Decoding Reed- Muller Codes by Using Hadamard Matrices

*Mohammed Ali Morad**

Date of acceptance 15/4 / 2009

Abstract:

This paper discusses the problem of decoding codeword in Reed- Muller Codes. We will use the Hadamard matrices as a method to decode codeword in Reed- Muller codes.In addition Reed- Muller Codes are defined and encoding matrices are discussed. Finally, a method of decoding is explained and an example is given to clarify this method, as well as, this method is compared with the classical method which is called Hamming distance.

Key words: Reed- Muller Codes, codeword, message words, Hadamard matrices, Hamming distance.

Introduction:

Reed- Muller Codes are some of the oldest error correcting codes. Error correcting codes are very useful in sending information over long distances or through channels where errors might occur in the message, [1].

Hadamard matrices were introduced by the French mathematician M.J. Hadamard, [2]. The elements of Hadamard matrices are 1 or -1, whose rows and columns are mutually orthogonal, [3]. Since, Hadamard matrices are orthogonal and belong to class of linear codes, [3], which are useful in elimination the interference in the channel. For these reasons, Hadamard matrices are used in coding theory; they are used to generate Walsh matrices which are important in the IS-95 system, [4], where the IS-95 system is on orthogonal spread-spectrum system designed to eliminate multiple access interference (MAI), [5].

Definitions and Operations:

The vector spaces used in this paper composed of strings of length 2^p , where p is a positive integer of numbers in $F_2 = \{0,1\}$ (and we can denoted it as F_2^p). The codeword of a Reed-Muller Code form a subspace of such a space. The addition and scalar multiplication operations of a binary p-tuple by a symbol over $F_2 = \{0,1\}$ are defined as follows:

For two vectors $r = (r_1, r_2, \ldots, r_p)$ and $s = (s_1, s_2, \ldots, s_p)$, addition is defined by

$$r \oplus s = (r_1 \oplus s_1, r_2 \oplus s_2, \ldots, r_p \oplus s_p)$$

Where each r_i or s_i is either 1 or 0, and

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

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

$$\alpha * r = (\alpha * r_1, \ \alpha * r_2, \ \ldots, \ \alpha * r_p)$$

Definition (1): The Hamming distance d (a,b) between two binary sequences a and b of length n is the number of the places in which they differ, [3].

The Communication Channel Description of the Ccommunication System:

In communication system, we represent an information as a sequence of 0 and 1 (binary form). Figure (1) shows the block diagram of the communication channel [1].

*Department of Mathematics/ College of Basic Educations/University of Diyala

A message is usually not transmitted in it's entirely, but rather sent piecewise in blocks of a fixed length called message words

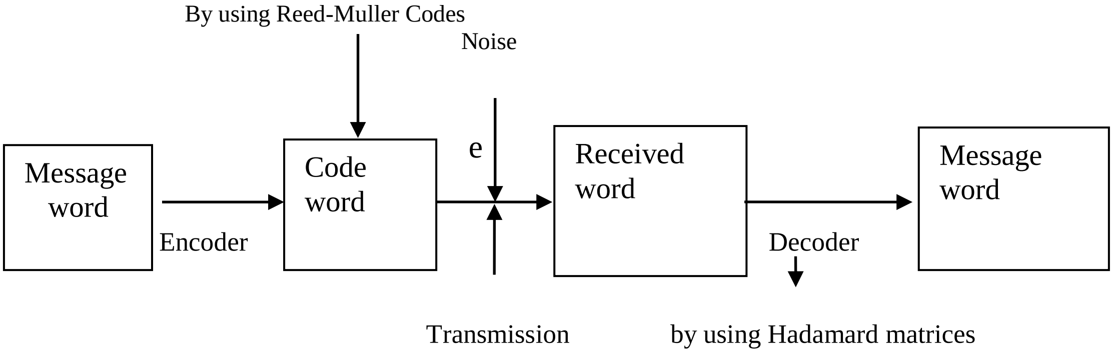

Fig. (1) The communication channel

Each message word is encoded into a codeword using a suitable coding algorithm and then sent across the noisy channel. The collection all code words are called a code.

While being transmitted, the codeword may get corrupted by an error e into a word. The decoder then has several jobs. First, it needs to detect that word is not a codeword, identify the error e that has occurred, and correct it accordingly to get the original codeword. It can easily be decoded to obtain the original message word as output for the receiver.

