On representation of Hadamard Codes

Ass.teacher
Hameed k. Dawiod
M.Sc mathematices

Ass.teacher
Khalid H. Hameed
M.Sc mathematices

Abstract:

In this paper, we give a form of Hadamard codes with respect to Rademacher functions. Hadamard codes are defined and encoding matrices and also discussed.Finally , two methods of decoding are explained and an example is given to clarify these methods.

1- Introduction :

Hadamard matrices (codes) were defined by the French mathematician M.J.Hadamard in 1893,[Hadamard," Resolution d'une question relative aux dêterminants " ,pp . 240-246,(1893)], called now Hadamard matrices.Hadamard matrix is a square array of +1,-1 whose rows and columns are mutually orthogonal.If the first row and first column contain only +1 ,the matrix is said to be in normal form.We can replace "+1" with "0" and "-1" with "1" to express Hadamard matrix using the logic elements {0,1}.

Since, Hadamard codes are orthogonal and belong to class of linear codes,they are used in error correcting codes.Error correcting codes (E.C.C)which are very useful in sending information over long distances or through channels where errors might occur in the message. Hadamard code was used by B.j.Falkowski and T.Sasao, [Falkowski and Sasao, "Unified algorithm to generate Walash functions in four different orderings and its programmable hardware implementations",p.822,2005], to generate Walsh functions.Walsh functions were invented in 1923 by the American mathematician J.L.Walsh (1895-1973) ,see,[Walsh, "Aclosed set of normal orthogonal functions",pp.5-

24,(1923)]. Walsh functions are used in image processing, see [Yaroslavsky,"Digital holography and digital image processing: principle,methods,algorithms",p.50].

2- preliminaries :

The vector spaces used in this paper composed of sequences of length $n = 2^p$ (where p is a positive integer),of numbers in $F_2 = \{0,1\}$,and we can denote it as F_2^n .The codewords of a Hadamard code form a subspace of such space.

For two vectors $u = (u_1, u_2, ..., u_n)$ and $v = (v_1, v_2, ..., v_n)$ addition is defined by:

$$u \oplus v = (u_1 \oplus v_1, u_2 \oplus v_2, ..., u_n \oplus v_n)$$

where, each u_i or v_i is either 1 or 0 , i = 1,2,...,n , and

$$1 \oplus 1 = 0 \quad ,0 \oplus 1 = 1 \quad ,1 \oplus 0 = 1 \quad ,0 \oplus 0 = 0$$

Multiplication is defined by the formula ,

$$u * v = (u_1 * v_1, u_2 * v_2, ..., u_n * v_n)$$

where, each u_i and v_i is either 1 or 0 , i = 1,2,...,n , and

$$1 * 1 = 1 \quad ,0 * 1 = 0 \quad ,1 * 0 = 0 \quad ,0 * 0 = 0$$

Definition (1) :

Let u , v be two vectors in F_2^n .The Hamming distance between two vectors u and v , denoted by d(u,v) , is the number of the places in which they differ.

For example ,if u and v are defined as u = (0,1,0,0) and v = (1,0,0,1) , then,the Hamming distance between u and v is 3, i.e . d(u,v) = d((0,1,0,0),(1,0,0,1)) = 3 .

3. Hadamard code and Encoding Matrices:

Hadamard matrix of order n is generated by the follwing formula :

$$H_1 = [\ 1\ ] \equiv [\ 0\ ]$$

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad H_n = H_2 \otimes H_{n/2}$$

where, $\otimes$ denotes the kronecker product.The kronecker product also called tensor product or the direct product of two matrices A and B is defined as follows :

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix}$$

For example :

$$H_4 = H_2 \otimes H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

In this section , we will use Radamecher functions to generate Hadamard matrices (codes) of order $n = 2^p$ (where, p is a positive integer) as follows:

$$G_{p\times n} = \begin{bmatrix} R_p \\ R_{p-1} \\ . \\ . \\ . \\ R_2 \\ R_1 \end{bmatrix} = \begin{bmatrix} r_{p,1} & r_{p,2} & \dots & r_{p,n} \\ r_{p-1,1} & r_{p-1,2} & \dots & r_{p-1,n} \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ r_{2,1} & r_{2,2} & \dots & r_{2,n} \\ r_{1,1} & r_{1,2} & \dots & r_{1,n} \end{bmatrix}$$

where $G_{p\times n}$ is p×n generator matrix whose rows are the consecutive p Rademacher functions (sequences),which form a basis for Hadamard matrix, and $r_{i,j} \in F_2 = \{0,1\}, \forall i, i = 1,2,\dots,p,\ j = 1,2,\dots,n.$

