On Encoding of Reed Solomon Code using Walsh Transforms

Khalid Hadi Hameed Al-Jourany

Diayala University / College of Science / Department of Mathematics.

Abstract

This paper presents a method to encode Reed Solomon code based on Walsh transforms. Reed Solomon code is an error correcting code that is very important in telecommunications. Reed Solomon code and Walsh transforms are defined and discussed.Then , a method of encoding of Reed Solomon code are explained with examples.The results prove that Walsh transforms are easy in encoding Reed Solomon code.

Keywords: Reed Solomon code , galois field , error correcting codes, Walsh transforms , Fourier transforms .

Introduction

In 1960 , Iraving Reed and Gus Solomon published a paper in the Journal of the society for Industrial and Applied Mathematic [10] . This paper described a new class of error correcting codes that are now called Reed Solomon (R-S) codes . Error correcting codes are very useful in sending information over long distances or through channels where errors might occur in the message . they have become more prevalent as telecommunications have expanded and developed a use for codes that can self-correct , [8]. Reed Solomon codes have great power and utility , and are today found in many applications likes : Reed Solomon codes used in storage and communications industry ; Reed Solomon codes are used for orthogonal frequency division Multiplexing system ; compact discs (CD's) use Reed Solomon code so that a CD's player can read data from CD even if it has been corrupted by noise in the form of imperfections on the CD ; a new methods are designs Reed Solomon code for low power transceivers [2 ,4 , 5 ,7]. Petrus M. , [9] gave a new method to generate Reed Solomon encoder which is able to handle generic width of data variable length of information , number of error as well as variable form of primitive Polynomial and generator Polynomial used in the storage system.

Walsh transforms are orthogonal , normal and complete , [14] . They are important spectral representations of logic functions as the spectral Walsh domain with its global information provides much deeper in sight in to the logic structure of combinatorial networks than logic domain , [12].Spectral representation based on the Walsh transforms have been used in the classification of logic functions , functional decomposition , multiplexer , testing , and technology mapping , [11 , 13].

Galois Fields

Definition(2.1):

A Galois field (finite field) GF(q) is a q-ary set with two binary arithmetic operations , usually denoted + (addition) and * (multiplication) . The set GF(q) is closed , i.e. $x+y \in GF(q)$ and $x*y \in GF(q)$ for all $x, y \in GF(q)$.

Remark: GF(q) is an additive group and GF(q)/{0} is a multiplicative group.

Definition(2.2):

The set GF(q) = { 0 , 1 , . . . , q-1 } , (where q is prime) is a field of order q under modulo-q addition and multiplication . This field is called a prime field .

Example(2.1): The set GF(2) = { 0 , 1 } is a field of order 2 under modulo-2 addition and modulo-2 multiplication. It has the following addition and multiplications tables :

+	0	1
0	0	1
1	1	0

Table(2.1):modulo-2addition

*	0	1
0	0	0
1	0	1

Table(2.2):modulo- 2multiplication

This field is called a binary field and it satisfies : **1+1=0 , -1=1 , -0=0 , 1^{-1}=1**

Definition(2.3):

The set of all n-tuples (also called blocks, vectors or words of length n) with components in GF(q) is denoted by :

$GF(q,n) = GF(p^m,n)=\{ (x_0 , x_1 , ... , x_{n-1}) / x_0 , x_1 , ... , x_{n-1} \in GF(q) \}$

Where p is prime , m is a positive integer and q = 2 , 3 , 4 , 5 , 7 , 8 , 9 , 11 , 13 , 16 , 17 , ...

Its cardinality is $|GF(q,n)| = q^n$. An addition and λ scallar multiplication are defined component - by – component , i.e. for x , y ∈ GF(q) and $\lambda \in$ GF(q) :

$$\mathbf{X+Y} = (x_0 , x_1 , ... , x_{n-1}) + (y_0 , y_1 , ... , y_{n-1})$$

$$= (x_0+y_0 , x_1+y_1 , ... , x_{n-1}+y_{n-1})$$

$$\lambda * \mathbf{X} = \lambda * (x_0 , x_1 , ... , x_{n-1})$$

$$= (\lambda *x_0 , \lambda *x_1 , ... , \lambda *x_{n-1})$$

Hence , $\mathbf{X+Y} \in GF(q,n)$ and $\lambda * \mathbf{X} \in GF(q,n)$ for all **X , Y** ∈ GF(q,n) and all $\lambda \in GF(q)$.

