Hadamard Matrices and PN Sequences

Kushagra Gupta, *2012MT50599*
Department of Mathematics

Abstract— **Hadamard Codes are orthogonal codes which are used as error correcting codes in very noisy environment. They were used to transmit images of mars captured by Mariner 9. They are also used in asynchronous CDMA. Pseudo Random Number sequences are long sequences that appear random statistically but are generated deterministically. They are used in synchronous CDMA and GPS.**

***Keywords*— CDMA, Hadamard Matrices, Walsh Codes, Maximal Length**

I. Introduction

WITH the huge blast in communication and information sciences, need to transmit data securely and correctly over very large distances has emerged out to be a situation which is needed to be dealt very efficiently. Over the past few decades many methods of encrypting the data and transmitting it safely without any external interference have been developed. Two of such methods are discussed here namely Hadamard Codes and PN sequences.

The Hadamard code is named after the French mathematician Jacques Hadamard and also known under the names Walsh code and Walsh–Hadamard code, in recognition of the American mathematician Joseph Leonard Walsh. It is used in synchronous code division multiple access (CDMA) communication to encode the messages. Hadamard Codes were also used on Mariner9 mission to send the images of mars back to earth.

PN Sequences are mainly used in Global Positioning System (GPS) and in asynchronous CDMA just like the Hadamard Codes.

II. Error Correcting Codes

When data is transmitted over a channel, they are often encountered with noises and the receiver may not be able to receive the exact message as transmitted. So we need a mechanism that can be able to correct the error. One of such mechanism is Forward Error Correction (FEC). In FEC instead of the original message M is converted to a code C which is a function of M is transmitted and the original message is recovered back from the code. Such codes are called error correcting codes.

For example: Let us assume we are transmitting only one bit over a noisy channel. So if we transmit 1 there is a certain probability that the receiver may get 0. So we need an error correcting code here. So the simplest way is to transmit the data 3 times ((3, 1)-repetition code) and the received code is taken as the majority bit of the code.

TABLE I
Decoded messages for (3, 1) repetition code

Received Message	Decoded Message
111	1
110/011/101	1
001/010/100	0
000	0

But if there are 2 errors in the transmission i.e. if 1 is transmitted as 100 the decoded output would be wrong. So it is a 1 error correcting code. Similarly if we transmit it 5 times, it would be 2 error correcting.

III. Hadamard Matrices

A matrix H is said to be Hadamard Matrix of order n if $H_n H_n^t = nI_n$ (where I_n is the identity matrix of order n) and all the elements of H are either 1 or -1.

For example

$$H_1 = [\,1\,]$$

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

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

These matrices were introduced by Jacques Hadamard in 1893. We could see easily from the definition that given H is a Hadamard matrix –H is also a Hadamard matrix. Equivalently, a Hadamard matrix is an n × n matrix of +1s and -1s in which any two distinct rows agree in exactly n/2 positions (and thus disagree in exactly n/2 positions.) Hadamard matrices only exist for n=1, 2 or if n=4k where k is any natural number. (Conjecture) .

A. Recursive Property

If H_n is a Hadamard matrix of order n then $\begin{bmatrix} Hn & Hn \\ Hn & -Hn \end{bmatrix}$ is also a Hadamard matrix of order 2n i.e. if H_n is a Hadamard matrix of order n then $H_2 \otimes H_n$ is a Hadamard matrix of order $2n$.

B. Sylvester Construction

Examples of Hadamard matrices were actually first constructed by James Joseph Sylvester in 1867. He used the above stated property to construct matrices of order 2^n.

$$H_1 = [\,1\,]$$

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

And

$$H_{2^k}=\begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} = H_2 \otimes H_{2^{k-1}}$$

These matrices constructed using this method are called Walsh matrices.

C. *Orthogonal Property*

Since any two distinct rows of Hadamard matrices agree in exactly n/2 positions (and thus disagree in exactly n/2 positions) and the values are either 1 or -1. Hence if we dot product the two distinct row vectors the product comes to be zero.