Rademacher functions were defined by the German mathematician Rademacher in 1922, [Rademacher, ” Einige Sätze von allgenein orthogonal funktionen”,pp.112-138,(1922)] . Rademacher functions with $n=2^4=16$ pulses are shown in figure(3.1), along with the sequence representation of the functions in the logical elements {0,1}, which are called Rademacher sequences.

Example (1)

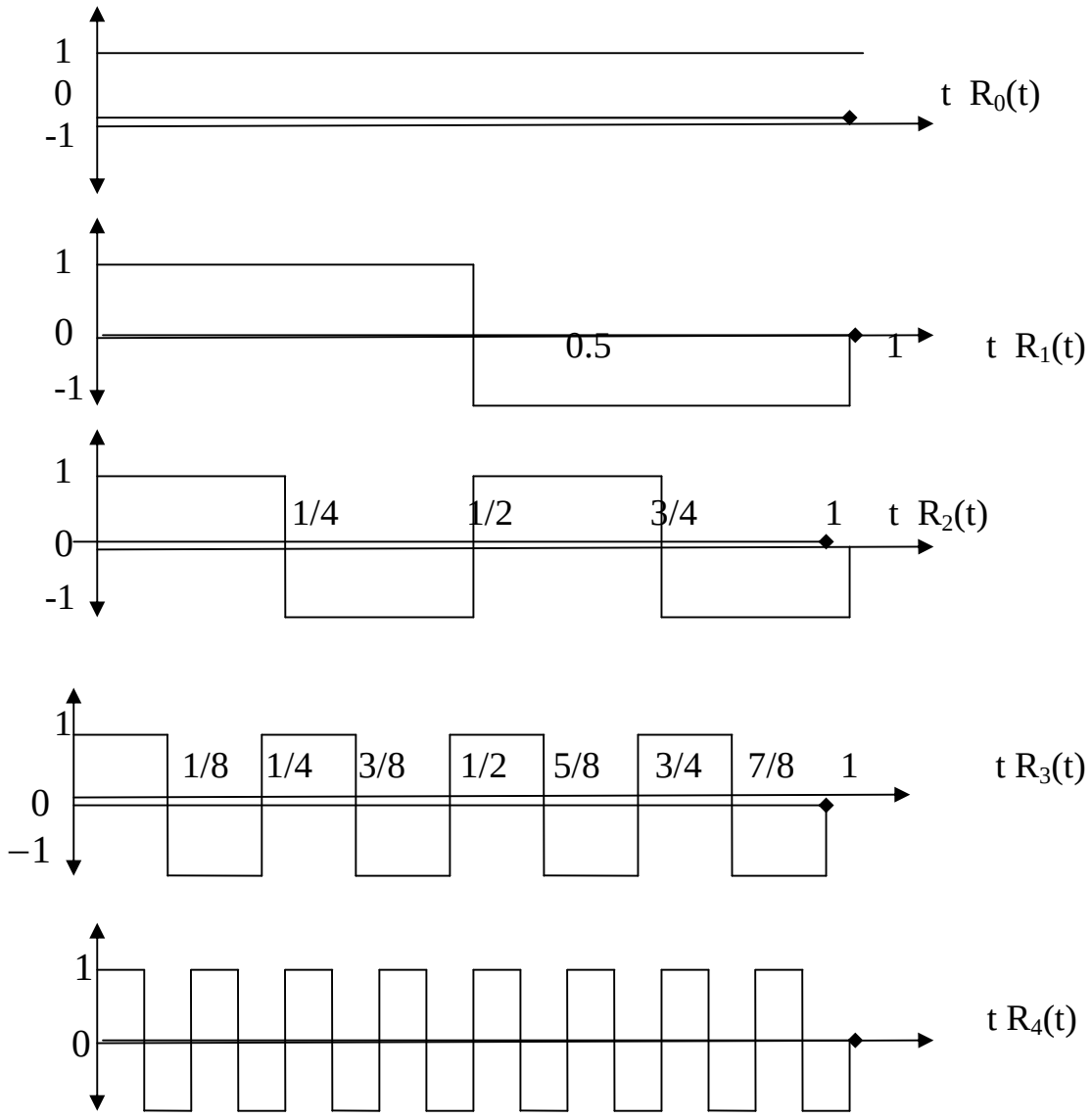
The generator matrix for Hadamard matrix(code) of order two i.e n = 2, (p = 1) is :

