Application of Paley Functions in Error Correcting Codes

Khalid Hadi Hameed

Rokan khaji Mohammed

Diayala University / College of Science /

Department of Mathematics

Abstract:

In this Paper, we will use the Paley functions definition to correcting codes, as well as, we will give some properties of Paley functions in linear codes. Also, we will construct the first, second and third of Paley functions. These orders are representing as binary code which take only two value 0 or 1.

Such a Paley function (matrix) generator can be used to encode and decode the message transform.

Finally, we give some examples to show how this method work.

Key Words:- Paley Function, Linear Cods, Hamming Distance, Hamming Weight, Paley Matrices.

الخلاصـة:

في هذا البحث سوف نتناول تعريف دوال البيلي لتصحيح الشفرات و خواص دوال البيلي في الشفرات الخطية، ومن ثم نشتق دوال البيلي من الرتب الأولى و الثانية والثالثة وهذه الدوال تمثل بالشفرة الثنائية والتي تأخذ القيم 0 أو 1 .

حيث استخدمنا مصفوفة دالة البيلي بعد اشتقاقها لتشفير و إلغاء تشفير الرسالة المرسلة وبعض الأمثلة أعطيت لتوضيح كيفية عمل هذه الطريقة.

Introduction:

The Paley function were first defined by the American mathematician Paley, [7]. His definition is based on finite products of Rademacher function,[1].

Paley functions are belong to class of orthogonal functions which contain only the value +1 and -1, which is very useful in error correcting codes. These functions are used to define a new way to generate Walsh functions, [2],[3],[6].

Walsh functions are orthogonal functions on the half interval [0,1), which take only the value +1 and -1. These functions are used in many field, like, signal processing (spectroscopy, speech processing, medical applications and seismology) and communications (multiplexing system, coding system and non-sinusoidal electromagnetic radiation),[1],[2].

1- Definitions of Terms and Operations:

Definition(1):

A linear code of length n over the alphapet F_p . where, p is a positive integer and F be a field is a subspace of F_p^n . The dimension k of linear code C is the dimension of C as an F_p -vector space ,[4].

Definition(2):

A word of length n over the alphapet F_p is a vector $x=(x_1,x_2,...,x_n)\in F_p^n$. Let $x=(x_1,x_2,...,x_n)\in F_p^n$ and $y=(y_1,y_2,...,y_n)\in F_2^n$ be two vectors of length n ; then their Hamming distance is defined by:

$$d_H(x,y)=\#\{i:x_i\neq y_i, i=1,2,...,n\} \qquad ... (1-1)$$

i.e it is the number of positions in which the two words differ,[4].

For example: Let $x=(0,1,1,0,1)$ and $y=(0,1,0,1,1)$. Then, the Hamming distance is 2 .

Definition(3):

The Hamming weight $W_t(x)$ of an element $x \in F_p^n$ is the number of its nonzero coordinates, [4].

For example: The Hamming weight of $x = (0,1,1,0,1)$ is 3.

The vector space used in this paper composed of strings of length 2^m. Where m is a positive integer of numbers in field $F_2 = \{0,1\}$. Vectors can be manipulated by three main operations: addition, multiplication and the dot product.

For two vectors $x = (x_1, x_2, \ldots, x_n) \in F_2^n$ and $y = (y_1, y_2, \ldots, y_n) \in F_2^n$, addition is defined by:

$$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \in F_2^n \qquad \ldots(1-2)$$

Where, each x_i *or* y_i is either 1 *or* 0, $\forall i, i = 1,2,\ldots,n$ and $1+1=0$, $0+1=1, 1+0=1, 0+0=0$.

For example: if x and y are in F_2^8 as follow:

$x = (1,0,0,1,1,1,1,0)$ and $y = (1,1,1,0,0,0,0,1)$, then

the sum of x and y is

$$\begin{aligned} x + y &= (1,0,0,1,1,1,1,0) + (1,1,1,0,0,0,0,1) \\ &= (1+1, 0+1, 0+1, 1+0, 1+0, 1+0, 1+0, 0+1) \\ &= (0,1,1,1,1,1,1,1) \end{aligned}$$

The addition of a scalar $\alpha \in F_2 = \{0,1\}$ to vector x is defined by:

$$\alpha + x = (\alpha + x_1, \alpha + x_2, \ldots, \alpha + x_n) \qquad \ldots(1-3)$$

Multiplication is defined by the formula:

$$x * y = (x_1 * y_1, x_2 * y_2, ..., x_n * y_n) \qquad ...(1-4)$$

Where, each x_i *or* y_i is either 1 *or* 0, $\forall i, i = 1, 2, ..., n$ and $1 * 1 = 1$, $0 * 1 = 0, 1 * 0 = 0, 0 * 0 = 0$.