Reed- Muller Codes:

The generator matrix for the rth-order Reed-Muller Code of length $n = 2^p$ can be constructed as follow, [6]:

First, define the product of two vectors A and B by a component wise multiplication. That is, let,

$$A = (a_0, a_1, ..., a_{n-1}) \in F_2^n$$
$$B = (b_0, b_1, ..., b_{n-1}) \in F_2^n$$

Where,

$a_i \; and \, b_i \in F_2 = \{0,1\}, \forall \, i = 0,1,..., n-1.$

Then the product is the vector

$$AB = \{a_0 b_0, a_1 b_1, ..., a_{n-1} b_{n-1}\} \in F_2^n$$

The generator matrix for the rth-order Reed- Muller Code of length 2^p is defined as any array of block:

$$G_{RM_{(r,p)}} = \begin{bmatrix} G_0 \\ G_1 \\ . \\ . \\ . \\ G_{r-1} \\ G_r \end{bmatrix} \quad ...(4.1)$$

where, G_0 is the vector of length $n=2^p$ containing all ones; G_1, an P by 2^p matrix, has each binary p-tuple appearing once as column; and G_L is constructed from G_1 by taking its rows to be all possible products of rows of G_1,L rows of G_1 to a product. For definiteness, we take the left most column of G_1 to be all zeros, the right most to be all ones, and the others to be the binary p-tuples in increasing order, with the low-order bit in the bottom row.

If r=1, then the set of codeword is said to be a Reed- Muller alphabet of the first-order and denoted by RM (1, p) code. For example, the generator matrix for the first-order Reed-Muller Code of block length 8 is the 4 by 8 matrix:

$$G_{RM_{(1,3)}} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \text{.....(4.2)}$$

This generator matrix gives 16 codeword. Figure (2) shows the first-order Reed- Muller Code of block length 8, RM $_{(1,\,3)}$ code.

N	0	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1	1
2	1	1	1	1	0	0	0	0
3	1	1	0	0	0	0	1	1
4	1	1	0	0	1	1	0	0
5	1	0	0	1	1	0	0	1
6	1	0	0	1	0	1	1	0
7	1	0	1	0	0	1	0	1
8	1	0	1	0	1	0	1	0
9	0	1	0	1	0	1	0	1
10	0	1	0	1	1	0	1	0
11	0	1	1	0	1	0	0	1
12	0	1	1	0	0	1	1	0
13	0	0	1	1	0	0	1	1
14	0	0	1	1	1	1	0	0
15	0	0	0	0	1	1	1	1
16	0	0	0	0	0	0	0	0

Fig. (2) the first-order Reed-Muller Code of block length 8, RM $_{(1,\,3)}$ code.

The Main Results:

Hadamard Decoding algorithm: Hadamard matrix of order n=2^{p} is generated by the following recursive formula:

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{....(5.1)}$$

$$H_n = H_2 \otimes H_{nl2} \text{ ....(5.2)}$$

where ⊗ denotes the kronecker product, [5]:

The kronecker product also called tensor product or the direct product of two matrices C and D is defines as follows:

$$C \otimes D = \begin{bmatrix} C_{11}D & C_{12}D & . & . & . & C_{1n}D \\ C_{21}D & C_{22}D & . & . & . & C_{2n}D \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ C_{m1}D & C_{m2}D & . & . & . & C_{mn}D \end{bmatrix} \text{...(5.3)}$$

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 define two methods to decode Reed- Muller Codes, as follows:

Let $\underline{r}$ be a received word:

(1) Find the closest codeword

$\bar{c}$ ∈R-M code

Such that

$$d(\underline{r}, \bar{c}) \le d(\underline{r}, c) \;\; , \; \forall \; c \in R-M \;\; code$$

(2) Let $\underline{m} \in F_2^p$ be a sent message. Using the generator matrix $G_{RM_{(1,p)}}$, then the encoded message $\underline{m}$ is $\underline{c} = \underline{m}G_{RM_{(1,p)}}$.

The received word $\underline{r}$ is multiplied by a Hadamard matrix of order n to form $\underline{r}H_n$. If $\underline{r}H_n = \underline{\theta}$, then the received word $\underline{r}$ is in $RM_{(1,p)}$ code, but, if $\underline{r}H_n \ne \underline{\theta}$ then the received word is not in $RM_{(1,\,p)}$ code, this means that the received word is received in error. In order to find the location of error in $\underline{r}$, we compared the result in $\underline{r}H_n$ with each column of Hadamard matrix which gives the location of error in r̲.

