Hadamard's Coding Matrix and Some Decoding Methods

Hizer Leka, Azir Jusufi and Faton Kabashi

April 22, 2020

Hadamard's coding matrix and some decoding methods

Hizer Leka[1] Azir Jusufi[2] Faton Kabashi[3]

[8th] UBT, Higher Education Institution, Kosova

[1]*hizer.leka@ubt-uni.net*, [2]azir.jusufi@ubt-uni.net , [3]faton.kabashi@ubt-uni.net

Abstact

In this paper, we will show a way to form Hadamard's code order $n = 2^p$ (where p is a positive integer) with the help of Rademacher functions, through which matrix elements are generated whose binary numbers $\{0,1\}$, while its columns are Hadamard's encodings and are called Hadamard's coding matrix. Two illustrative examples will be taken to illustrate this way of forming the coding matrix. Then, in a graphical manner and by means of Hadamard's form codes, the message sequence encoding as the order coding matrix will be shown. It will also give Hadamard two methods of decoding messages, which are based on the so-called Haming distance. Haming's distance between two vectors u and v was denoted by $d(u,v)$ and represents the number of places in which they differ. In the end, four conclusions will be given, where a comparison will be made of encoding and decoding messages through Haming's coding matrices and distances.

Keywords: *Hadamard's code,* encoding, *decoding, Rademache function, Hamming distance*

1 Introduction

Definition 1.1. A Hadamard matrix of order n, H_n, is an $n \times n$ square matrix with elements $+1$ 'shat n and -1's such $H_n \cdot H_n^T = nI_n$, where I_n is the identity matrix of order n. [3]

Examples of Hadamard matrix order 1, 2 and 4 [3]:

$$H_1 = [1] \text{ ; } H_1^{'} = [-1] \text{ ; } H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ ; } H_2^{'} = \begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix} \text{ ; } H_2^{''} = \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \text{ ; } H_4^{'} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix} \text{ ; } H_4^{''} = \begin{bmatrix} -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{bmatrix}.$$

Hadamard's matrix of order n is generated by the following formula:

$$H_n = H_2 \otimes H_{n/2}$$

where $\otimes$ is the product of Kroneker.

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

Exemple,

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

$$H_8 = H_2 \otimes H_4 = \begin{bmatrix} H_4 & H_4 \\ H_4 & -H_4 \end{bmatrix} \quad \text{and} \quad H_{16} = H_2 \otimes H_8 = \begin{bmatrix} H_8 & H_8 \\ H_8 & -H_8 \end{bmatrix}$$

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. $d(u,v) = d((0,1,0,0),(1,0,0,1)) = 3$. [1]

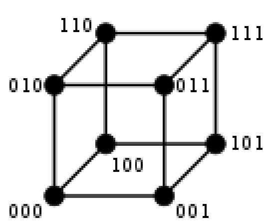

Fig.1.1

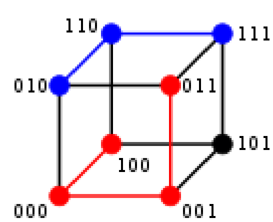

Fig.1.2

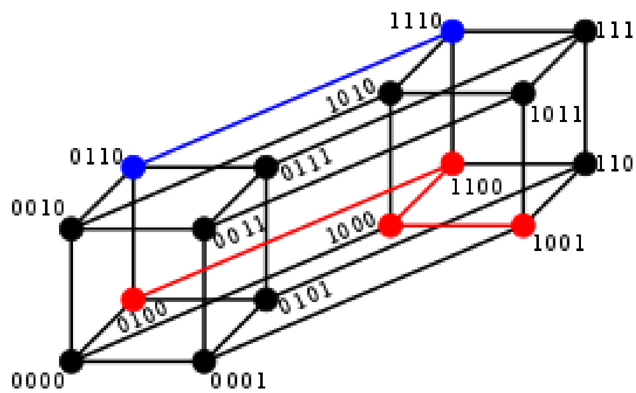

Fig. 1.3

Each non-zero message has a certain Hamming distance, which means that even the distance of the codes is also set. Hadamard's generated code forbids generating a Hadamard code from a Hadamard matrix, the rows of which constitute an orthogonal code set.