For example: Let

$x = (1, 0, 0, 1, 1, 1, 1, 0)$ and $y = (1, 1, 1, 0, 0, 0, 0, 1)$, then the multiplication of x and y is

$$\begin{aligned} x * y &= (1,0,0,1,1,1,1,0) * (1,1,1,0,0,0,0,1) \\ &= (1*1, 0*1, 0*1, 1*0, 1*0, 1*0, 1*0, 0*1) \\ &= (1,0,0,0,0,0,0,0) \end{aligned}$$

The multiplication of a scalar $\alpha \in F_2 = \{0,1\}$ to vector x is defined by:

$$\alpha * x = (\alpha x_1, \alpha x_2, ..., \alpha x_n) \qquad ...(1-5)$$

An example:

$$\begin{aligned} 0 * (1,0,0,1,1,1,1,0) &= (0*1, 0*0, 0*0, 0*1, 0*1, 0*1, 0*1, 0*0) \\ &= (0,0,0,0,0,0,0,0) \end{aligned}$$

The dot product of x and y is defined by :

$$x \bullet y = (x_1 * y_1 + x_2 * y_2 + ... + x_n * y_n) \in F_2 \qquad ...(1-6)$$

For example: using x and y from above

$$\begin{aligned} x \bullet y &= 1*1 + 0*1 + 0*1 + 1*0 + 1*0 + 1*0 + 1*0 + 0*1 \\ &= 1 + 0 + 0 + 0 + 0 + 0 + 0 + 0 \\ &= 1 + 0 \\ &= 1 \end{aligned}$$

2-Paley Functions:

For integer $i = 0,1,\ldots,2^n - 1, t \in [0,1),$ the Paley function is

$$P_i(t) = \prod_{k=1}^{n} R_k(t) = \prod_{k=1}^{n} (-1)^{i_k t_k} \qquad \ldots (2-1)$$

Where, $\boldsymbol{R}$ is the Rademacher function,[5].

$$i = (i_n, i_{n-1}, \ldots, i_1)_2, \quad i_k \in F_2 = \{0,1\}, \forall k, k = 1,2,\ldots,n$$

$$t = \frac{i}{2^n}, \; i = 0,1,\ldots,2^n - 1 \;\; and \; t_k = (0.t_n, t_{n-1}, \ldots, t_1)_2,$$

$$t_k \in F_2 = \{0,1\}, \forall k, k = 1,2,\ldots,n.$$

The first order of Paley functions (n=1):

If $n = 1$, then, we have:

$i = 0,1$, $t = \frac{i}{2}$, $i = 0,1$:

Where, $i = 0$ then $t = 0, \frac{1}{2}$:

$$P_0(0) = \prod_{k=1}^{1} (-1)^{i_k t_k} = (-1)^0 = 1$$

$$P_0(\tfrac{1}{2}) = P_0(0.5) = P_0((0.1)_2) = \prod_{k=1}^{1} (-1)^{i_k t_k} = (-1)^0 = 1$$

Where, $i = 1$, then $t = 0, \frac{1}{2}$:

$$P_1(0) = \prod_{k=1}^{1} (-1)^{i_k t_k} = (-1)^{i_1 t_1} = (-1)^0 = 1$$

$$P_1(\tfrac{1}{2}) = P_1(0.5) = \prod_{k=1}^{1} (-1)^{i_k t_k} = (-1)^1 = -1$$

We can represent the first order of Paley functions in the matrix form:

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{matrix} P_0(t) \\ P_1(t) \end{matrix}$$

Also, we can represent the first order Paley matrix in the binary form by replacing "1" with "0" to express the matrix using in the logic elements $\{0,1\}$:

