하다마드 행렬을 생성하는 Sylvester방법의 일반화

한국통신학회 하계종합학술대회

1999년 7월

*신민호, *송홍엽, **노종선

*연세대학교, **건국대학교

1. 서론

크기 n인 하다마드 행렬은 n^2개의 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 왈시부호라 불리는데, 이는 IS-95의 셀룰라 CDMA 통신 시스템의 직교채널구성에 필수적인 요소이다. 또한 직교성을 이용하여 오류정정부호와 경로탐색 알고리듬에도 필수적이다.[2]

임의의 $n \times n$ 하다마드 행렬이 주어지면 그 크기 n이 1, 2,

혹은 4의 배수이어야 함을 쉽게 증명할 수 있다. 그러나, 임의의 4의 배수 n에 대하여 $n \times n$ 하다마드 행렬이 존재하는가에 대해서는 아직 완전히 알려지지 않았다.

본 논문에서는 {+1,-1}을 {0,1}로 바꾸어 생각한다. 즉, 하다마드 행렬의 성분은 0 혹은 1이며, 이 경우 두 개의 임의의 행의 직교성은 두 행을 겹쳐놓고 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 모드2덧셈 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 반복하여도 그 결과는 하다마드 행렬이며, 이를 하다마드보존변형(Hadamard-Preserving Transformation)이라 부른다. 임의의 두 개의 $n \times n$ 하다마드 행렬 H_1과 H_2는 특정한 하다마드보존변형에 의하여 H_1이 H_2로 바뀌어질 수 있을 때 동치(Equivalent)관계에 있다고 한다. 하다마드보존변형을 이용하면, 주어진 하다마드 행렬의 첫째 행과 첫째 열을 모두 0이 되도록 만들어 줄 수 있는데, 이를 표준형이라 부른다. 즉, 임의의 하다마드 행렬은 어떠한 표준형 하다마드 행렬과 동치이다.

$$
\begin{matrix} 0 & 0 \\ 0 & 1 \end{matrix}\Bigg] \qquad
\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \qquad
\left[\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{matrix}\right.
$$

그림 1. 크기 2, 4, 8의 하다마드 행렬

예를 들어 그림1에 $n = 2, 4, 8$의 크기에 대한 표준형 하다마드 행렬을 보인다. 임의의 크기 n에 대해서, 표준형 $n \times n$ 하다마드 행렬은 유일하지 않으며, 두 개의 동일한 크기의 하다마드 행렬

의 동치성을 조사하고자 할 때 각각을 표준형으로 변형시켜 조사하면 편리하다.

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

2. Sylvester 생성방법

하다마드 행렬의 생성방법 중에서 가장 잘 알려진 Sylvester생

성방법은 임의의 두 개의 하다마드 행렬로부터 새로운 크기의 하다마드 행렬을 생성하는 방법이다. 즉, 크기 $n \times n$ 하다마드 행렬 $A = [\, a(\, i,j\,)\,]$와 크기 $m \times m$ 하다마드 행렬 $B = [\, b(\, i,j\,)\,]$가 주어지면 크기 $nm \times nm$의 하다마드 행렬 C를 다음과 같이 구성할 수 있다.

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

여기에서 $a(i,j)+B$는 $m\times m$ 행렬로서, 행렬 B의 모든 성분에 $a(i,j)$를 모드2덧셈한 결과를 성분으로 갖는다. 예를 들어, 그림1에 보인 2×2 하다마드 행렬로부터 4×4, 8×8, ..., 일반적으로 $2^r\times2^r$ 하다마드 행렬을 생성할 수 있다. 그림1의 4×4 행렬

은 이 방법으로 생성한 예이며, 아래의 그림2에는 이 방법으로 생성한 8×8 하다마드 행렬을 보인다. CDMA 이동 통신에 사용되는 월쉬부호는 이러한 방법으로 생성된 64×64 하다마드 행렬이다.

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

그림 2. 크기 8의 하다마드 행렬 - Sylvester 생성방법

3. 일반화된 생성법 및 증명

앞 절에서 소개한 Sylvester 생성 방법에서 연산 $a(i,j)+B$

를 살펴보자. 만일 B가 하다마드 행렬이고 $a(i,j)$가 0 혹은 1로서 B의 모든 성분에 성분별 모드2 덧셈을 한 결과라면 행렬 $a(i,j)+B$도 역시 하다마드 행렬이다. 만일 $a(i,j) = 0$이면, 이는 행렬 B와 일치하게 되고, $a(i,j) = 1$이면, 이는 행렬 B의 complement 형태가 된다. 여기서 우리는 최종적으로 얻어지는 행렬 $C = A \oplus B$에서 $m \times m$ 부행렬의 열이 모두 동일한 행렬 B일 필요는 없음을 쉽게 알 수 있다. 이점이 본 논문에서 새로이 제안하는 일반화된 Sylvester생성방법의 핵심이다.

