

하다마드 행렬을 생성하는 실베스터 방법의 일반화

정희원 신민호*, 송홍엽*, 노종선**

Generalized Sylvester Construction for Hadamard Matrices

Min-Ho Shin*, Hong-Yeop Song*, Jong-Seon No** *Regular Members*

요 약

하다마드 행렬은 직교부호를 설계함에 있어서 매우 중요한 행렬이다. 본 논문에서는 하다마드 행렬을 구성하는 실베스터(Sylvester) 방식의 새로운 일반화된 방법을 소개하고 이를 증명한 후, 크기 16에서 예를 들어 설명한다. 이 방법을 사용하면 서로 비동치관계에 있는 다양한 종류의 하다마드 행렬을 쉽게 생성할 수 있다.

ABSTRACT

Hadamard matrices are known to be important in designing of the orthogonal codes. In this paper we propose generalized Sylvester construction for Hadamard matrices. We prove it and give an example for the case of Hadamard matrices of order 16.

I. 서 론

크기 n 인 하다마드 행렬은 n^2 개의 성분(component)으로 +1 또는 -1을 가지는 $n \times n$ 행렬이며 $HH^T = nI$ 로 정의된다^[1]. 하다마드 행렬은 직교부호를 설계함에 있어서 매우 중요한 요소로 작용한다^[6]. 하다마드 행렬의 각 행은 Walsh부호라고도 불리는데, 이는 IS-95의 셀룰라 CDMA 통신 시스템의 직교채널구성에 필수적인 요소이다. 또한 직교성을 이용하여 오류정정부호와 경로탐색 알고리즘에도 필수적이다^{[2],[3],[6]}.

임의의 $n \times n$ 하다마드 행렬이 주어지면 그 크기 n 이 1, 2, 혹은 4의 배수이어야 함을 쉽게 증명할 수 있다. 그러나, 임의의 4의 배수 n 에 대하여 $n \times n$ 하다마드 행렬이 존재하는가에 대해서는 아직 완전히 알려지지 않았다^{[4],[5],[7]}.

본 논문에서는 $\{+1, -1\}$ 을 $\{0, 1\}$ 로 바꾸어 생각한

다. 즉, 하다마드 행렬의 성분은 0 혹은 1이며, 이 경우 두 개의 임의의 행의 직교성은 두 행을 겹쳐 놓고 볼 때 일치하는 성분과 일치하지 않는 성분의 수가 같음으로 규정한다.

주어진 하다마드 행렬에 대하여 특정 행(또는 열)을 선택하여 그 행(또는 열)의 모든 값에 1을 모두 2 덧셈 하여도 그 결과는 하다마드 행렬이다. 또한, 하다마드 행렬의 임의의 두 행(또는 두 열)을 선택하여 이를 맞바꾸어도 그 결과는 하다마드 행렬이며, 하다마드 행렬의 전치행렬(transpose)도 하다마드 행렬이다. 더욱이, 이러한 작업을 몇 번을 반복 하여도 그 결과는 하다마드 행렬이며, 이를 하다마드 보존변형(Hadamard-Preserving Transformation)이라 부른다^{[1],[5]}. 임의의 두 개의 $n \times n$ 하다마드 행렬 H_1 과 H_2 는 특정한 하다마드 보존변형에 의하여 H_1 이 H_2 로 바뀌어질 수 있을 때 동치(equivalent) 관계에 있다고 한다. 하다마드 보존변형을 이용하면, 주어진 하다마드 행렬의 첫째 행과 첫째 열을 모두

* 연세대학교 전기·컴퓨터공학과 부호 및 정보이론 연구실 (hysong@yonsei.ac.kr)

** 서울대학교 전기공학부 (jano@amu.ac.kr)

논문번호 : 99309-1006, 접수일자 : 1999년 10월 6일

※ 본 연구는 한국 과학재단 특정기초연구(97-0100-05-01-3)지원사업에 의한 결과입니다.

0이 되도록 만들어 줄 수 있는데, 이를 표준형이라 부른다. 즉, 임의의 하다마드 행렬은 어떠한 표준형 하다마드 행렬과 동치이다.

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

그림 1. 크기 2, 4, 8의 하다마드 행렬

예를 들어 그림1에 $n=2,4,8$ 의 크기에 대한 표준형 하다마드 행렬을 보인다. 임의의 크기 n 에 대해서, 표준형 $n \times n$ 하다마드 행렬은 유일하지 않으며, 두 개의 동일한 크기의 하다마드 행렬의 동치성을 조사하고자 할 때 각각을 표준형으로 변형시켜 조사하면 충분하다.