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

The second order of Paley Functions (n=2):
if $n = 2$, then , we get:
$i = 0,1,2,3 \quad , \ t = \frac{i}{4} \ , \ i = 0,1,2,3 :$
Where $i = 0 \quad , \ t = 0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$

$$P_0(0) = \prod_{k=1}^{2}(-1)^{i_k t_k} = (-1)^{i_1 t_1}(-1)^{i_2 t_2} = (-1)^0 (-1)^0 = 1 * 1 = 1$$

$$P_0(\tfrac{1}{4}) = P_0(0.25) = P_0((0.01)_2) = \prod_{k=1}^{2}(-1)^{i_k t_k} = (-1)^{i_1 t_1}(-1)^{i_2 t_2} = (-1)^0 (-1)^0 = 1$$

$$P_0(\tfrac{1}{2}) = P_0(0.5) = P_0((0.10)_2) = \prod_{k=1}^{2}(-1)^{i_k t_k} = (-1)^{i_1 t_1}(-1)^{i_2 t_2} = (-1)^0 (-1)^0 = 1$$

$$P_0(\tfrac{3}{4}) = P_0(0.75) = P_0((0.11)_2) = \prod_{k=1}^{2}(-1)^{i_k t_k} = (-1)^{i_1 t_1}(-1)^{i_2 t_2} = (-1)^0 (-1)^0 = 1$$

Where $i = 1 \quad , \ t = 0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$

$$P_1(0) = \prod_{k=1}^{2}(-1)^{i_k t_k} = (-1)^{i_1 t_1}(-1)^{i_2 t_2} = (-1)^0 (-1)^0 = 1 * 1 = 1$$

$$P_1(\tfrac{1}{4}) = P_1(0.25) = P_1((0.01)_2) = \prod_{k=1}^{2}(-1)^{i_k t_k} = (-1)^{i_1 t_1}(-1)^{i_2 t_2} = (-1)^1 (-1)^0 = -1$$

$$P_1(\tfrac{1}{2}) = P_1(0.5) = P_1((0.10)_2) = \prod_{k=1}^{2}(-1)^{i_k t_k} = (-1)^{i_1 t_1}(-1)^{i_2 t_2} = (-1)^0 (-1)^0 = 1$$

$$P_1(\tfrac{3}{4}) = P_1(0.75) = P_1((0.11)_2) = \prod_{k=1}^{2}(-1)^{i_k t_k} = (-1)^{i_1 t_1}(-1)^{i_2 t_2} = (-1)^1 (-1)^0 = -1$$

Where $i = 2 \quad , \ t = 0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$

$$P_2(0)=\prod_{k=1}^{2}(-1)^{i_k t_k}=(-1)^{i_1 t_1}(-1)^{i_2 t_2}=(-1)^0(-1)^0=1*1=1$$

$$P_2(\tfrac{1}{4})=P_2(0.25)=P_2((0.01)_2)=\prod_{k=1}^{2}(-1)^{i_k t_k}=(-1)^{i_1 t_1}(-1)^{i_2 t_2}=(-1)^0(-1)^0=1$$

$$P_2(\tfrac{1}{2})=P_2(0.5)=P_2((0.10)_2)=\prod_{k=1}^{2}(-1)^{i_k t_k}=(-1)^{i_1 t_1}(-1)^{i_2 t_2}=(-1)^0(-1)^1=-1$$

$$P_2(\tfrac{3}{4})=P_2(0.75)=P_2((0.11)_2)=\prod_{k=1}^{2}(-1)^{i_k t_k}=(-1)^{i_1 t_1}(-1)^{i_2 t_2}=(-1)^0(-1)^1=-1$$

Where $i=3$, $t=0,\frac{1}{4},\frac{1}{2},\frac{3}{4}$

$$P_3(0)=\prod_{k=1}^{2}(-1)^{i_k t_k}=(-1)^{i_1 t_1}(-1)^{i_2 t_2}=(-1)^0(-1)^0=1*1=1$$

$$P_3(\tfrac{1}{4})=P_3(0.25)=P_3((0.01)_2)=\prod_{k=1}^{2}(-1)^{i_k t_k}=(-1)^{i_1 t_1}(-1)^{i_2 t_2}=(-1)^1(-1)^0=-1$$

$$P_3(\tfrac{1}{2})=P_3(0.5)=P_3((0.10)_2)=\prod_{k=1}^{2}(-1)^{i_k t_k}=(-1)^{i_1 t_1}(-1)^{i_2 t_2}=(-1)^0(-1)^1=-1$$

$$P_3(\tfrac{3}{4})=P_3(0.75)=P_3((0.11)_2)=\prod_{k=1}^{2}(-1)^{i_k t_k}=(-1)^{i_1 t_1}(-1)^{i_2 t_2}=(-1)^1(-1)^1=1$$