In this section , we construct the galois field $GF(2^n)$ of 2^n elements ($n > 1$) from the binary field GF(2) . we begin with the two elements 0 and 1 , from GF(2) and anew symbol α . Then , we define a multiplication (*) to introduce a sequence of power of α as follows :

$\alpha^2 = \alpha * \alpha$, $\alpha^3 = \alpha * \alpha * \alpha$ . . . , $\alpha^j = \alpha * \alpha * . . . * \alpha$ for j –times , . . .

Now , we have the following set of elements :

$GF(2^n) = \{ o , 1 , \alpha , \alpha^2 , \alpha^3 , . . . , \alpha^j , . . . \}$ .Now , suppose $\mathbf{p}(x)$ is a primitive polynomial of degree n over GF(2) such that $\mathbf{p}(\alpha) = 0$, then $\mathbf{p}(x)$ divides $x^{2^n-1} +1$,and so we have : $x^{2^n-1} +1 = Q(x)\, \mathbf{p}(x)$. If we replace x by α , we obtain :

$$\alpha^{2^n-1} +1 = Q(\alpha)\, \mathbf{p}(\alpha) = Q(\alpha) .0 = 0$$

This implies : $\alpha^{2^n-1} +1 = 0$

Adding 1 to both sides (use modulo-2 addition) :

$\alpha^{2^n-1} =1$, and hence $\alpha^{2^n} = \alpha$. Therefore , the set above becomes finite and consist of the 2^n elements : $GF(2^n) = \{ o , 1 , \alpha^1, \alpha^2 , \alpha^3 , . . . , \alpha^{2^n-2} \}$

$$= \{ o , \alpha^0 , \alpha^1, \alpha^2 , \alpha^3 , . . . , \alpha^{2^n-2} \}$$

Note :

1-In the construction of the Galois field $GF(2^n)$, we use a primitive polynomial $\mathbf{p}(x)$ of degree n and require that the element α be a root of $\mathbf{p}(x)$. Since the powers of α generate all the nonzero elements of $GF(2^n)$, α is a primitive element . Table (2.3) shows some primitive polynomials .

2-The power representation is used in multiplying or dividing the elements of $GF(2^n)$ as :

$$\alpha^i * \alpha^j = \alpha^{i+j} = \begin{cases} \alpha^{i+j} & ; \quad i+j < 2^n - 1 \\ \alpha^{i+j-(2^n-1)} & ; \quad i+j > 2^n - 1 \\ 1 & ; \quad i+j = 2^n - 1 \\ o & \quad o.w \end{cases} \quad . . . (1)$$

3-A n-tuple representation is used for adding the elements of GF(2^n) by adding the corresponding components of their n-tuples in modulo-2 addition .

Table (2.3) : Some primitive polynomials.

N	p(x)
3	$1+ x+ x^3$
4	$1+ x+ x^4$
5	$1+ x^2+ x^5$
6	$1+ x+ x^6$
7	$1+ x^3+ x^7$

Example(2.1):

Let galois field GF(2^3)be construct as follow :

Since , n = 3 , then , from table (2.3) the primitive polynomial is **p**(x) = $1+ x+ x^3$ and let ∝ an element of the extension field be defined as a root of the polynomial **p**(x) : **p**(∝) = 0

$$1+\alpha+\alpha^3 = 0$$

$$\alpha^3 = -1-\alpha \qquad . . . \quad (2)$$

Since , in the binary field +1 = -1 , then , $\propto^3$ can be represented as follows :

$$\propto^3 = 1+\propto$$

$$\propto^4 = \propto + \propto^2$$

Now , consider $\propto^5$, where , $\propto^5 = 1+\propto +\propto^2$

Now , for $\propto^6$: $\propto^6 = 1+\propto^2$

Now , for $\propto^7$: $\propto^7 = 1 = \propto^0$

There for the eight finite field elements of $GF(2^3)$ are :

$GF(2^3) = \{ o , \propto^0 , \propto^1, \propto^2 , \propto^3 , \propto^4, \propto^5 , \propto^6 \} = \{ (0,0,0) , (0,0,1) , (0,1,0) , (0,1,1) , (1,0,0) , (1,0,1) , (1,1,0) , (1,1,1) \}$

Two arithmetic operations , addition and multiplication for this $GF(2^3)$ are shown in table (2.4) and table (2.5) .

