행벡터 집합이 벡터공간을 이루는 하다마드 행렬의 동치관계

정회원 진 석 용*, 김 정 헌**, 박 기 현*, 종신회원 송 홍 엽*

Equivalence of Hadamard Matrices Whose Rows Form a Vector Space

Seok-Yong Jin*, Jeong-Heon Kim**, Ki-Hyeon Park* ***Regular Members***
Hong-Yeop Song* ***Lifelong Member***

요 약

본 논문에서는 행벡터의 집합이 이진 벡터합 연산에 관해 닫혀있는 모든 하다마드 (Hadamard) 행렬들은 서로 동치(equivalent)임을 증명한다. 이를 이용하면, 최대길이 수열로부터 생성된 순회 (cyclic) 하다마드 행렬과 크로네커 (Kronecker) 곱에 의해 생성된 월쉬-하다마드 (Walsh-Hadamard) 행렬이 동치임을 간단히 보일 수 있다.

Key Words : Hadamard matrices, Hadamard equivalence, Walsh-Hadamard matrices, Kronecker product, m-sequences

ABSTRACT

In this paper, we show that any two Hadamard matrices of the same size are equivalent if they have the property that the rows of each Hadamard matrix are closed under binary vector addition. One of direct consequences of this result is that the equivalence between cyclic Hadamard matrices constructed by maximal length sequences and Walsh-Hadamard matrix of the same size generated by Kronecker product can be established.

Ⅰ. 서 론

원소가 -1과 +1로 이루어진 $n \times n$ 정방 행렬 H_n이 다음 성질

$$H_n H_n^T = nI_n \tag{1}$$

을 만족하면 H_n을 n차 하다마드 (Hadamard) 행렬이라 한다. 여기서 I_n은 n차 단위행렬이다. 하다마드 행렬은 오류 정정 부호를 비롯한 통신용 신호 설계 분야에서 영상 신호 처리 분야까지 광범위하게 응용된다[1]-[4]. 하다마드 행렬이 1960년대 미국 JPL(Jet Propulsion Laboratory)의 M. Hall, Jr., L. Baumert, 그리고 S. Golomb 등에 의해 Mariner, Voyager 우주 탐사선의 이미지 전송에 채용된 이래로 90년대 Gallileo 탐사선에서도 사용되었음은 잘 알려져 있다[5].

하다마드 행렬 H_n이 존재하면 n은 1, 2, 혹은 4의 배수이며, H_n의 임의의 행 혹은 열에 -1을 곱하거나 임의의 두 행 혹은 열을 맞바꾸어도 (1)을 만족함을 쉽게 알 수 있다. 두 하다마드 행렬 H와 H'에 관하여 H에 행렬 연산 a)와 연산 b)를 반복

※ 본 연구는 한국과학재단 특정기초연구(R01-2008-000-11104-0) 지원으로 수행되었습니다.
* 연세대학교 전기전자공학과 부호및암호 연구실({sy.jin, kh.park, hysong}@yonsei.ac.kr) ** 삼성전자(jeongheon.kim@samsung.com)
논문번호 : KICS2009-05-186, 접수일자 : 2009년 5월 5일, 최종논문접수일자 : 2009년 7월 1일

적용해서 H'을 얻을 수 있으면 H와 H'은 동치(equivalent)인 하다마드 행렬이라고 정의한다.

연산 a) 임의의 두 행 (혹은 열)을 서로 맞바꾼다.
연산 b) 임의의 행(혹은 열)에 -1을 곱한다.

하다마드 행렬의 생성 및 분류 그리고 그 응용분야에 관한 다양한 연구 주제 중, 하다마드 행렬의 동치관계에 관한 연구는 오랫동안 주목을 받고 있는 중요한 연구 주제이다. 서로 다른 (inequivlanet) n차 하다마드 행렬의 개수를 구하는 문제는 매우 어려운 문제로 알려져 있다[6],[7]. 현재까지는 그 크기 $n \le 28$에 대해서만 서로 다른 (inequivalent) 하다마드 행렬의 개수가 완전히 알려져 있을 뿐이다. 특히 1960년대에 16차 하다마드 행렬이 완전히 분류된 이후 1990년대 초반에 이르러서야 28차 하다마드 행렬의 분류작업이 마무리되었으며, 이에 관한 연구는 현재까지도 계속되고 있다[6]-[8].

본 논문에서는 하다마드 행렬의 동치관계에 관한 다음 성질을 증명한다. 즉, 행벡터 (row vector) 집합이 이진 벡터합 (vector addition) 연산에 관해 닫혀있어 그 자체로 벡터 공간을 이루는 2^m차 하다마드 행렬들은 모두 동치임을 보인다. 이는 특정 생성방법에 구애받지 않고 하다마드 행렬의 동치관계를 확립하는데 중요하게 사용될 수 있다.