Definition 2. For $k \in N$, the k^{th} Rademacher function $r_k : [0,1] \to \{-1,+1\}$ is defined by

$$r_k(t) = 1 - 2\varepsilon_k(t), \text{ where } t \in [0,1]. \text{ [7]}$$

2. Hadamard code and Encoding Matrices

Hadamard's code is an example of a linear code with binary digits that determines the length of code length messages. Hadamard's codes are orthogonal and belong to a linear class of codes. They are used as error correction codes which are very useful in delivering information over long distances or through channels where errors can occur in messages.

Definition 2.1 [6] (*Hadamard code*) Let $r \in N$. The generation matrix of Hadamard code is a $2^r \times r$ matrix where the rows are all possible binary strings in F_2^r.

Example.[6] For $r = 2$, we have

$$G = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix},$$

which maps the messages to

$$Gx = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right\}.$$

In general, the Hadamard code based on the Hadamard matrix H_n, where $n = 2^k$, has a generator matrix that is $(k+1) \times 2^k$. The rate is $(k+1)/2^k$ - terrible, especially as k increases. The code can correct $2^{k-2} - 1$ errors in a 2^k-bit encoded block, and in addition detect one more error- excellent. [4]

If $u = (u_1, u_2, \Lambda, u_n)$ and $v = (v_1, v_2, \Lambda, v_n)$ are vectors over Z_2, define:

$$u \oplus v = (u_1 \oplus v_1, u_2 \oplus v_2, \Lambda, u_n \oplus v_n)$$
$$uv = (u_1 v_1, u_2 v_2, \Lambda, u_n v_n) \qquad [4]$$

In the following, we will use Radamecher functions to generate Hadamard's coding matrices of the order $n = 2^p$ (where, p is a positive integer) as follows:

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

where $G_{p\times n}$ is $p \times n$ the matrix generated, whose rows are p successive functions of Rademacher (sequences), which form a basis for Hadamard's matrices where $r_{ij} \in F_2 = \{0,1\}, \forall i, j : i = 1,2,...,m$ and $j = 1,2,...,n$. Rademacher's functions were determined by German mathematician Rademacher in 1922, [Rademacher, "Einige Sätze von allgenein orthogonal function," p. 112-138, (1922)). [1]

Rademacher functions with $n = 2^4 = 16$ pulses are shown in figure(2.1), along with the sequence representation of the functions in the logical elements {0,1}, which are called Rademacher sequences.

Example 2.1[1]. The generator matrix for Hadamard matrix (code) of order two i.e $n=2$, $(p=1)$ is :

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

Example 2.2 [1]and[5]. The generator matrix for Hadamard matrix (code) of order four i.e $n=2^2=4$, (p =2) is :