본 논문에서는 하다마드 행렬의 생성방법 중에서 가장 잘 알려진 실베스터 방법을 일반화한다. 이를 위하여 우선 제2절에서 하다마드 행렬의 실베스터 생성방법을 설명하고, 제3절에서 제안한 방법과 이의 증명을 소개하며, 작은 크기의 하다마드 행렬에 대하여 이를 적용해본다. 제4절에서 결론을 맺는다.

II. 실베스터 생성방법

하다마드 행렬의 생성방법 중에서 가장 잘 알려진 실베스터 생성방법은 임의의 두 개의 하다마드 행렬로부터 새로운 더 큰 크기의 하다마드 행렬을 생성하는 방법이다. 즉, $n \times n$ 하다마드 행렬 $A = [a(i, j)]$ 와 $m \times m$ 하다마드 행렬 $B = [b(i, j)]$ 가 주어지면 이로부터 $nm \times nm$ 하다마드 행렬 C 를 다음과 같이 생성할 수 있다^[1].

$$C = A \oplus B$$

$$= \begin{bmatrix} a(1,1)+B & a(1,2)+B & \cdots & a(1,n)+B \\ a(2,1)+B & a(2,2)+B & \cdots & a(2,n)+B \\ \vdots & \vdots & \cdots & \vdots \\ a(n,1)+B & a(n,2)+B & \cdots & a(n,n)+B \end{bmatrix}$$

여기에서 $a(i, j)+B$ 는 $m \times m$ 행렬로서, 행렬 B 의 모든 성분에 $a(i, j)$ 를 모드2 덧셈한 결과이다. 예를 들어, 그림1에 보인 2×2 하다마드 행렬로부

터 $4 \times 4, 8 \times 8, \dots$, 일반적으로 $2^k \times 2^k$ 하다마드 행렬을 생성할 수 있다. 그림1의 4×4 행렬은 이 방법으로 생성한 예이며, 아래의 그림2에는 이 방법으로 생성한 8×8 하다마드 행렬을 보인다. CDMA 이동 통신에 사용되는 윌쉬부호는 이러한 방법으로 생성된 64×64 하다마드 행렬이다^[2].

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

그림 2. 크기 8의 하다마드 행렬 - 실베스터 생성방법

III. 일반화된 생성법 및 증명

앞 절에서 소개한 실베스터 생성방법에서 연산 $a(i, j)+B$ 를 살펴보자. 만일 B 가 하다마드 행렬이고 $a(i, j)$ 가 0 혹은 1로서 B 의 모든 성분에 성분별 모드2 덧셈을 한 결과라면 행렬 $a(i, j)+B$ 도 역시 하다마드 행렬이다. 만일 $a(i, j) = 0$ 이면, 이는 행렬 B 와 일치하게 되고, $a(i, j) = 1$ 이면, 이는 행렬 B 에서 0은 1로 1은 0으로 바뀐 형태가 된다. 여기서 우리는 최종적으로 얻어지는 행렬 $C = A \oplus B$ 에서 $m \times m$ 부행렬의 열이 모두 동일한 행렬일 필요는 없음을 쉽게 알 수 있다. 이점이 본 논문에서 새로이 제안하는 일반화된 실베스터 생성방법의 핵심이다.

예비정리 1. 행렬 B 가 $n \times n$ 하다마드 행렬이고 $a \in (0, 1)$ 이면, 행렬 B 의 모든 성분에 a 를 모드 2 덧셈한 결과로 얻어지는 행렬 $a+B$ 도 $n \times n$ 하다마드 행렬이다.

증명: 생략.

예비정리 2. n 개의 임의의 하다마드 행렬 B_1, B_2, \dots, B_n 과 임의의 이진벡터 (c_1, c_2, \dots, c_n) 로부터 만들어지는 다음의 $m \times nm$ 행렬을 생각하자.

$$[c_1+B_1, c_2+B_2, \dots, c_n+B_n]$$

위 행렬의 m 개의 행벡터는 서로 직교한다.

증명: 생략.

정리 1. 임의의 양의 정수 n 과 m 에 대해서,

$n \times n$ 허다마드 행렬 $A = [a(i, j)]$ 와 n 개의 $m \times m$ 허다마드 행렬 B_1, B_2, \dots, B_n 가 주어지면, 다음의 $nm \times nm$ 행렬 H 는 허다마드 행렬이다.

$$H = \begin{bmatrix} a(1,1)+B_1 & a(1,2)+B_2 & \dots & a(1,n)+B_n \\ a(2,1)+B_1 & a(2,2)+B_2 & \dots & a(2,n)+B_n \\ \vdots & \vdots & \dots & \vdots \\ a(n,1)+B_1 & a(n,2)+B_2 & \dots & a(n,n)+B_n \end{bmatrix}$$