논문의 구성은 다음과 같다. 제 Ⅱ절에서는 본 논문의 주된 결과를 증명한다. 제 Ⅲ절에서는 제 Ⅱ절의 결과를 이용한 하나의 이론적 응용으로서, 월쉬-하다마드(Walsh-Hadamard) 행렬과 최대길이 수열(m-sequences)을 이용하여 생성한 순회(cyclic) 하다마드 행렬의 동치관계 확립 및 기존 방법과의 차별성을 소개한다. 마지막으로 제 Ⅳ절에서는 본 논문의 결과를 요약한다.

표 1. 비동치 (inequivalent) 하다마드 행렬의 개수[8, prop. 1.49]

n	4	8	12	16	20	24	28	32	36
#	1	1	1	5	3	60	487	$>3.6\times10^6$	$>15\times10^6$

Ⅱ. 주된 결과: 벡터합 연산에 관해 닫혀있는 행벡터들로 이루어진 하다마드 행렬의 동치관계

지금부터는 하다마드 행렬을 지칭할 때, 편의상 원소 -1을 1로, +1을 0으로 변경한 행렬을 뜻하기로 하고, $\mathbb{V}_n$을 n차원 이진 벡터공간이라 하자. 즉, $\mathbb{V}_n = \{(a_1,...,a_n) : a_i \in GF(2), i=1,...,n\}$. 만약 n차 하다마드 행렬 H의 모든 행벡터들로 이루어진 집합 $S(H)$가 벡터합에 관해 닫혀있으면, $S(H)$ 자신이 벡터공간이다[9]. $S(H)$를 $\mathbb{V}_n$의 m차원 부분공간(subspace)이라 하면, $S(H)$는 길이가 n인 영벡터(zero vector)를 포함한 2^m개의 벡터를 원소로 갖는다.

정리 1 행벡터 집합이 벡터합에 관해 닫혀있는 모든 2^m차 하다마드 행렬은 서로 동치이다.

증명 H와 H'을 주어진 조건을 만족하는 임의의 두 하다마드 행렬이라 하자. 편의상 $n=2^m$이라 하면, $S(H)$와 $S(H')$ 공히 $\mathbb{V}_n$의 m차원 부분공간이다.

먼저, $S(H)$의 기저(basis)를 $\{\boldsymbol{b_1}, \boldsymbol{b_2}, ..., \boldsymbol{b_m}\}$이라 하고, 이를 (2)와 같이 행렬 형태로 표시한다.

$$B = \begin{bmatrix} \boldsymbol{b_1} \\ \boldsymbol{b_2} \\ \vdots \\ \boldsymbol{b_m} \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & ... & b_{1n} \\ b_{21} & b_{22} & ... & b_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{m1} & b_{m2} & ... & b_{mn} \end{bmatrix} \quad (2)$$

이 때, B의 모든 열(column)은 서로 다르다. 왜냐하면 B에 동일한 열이 있다면 H에도 동일한 열이 있어야 하고, 이는 하다마드 행렬의 정의상 불가능하기 때문이다. 따라서 행렬 B는 정확히 2^m개의 길이 m인 이진 열벡터(column vector)로 구성된다.

마찬가지로 $S(H')$의 기저를 (2)와 같은 형태로 적고 이를 B'이라 하면 행렬 B' 역시 정확히 2^m개의 길이 m인 이진 열벡터로 구성된다.

그러므로 B의 열벡터의 순서를 재배치하여 B'과 일치시킬 수 있다. 즉 B의 열벡터 위치를 치환하는 $n\times n$ 치환 행렬 (permutation matrix) σ가 존재해서 다음을 만족한다.

$$B' = B\sigma$$

이는 $S(H')$과 $S(H\sigma)$가 동일한 기저에 의한 펼침 (span) 공간임을 뜻하므로 $S(H')$과 $S(H\sigma)$는 집합으로서 동일하다. 즉, H'과 $H\sigma$는 동일한 행벡터들로 이루어진다. 따라서 H와 H'은 동치인 하다마드 행렬이다. ■

예 1 아래에 표시된 두 개의 8차 하다마드 행렬 H와 H'을 고려하자.

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

H의 행벡터 집합 $S(H)$와 H'의 행벡터 집합 $S(H')$ 모두 벡터합에 관해 닫혀 있으므로 그 자신이 각각 3차원 벡터 공간이다. 각각의 기저 B와 B'를 아래와 같이 선택하자.