Table(2.4):Addition of $GF(2^3)$

+	$\propto^0$	$\propto^1$	$\propto^2$	$\propto^3$	$\propto^4$	$\propto^5$	$\propto^6$
$\propto^0$	0	$^3\propto$	$\propto^6$	$\propto^1$	$\propto^5$	$\propto^4$	$^2\propto$
$\propto^1$	$^3\propto$	0	$^4\propto$	$^0\propto$	$^2\propto$	$^6\propto$	$^5\propto$
$\propto^2$	$^6\propto$	$^4\propto$	0	$^5\propto$	$^1\propto$	$^3\propto$	$^0\propto$
$\propto^3$	$^1\propto$	$^0\propto$	$^5\propto$	0	$^6\propto$	$^2\propto$	$^4\propto$
$\propto^4$	$^5\propto$	$^2\propto$	$^1\propto$	$^6\propto$	0	$^0\propto$	$^3\propto$
$\propto^5$	$^4\propto$	$^6\propto$	$^3\propto$	$^2\propto$	$^0\propto$	0	$^1\propto$
$\propto^6$	$^2\propto$	$^5\propto$	$^0\propto$	$^4\propto$	$^3\propto$	$^1\propto$	0

*	$\propto^0$	$\propto^1$	$\propto^2$	$\propto^3$	$\propto^4$	$\propto^5$	$\propto^6$
$\propto^0$	${}^0\propto$	${}^1\propto$	$\propto^2$	$\propto^3$	$\propto^4$	$\propto^5$	${}^6\propto$
$\propto^1$	${}^1\propto$	${}^2\propto$	${}^3\propto$	${}^4\propto$	${}^5\propto$	${}^6\propto$	${}^0\propto$
$\propto^2$	${}^2\propto$	${}^3\propto$	${}^4\propto$	${}^5\propto$	${}^6\propto$	${}^0\propto$	${}^1\propto$
$\propto^3$	${}^3\propto$	${}^4\propto$	${}^5\propto$	${}^6\propto$	${}^0\propto$	${}^1\propto$	${}^2\propto$
$\propto^4$	${}^4\propto$	${}^5\propto$	${}^6\propto$	${}^0\propto$	${}^1\propto$	${}^2\propto$	${}^3\propto$
$\propto^5$	${}^5\propto$	${}^6\propto$	${}^0\propto$	${}^1\propto$	${}^2\propto$	${}^3\propto$	${}^4\propto$
$\propto^6$	${}^6\propto$	${}^0\propto$	${}^1\propto$	${}^2\propto$	${}^3\propto$	${}^4\propto$	${}^5\propto$

Table(2.5):Multiplication of GF(2^3)

Example(2.2): If $n = 4$, then , the galois field GF(2^4) can be construct as follow :

From table (2.3) , the primitive polynomial is $\mathbf{p}(x) = 1 + x + x^4$ and let $\propto$,an element of the extension field be defined as a root of the polynomial $\mathbf{p}(x)$:

$$\mathbf{p}(\propto) = 0$$

$$1 + \propto + \propto^4 = 0$$

$$\propto^4 = -1 - \propto$$

Since , in the binary field $+1 = -1$, $\propto^4$ can be represented as follows :

$$\propto^4 = 1 + \propto$$

Now , consider $\propto^5$, where $\propto^5 = \propto + \propto^2$

Now , for $\propto^6$: $\propto^6 = \propto^2 + \propto^3$

Now , for $\propto^7$: $\propto^7 = 1 + \propto + \propto^3$

For α^8 : $\alpha^8 == 1+\alpha^2$

Now , consider α^9 : $\alpha^9= \alpha+\alpha^3$

Now , for α^{10} : $\alpha^{10}= 1+\alpha+\alpha^2$

Now , for α^{11} : $\alpha^{11} = \alpha+\alpha^2+\alpha^3$

Now , for α^{12} : $\alpha^{12} = 1+\alpha+\alpha^2+\alpha^3$

Now , consider , α^{13} : $\alpha^{13} = 1+\alpha^2 +\alpha^3$

Now , for α^{14} : $\alpha^{14}= 1+\alpha^3$

Now , for α^{15} : $\alpha^{15}=1$

There for the sixteen finite field elements of $GF(2^4)$ are :