D. *Other Properties*

Other important properties of Walsh codes are:

- These Matrices are symmetric.
- Trace of these matrices are 0.
- First row and first column consists of only 1.
- Rest of the rows and column have half of the entries 1 and rest of the half are -1.

IV. Hadamard Codes

It is a type of error correcting code which is used when messages are transferred in very noisy environments. It is a linear code (linear combination of any such codes is also a code). It maps a message of length m to a code word of length 2^n. A Hadamard code based on Hadamard-Sylvester Matrix of order 2^n is $2^{n-2}-1$ error correcting. Hadamard Codes are also known as Walsh Codes. The punctured Hadamard code is a slightly improved version of the Hadamard code. It maps a message of length m to a code word of length 2^{n-1}.

A. *Generating Matrices*

Hadamard codes could be generated from Generator Matrix (all linear codes could be generated from the generating matrix).

Matrix of dimensions $n \times 2^n$ where columns are binary vector of length n in the lexicographical order are generating matrices of Hadamard codes of length n. For example: Generating matrices of order 2 is $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$.

Generating Matrices of Punctured Hadamard Codes are same as normal generating matrices except that they only have columns whose first element is 1. Generating matrices of punctured Hadamard Codes of order 2 is $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

B. *Converting Messages to Hadamard Codes*

We could encode messages to Hadamard Codes in two ways.

Firstly for a message of k bits we have 2^k possible inputs. So if we make Hadamard matrix H of order 2^k and change all '-1's to '0's then rows of H and will make a total of 2^k codes. So we can map each message to a code word and transmit the code. (In punctured Hadamard code we map the 2^k codes to $2 \times 2^{k-1}$ rows of H and –H where H denotes the Hadamard Matrix of order 2^{k-1}. So the length of code word reduces by one bit as compared to normal Hadamard Code)

Secondly we could generate codes using Generator Matrices.

To encode a message x of length m, take a Generator matrix G of dimension $m \times 2^m$(in case of punctured Hadamard codes dimension $m \times 2^{m-1}$). Then the code C is defined as $x \circ G$wher dot product is defined as

$$C_i = (\sum_{j=1}^{m} x_j \cdot G_{ji}) \; mod \; 2$$

For example: Coding $x = 1011$ to corresponding punctured Hadamard Code:

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

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

C. *Decoding Hadamard Codes*

To extract Hadamard code from the message corrupted with noise we need to follow the following algorithm. Let the received message be$(w_0, w_1, \dots \dots, w_{2^{n-1}})$ of 2^n bits. And the decoded message is$(m_0, m_1, \dots \dots, m_{2^{n-1}})$. For i ranging from 1 to n.

1) Pick j randomly from $\{0,1 \dots, 2^{n-1}\}$

2) Select k from $\{0,1 \dots, 2^{n-1}\}$ such that $j + k = e_i$ (+ denotes bitwise XOR of j and k.

3) $m_i = w_k \oplus w_j$

The decoded message is the actual code transmitted.

Now to extract the message $\widehat{m}$ from the code Change all the '0's to'-1's of the message m. Now calculate $s = m \circ H_m$ (where H_m denotes Hadamard Matrix of order m). Due to orthogonal property s will have all the columns except one which will be equal to $\pm m$. If k is the non-zero column then the message is the kth column of the Generation Matrix.

For example:

$$\text{Let } m = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\text{On transformation } m = \begin{bmatrix} 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \end{bmatrix}$$

$$m \circ H_8 = \begin{bmatrix} 0 & 0 & 0 & 8 & 0 & 0 & 0 & 0 \end{bmatrix}$$

So the message is fourth column of Hadamard Matrix i.e. 1011.

