2013년 5월 전자공학회 논문지 제 50 권 제 5 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 5, May 2013 http://dx.doi.org/10.5573/ieek.2013.50.5.009

논문 2012-50-5-2

3/5-Modular Hadamard-Jacket 대칭 행렬

(3/5-Modular Hadamard-Jacket Symmetric Matrices)

박 주 용*, 김 정 수**, 페렌스 스졸로시***, 이 문 호****

(Ju Yong Park, Jeong Su Kim, Ference Szollosi and Moon Ho Lee©)

요 약

본 논문에서는 modular 대칭 설계에 대해 소개하고 이를 이용하여 Hadamard-Jacket 행렬의 modular 3/5가 존재한다는 것을 제시한다. 그리고 n차 5-modular Hadamard 행렬의 필요충분조건이 $n \neq 3,7 \pmod{10}$와 $n \neq 6,11$ 임을 증명한다. 특히 Hadamard-Jacket 추측(conjecture)에 대한 5-modular 버전을 구한다.

Abstract

In this paper we introduce modular symmetric designs and use them to study the existence of Hadamard-Jacket matrices modulo 3/5. We prove that there exist 5-modular Hadamard-Jacket matrices of order n if and only if $n \neq 3,7 \pmod{10}$ and $n \neq 6,11$. In particular, this solves the 5-modular version of the Hadamard conjecture.

Keywords : Modular Hadamard-Jacket matrix, Combinatorial design, Modular symmetric design.

Ⅰ. 서 론

기본 Hadamard 행렬이나 일반식으로 표현된 Hadamard 행렬은 수학적으로 많은 분야에 응용되고 있다[6~7]. n차 기본 Hadamard 행렬은 $n \times n$ 행렬 H로 나타내고 원소가 ± 1이며 $HH^T = nI$이다. 여기서 T는 transpose이고 I는 단위행렬을 나타낸다. Hadamard행렬은 행과 열이 직교(orthogonal)한다는 중요한 성질을 가지고 있다. 따라서 modular Hadamard-Jacket[21] 행렬에 대해 살펴보면, 계수 m이 $m \geq 2$ 와 같이 주어질 때, 크기가 n인 m-modular Hadamard 행렬 H 는 원소가 ± 1인 $n \times n$ 행렬로 $HH^T \equiv nI \pmod{m}$이다. modular Hadamard 행렬은 첫 번째 행과 열의 모든 원소들이 1이다. modular Hadamard행렬은 1972년 Marrero 와 Butson에 의해 처음 소개 되었고[14], 이들은 이 행렬을 여러 복합설계에 연결시키고 modular Hadamard를 포함하는 다양한 일반적 구조를 제시했다[5, 12~13]. 최근 [2]에서 Eliahou와 Kervaire가 modular Golay 시퀀스[3]를 이용하여, 4로 나누어질 수 있는 n차 32-modular Hadamard 행렬의 존재를 증명했다. 그들의 노력은 Hadamard 추측(conjecture)과 Ryser의 추측으로부터 동기를 얻어 수행되었다. Hadamard 추측은 두 배수 짝수 차원의 real Hadamard 행렬이 존재함을 예상한 반면 Ryser는 $n > 4$ 차원의 순환 real Hadamard 행렬이 존재하지 않는다고 추측했

* 평생회원, 신경대학교 인터넷정보통신학과
(Department of Internet, Information & Communication, Shyngyeong University)
** 정회원, 숭실사이버대학교 컴퓨터정보통신학과
(Department of Computer, Information & Communication, Korea Soongsil Cyber University)
*** Budapest University of Technology and Economic, Hungary
**** 평생회원, 전북대학교 정보공학부
(Division of Electronic Engineering, Chonbuk National University)
※ 본 연구는 한국연구재단의 세계 수준의 연구중심대학 (World Class University, WCU R32-2013-000-20014-0, BSRP 2010-0020942, 그리고 MEST 2012-002521의 지원으로 수행되었음.
© Corresponding Author(E-mail:moonho@jbnu.ac.kr)
접수일자: 2012년12월24일, 수정완료일: 2013년4월18일

다[18, 21]. 최근 이 두 추측은 [11]과 [16]의 노력에도 불구하고 결코 달성이 쉽지 않다는 사실이 밝혀졌다.

modular Hadamard 행렬의 개념이 최근 Jacket행렬을 연구하는 과정에서 공학적으로 다시 재조명되고 있다[8]. 특히 [9]에서 암호학과 연결할 수 있는 가능성이 언급되었다[17, 20]. 본 논문에서 MHJ(n,m)라는 표현은 사이즈가 n인 m-modular Hadamard-Jacket행렬을 나타내며, n차 real Hadamard-Jacket 행렬은 MHJ$(n,0)$으로 나타내었다. 또 (a,b)라는 표현은 정수 $a,b \geq 0$ 에 대해 최대공약수(greatest common divisor)를 나타낸다.