$GF(2^4) = \{ 0 , \alpha^0 , \alpha^1 , \alpha^2 , \alpha^3 , \alpha^4, \alpha^5 , \alpha^6 , \alpha^7 , \alpha^8, \alpha^9 , \alpha^{10}, \alpha^{11} , \alpha^{12}, \alpha^{13} , \alpha^{14} \}$

The arithmetic operations ,addition and multiplication for this $GF(2^4)$are shown in the table(2.6)and the table (2.7)

+	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$
$^{0}\alpha$	0	$^{4}\alpha$	$^{8}\alpha$	$^{14}\alpha$	$^{1}\alpha$	$^{10}\alpha$	$^{13}\alpha$	$^{9}\alpha$	$^{2}\alpha$	$^{7}\alpha$	$^{5}\alpha$	$^{12}\alpha$	$^{0}\alpha$	$^{6}\alpha$	$^{3}\alpha$
$^{1}\alpha$	$^{4}\alpha$	0	$^{5}\alpha$	$^{9}\alpha$	$^{0}\alpha$	$^{2}\alpha$	$^{11}\alpha$	$^{14}\alpha$	$^{10}\alpha$	$^{3}\alpha$	$^{8}\alpha$	$^{6}\alpha$	$^{0}\alpha$	$^{12}\alpha$	$^{7}\alpha$
$^{2}\alpha$	$^{8}\alpha$	$^{5}\alpha$	0	$^{6}\alpha$	$^{10}\alpha$	$^{1}\alpha$	$^{3}\alpha$	$^{12}\alpha$	$^{0}\alpha$	$^{11}\alpha$	$^{4}\alpha$	$^{9}\alpha$	$^{0}\alpha$	$^{14}\alpha$	$^{13}\alpha$
$^{3}\alpha$	$^{14}\alpha$	$^{9}\alpha$	$^{6}\alpha$	0	$^{7}\alpha$	$^{11}\alpha$	$^{2}\alpha$	$^{4}\alpha$	$^{13}\alpha$	$^{1}\alpha$	$^{1}\alpha$	$^{5}\alpha$	$^{0}\alpha$	$^{8}\alpha$	$^{0}\alpha$
$^{4}\alpha$	$^{1}\alpha$	$^{0}\alpha$	$^{10}\alpha$	$^{7}\alpha$	0	$^{8}\alpha$	$^{12}\alpha$	$^{3}\alpha$	$^{5}\alpha$	$^{14}\alpha$	$^{2}\alpha$	$^{13}\alpha$	$^{0}\alpha$	$^{11}\alpha$	$^{9}\alpha$
$^{5}\alpha$	$^{10}\alpha$	$^{2}\alpha$	$^{1}\alpha$	$^{11}\alpha$	$^{8}\alpha$	0	$^{9}\alpha$	$^{13}\alpha$	$^{4}\alpha$	$^{6}\alpha$	$^{0}\alpha$	$^{3}\alpha$	$^{0}\alpha$	$^{7}\alpha$	$^{12}\alpha$
$^{6}\alpha$	$^{13}\alpha$	$^{11}\alpha$	$^{3}\alpha$	$^{2}\alpha$	$^{12}\alpha$	$^{9}\alpha$	0	$^{10}\alpha$	$^{14}\alpha$	$^{5}\alpha$	$^{7}\alpha$	$^{1}\alpha$	$^{0}\alpha$	$^{0}\alpha$	$^{8}\alpha$