V. Pseudo-Random Noise Sequences

Pseudorandom Noise sequence is bit stream of '0' and '1' similar to noise that appear statistically random but are deterministically generated and repeat themselves over time. The period of repetition could be very large (millions of digits).

They are like random sequences in the way that they have very low correlation with any other element of the set and unlike them they could be generated easily on both the receiver's end and the transmitter's end and thus the transmitted message has high correlation with the sequence generated at receiver's end. (Correlation refers to any of a broad class of statistical relationships involving dependence.)

A. *Randomness*

The sequence appears completely random (noise) to anyone who does not know how the sequence is generated but one who knows the generation knows all the properties of code.

B. Run Length

A sequence of consecutive ‘0’s or ‘1’s is called run length and the number of ‘0’s and ‘1’s is called the run length.

In PN sequence number of 1s and 0s differ by only one.

TABLE II
NUMBER RUNS OF ‘0’S AND ‘1’S OF VARIOUS LENGTHS IN PN SEQUENCE OF LENGTH $2^n - 1$

Run Length	‘1’s	‘0’s
n	1	0
$n-1$	0	1
$n-2$	1	1
$n-3$	2	2
$\vdots$	$\vdots$	$\vdots$
2	2^{n-4}	2^{n-4}
1	2^{n-3}	2^{n-3}

C. Shift and Add

If we shift the PN sequence and then perform bitwise XOR with the original sequence, the new sequence is also the same sequence with a different shift.

D. Correlation

If we shift the PN sequence and then perform bitwise XOR with the original sequence

The correlation of two PN sequences is defined as:

$$R(m) = \frac{number\ of\ agreeement}{total\ no\ of\ bits}$$

Number of agreements could be calculated using bitwise XNOR of two sequences.

If the two sequences are same then the correlation is called autocorrelation. The autocorrelation comes to be 1 if the sequences are in phase. For any change in phase it is 0.5.If the two sequences are different then the correlation is called cross correlation.

E. Acquisition of PN sequences

The PN sequences could be accurately detected using the correlation properties of PN sequences. The PN sequence is generated at receiver’s end in the same way as generated at transmitter’s end. We calculate the cross-correlation of the generated sequence and received sequence. So if the received sequence is same as generated one except at some bits where it is corrupted by noise the cross-correlation comes almost 1(if they are in same phase) and almost 0.5 if they are out of phase. In latter case we keep comparing by shifting one sequence until they come in same phase. Otherwise if the generated sequence and received message are completely different the correlation comes to be very low and we can attribute the sequence as noise.

F. Some important PN Sequences

Some of the important PN sequences are:

1.) Maximal Length Sequence

These sequences are generated using Linear Feedback Shift Registers (a shift register whose input bit is a linear function of its previous state). These sequences are periodic and using a m length shift register we could produce a sequence of length $2^m - 1$.

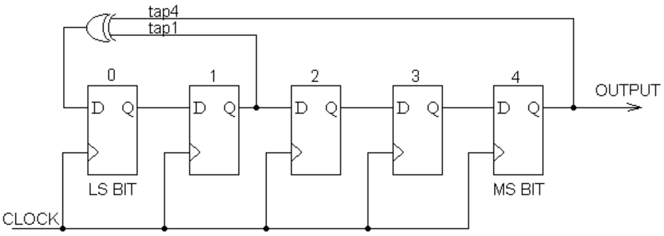

Fig. 1 Generation of MLS using Linear Feedback Shift Registers

Only certain outputs or tap can generate MLS. The generated output could be expressed as a polynomial in x. For example in Fig.1 the output is expressed as $1 + x^1 + x^4$ because the output of stage 4 and 1 is modulo-2 added.

Note : We need to eliminate the zero state condition of shift register because if all the flip flops are in zero state then the shift register remains latched to it.

2.) Gold Codes

The cross-correlation of gold codes is very low within a set. Hence it is useful when multiple devices are broadcasting in the same frequency range. It is used in GPS devices and CDMA.