본 논문의 구성은 Ⅱ장에서 기존의 3-modular Hadamard-Jacket행렬에 대해 살펴보고, Ⅲ장에서 기존 논문의 결과들을 분석하여 modular Hadamard-Jacket 행렬의 존재에 대해 간단히 언급하며, Ⅳ장에서는 Marrero의 개념을 정규화하고 m-modular 대칭 설계를 소개한다. 또한 modular Hadamard-Jacket 행렬의 일반적인 직합(direct sum)형태의 구성에 대해 언급하고, 응용예로서 새롭게 개발된 이론을 사용하여 5-modular Hadamard-Jacket 행렬의 존재를 결정한다. 그리고 Ⅴ장에서 결론을 맺는다.

Ⅱ. 기존의 3-Modular Hadamard-Jacket 행렬[22]

Sylvester Hadamard 행렬은 가장 먼저 알려져 있으며 여전히 중요한 Hadamard 행렬이다. Hadamard 기본 행렬은 다음과 같다.

$$S_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1}$$

Sylvester Hadamard 행렬은 다음과 같이 정의된다.

$$S_k = \otimes^k S_1, k \geq 1 \tag{2}$$

여기서 $\otimes^k$ 는 k번의 kronecker를 나타낸다.

Sylvester Hadamard 행렬은 여러 가지로 표현될 수 있다. 그중 한 가지가 행렬의 색인 (g,h) 에 대한 2진수 표현을 사용하고 $< g,h >$ 를 $GF(2)$ 위에서의 g와 h의 내적이라고 하면, Sylvester Hadamard 행렬 S_k 는 다음과 같이 표현할 수 있다.

$$S_k = [(-1)^{< g,h >}]_{0 \leq g,h \leq 2^k-1} \tag{3}$$

여기서 g와 h , $< g,h >$ 는 다음과 같다.

$$\forall i, g_i, h_i \in GF(2),$$

$$g = \sum_{i=0}^{k-1} 2^i g_i = g_0 + 2g_1 + \cdots + 2^{k-1} g_{k-1},$$

$$h = \sum_{i=0}^{k-1} 2^i h_i = h_0 + 2h_1 + \cdots + 2^{k-1} h_{k-1},$$

$$< g,h > = g_0 h_0 + g_1 h_1 + \cdots + g_{k-1} h_{k-1} \pmod 2$$

$$= g_0 h_0 \oplus g_1 h_1 \oplus \cdots \oplus g_{k-1} h_{k-1} \tag{4}$$

예로서 4×4 Sylvester Hadamard 행렬은 다음과 같이 표현할 수 있다.

$$S_2 = \begin{bmatrix} (-1)^{<00,00>} & (-1)^{<00,01>} & (-1)^{<00,10>} & (-1)^{<00,11>} \\ (-1)^{<01,00>} & (-1)^{<01,01>} & (-1)^{<01,10>} & (-1)^{<01,11>} \\ (-1)^{<10,00>} & (-1)^{<10,01>} & (-1)^{<10,10>} & (-1)^{<10,11>} \\ (-1)^{<11,00>} & (-1)^{<11,01>} & (-1)^{<11,10>} & (-1)^{<11,11>} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{5}$$

식 (5)의 4×4 Hadamard 행렬을 7×7 로 확장하면 다음과 같다.

$$V_7 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 & -1 & -1 & 1 \end{bmatrix}. \tag{6}$$

$V_7 \times V_7$ 은 다음과 같다.

$$V_7 \times V_7 = \begin{bmatrix} 7 & 3 & 3 & 3 & 3 & 3 & -3 \\ 3 & 7 & 3 & 3 & 3 & 3 & -3 \\ 3 & 3 & 7 & 3 & 3 & 3 & -3 \\ 3 & 3 & 3 & 7 & 3 & 3 & -3 \\ 3 & 3 & 3 & 3 & 7 & 3 & -3 \\ 3 & 3 & 3 & 3 & 3 & 7 & -3 \\ 3 & -3 & -3 & -3 & -3 & -3 & 7 \end{bmatrix}. \tag{7}$$

이 때 행렬의 원소를 $GF(3)$ 위에서 정의 한다면, 식 (7)을 다음과 같이 나타낼 수 있다.