The second order of Paley function can be represent as matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{matrix} P_0(t) \\ P_1(t) \\ P_2(t) \\ P_3(t) \end{matrix}$$

This matrix can be transform to binary form as follows:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

The third order of Paley functions(n=3):

if $n = 3$, then:

$i = 0,1,2,3,4,5,6,7 \quad , \; t = \frac{i}{8} \; , \; i = 0,1,2,3,4,5,6,7$:

Table (2-1) shows the third order of Paley functions.

$t = (0, t_1, \ldots$ / $i = (i_n, \ldots i_1)_2$	(0.0,0,0)	(0.0,0,1)	(0.0,1,0)	(0.0,1,1)	(0.1,0,0)	(0.1,0,1)	(0.1,1,0)	(0.1,1,1)
$(0,0,0)_2$	1	1	1	1	1	1	1	1
$(0,0,1)_2$	1	−1	1	−1	1	−1	1	−1
$(0,1,0)_2$	1	1	−1	−1	1	1	−1	−1
$(0,1,1)_2$	1	−1	−1	1	1	−1	−1	1
$(1,0,0)_2$	1	1	1	1	−1	−1	−1	−1
$(1,0,1)_2$	1	−1	1	−1	−1	1	−1	1
$(1,1,0)_2$	1	1	−1	−1	−1	−1	1	1
$(1,1,1)_2$	1	−1	−1	1	−1	1	1	−1

Table (2-1) the third order of Paley functions

Also, we can be represent the third order of Paley functions in the form of matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \end{bmatrix}$$

The binary form of this matrix is shown as follows:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Table (2-3) shows the Hamming distance and the Hamming weight, for first, second and third order of Paley functions.

order n	*Hamming distance*	*Hamming weight*
1	1	2 , 1
2	2 , 2	4,2,2,2
3	4	8,4,4,4,4,4,4,4

Table (2-3): the Hamming distance and Hamming weight

3- Encoding messages by using Paley matrices:

In this section, we will generate the first , second and third order of paley matrices the form of binary form to encode the messages transform. These are shown as follows:

The generating matrix of the first order Paley matrix is

$$G_{p_1} = (1,1)$$

To encode the message, we multiply each vector of length one in $F_2 = \{0,1\}$ with G_{p_1} as follows:

$$0 * G_{p_1} = 0*(1,1) = (0,0)$$
$$0 * G_{p_1} = 1*(1,1) = (1,1)$$

Also, the generating matrix of the second order Paley matrix is:

$$G_{p_1} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

To encode the message, we multiply each vector of length two in F_2^2 with G_{p_2} . This is shown as follows:

$$(0,0) * G_{p_2} = (0,0) * \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} = (0,0,0,0)$$
$$(0,1) * G_{p_2} = (0,1) * \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} = (1,1,0,0)$$
$$(1,0) * G_{p_2} = (1,0) * \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} = (1,0,1,0)$$

$$(1,1)*G_{p_2} = (1,1)*\begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} = (0,1,1,0)$$

Also, the generating matrix of the third order Paley matrix is:

$$G_{p_1} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

To encode the message, we multiply each vector of length three in F_2^3 with G_{p_3}, as follows:

$$(0,0,0)*G_{p_3} = (0,0,0,0,0,0,0,0)$$
$$(0,0,1)*G_{p_3} = (1,0,0,1,1,0,0,1)$$
$$(0,1,0)*G_{p_3} = (1,1,0,0,1,1,0,0)$$
$$(0,1,1)*G_{p_3} = (0,1,0,1,0,1,0,1)$$
$$(1,0,0)*G_{p_3} = (1,0,1,0,1,0,1,0)$$
$$(1,0,1)*G_{p_3} = (0,0,1,1,0,0,1,1)$$
$$(1,1,0)*G_{p_3} = (0,1,1,0,0,1,1,0)$$
$$(1,1,1)*G_{p_3} = (1,1,1,1,1,1,1,1)$$