$^{7}\alpha$	$^{9}\alpha$	$^{14}\alpha$	$^{12}\alpha$	$^{4}\alpha$	$^{3}\alpha$	$^{13}\alpha$	$^{10}\alpha$	0	$^{11}\alpha$	$^{0}\alpha$	$^{6}\alpha$	$^{8}\alpha$	$^{0}\alpha$	$^{5}\alpha$	$^{1}\alpha$
$^{8}\alpha$	$^{2}\alpha$	$^{10}\alpha$	$^{0}\alpha$	$^{13}\alpha$	$^{5}\alpha$	$^{4}\alpha$	$^{14}\alpha$	$^{11}\alpha$	0	$^{12}\alpha$	$^{1}\alpha$	$^{7}\alpha$	$^{0}\alpha$	$^{3}\alpha$	$^{6}\alpha$
$^{9}\alpha$	$^{7}\alpha$	$^{3}\alpha$	$^{11}\alpha$	$^{1}\alpha$	$^{14}\alpha$	$^{6}\alpha$	$^{5}\alpha$	$^{0}\alpha$	$^{12}\alpha$	0	$^{13}\alpha$	$^{2}\alpha$	$^{0}\alpha$	$^{10}\alpha$	$^{4}\alpha$
$^{10}\alpha$	$^{5}\alpha$	$^{8}\alpha$	$^{4}\alpha$	$^{12}\alpha$	$^{2}\alpha$	$^{0}\alpha$	$^{7}\alpha$	$^{6}\alpha$	$^{1}\alpha$	$^{13}\alpha$	0	$^{14}\alpha$	$^{0}\alpha$	$^{9}\alpha$	$^{11}\alpha$
$^{11}\alpha$	$^{12}\alpha$	$^{6}\alpha$	$^{9}\alpha$	$^{5}\alpha$	$^{13}\alpha$	$^{3}\alpha$	$^{1}\alpha$	$^{8}\alpha$	$^{7}\alpha$	$^{2}\alpha$	$^{14}\alpha$	0	$^{0}\alpha$	$^{4}\alpha$	$^{10}\alpha$
$^{12}\alpha$	$^{11}\alpha$	$^{13}\alpha$	$^{7}\alpha$	$^{10}\alpha$	$^{6}\alpha$	$^{14}\alpha$	$^{4}\alpha$	$^{2}\alpha$	$^{9}\alpha$	$^{8}\alpha$	$^{3}\alpha$	$^{0}\alpha$	0	$^{1}\alpha$	$^{5}\alpha$
$^{13}\alpha$	$^{6}\alpha$	$^{12}\alpha$	$^{14}\alpha$	$^{8}\alpha$	$^{11}\alpha$	$^{7}\alpha$	$^{0}\alpha$	$^{5}\alpha$	$^{3}\alpha$	$^{10}\alpha$	$^{9}\alpha$	$^{4}\alpha$	$^{0}\alpha$	0	$^{2}\alpha$
$^{14}\alpha$	$^{3}\alpha$	$^{0}\alpha$	$^{13}\alpha$	$^{0}\alpha$	$^{9}\alpha$	$^{12}\alpha$	$^{8}\alpha$	$^{1}\alpha$	$^{6}\alpha$	$^{4}\alpha$	$^{11}\alpha$	$^{10}\alpha$	$^{0}\alpha$	$^{2}\alpha$	0

