하다마드 행렬의 동치성에 관한 연구

김정헌, 송홍엽
연세대학교 전기컴퓨터공학과

On the Equivalence of Some Hadamard Matrices

Jeong-Heon Kim and Hong-Yeop Song
Dept. of Electrical and computer Engineering, Yonsei univ.

Abstract

In this paper, it is proved that the normalized Hadamard matrices with the property that the component-wise sum of any two rows of a matrix is a row of the matrix are equivalent to cyclic Hadamard matrices of the same order which are made from m-sequences.

I. Introduction

A Hadamard matrix[1] of order n is an $n \times n$ matrix of +1's and -1's such that any two rows of the matrix are orthogonal. One can easily check that the orthogonality of rows is not affected by permuting rows or columns or multiplying rows or columns by -1. The Hadamard matrices obtained by those operations are said to be equivalent. Given a Hadamard matrice, we can always find an equivalent one whose top row and leftmost column consist entirely of +1's. We call this Hadamard matrix normalized or normalized Hadamard matrix. If every row of the $(n-1)\times(n-1)$ matrix H' obtained by removing the top row and the leftmost column of a normalized Hadamard matrix H is a cyclic shift of the first row, H is called cyclic Hadamard matrix. In fact, the rows of H' are binary sequences with ideal autocorrelation property. One may figure out that there is one to one correspondence between binary sequences with ideal autocorrelation and cyclic Hadamard matrices. m-sequences[2] which is one of the most popular binary sequences with ideal autocorrelation can also give cyclic Hadamard matrices.

In this paper, we prove that cyclic Hadamard matrices induced from m-sequences are equivalent to Hadamard matrices with the property that the component-wise sum of any two rows of a matrix is itself a row of the matrix. In the following, we call this property ''closure'' property. It is also proved that Hadamard matrices given by repeatedly applying Kronecker product to $\begin{pmatrix} + & + \\ + & - \end{pmatrix}$ have the closure property.

II. The equivalence of some Hadamard matrices

Theorem 1 : All the normalized Hadamard matrices of order 2^n with closure property are equivalent.

proof : Let H be a matrix as above. Let V be the vector space of dimension 2^n over $GF(2)$ and S be the set of rows of H. Then one can easily check that S is a subspace of V of dimension n. Thus there exists a basis $\{b_{1,}b_{2},\cdots,b_{n}\}$ of S. Write the basis as

$$B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{12^n} \\ b_{21} & b_{22} & \cdots & b_{22^n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{n2^n} \end{bmatrix}$$

Then S is the row space of B. B must have all distinct columns because otherwise the Hadamard matrix H has the same columns more than once which is impossible. Thus B have all distinct columns and consequently every n-tuple appears in columns of B exactly once. Suppose H' is another Hadamard matrix of order 2^n with closure property. Let S' be the set of rows of H'. Then similarly, there is a matrix B' of which rows span S'. Since B and B' have all n-tuples as their columns, there exists a permutation matrix σ such that $B\sigma = B'$. In view of the matrices H and H', this means that there exists a permutation of columns such that the sets of rows of two matrices become the same. Thus H and H' are equivalent.

Theorem 2 : Every Hadamard matrice which is obtained by succesive Kronecker product of

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

has closure property.

proof : Let H_{2^k} be the Hadamard matrice of order 2^k given by succesive Kronecker product. We will prove the theorem by an induction on k. Firstly, one can easily check that H_2 satisfies closure property. Suppose H_{2^n} satisfies closure property.

$$H_{2^{n+1}} = \begin{bmatrix} H_{2^n} & H_{2^n} \\ H_{2^n} & -H_{2^n} \end{bmatrix}$$

Let h_i be the i-th row of H_{2^n}. Then the sums of two rows of $H_{2^{n+1}}$ have the following three cases:

1. $r_1 = (h_i \mid h_i) \oplus (h_j \mid h_j)$
2. $r_2 = (h_i \mid -h_i) \oplus (h_j \mid -h_j)$
3. $r_3 = (h_i \mid h_i) \oplus (h_j \mid -h_j)$

r_1 and r_2 are obviously some rows of $H_{2^{n+1}}$ by the induction hypothesis on H_{2^n}. For r_3,

$$\begin{aligned} r_3 &= (h_i \mid h_i) \oplus (h_j \mid -h_j) \\ &= (h_i \oplus h_j \mid h_i \oplus -h_j) \\ &= (h_i \oplus h_j \mid -(h_i \oplus h_j)). \end{aligned}$$

Thus r_3 is also a row of $H_{2^{n+1}}$ and the theorem follows.

A cyclic Hadamard matrice obtained from an m-sequence also satisfies the property in Theorem 1 because of the cycle-and-add property of m-sequences. Thus we have the following corollary.

Corollary 1 : The Hadamard matrice H_{2^n} given in Theorem 2 is equivalent to a cyclic Hadamard matrice obtained from an m-sequence of length $2^n - 1$.

For an illustration, we give the following example.

Example 1 : Let's consider the following two Hadamard matrices. Here, we use 0 and 1 instead of +1 and -1.

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

$$H' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

H is a Hadamard matrix obtained by successive direct product and H' is a cyclic Hadamard matrix made from an m-sequence. Let us denote the sets of rows of H and H' by S and S' respectively. Then as in Theorem 1, we can find matrices B and B' which span S and S' respectively.

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

$$B' = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

We can easily find the permutation matrix σ such that $B' = B\sigma$.

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

and

$$H\sigma = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

We have another permutation matrix γ such that $H' = \gamma H\sigma$.

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

Acknowledgements

This work is supported by University Research Program of Ministry of Information & Communication in South Korea in the program year 1998.

References

[1] Jr. Marshall Hall, Combinatorial Theory, John Wiley & Sons, 2nd edition, 1986.

[2] S. W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, CA (Revised Edition, Aegean Park Press, Laguna Hills, CA, 1982), 1967.