To generate a set of gold codes, take two MLS of same length $2^m - 1$ such that their cross-correlation is low. Then the one MLS is kept fixed and other one is translated into all the relative positions and the sequences are bitwise modulo-2 added (XORed). The set of the $2^m - 1$ xors of the two sequences in their various phases is the required set of Gold codes.

VI. APPLICATION IN CDMA

CDMA (Code Division Multiple Access) is an example of multiple access i.e. many transmitters send information over a single channel but the receiver can only access the intended data. So several users Share a common band of frequency.

The CDMA transmission is basically classified into two categories:

A. Synchronous CDMA

CDMA system in which the transmitted message and the code generated at the receiver’s end are in same phase (they are synchronised). Walsh codes are used to encode messages in Synchronous CDMA.

Each user is assigned a unique Walsh Code. In the case of IS-95 64 bit Walsh codes are used to encode the signal to separate different users. So we could send 64 independent messages at a single time.

For example:

1.) Encoding

Let us assign 4 bit unique Walsh codes to users.

Code A = [1,-1,-1,1] and Code B = [-1,-1,1,1].

Message A = [0,0] and Message B = [1,0].

Now change the values of ‘0’s to ‘-1’s

Message A = [-1,-1] and Message B = [1,-1].

To encode take the Kronecker Product of the message and the corresponding sender’s code.

Encoded A is

$$[-1,-1] \otimes [1,-1,-1,1] = [-1,1,1,-1,-1,1,1,-1].$$

Encoded B is

$$[1,-1] \otimes [-1,-1,1,1] = [-1,-1,1,1,1,1,-1,-1].$$

2.) Decoding

Now since both the codes are transmitted over a common channel they overlap and thus the received message will be $[-2,0,2,0,0,2,0,-2]$. Now convert the message to a column matrix of dimension 4×2 (code length × message length).

$$\begin{bmatrix} -2 & 0 \\ 0 & 2 \\ 2 & 0 \\ 0 & -2 \end{bmatrix}$$

Now dot product it with the code-word to get the message

$$[1 - 1 - 1 \;\; 1] \circ \begin{bmatrix} -2 & 0 \\ 0 & 2 \\ 2 & 0 \\ 0 & -2 \end{bmatrix} = [-4,-4]$$

$$[-1 - 1 \;\; 1 \;\; 1] \circ \begin{bmatrix} -2 & 0 \\ 0 & 2 \\ 2 & 0 \\ 0 & -2 \end{bmatrix} = [4,-4]$$

Now anything positive is evaluated as 1 and negative as 0. If the value comes to be 0 means the user didn't transmitted anything. Hence the finally decoded messages are [0,0] and [1,0].

B. Asynchronous CDMA

CDMA system in which the transmitted message and the code generated at the receiver's end are not necessary in the same phase (because mobile-to-base links cannot be precisely coordinated, particularly due to the mobility of the handsets). PN Sequences are used to encode messages in Synchronous CDMA because the orthogonal property doesn't remains valid for shifted sequence.

The encoding process is similar as in the synchronous CDMA. The decoding uses the correlation properties as discussed in the 'acquisition of PN sequences'. So if cross-correlation is high other signals may interfere with the messages. We need to select PN sequences with low correlation.

VII. Conclusion

This paper has discussed the key concepts related to error correcting codes namely Hadamard Codes and PN Sequences. Hadamard Codes have unique property of orthogonality hence have very low cross-correlation. On the other end PN sequences have unique property of shift and add which makes them easy to use even when the messages are out of phase. These two techniques have been used very efficiently in CDMA transmissions.

Acknowledgment

I wish to thank our Digital Electronics' professors namely Dr. G. Vishvesharan and Dr. Anuj Dhawan for giving us this wonderful opportunity to write a term paper on something beyond the classroom studies.

References

[1] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[4] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[5] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[6] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[7] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/

[8] *FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

[9] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[10] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[11] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[12] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.