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

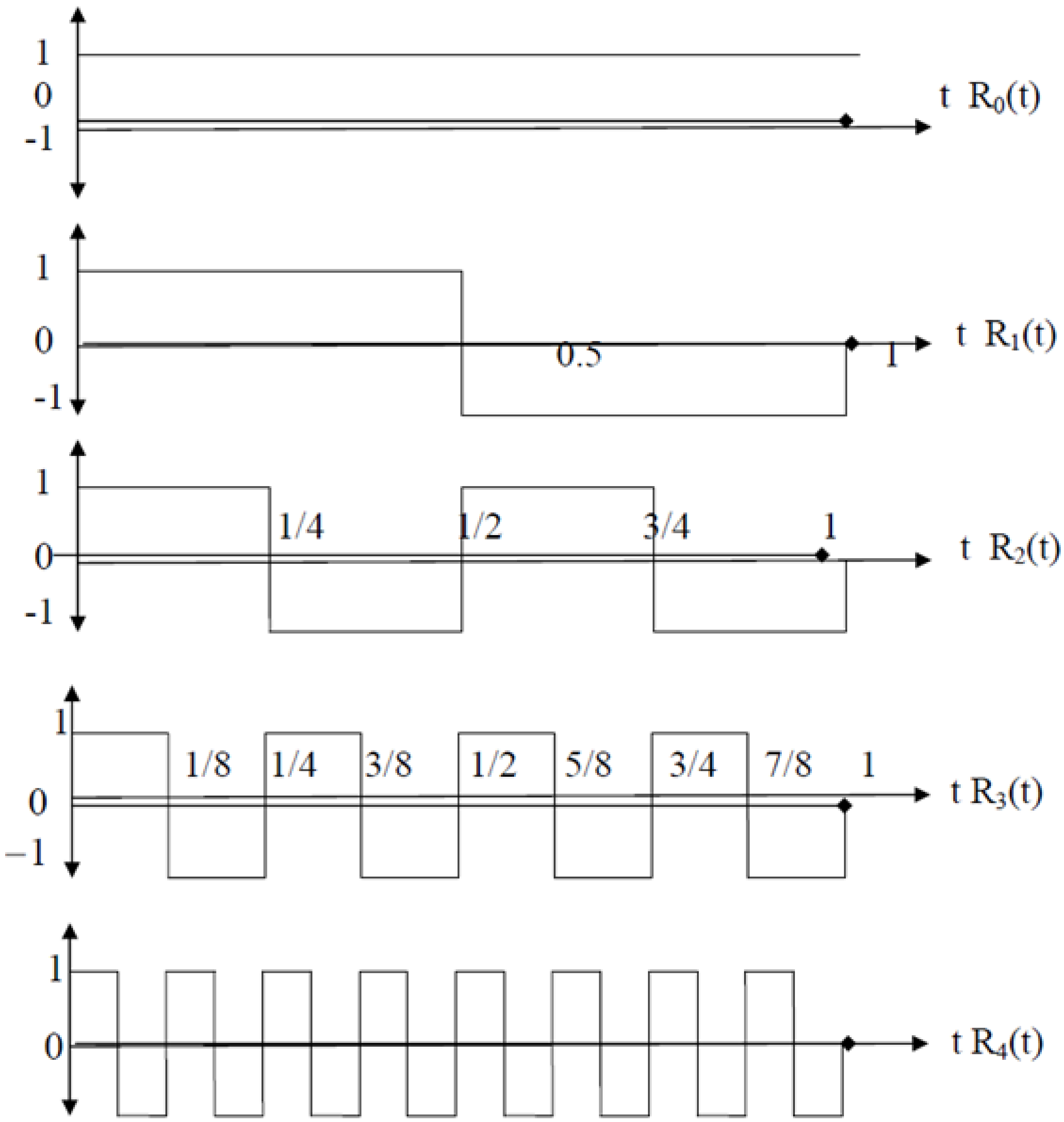

Fig.2.1

$$R_0 = (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$$
$$R_1 = (0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1)$$
$$R_2 = (0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1)$$
$$R_3 = (0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1)$$
$$R_4 = (0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1)$$

Fig.(2.1): The graphs of R_0, R_1, R_2, R_3, R_4 Rademacher functions (Rademacher sequences). The encoding of p-tuple message sequences in to 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 :

$(m)_b = (\alpha_i, \alpha_{i-1}, \Lambda\ , \alpha_1, \alpha_0)$, then $H_m = (m)_b * G_{p\times n}$, ku $\alpha_i \in F_2, \forall i, i = 0,1,2,\Lambda\ , p$. $(m)_b$ is p-tuple message sequences and H_m is $m-th$ Hadamard sequence (codeword). Hadamad matrices (codes) of order $n = 2,4,8,16$ are shown in tables 1,2,3 and 4 respectively.[1]

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

Integer (m)	4-tuple message sequence ($(m)_b$)	Hadamard codeword $H_m = (m)_b G_{4\times 16}$
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)

3. [1] 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:

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

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 $d(w,H_6) \leq d(w,H_i), \forall i, i = 0,1,...,7$, 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).

4 Conclusions

1. Generating or rpresenting of Hadamard matrices (codes) from using Rademacher functions (sequences) is easy to find.

2. Using the Kronecker product method, coding Hadamard matrices is very quick and easy.

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.

4. Both the Hamming codes and the Hadamard codes are actually special cases of a more general class of codes: Reed-Muller codes.

References

[1]Hameed k. Dawiod Khalid H. Hameed "On representation of Hadamard Codes" AL- Fatih Journal . No . 32 .2008,

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

[3]] Hong-Yeop Song "*Examples and Constructions of Hadamart matrices*" Yonsei University, Seoul 120-749, Korea , June 2002.

[4] Hadamard code, Massoud Malek, California State University, East Bay

[5] Rademacher,H.,”Einige Sätze von allgemeinen orthogonal funktionen”,Math.Annal.,112-138, 1922.
[6] Yuan Zhou and Kaiyuan Zhu, “Hamming and Hadamard Codes” CSCI-B609: A Theorist’s Toolkit, Fall 2016 Oct 6.

[7] Jordan Bell,” Rademacher functions”, Department of Mathematics, University of Toronto, July 16, 2014.

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

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