Table (2.6) : Addition of GF(2^4)

*	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$
$^{0}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$
$^{1}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$
$^{2}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$
$^{3}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$
$^{4}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$
$^{5}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$
$^{6}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$
$^{7}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$
$^{8}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$
$^{9}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$
$^{10}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$
$^{11}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$
$^{12}\alpha$	$^{12}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$
$^{13}\alpha$	$^{13}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$
$^{14}\alpha$	$^{14}\alpha$	$^{0}\alpha$	$^{1}\alpha$	$^{2}\alpha$	$^{3}\alpha$	$^{4}\alpha$	$^{5}\alpha$	$^{6}\alpha$	$^{7}\alpha$	$^{8}\alpha$	$^{9}\alpha$	$^{10}\alpha$	$^{11}\alpha$	$^{12}\alpha$	$^{13}\alpha$

Table (2.7) : Multiplication of GF(2^4)

Reed Solomon code

Reed Solomon code is the widespread use for forward error correcting in digital transmission which was able to correct multiple noise/ errors , especially in correcting burst noise/error.Multiple random symbol errors can be detect and correct in a systematic way which described by Reed Solomon codes. Reed Solomon codes are non binary cyclic codes with symbols that made up of n-bit sequences , where n is any positive integer value greater than 2 .

Reed Solomon codes can be defined as (m,k) as below :

$$(m,k) = (2^n-1 , 2^n-1-2t)$$

Where , n is the symbol length , m is the codeword length , k is the information data length , t is the error correcting capability , and m-k = 2t is the number of parity symbols .

Walsh Transforms Techniques for Reed Solomon code

In this section , we define Walsh transform of order $N = 2^n$, where n is appositive integer , then ,we will use these transforms to encode Reed Solomon code . These are shown as follows :

Let $C_i , i = 0,1,2, \ . \ . \ ., N-1$, be a sequences of numbers . The discrete Walsh transform of the given sequence is a sequence of N spectral values defined as :

$$W_k = \sum_{i=0}^{N-1} C_i \, w_{ik} \qquad ,k = 0,1, \dots , N-1 \qquad . \ . \ . \ (3)$$

Where , w_{ik} take only the value 0 or 1 . Figure (4.1) shows the Walsh transforms of order $= 2^3 = 8$, and , $N = 2^4 = 16$

$$w_{ik} = \begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 1&1&1&1&0&0&0&0 \\ 1&1&0&0&0&0&1&1 \\ 1&1&0&0&1&1&0&0 \\ 1&0&0&1&1&0&0&1 \\ 1&0&0&1&0&1&1&0 \\ 1&0&1&0&0&1&0&1 \\ 1&0&1&0&1&0&1&0 \end{bmatrix}$$

(a)Walsh transform of order $N = 2^3 = 8$

$$w_{ik} = \begin{bmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1 \\ 1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1 \\ 1&1&0&0&0&0&1&1&0&0&1&1&1&1&0&0 \\ 1&1&0&0&1&1&0&0&0&0&1&1&0&0&1&1 \\ 1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0 \\ 1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1 \\ 1&0&0&1&1&0&0&1&0&1&1&0&0&1&1&0 \\ 1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1 \\ 1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1 \\ 1&0&1&0&0&1&0&1&1&0&1&0&0&1&0&1 \\ 1&0&1&0&0&1&0&1&0&1&0&1&1&0&1&0 \\ 1&0&1&0&1&0&1&0&0&1&0&1&0&1&0&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0 \end{bmatrix}$$

(b) Walsh transform of order $N = 2^4 = 16$

Figure (4.1) : Walsh transform [3].

The discrete Walsh transform , in eq. (3) required only $N(N\text{-}1)$ additions and multiplications .

Let us show how Walsh transform used to encode of Reed Solomon codes . This is shown as follows :

Let $r = r_0 , r_1 , ... , r_{N-1}$ be a vector of finite field elements in GF(2^n) , where N is the order of a primitive element $\propto$ of GF(2^n) . The finite field Walsh transform of r is another vector of N elements in $GF(2^n)$, which we denote as **R={** R_k} , k= 0,1,2,. . . , N-1 , where the elements of **R** are given by :

$$R_k = \sum_{i=0}^{N-1} r_i w_{ik} \quad ,k = 0,1,\ldots,N-1 \qquad \ldots (4)$$

For our present , it is useful to write eq. (4) in the form of matrix equation as :

$$\mathbf{R} = \mathbf{r}\,\mathbf{W} \qquad \ldots \quad (5)$$

Example:

Encode the Reed Solomon RS(7,3) code by using Walsh transform method

Solution:

$$RS(m,k) = (2^n-1\ ,\ 2^n-1-2t) = (7,3)$$

From above , we have : n=3 , k=3 , and t=2. Since , n=3 , then , from example(2.1) in section 2 , we have the galoise field $GF(2^3)$ as follow :

$GF(2^3) = \{ o\ , \alpha^0\ , \alpha^1, \alpha^2\ , \alpha^3\ , \alpha^4, \alpha^5\ , \alpha^6 \} = \{r_0\ , r_1\ , r_2\ , r_3\ , r_4\ , r_5\ , r_6\ , r_7\}$.