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

이 때 $B'=B\sigma$인 치환 행렬 σ를 쉽게 찾을 수 있고 $S(H')=S(H\sigma)$이므로 H와 H'은 서로 동치인 하다마드 행렬이다. ■

Ⅲ. 주 결과의 응용 예 : 월쉬-하다마드 행렬과 최대길이 수열에 의한 순회 하다마드 행렬

월쉬-하다마드 행렬과 순회 하다마드 행렬은 가장 널리 활용되는 두 종류의 하다마드 행렬로서, 오류정정부호로서의 직교 부호와 밀접한 관련이 있으며 영상신호처리를 위한 월쉬-하다마드 변환 (Wash-Hadamard transform) 등에 응용된다[1]-[5].

먼저, 월쉬-하다마드 행렬은 (3)과 같이 연속된 크로네커 곱 (Kronecker product)에 의해 재귀적으로 생성된 2^m차 정방행렬이다.

$$K_1=\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}$$
$$K_{m+1}=\begin{bmatrix}K_m & K_m\\ K_m & \overline{K_m}\end{bmatrix},\ m\geq 1 \qquad (3)$$

수학적 귀납법을 이용하여 월쉬-하다마드 행렬의 행벡터 집합이 벡터합에 관해 닫혀있음을 쉽게 보일 수 있다.

이번에는 최대길이 수열로부터 생성된 순회 하다마드 행렬을 고려한다. 제 I절의 연산 b)에 의해 임의의 하다마드 행렬의 첫 번째 행과 첫 번째 열의 모든 원소를 +1로 정규화 (normalize) 할 수 있다. 정규화된 n차 하다마드 행렬 H의 첫 번째 행과 첫 번째 열을 제외한 $(n-1)$차 정방행렬 H_c가 순환 (circulant) 행렬이면 H를 순회 (cyclic) 하다마드 행렬이라 한다. 그 정의에 의해, 순회 하다마드 행렬은 최적 자기상관 특성을 갖는 수열[2],[10],[11], 즉 모든 시간 지연에 대한 주기적 자기상관 (periodic auto-correlation) 값이 -1인 이진 수열로부터 생성된다. 최적 자기상관 특성을 갖는 수열 중 가장 널리 활용되는 최대길이 수열은 여러 가지 의사 잡음 (PN: Pseudo-Noise) 특성을 지니며, 특별히 "cycle-and-add" 성질[2],[10],[11]을 가진다. 그러므로 최대길이 수열을 이용하여 생성한 순회 하다마드 행렬의 행벡터 집합 역시 벡터합에 관해 닫혀있다.

따라서 정리 1에 의해, 2^m차 월쉬-하다마드 행렬과 주기 2^m-1인 최대길이 수열로부터 생성된 2^m차 순회 하다마드 행렬은 서로 동치인 하다마드 행렬이다. 예 1의 H는 2^3차 월쉬-하다마드 행렬이고 H'은 주기가 7인 최대길이 수열 1110100로부터 생성된 순회 하다마드 행렬이다.

논의를 최대길이 수열을 이용한 순회 하다마드 행렬과 월쉬-하다마드 행렬에 국한했을 때, 두 하다마드 행렬의 동치관계는 각각의 행렬 인수분해 특성을 이용하여 보일 수도 있다[12],[Ch.18]. 월쉬-하다마드 행렬 K_m은 $2^m\times m$ 행렬 X에 관해 $K_m=XX^T$와 같은 형태로 인수분해 되며 이 때 행렬 X는 모든 2^m개의 서로 다른 이진 m-tuple을 그 행으로 갖는다[13]. 최대길이 수열에 의한 순회 하다마드 행렬 역시 (X와 같은 크기의) 행렬 Y에 관해 YY^T 형태로 인수분해 되며, 이 때 인수행렬 Y가 최대 계수(rank) 값을 가져야 함은 Lempel의 이진 대칭 행렬의 인수 분해 구조에 관한 결과[14]로부터 알 수 있다.

반면 본 논문의 정리 1은 그 대상을 특정 생성 방법에 의한 하다마드 행렬로 한정하지 않는다. 또한 그 증명과정에서 드러나듯이, 임의의 하다마드 행렬의 행벡터 집합이 벡터 부공간을 이룰 때 그 기저를 행렬 형태로 표시하면 최대 계수(full rank)를 가져야만 한다는 관찰에서 비롯되었다. 이 사실은, 최대길이 수열에 의해 생성된 순회 하다마드 행렬이나 월쉬-하다마드 행렬 등의 공통적 성질을 추출한 것으로서 두 하다마드 행렬 공히 앞 단락에서 설명한 형태로 인수분해되는 근거를 제공한다.

Ⅳ. 결 론

본 논문에서는 행벡터 집합이 벡터합 연산에 관

해 닫혀있는 모든 2^m차 하다마드 행렬은 서로 동치임을 보였다. 이 결과는 생성 방법이 상이한 하다마드 행렬의 연관성 규명 및 빠른 하다마드 변환 (fast Hadamard transform) 구현에 응용될 수 있다.