예비정리 1. 행렬 B가 $n \times n$ 하다마드 행렬이고 $a \in \{0,1\}$

이면, 행렬 B의 모든 성분에 a를 모드2 덧셈한 결과로 얻어지는 행렬 $a+B$도 $n\times n$ 하다마드 행렬이다.

증명: 생략.

예비정리 2. If $(c_1, c_2, \ldots, c_n)$ is any binary vector, $c_i \in \{0, 1\}$, and $B_1, B_2, \ldots, B_n$ are (not necessarily distinct) $m\times m$ Hadamard matrices, then the m rows of the following $m\times nm$ matrices

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

are orthogonal to each other in the sense that the number of agreements is the same as the number of disagreements when one is compared with the other.

증명: 생략.

정리 1. Given an $n \times n$ Hadamard matrix $A = [\, a(i,j)\,]$ and n Hadamard matrices $B_1, B_2, \ldots, B_n$ each of size $m \times m$ for any positive integers n and m, the $nm \times nm$ matrix H given below is a Hadamard matrix:

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

증명: 우선 행렬 H 의 nm 개의 행 벡터를 m 개씩 순서대로 묶어서 각각을 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 행벡터가 동

일한 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 모드2

덧셈한 결과이다. 이는 하다마드 행렬의 하다마드보존변형된 결과이므로 두 행은 직교한다. 마찬가지로 주어진 두 행의 다음 m개의 성분도 직교하며, 결과적으로 길이 nm인 두 행의 직교성이 입증된다.

(2) 각각의 블록에서 서로 다른 위치의 행벡터인 경우:

주어진 두 개의 행에 대해서 처음 m개의 성분만을 살펴보자. 이는 B_1의 서로 다른 두 행에 이진수 $a(i,1)$과 $a(j,1)$을 각각 성분별 모드2덧셈한 결과이다. 그런데 하다마드 행렬 B_1의 서로

다른 두 행은 직교하며, 이 두 행벡터를 $\underline{b_x}$ 와 $\underline{b_y}$ 라 두면, 역시 하다마드보존변형에 의해서 $a(i, 1) + \underline{b_x}$ 와 $a(j, 1) + \underline{b_y}$ 도 직교함을 쉽게 알 수 있다. 마찬가지로 주어진 두 행의 다음 m 개의 성분도 직교하며, 결과적으로 길이 nm 인 두 행의 직교성이 입증된다.

계 1. Sylvester 생성방법은 정리1에서 $B_1 = B_2 = \cdots = B_n$ 인 경우이다.

증명: 생략.

계 2. Given an $n \times n$ Hadamard matrix $A = [a(i,j)]$ and n Hadamard matrices $B_1, B_2, \ldots, B_n$ each of size $m \times m$ for any positive integers n and m, the $nm \times nm$ matrix H given below is a Hadamard matrix:

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

증명: 생략.

위의 정리1에 의한 생성법을 $n=2$와 $m=8$에 적용하면 그림3에 보인 16×16 하다마드 행렬을 얻는다. 여기에서 2×2 하다

마드 행렬은 그림1에 보인 예를 이용하고, 8×8 하다마드 행렬 두 개는 그림1에 보인 것을 B_1으로, 그림2에 보인 것을 B_2로 사용 한다. 즉, 그림3에 보인 하다마드 행렬은 $\begin{bmatrix} B_1 & B_2 \\ B_1 & 1+B_2 \end{bmatrix}$의 형태를 갖는다.

4. 결론

본 논문에서는 하다마드 행렬을 생성하는 Sylvester방법을 소개하고, 이를 일반화 시켰다. 일반화시킨 생성방법을 증명하였으며,

$$\begin{bmatrix} B_1 & B_2 \\ B_1 & 1 + B_2 \end{bmatrix}$$

그림 3. 크기 16의 하다마드 행렬

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_1의 몇 개의 행을 서로 바

꾸어서 얻어진 것을 B_2로 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_1으로 사용하고, B_1의 행을 서로 바꾸어주는 모든 가능한 경우를 B_2로 사용하여 서로 비동치 관계에 있는 모든 가능한 16×16 하다마드 행렬을 얻을 수 있었다.

이로부터 우리는 다음의 향후 연구과제를 생각해볼 수 있다.

(가) 주어진 두 개의 하다마드 행렬의 동치성을 조사하는 알고리듬은 얼마나 빨리 수행가능한가.

(나) 고전적인 Sylvester방식으로 얻어진 크기 2^r의 하다마드 행렬을 B_1으로 사용하고 이것의 행을 적당히 바꾸어 B_2로 사용하여 정리1의 생성방법을 적용하면 크기 2^{r+1}의 모든 가능한 비동치 하다마드 행렬을 얻을 수 있는가.

(다) 하다마드 행렬 B_2가 단순히 B_1으로부터 행을 바꾸어준 형태일 때 (row permutation), 어떠한 특정 permutation에 대하여 비동치성이 확정되는가.