$$G_{1\times 2} = [R_1] = [r_{1,2} \quad r_{1,2}] = [0 \quad 1]$$

Example (2)

The generator matrix for Hadamard matrix (code) of order four i.e $n = 2^2 = 4$, (p =2) is :

$$G_{2\times 4} = \begin{bmatrix} R_2 \\ R_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$



$R_0 \equiv (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
$R_1 \equiv (0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1)$
$R_2 \equiv (0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1)$
$R_3 \equiv (0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1)$
$R_4 \equiv (0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1)$

Fig.(3.1): The graphs of $R_0, R_1, \ldots, R_4$ Rademacher functions (Rademacher sequences) .

The encoding of p-tuple message sequences into Hadamard sequences (Hadamard codewords) of length $n = 2^p$ is shown as follows :

For $m \le n-1$,we write the binary of m as :

$(m)_b = (\alpha_i, \alpha_{i-1}, ..., \alpha_1, \alpha_0)$,then $H_m = (m)_b * G_{p \times n}$,

where, $\alpha_i \in F_2, \forall\, i, i = 0,1,...., p, (m)_b$ is p-tuple message sequence, and H_m is the m- th Hadamard sequence (codeword).Hadamard matrices (codes) of order n = 2,4,8,16 are shown in tables (3.1) ,(3.2),(3.3) and (3.4) respectively.

Table (3.1): Hadamard matrix(code) of order n = 2,($H_{(2,1)}$ code)

Integer (m)	1-tuple message sequence ($(m)_b$)	Hadamard codeword $H_m = (m)_b\, G_{1\times 2}$
0	(0)	H_0 = (0,0)
1	(1)	H_1 = (0,1)

Table (3.2) : Hadamard matrix(code) of order n = 4, ($H_{(4,2)}$ code)

Integer (m)	2-tuple message sequence ($(m)_b$)	Hadamard codeword $H_m = (m)_b\, G_{2\times 4}$
0	(0,0)	H_0 = (0,0,0,0)
1	(0,1)	H_1 = (0,0,1,1)
2	(1,0)	H_2 = (0,1,0,1)
3	(1,1)	H_3 = (0,1,1,0)

Table (3.3) : Hadamard matrix(code) of order n = 8, ($H_{(8,3)}$ code)

Integer (m)	3-tuple message sequence ($(m)_b$)	Hadamard codeword $H_m = (m)_b\, G_{3\times 8}$
0	(0,0,0)	H_0 = (0,0,0,0,0,0,0,0)
1	(0,0,1)	H_1 = (0,0,0,0,1,1,1,1)
2	(0,1,0)	H_2 = (0,0,1,1,0,0,1,1)
3	(0,1,1)	H_3 = (0,0,1,1,1,1,0,0)
4	(1,0,0)	H_4 = (0,1,0,1,0,1,0,1)
5	(1,0,1)	H_5= (0,1,0,1,1,0,1,0)
6	(1,1,0)	H_6= (0,1,1,0,0,1,1,0)
7	(1,1,1)	H_7= (0,1,1,0,1,0,0,1)

Table (3.4) : Hadamard matrix(code) of order n = 16 , ($H_{(16,4)}$ code)