From eq. (3) , and fig. (4.1,a) , we get :

$$\mathbf{R} = \mathbf{r}\,\mathbf{W} = (o\ , \alpha^0\ , \alpha^1, \alpha^2\ , \alpha^3\ , \alpha^4, \alpha^5\ , \alpha^6)\begin{bmatrix} 1&1&1&1&1&1&1&1\\ 1&1&1&1&0&0&0&0\\ 1&1&0&0&0&0&1&1\\ 1&1&0&0&1&1&0&0\\ 1&0&0&1&1&0&0&1\\ 1&0&0&1&0&1&1&0\\ 1&0&1&0&0&1&0&1\\ 1&0&1&0&1&0&1&0 \end{bmatrix}$$

$$= [\ 0, 0+\alpha^0+\alpha^1+\alpha^2, 0+\alpha^0+\alpha^5+\alpha^6, 0+\alpha^0+\alpha^3+\alpha^4, 0+\alpha^2+\alpha^3+\alpha^6, 0+\alpha^2+\alpha^4+\alpha^5,$$
$$0+\alpha^1+\alpha^4+\alpha^6, 0+\alpha^1+\alpha^3+\alpha^5]$$

$$= [\ 0, \alpha^5, \alpha^3, \alpha^2, \alpha^1, \alpha^6, \alpha^0, \alpha^4] \qquad \text{(By using table (2.4))}$$

The number of arithmetic operations in this example is 56 additions and multiplications .

Example(4.2):

Encode the Reed Solomon RS(15,7) code by using Walsh transform method

Solution :

$$RS(m,k) = (2^n-1 , 2^n-1-2t) =(15,7)$$

From above , we get : n=4 , k=7 , and t=4. Since , n=4 , then , from example(2.2) in section 2 , we have the galoise field $GF(2^4)$ as follow :

$GF(2^3) =\{ o , \alpha^0 , \alpha^1, \alpha^2 , \alpha^3 , \alpha^4, \alpha^5 , \alpha^6, \alpha^7 , \alpha^8, \alpha^9 , \alpha^{10} , \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}$

$=\{r_0 , r_1 , r_2 , r_3 , r_4 , r_5 , r_6 , r_7, r_8 , r_9 , r_{10} , r_{11} , r_{12} , r_{13} , r_{14} , r_{15}\}$

From eq. (3) , and fig. (4.1,b) , we get :

R = r W$=[o + \alpha^0 +\alpha^1+ \alpha^2 +\alpha^3 + \alpha^4+ \alpha^5 + \alpha^6+ \alpha^7 + \alpha^8+ \alpha^9 + \alpha^{10} + \alpha^{11}+ \alpha^{12}+ \alpha^{13}+ \alpha^{14}, o + \alpha^0 +\alpha^1+ \alpha^2 +\alpha^3 + \alpha^4+ \alpha^5 + \alpha^6, o + \alpha^0 +\alpha^1+ \alpha^2 +\alpha^{11}+ \alpha^{12}+ \alpha^{13} + \alpha^{14}, o + \alpha^0 +\alpha^1+ \alpha^2 +\alpha^7 + \alpha^8+ \alpha^9+ \alpha^{10}, o + \alpha^0 +\alpha^5+ \alpha^6 +\alpha^7 + \alpha^8+ \alpha^{13} + \alpha^{14}, o + \alpha^0 +\alpha^5+ \alpha^6 +\alpha^9 + \alpha^{10}+ \alpha^{11} + \alpha^{12}, o + \alpha^0 +\alpha^3+ \alpha^4 +\alpha^9 + \alpha^{10}+ \alpha^{13} + \alpha^{14}, o + \alpha^0 +\alpha^3+ \alpha^4 +\alpha^7 + \alpha^8+ \alpha^{11} + \alpha^{12}, o + \alpha^2 +\alpha^3+ \alpha^6 +\alpha^7+ \alpha^{11}+ \alpha^{14} , o + \alpha^2 +\alpha^3+ \alpha^6 +\alpha^8 + \alpha^9+ \alpha^{10} + \alpha^{12}+ \alpha^{13}, o + \alpha^2 +\alpha^4+ \alpha^5 +\alpha^8 + \alpha^9+ \alpha^{10} + \alpha^{11}+ \alpha^{14} , o + \alpha^2+\alpha^4+ \alpha^5 +\alpha^7 + \alpha^{12}+ \alpha^{13} , o + \alpha^1 +\alpha^4+ \alpha^6 +\alpha^7 + \alpha^9+ \alpha^{19} + \alpha^{12}+ \alpha^{14} , o + \alpha^1+\alpha^4+ \alpha^6 +\alpha^8 + \alpha^{11}+ \alpha^{13} , o + \alpha^1 +\alpha^3+ \alpha^5 +\alpha^8 + \alpha^{12}+ \alpha^{14} , o + \alpha^1 +\alpha^3+ \alpha^5 +\alpha^7 + \alpha^9+ \alpha^{10}+ \alpha^{11}+ \alpha^{13}]$