증명: 우선 행렬 H 의 nm 개의 행 벡터를 m 개씩 순서대로 묶어서 각각의 행벡터블록이라 하자. 즉, H 에는 n 개의 행 벡터 블록이 있다. H 의 nm 개의 행 벡터에 대해서 그 직교성을 증명하고자 한다. 다음 두 가지를 구분하자. 첫째는 두 개의 행 벡터가 동일한 행벡터블록에 있는 경우와 둘째는 두 개의 행벡터가 서로 다른 행벡터블록에 있는 경우이다. 우선, 예비정리2에서 첫 번째 경우를 해결한 셈이다. 그러므로, 둘째 경우만 고려하면 충분하다. 서로 다른 두 개의 행벡터블록에서 행벡터 한 개씩을 선택하여 이들의 직교성을 따져보자. 다음의 두 경우에 대하여 구분하면 편리하다.

(1) 각각의 블록에서 동일한 위치의 행벡터인 경우 : 주어진 두 개의 행에 대해서 처음 m 개의 성분만을 살펴보자. 이는 B_1 의 동일한 행에 이진수 $a(i,1)$ 과 $a(j,1)$ 을 성분별 모드2덧셈한 결과이다. 따라서 $a(i,1) = a(j,1)$ 인 경우에는 m 개의 성분이 완전히 일치하게 되고, $a(i,1) \neq a(j,1)$ 인 경우는 m 개의 성분이 모두 불일치하게 된다. 한편 행렬 A 또한 허다마드 행렬이기 때문에 $k = 1, 2, \dots, n$ 일때 $a(i, k) = a(j, k)$ 인 경우의 수와 $a(i, k) \neq a(j, k)$ 인 경우의 수는 각각 $n/2$ 로 같다. 따라서 m 개의 성분씩 살펴볼 때 i 번째 행과 j 번째 행에서 일치하는 성분과 일치하지 않는 성분이 같으므로 이 경우 두 행은 직교함을 알 수 있다.

(2) 각각의 블록에서 서로 다른 위치의 행벡터인 경우 : 주어진 두 개의 행에 대해서 처음 m 개의 성분만을 살펴보자. 이는 B_1 의 서로 다른 두 행에 이진수 $a(i,1)$ 과 $a(j,1)$ 을 각각 성분별 모드2덧셈한 결과이다. 그런데 허다마드 행렬 B_1 의 서로 다른 두 행은 직교하며, 이 두 행벡터를 b_u 와 b_v 라 두면, 역시 허다마드보존변형에 의해서 $a(i,1)+b_u$ 와 $a(j,1)+b_v$ 도 직교함을 쉽게 알 수 있다. 마찬가지로 주어진 두 행의 다음 m 개의 성분도 직교하

며, 결과적으로 길이 nm 인 두 행의 직교성이 입증된다.

계 1. 실베스터 생성방법은 정리1에서 $B_1 = B_2 = \dots = B_n$ 인 경우이다.

증명 : 생략.

계 2. 임의의 양의 정수 n 과 m 에 대해서, $n \times n$ 허다마드 행렬 $A = [a(i, j)]$ 와 n 개의 $m \times m$ 허다마드 행렬 B_1, B_2, \dots, B_n 가 주어지면, 다음의 $nm \times nm$ 행렬 H 는 허다마드행렬이다.

$$H = \begin{bmatrix} a(1,1)+B_1 & a(1,2)+B_1 & \dots & a(1,n)+B_1 \\ a(2,1)+B_2 & a(2,2)+B_2 & \dots & a(2,n)+B_2 \\ \vdots & \vdots & \dots & \vdots \\ a(n,1)+B_n & a(n,2)+B_n & \dots & a(n,n)+B_n \end{bmatrix}$$

증명 : 이는 $n \times n$ 허다마드행렬 $A = [a(i, j)]$ 의 전치행렬 A^T 와 n 개의 $m \times m$ 허다마드 행렬 $B_1^T, B_2^T, \dots, B_n^T$ 둘로 정리1에 의하여 허다마드 행렬을 만든 후 이를 transpose한 행렬로 허다마드행렬보존변환에 의해 허다마드행렬이 된다

위의 정리1에 의한 생성법을 $n=2$ 와 $m=8$ 에 적용하면 그림3에 보인 16×16 허다마드 행렬을 얻는다. 여기에서 2×2 허다마드 행렬은 그림1에 보인 예를 이용하고, 8×8 허다마드 행렬 두 개는 그림1에 보인 것을 B_1 으로, 그림2에 보인 것을 B_2 로 사용한다.

$$\begin{bmatrix} B_1 & B_2 \\ B_1 & 1+B_2 \end{bmatrix} = \begin{bmatrix} 00000000 & 00000000 \\ 00001111 & 01010101 \\ 01011010 & 00110011 \\ 00111000 & 01100110 \\ 01010101 & 00001111 \\ 00110011 & 01011010 \\ 01100110 & 00111100 \\ 01101001 & 01101001 \\ \hline 00000000 & 11111111 \\ 00001111 & 10101010 \\ 01011010 & 11001100 \\ 00111000 & 10011001 \\ 01010101 & 11110000 \\ 00110011 & 10100101 \\ 01100110 & 11000011 \\ 01101001 & 10010110 \end{bmatrix}$$

그림 3. 크기 16의 허다마드 행렬

즉, 그림3에 보인 하다마드 행렬은 $\begin{bmatrix} B_1 & B_2 \\ B_1 & 1+B_2 \end{bmatrix}$ 의 형태를 갖는다.