Figure (3-1) shows the block code of first, second and third code of Paley matrices:

$$P_1 = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \quad , \quad P_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

a- first block code of Paley matrix

b- second block code of Paley matrix

$$P_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

c- third block code of Paley matrix

Figure (3-1) shows the block codes of Paley matrix

4- Decoding messages by using Paley matrix codes:

In this section, we will use P_1, P_2, P_3 of Paley matrix code to decode the messages transform.
This method is shown as:
Before, we begin, we will give mention to the error-correcting code capabilities of Paley matrix code of order $1,2,3$.

The distance between any two code word in P_1, P_2 *and* P_3 are 2^{p-1} , where , $p-tuples$ over the field F_2. The received word w is multiplied by a Paley matrix code (P_1, P_2, P_3) to form $w * P_n$, where n is the order of Paley matrix code.

If $w * P_n = \theta$, (θ *is zero vector*) ,then , the received word w is in Paley matrix code (P_1, P_2, P_3) but if $w * P_n \neq \theta$, then ,the received word is not in Paley matrix code , this means that , the received word is received in error. In order to find the location of error in w in $r * P_n$, with the each column of Paley matrix which gives the location of error in w . Some examples are given to show how this method work:

Example (1):

If the original message is $m=(0,1,1)$ using P_3, then, the encoded massage is $(0,1,0,1,0,1,0,1)$ because the distance in P_3 is $2^{3-1}=4$, this code can correct one error. Let the encoded massage after the error be $w=(0,1,0,1,0,1,0,0)$. we decoded it as follows:

$$w*P_3=(0,1,0,1,0,1,0,0)*\begin{bmatrix}0&0&0&0&0&0&0&0\\1&0&0&1&1&0&0&1\\1&1&0&0&1&1&0&0\\0&1&0&1&0&1&0&1\\1&0&1&0&1&0&1&0\\0&0&1&1&0&0&1&1\\0&1&1&0&0&1&1&0\\1&1&1&1&1&1&1&1\end{bmatrix}$$

$$=(1,0,1,0,1,0,1,0)$$

This vector is similar to eight column of , then , we an see that, the error was in the eight place, and we write $w=(0,1,0,1,0,1,0,1)$, then, we can see that, the original message was $m=(0,1,1)$.

Example (2):

If the original message is $m=(1,1,0)$ using P_3, then, the encoded massage is $(0,1,1,0,0,1,1,0)$. Let the encoded the massage after the error be $w=(1,1,1,0,0,1,1,0)$ we decoded it as follows:

$$w*P_3=(1,0,0,1,0,1,1,0)$$

This vector is similar to one column of P_3, then, we can see that, the error was in the one place, and we write $w=(0,1,1,0,0,1,1,0)$, then, we can see that, the original massage was $m=(1,1,0)$.

5- Conclusion:

1- in this paper, we construct the first, second, third and fourth order of paley functions and transform these order to binary form to use in error correcting codes.

2- Since, Paley functions are belong to class of orthogonal functions, they are can be used in coding theory, and error correcting codes and others.

3- Finally, the encode and decode messages transform by using Paley matrix code is very easy.

References:

1- Beauchamp, K. G., "Applications of walsh functions and related functions with an introduction to sequency theory", Academic press, London, 1984.

2- Beauchamp, K. G., "walsh Functions and their Applications", Academic press, London, 1975.

3- Blyth, W. F., May, R. L., and Widyaningsih p., "volterra integral equations solved in fredholm from using walsh functions", ANZIAM J.45(E), pp. c269-c282, 2004.

4- Jacobus, H. 1973. "coding theory", springerverlag, Berlin, Heidelberg, New York.

5- Oliver Hunt., November, 2004. "Image coding using orthogonal Basic Functions", University of Canterbury Christchurch, New Zealand America.

6- Porwik P., 2002, " Efficient Calculation 0f the Reed-Muller forms by Means of the Walsh Spectrum". Int. J. Appl. Math. Comp. Sci. 12(4): 571-579.

7- Paley, R. E. A. C., "Aremarkable series of orthogonal functions". Proc. London. Math. Soc. 34, 241-297, (1932).