$=[o , \alpha^1 , \alpha^1, \alpha^2 , \alpha^0 , \alpha^{10}, \alpha^4 , \alpha^8, \alpha^6 , \alpha^9, \alpha^{11} , \alpha^3 , \alpha^{13}, \alpha^7, \alpha^{12}, \alpha^{12}]$ (By using table (2.6))

The number of arithmetic operations in this example is 240 additions and multiplications. Arnold,M., and Allen ,H. [1] used the discrete Fourier transform to encode Reed Solomon code . The number of arithmetic operations in discrete Fourier transform is N^2 complex multiplications and N(N-1) complex additions. If we use the discrete Fourier transform in example(4.1) , we have (64) complex multiplications and (56) complex additions, also, in example(4.2), we have (256) complex multiplications and (240) complex additions.

Conclusions

1-In this paper ,the galois field of order 8 and 16 is constructed with two operations : addition and multiplication , which is very useful in coding theory .

2-The encoding of Reed Solomon code by using Walsh transform is very easy .

3- The discrete Walsh transform has an inherent computational advantage over the discrete Fourier transform . The discrete Walsh transform requires only real addition operations while the discrete Fourier transform requires complex multiplications .

References

1. Arnold,M., and Allen,H., "Error-control techniques for digital communication"United states of America.John Wiley and Sons,1985.
2. Chen,l., and Carrasco,R.,"Soft decoding of algebraic-geometric codes using koetter-vardyalgorithm".Electronics letters 3rd December 2009.Vol.45.No.25.
3. Falkowski,B., and Sasao,T.,"Unified algorithm to generate Walsh functions in four different orderings and its programmable hard ware implementations".IEEproc.Image signal process.,Vol.152,No.6,December 2005.
4. Hamood,S.,and Widad,I.,"The development and implementation of Reed Solomon codes for OFDM using soft ware defined Radio platform"International Journal of computer science and communication.Vol.1,No.1,January-June 2010,pp.129-136.
5. Hoeve,H.,Timmermans.J., and Vries,L.,"Error correction and concealment in the compact disc system ".philips Tech .Rev.,40:166-172,1982.
6. Kabatiansky ,G.,Krouk,E.,and Semenor,S."Error correcting coding and security for data net works".John wiley and Sons ,ltd,2005.
7. Loinel,B.,"Reed Solomon codes for low power communications".Journal of communications,Vol.3,No.2,April 2008 .
8. Moon,T.,"Error correcting coding :Mathematical Methods and Algorithms".United states of America :Johnwily and Sons ;2005.

9. petrus,M.,"Generic ReedSolomonencoder".Makara,Sains ,Vol.10,No.2,November 2006. pp.58-62.
10. Reed,I.,S.,and Solomon ,G.,"polynomial codes over certain Finite Fields".SIAM Journal of applied Mathe.,Vol.8,1960,pp.300-304.
11. Sasao,T.,"Cascade realizations of two-input valued output functions using decompositions of group functions."Proc.33rd IEEE Int.symp.on Multiple. Valued Logic ,Tokyo,Japan,May 2003.
12. Stankovic,R.,S., Stankovic, M., and Jankovic, D., Spectral transforms in switchingtheory, definitions and calculations".Nauka,Belgrade,Yougoslavia,1998.
13. Stankouic,R.,S.,and Astola,J.,T.,"Spectral Interpretation of decision diagrams".Springer-Verlag ,NewYork,2003.
14. Yaroslavsky,L.,P.,"Digital holography and digital image processing :principles ,methods, algorithms". Kluwer Academic ,Boston ,2003.