IV. 결론

본 논문에서는 하다마드 행렬을 생성하는 실베스터 방법을 소개하고, 이를 일반화 시켰다. 일반화시킨 생성방법을 증명하였으며, 이를 이용하여 16×16 하다마드 행렬을 생성하였다. 우리는 이제 다음의 두 가지 사실에 주목하고 향후 연구과제를 언급하고자 한다.

(1) 우리는 8×8 하다마드 행렬 B_1 의 몇 개의 행을 서로 바꾸어서 얻어진 것을 B_2 로 사용하고 정리1의 생성방법을 이용하여 서로 비동치 관계에 있는 두 개의 16×16 하다마드 행렬을 얻을 수 있었다.

(2) 더 나아가, 그림1에 보인 예를 8×8 하다마드 행렬 B_1 으로 사용하고, B_1 의 행을 서로 바꾸어 주는 모든 가능한 경우를 B_2 로 사용하여 서로 비동치 관계에 있는 모든 가능한 16×16 하다마드 행렬을 얻을 수 있었다.

이로부터 우리는 다음의 향후 연구과제를 생각해 볼 수 있다.

(가) 주어진 두 개의 하다마드 행렬의 동치성을 조사하는 알고리즘은 얼마나 빨리 수행 가능한가.

(나) 고전적인 실베스터 방식으로 얻어진 크기 2^n 의 하다마드 행렬을 B_1 으로 사용하고 이것의 행을 적당히 바꾸어 B_2 로 사용하여 정리1의 생성방법을 적용하면 크기 2^{n+1} 의 모든 가능한 비동치 하다마드 행렬을 얻을 수 있는가.

(다) 하다마드 행렬 B_2 가 단순히 B_1 으로부터 행을 바꾸어준 형태일 때 (row permutation), 어떠한 특정 permutation에 대하여 비동치성이 확정되는가.

참고문헌

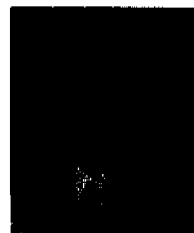
[1] J. H. Van Lint and R. M. Wilson, *A Course In Combinatorics*, Cambridge University Press, 1992.
 [2] TIA/CIA/IS-95, *Mobile Station-Base Station Compatibility Standard for Dual-Mode Side-*

band Spread Spectrum Cellular System, Telecommunication Industry Association as a North American 1.5MHz Cellular CDMA Air-Interface Standard, July, 1993.

[3] Rao K. Yarlagadda and John E. Hershey, *Hadamard Matrix Analysis and Synthesis*, Kluwer Academic Publishers, 1997.
 [4] M. Hall Jr, *Combinatorial Theory*, Second Edition, John Wiley and Sons, 1986.
 [5] R. Craigen, *Hadamard matrices and designs*, Chapter IV.24, CRC handbook of Combinatorial Designs, edit*1 by C. J. Colbourn and J. H. Dinitz, CRC Press, New York, pp. 370-377, 1996.
 [6] S. W. Golomb, *Shift-Register Sequences*, Holden-Day, San Francisco, CA, 1967; Aegean Park Press, Laguna Hills, CA 1982.
 [7] J. Seberry and M. Yamada, "Hadamard Matrices, Sequences, and Block Design," in book, *Contemporary Design Theory: A Collection of Surveys*, edited by J. H. Dinitz and D. R. Stinson, John Wiley and Sons, pp. 431-560, 1992.

신 민 호(Min-Ho Shin)

학생회원



1996년 2월 : 연세대학교 전자공학과 졸업
 2000년 2월 : 연세대학교 전기컴퓨터공학과 졸업(석사)
 2000년 3월~현재 : 연세대학교 전기 컴퓨터공학과 박사과정

<주관심 분야> Error Correcting Codes, PN Sequences, CDMA, Spread Spectrum Communication

송 흥 엽(Hong-Yeop Song)

정회원



1984년 2월 : 연세대학교 전자공학과 졸업(학사)
 1986년 5월 : USC 전자공학과 졸업(석사)
 1991년 12월 : USC 전자공학과 졸업(박사)

