right]$, with:length $\underline{N} = n(2^n - 1)$, minimum distance $\underline{d} = n\,2^{n-1} - w\left(\frac{1}{1+\alpha}\right)$ and dimension $\underline{K} \geq 2$.
3. The set $\tilde{C}$, extending C by adding $\frac{1}{1+\alpha}$, is nonlinear, not cyclic sequence and form codes with: length $\tilde{N} = 2^n$, minimum distance $\tilde{d} = 2^n - 1$ and *Span* $\tilde{C}$ of dimension $\tilde{k} \geq 2$.
4. The set $\tilde{\underline{C}}$ is nonlinear, not cyclic sequences and *Span* $\tilde{\underline{C}}$ form an orthogonal set (code) with:

length $\underset{\sim}{\tilde{N}} = n2^n$, minimum distance $\underset{\sim}{\tilde{d}} = n2^{n-1}$, and dimension $\underset{\sim}{\tilde{k}} \geq 2$.

5. The sets $\underline{P} = \underline{C}(\underline{C})$ are nonlinear, not cyclic and quasi-orthogonal sets with degrees:

$$\left[\left(n - 2w\left(\frac{1}{\underline{1+\alpha}}\right)\right)^2, \left[n^2 - 2n\, w\left(\frac{1}{\underline{1+\alpha}}\right)\right]\right]$$

6. The sets $\underset{\sim}{\tilde{P}} = \underset{\sim}{\tilde{C}}(\underset{\sim}{\tilde{C}})$ are orthogonal sequences with: length $\tilde{N}_{\underset{\sim}{\tilde{P}}} = n^2 2^{2n}$, minimum distance $\tilde{d}_{\underset{\sim}{\tilde{P}}} = 2n^2 2^{2(n-1)}$ and dimension ≥ 2.

7. The sets $\underline{Z} = \underline{C}(\underset{\sim}{\tilde{C}})$ are orthogonal sequences with: length $N_{\underline{z}} = n^2 2^n \left(2^n - 1\right)$, minimum distance $d_{\underline{z}} = 2n^2 2^{2(n-1)} - n^2 2^{n-1}$ and dimension $k_z \geq 2$.

8. The sets $\underset{\sim}{\tilde{Z}} = \underset{\sim}{\tilde{C}}(\underline{C})$ are orthogonal sequences with: length $N_{\underset{\sim}{\tilde{z}}} = n^2 2^n \left(2^n - 1\right)$, minimum distance $d_{\underset{\sim}{\tilde{z}}} = 2n^2 2^{2(n-1)} - n^2 2^{n-1}$ and dimension $k_{\underset{\sim}{\tilde{z}}} \geq 2$

5. Acknowledgment

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

References

1. Al Cheikha,A. H., Ruchin, J. (2014), Generation of orthogonal sequences by Walsh sequences, International Journal of Soft Computing and Engineering. 4(1), 182-184.
2. Al Cheikha, A. H. (2014), Composed Short Walsh's Sequences, American International Journal for Contemporary Scientific Research, 1(2), 81-88.
3. Al Cheikha, A. H. (2016, Feb.), Composed Reed Solomon Sequences. Paper presented at the 5th International Conference on Mathematics and Information Sciences, Cairo, Egypt, 11-13 Feb, 121-128.
4. Al Cheikha, A. H. (2016, July), Compose M-Sequences. Paper presented at Australian and New Zealand Business and Social Science Research Conference (ANZBSRC), Sydney, Australia, 17-18Sep, AJBSSIT , 3(3). (in press) ASIT
5. Al Cheikha, A. H. (2005), Generation of sets of sequences isomorphic to Walsh sequences. Qatar University Science Journal, 25, 16-30.
6. Fraleigh, J. B. (1971), A First course In Abstract Algebra. Fourth printing, USA: Addison-Wesley publishing company.
7. Gong, G., Youssef, A. M. (2002), Cryptographic properties of the Welch – Gong transformation

sequence Generators. IEEE- trans. information theory, l(48), No 11, 2837-2846.

8. Jong, N.S., Golomb, S.W., Gong, G., Lee, H.K., Gaal, P. (1998), Binary pseudorandom sequences for period 2n-1 with ideal autocorrelation. IEEE Transactions Information Theory, 44(2), 814-817.
9. Lee, J. S., Miller. L. E. (1998), CDMA Systems Engineering Handbook. Boston, London: Artech House.
10. Lidl, R., Niederreiter, H. (1986), Introduction to Finite Fields and Their Application. USA: Cambridge University
11. Mac Williams, F. J., Sloane, N. J. A., (1978), The theory of Error- correcting Codes, Amsterdam: North- Holland Publishing Company
12. Yang, K. Kim, P. Kumar, P., (2000), Quasi-orthogonal sequences for code -division - multiple- access systems, IEEE- Trans. information theory ,vol. 46 No 3, 982-993.