참 고 문 헌

〔1〕 S. S. Agaian, *Hadamard Matrices and Their Applications*, Lecture Notes in Mathematics 1168, Springer-Verlag, 1985.

〔2〕 S. W. Golomb and G. Gong, *Signal Design for Good Correlation*, Cambridge University Press, 2005.

〔3〕 F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977, Tenth impression, 1998.

〔4〕 H.-Y. Song and S. W. Golomb, "Some new constructions for simplex codes," *IEEE Transactions on Information Theory*, 40:(2), pp.504-507, March, 1994.

〔5〕 J. Seberry and M. Yamada, "Hadamard matrices, sequences, and block designs," in *Contemporary Design Theory*, edited by J. H. Dinitz and D. R. Stinson, John Wiley & Sons, pp.431-560, 1992.

〔6〕 N. J. A. Sloane and S. Plouffee, *The Encyclopedia of Integer Sequences,* Academic Press, 1995. See also: N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences/A007299.

〔7〕 N. J. A. Sloane, "My favorite integer sequences," in *Sequences and Their Applications*, edited by C. Ding, T. Helleseth and H. Niederreiter, Springer, 1999, pp.103-130. See also the extended version: http://www.research.att.com/~njas/doc/sg.pdf

〔8〕 R. Craigen and H. Kharaghani, "Hadamard matrices and Hadamard designs," in *Handbook of Combinatorial Designs, 2nd Ed.*, edited by C. J. Colbourn and J. H. Dinitz, Chapman & Hall/CRC, 2007, pp.273-280.

〔9〕 S. Lang, *Linear Algebra*, Third Edition, Springer, 1987.

〔10〕 S. W. Golomb, *Shift Register Sequences*, Revised Edition, Aegean Park Press, 1982, originally published by Hoden-Day in 1967.

〔11〕 H.-Y. Song, "Feedback shift register sequences," in *Wiley Encyclopedia of Telecommunications*, edited by J. G. Proakis, John Wiley & Sons, pp.789-802, 2003.

〔12〕 R. K. Yarlagadda and J. E. Hershey, *Hadamard Matrix Analysis and Synthesis*, Kluwer Academic Publishers, 1997.

〔13〕 K. W. Henderson, "Comment on 'Computations of the fast Walsh-Fourier transform,'" *IEEE Transactions on Computers*, 19:(9), pp.850-851, September, 1970.

〔14〕 A. Lempel, "Matrix factorization over GF(2) and trace-orthogonal bases of GF(2n)," *SIAM Journal of Computation*, 4:(2), pp.175-186, June, 1975.

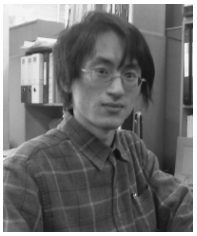
진 석 용 (Seok-Yong Jin) 정회원

2001년 8월 연세대학교 전기전자공학과 졸업
2003년 8월 연세대학교 전기전자공학과 석사
2003년 9월~현재 연세대학교 전기전자공학과 박사과정
<관심분야> PN Sequences, Error-Correcting Codes, Spread Spectrum Communications, Block/Stream Cipher Systems

김 정 헌 (Jeong-Heon Kim) 정회원

1996년 2월 연세대학교 전자공학과 졸업
1998년 2월 연세대학교 전자공학과 석사
2002년 2월 연세대학교 전기전자공학과 박사
2002년 3월~현재 삼성전자 책임연구원
<관심분야> Mobile WiMax(WiBro), Error Correcting Codes, PN Sequences, CDMA

박 기 현 (Ki-Hyeon Park) 정회원



2007년 2월 연세대학교 전기전자공학과 졸업

2009년 2월 연세대학교 전기전자공학과 (석사)

2009년 3월~현재 연세대학교 전기전자공학과 박사과정

<관심분야> PN Sequences, Cryptography, Error-Correcting Codes

송 홍 엽 (Hong-Yeop Song) 종신회원

1984년 2월 연세대학교 전자공학과 졸업

1986년 5월 USC(University of Southern California, USA) 대학원 전자공학과 (공학석사)

1991년 12월 USC 대학원 전자공학과 (공학박사)

1992년 1월~1994년 4월 USC Communication Science Institute, 박사 후 연구원 (Post-Doc)

1994년 5월~1996년 8월 Qualcomm Inc., San Diego, USA, 선임연구원

1995년 9월~1998년 2월 연세대학교 전자공학과 조교수

1998년 3월~2003년 2월 연세대학교 전기전자공학과 부교수

2002년 3월~2003년 2월 University of Waterloo, Canada, 방문연구교수

2003년 3월~현재 연세대학교 전기전자공학과 교수

<관심분야> PN Sequences, Error Correcting Codes, Spread Spectrum Communication Systems, Steam Cipher Systems