Example (1): Consider the original message $\underline{m} = (0, 1, 0, 0)$. Using $G_{RM(1,3)}$ the encoded message $\underline{m}$ is:

$$\underline{c} = (0,\ 1,\ 0,\ 0) * \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

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

Let the encoded message after the error be

$\underline{r}$ = (0, 0, 0, 0, 1, 1, 1, 0)

We can correct the error in $\underline{r}$ as follows:

By 1st method:

$d(\underline{r}, RM_1) = 5$, $d(\underline{r}, RM_2) = 7$
$d(\underline{r}, RM_3) = 4$, $d(\underline{r}, RM_4) = 3$
$d(\underline{r}, RM_5) = 5$, $d(\underline{r}, RM_6) = 3$
$d(\underline{r}, RM_7) = 5$, $d(\underline{r}, RM_8) = 3$
$d(\underline{r}, RM_9) = 5$, $d(\underline{r}, RM_{10}) = 3$
$d(\underline{r}, RM_{11}) = 5$, $d(\underline{r}, RM_{12}) = 3$
$d(\underline{r}, RM_{13}) = 5$, $d(\underline{r}, RM_{14}) = 5$
$d(\underline{r}, RM_{15}) = 1$, $d(\underline{r}, RM_{16}) = 3$

We see that

$d(\underline{r}, RM_{15}) \le d(\underline{r}, RM_i)$, $\forall\ i = 1,2,...,16$,

and thus RM$_{15}$ is the sequence (codeword) that is most likely to have been transmitted.

By 2nd method:

$$\underline{r}H_8 = (0, 0, 0, 0, 1, 1, 1, 1)* \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

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

This vector is similar to eight column of Hadamard matrix of order 8, then we can see that the error was in the eight place, and we write $\underline{c}$ = (0, 0, 0, 0, 1, 1, 1, 1).

Since, $\underline{c} \in$ RM$_{(1,3)}$ code, then we can see that the original message was

$\underline{m}$ = (0, 1, 0, 0).

Conclusions:

1. Since, Hadamard Matrices (codes) are orthogonal and belong to linear block codes, they are very important in coding system.
2. Decoding Hadamard algorithm for first order Reed-Muller Codes is very useful than Hamming distance.

References:

1. Arnold, M.M, and Allen, H.L. 1985,"Error- Control Techniques for Digital Communication". John Wiley and Sons, Inc, First edition, 255.

2. Hadmard, M.J. 1893, "Resolution d'une question relative aux determinants", Bull.Sc. Math. A17: 240-246.

3. Piot Porwik, 2003, "The Spectral Test of the Boolean Function Linearity",Int. J. Appl. Math. Comput. Sci., 13(4): 567-575.

4. Lee, J.S., and Miller L.E.,1998, "CDMA Systems Engineering Handbook", Artech House, Boston, MA,first edition,1151.

5. Falkowski; B. J. and Saso T.2005, "Unifed Algorithm to Generate Walsh Functions in Four Different Orderings and its Programmable Hardware Implementations", Proc. Vis. Image process,152:6.

6. Richard, E.B.1983,"Theory and Practice of Error Control Codes". Addison- Wesley publishing Company, Inc, first edition,359.

كشف شفرات ريد-مولر(Reed-Mulle) باستخدام مصفوفات هادمارد(Hadamard)

محمد علي مراد*

*قسم الرياضيات/ كلية التربية الأساسية/جامعة ديالى

الخلاصة:

يناقش في هذا البحث مسألة كشف الرسائل المرسلة بواسطة شفرات ريد-مولر (Reed-Muller Codes). سوف نستخدم مصفوفات هادمارد كطريقة لكشف هذه الرسائل المرسلة من خلال شفرات ريد- مولر (Reed-Muller Codes) بالإضافة إلى ذلك تم تعريف شفرات ريد- مولر ومناقشة مصفوفات كشف الشفرات. وأخيراً تم توضيح طريقة كشف الشفرات وأعطي مثال لتوضيح هذه الطريقة ومقارنتها مع الطريقة التقليدية المسماة Hamming distance .