$$V_7 \times V_7 = \begin{bmatrix} 7 & 3 & 3 & 3 & 3 & 3 & -3 \\ 3 & 7 & 3 & 3 & 3 & 3 & -3 \\ 3 & 3 & 7 & 3 & 3 & 3 & -3 \\ 3 & 3 & 3 & 7 & 3 & 3 & -3 \\ 3 & 3 & 3 & 3 & 7 & 3 & -3 \\ 3 & 3 & 3 & 3 & 3 & 7 & -3 \\ 3 & -3 & -3 & -3 & -3 & -3 & 7 \end{bmatrix} \pmod 3$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_7 \quad . \tag{8}$$

식 (8)은 3-modular Hadamard-Jacket행렬이다. 본 행렬 응용은 All or nothing 암부호[17, 20, 22]와 Massive MIMO[23]에 응용될 수 있다.

Ⅲ. Modular Hadamard-Jacket행렬 존재여부

본 장에서는 modular Hadamard-Jacket(MHJ) 행렬의 기본적인 결과를 요약하고자 한다. [14]와 [15]에서 소개되었던 간단한 방법을 이용하면 $m = 2,3,4$ 와 6인 경우 MHJ(n,m) 행렬이 존재한다는 것을 확신하게 되었다. 먼저 다음과 같은 몇 가지 필요조건들을 염두에 두면서 시작한다. 기존 표현과 같이 Euler의 totient 함수는 $\varphi(n)$과 같이 나타내기로 한다. 여기서 totient 함수 $\varphi(n)$은 1부터 n까지의 양의 정수 중에 n과 서로소인 수의 개수를 나타내는 함수이다.

정리 3.1 : ([13]의 Corollary 2.1참조) H 를 $n \geq 3$ 인 경우의 MHJ(n,m) 행렬이라 놓으면 다음이 성립한다.

(a) 만약 m이 짝수이면, n은 짝수이다[13]. 또한, $m \equiv 0 \pmod 4$ 이면 $n \equiv 0 \pmod 4$이다.

(b) 만약 m이 홀수이고 $n \not\equiv 0 \pmod m$이면, $n \geq 4r$ 이다. 이때 $1 \leq r \leq m-1$이고 $r \equiv 2^{\varphi(m)-2} n \pmod m$ 이다.

증명 : H 는 정규화(normalize) 되었다고 생각할 수 있다. A,B,C,D 가 H의 두 번째와 세 번째 행의 각 수직쌍(vertical pair) $[1,1]^T, [1,-1]^T, [-1,1]^T, [-1,-1]^T$의 개수라고 놓는다. 정규화에 의해 $A \geq 1$ 이라는 것을 알 수 있다. 분명히 $A+B+C+D = n$ 이다. 더욱이 첫 번째 3행 내에서 직교조건을 고려해보면 다음과 같은 관계, 즉, $A+B-C-D \equiv 0 \pmod m$, $A-B+C-D \equiv 0 \pmod m$, $A-B-C+D \equiv 0 \pmod m$ 와 $4A \equiv n \pmod m$을 발견할 수 있다. 따라서 이는 $(4,m) | n$ 의 조건에 맞는다. 반면에 m이 홀수이면 $n \not\equiv 0 \pmod m$처럼 $A \equiv B \equiv C \equiv D \equiv 2^{\varphi(m)-2} n \not\equiv 0 \pmod m$ 임을 쉽게 알 수 있다. 따라서 주장한 대로 $n = A+B+C+D \geq 4r$ 이 성립된다. □

또 다른 유용한 조건이 다음정리에서 알 수 있다.

정리 3.2 : ([14]의 Theorem 2.2참조) H 가 MHJ (n,m) 행렬이라 놓는다. 만약 $(n,m) = 1$ 이고 n 이 홀수이면 n은 m의 평방잉여(quadratic residue)이다.

증명 : $HH^T \equiv nI \pmod m$이기 때문에 결국 $(\det H)^2 \equiv n^2 \pmod m$ 이다. □

이제 modular Hadamard 행렬에 대해 알아본다. J 는 모든 원소가 1 인 행렬로 정의한다.

정리 3.3 : ([15]의 Theorem 2.3참조) 만약 $n \equiv 0 \pmod m$ 이거나 $n \equiv 4 \pmod m$ 이면 MHJ(n,m) 행렬이 존재한다.