Integer (m)	4-tuple message sequence $((m)_b)$	Hadamard codeword $H_m = (m)_b G_{4\times16}$
0	(0,0,0,0)	H_0 = (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
1	(0,0,0,1)	H_1 = (0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1)
2	(0,0,1,0)	H_2 = (0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1)
3	(0,0,1,1)	H_3 = (0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0)
4	(0,1,0,0)	H_4 = (0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1)
5	(0,1,0,1)	H_5= (0,0,1,1,0,0,1,1,1,1,0,0,1,1,0,0)
6	(0,1,1,0)	H_6= (0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0)
7	(0,1,1,1)	H_7= (0,0,1,1,1,1,0,0,1,1,0,0,0,0,1,1)
8	(1,0,0,0)	H_8= (0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1)
9	(1,0,0,1)	H_9= (0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0)
10	(1,0,1,0)	H_{10}= (0,1,0,1,1,0,1,0,0,1,0,1,1,0,1,0)
11	(1,0,1,1)	H_{11}= (0,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1)
12	(1,1,0,0)	H_{12}= (0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0)
13	(1,1,0,1)	H_{13}= (0,1,1,0,0,1,1,0,1,0,0,1,0,1,0,1)
14	(1,1,1,0)	H_{14}= (0,1,1,0,1,0,0,1,0,1,1,0,1,0,0,1)
15	(1,1,1,1)	H_{15}= (0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0)

4. Hadamard Decoding methods :

In this section,we will introduce two methods for decoding Hadamard codwords:

Let w be received word :

Method (1) :

Find the closest codeword $u \in H_{(n,p)}$ such that

$$d(w,u) \le d(w,v), \forall v \in H_{(n,p)}$$

Method (2) :

This method composed of two steps:

Step 1 :

Compute $S = H_{(n,p)} * w^t$

Step 2 :

If $S = \theta$,(where , θ is a zero vector),then the received word is a codeword in Hadamard code $H_{(n,p)}$,but,if $S \neq \theta$,the

receivedword w is received in error.Ih order to find the location of error in w, we compaired S with the each column of Hadamard code which gives the location of error in w.

For example ,if the original message is (1,1,0) by using Hadamard code of order n = 8, then the encoded message is H_6=(0,1,1,0,0,1,1,0). Let the encoded message H_6 after the error be $w=$ (0,1,0,0,0,1,1,0). We decode it as follows :

By 1st method :

$$d(w,H_0)=3, d(w,H_3)=5, d(w,H_6)=1$$

$$d(w,H_1)=3, d(w,H_4)=3, d(w,H_7)=5$$

$$d(w,H_2)=5, d(w,H_5)=3$$

We see that $d(w,H_6)\le d(w,H_i), \forall i, i=0,1,...,7,$ and thus H_6 is the codeword that is most likely to have been transmitted.

By 2nd method :

$$S=H_{(8,3)} * w^t = \begin{bmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&1&1&1&1\\ 0&0&1&1&0&0&1&1\\ 0&0&1&1&1&1&0&0\\ 0&1&0&1&0&1&0&1\\ 0&1&0&1&1&0&1&0\\ 0&1&1&0&0&1&1&0\\ 0&1&1&0&1&0&0&1 \end{bmatrix} * \begin{bmatrix} 0\\1\\0\\0\\0\\1\\1\\0 \end{bmatrix} = \begin{bmatrix} 0\\0\\1\\1\\0\\0\\1\\1 \end{bmatrix}$$

S is similar to third column of Hadamard code of order n=8 , therefore we can see that the error was in the third place of w ,and we write , w =(0,1,1,0,0,1,1,0) . Since , $w\in H_{(8,3)}$ code,therefore we can see that the original message was (1,1,0).

5- Conclusions

1- Generating or rpresenting of Hadamard matrices (codes) from using Rademacher functions (sequences) is easy to find.
2- Encoding Hadamard matrices are very quick and easy with respect to kronecker product method .
3- A new algorithm is given in section four which as we think is very efficient than Hamming method.It can be straightforward to implement.

6- References

[1] Falkowski,B.J. and Sasao T., "Unified algorithm to generate Walsh functions in four different orderings and its programmable hardware implementations", IEE proc. Vis. Image process., V.152,No.6,December 2005.

[2] Hadamard,M.J.," Rêsolution d'une question relative aux dêterminants" ,Bull. Sci. math. A17,240-246,1893.

[3] Rademacher,H.,"Einige Sätze von allgemeinen orthogonal funktionen",Math.Annal.,112-138, 1922.

[4] Walsh,J.L."Aclosed set of normal orthogonal functions" , Amer.J.Math.45,pp.5-24,1923.

[5] Yaroslavsky,L.P."Digital holography and digital image processing: principles,methods,algorithms",KluwerAcademic, Boston,2003.