증명 : n이 m의 배수이거나 $n-4$가 m의 배수이면, 각각 J 와 $J-2I$는 MHJ(n,m) 행렬이다. □

구형 행렬로부터 Kronecker product를 이용하면 새로운 행렬을 얻을 수 있다. 본 논문을 통해 변수들 중에 하나는 항상 식(9)과 같은 2×2 Hadamard 행렬이기 때문에, 보다 일반적인 다음과 같은 정리를 얻을 수 있다.

$$F_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{9}$$

정리 3.4 : ([15]의 Theorem 2.1참조) H 가 MHJ (n_1,m_1) 행렬이고 K 는 MHJ(n_2,m_2) 행렬이라 놓으

면 $H\otimes K$는 MHJ(n,m_1m_2)이다. 여기서 $n=GCD\{n_2m_1,n_1n_2,n_1m_2\}$이고, GCD는 최대공약수이다.

증명 : [2]로부터 정수 행렬 X 와 Y 에 대해서 $HH^T=n_1I_{n_1}+m_1X$ 와 $KK^T=n_2I_{n_2}+m_2Y$ 의 관계를 살펴보면 다음 관계가 성립함을 알 수 있다.

$$(H\otimes K)(H\otimes K)^T=n_1n_2I_{n_1n_2}+m_1n_2X\otimes I_{n_2}+m_2n_1I_{n_1}\otimes Y+m_1m_2X\otimes Y. \quad (10)$$ □

이 결과를 바탕으로 $m=2,3,4,6$에 대해 MHJ(n,m) 행렬의 존재를 쉽게 알 수 있다.

정리 3.5 : ([14],[15]) $n\geq 2$ 인 경우 다음이 성립한다.

(a) MHJ$(n,2)$이 존재하기 위한 필요충분조건은 n이 짝수이다.

(b) MHJ$(n,3)$이 존재하기 위한 필요충분조건은 $n\not\equiv 5$ (mod 6) 이다.

(c) MHJ$(n,4)$이 존재하기 위한 필요충분조건은 n=2 이거나 n이 이중도(doubly even) 이다.

(d) MHJ$(n,6)$이 존재하기 위한 필요충분조건은 n이 짝수이다.

증명 : 한편으로 (a),(c),(d)와 (b)의 경우에 여기서 설명한 필요조건들은 각각 정리 3.1과 정리 3.2로부터 나온 것이다. 반면에 이러한 modular Hadamard-Jacket 행렬의 존재는 (b)와 (c)에서 $n\equiv 2$(mod 6)의 경우를 제외하고 정리 3.3을 만족한다. 이와 같은 행렬은 2×2 Hadamard 행렬 F_2 와 MHJ$(3k+1,3)$ 의 Kronecker product를 취함으로서 구성할 수 있다.

Ⅳ. Modular 결합 설계와 Modular 5 Hadamard-Jacket 행렬

본 장에서는 modular 조합 디자인을 소개하고 이를 이용하여 5-modular Hadamard-Jacket 행렬의 존재를 살펴본다.

결과 4.1 : $n\equiv 0$, 4, 5, 8, 9(mod 10)인 경우 MHJ(n,5)행렬이 존재하고, $n\equiv 3$, 7(mod 10)인 경우는 MHJ(n,5)행렬이 존재하지 않는다.

증명 : $n\equiv 0$, 4, 5, 9(mod 10)인 경우의 MHJ(n, 5) 행렬은 정리 3.3에 의해 존재하고, $n\equiv 8$(mod 10)인 경우의 MHJ(n,5)행렬은 정리 3.4에 의해 MHJ$(5k+4,5)$ 행렬과 2×2 Hadamard 행렬 F_2 와 Kronecker 곱에 의해 얻어지며 존재함을 알 수 있다. 반면에 $n\equiv 3$, 7(mod 10)에 대해서는 정리 3.2에 의해 존재하지 않는다는 것을 알 수 있다. □

나머지의 경우는 간단치 않은 문제가 남아 있으며, 특히 $n\equiv 1$, 6(mod 10)인 경우는 정리 3.1에 의해 존재하지 않는다는 결과를 알 수 있다.

예제 4.1 : $n\equiv 5k, k\geq 0$ 인 경우 n=5, 10, 15, ⋯에 대한 행렬 J_n은 다음과 같다.

$$J_5=\begin{bmatrix}1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\end{bmatrix}$$과

$$J_{10}=\begin{bmatrix}1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&1&1\end{bmatrix},$$

은 모두 MHJ($5k$,5)행렬이다.

예제 4.2 : $n\equiv 5k+4, k\geq 0$인 경우 n=4, 9, 14, ⋯ 에 대한 행렬 $[J_n-2I_n]$은 다음과 같다.

$$[J_4-2I_4]=\begin{bmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{bmatrix}.$$

위 행렬의 역행렬은

$$[J_4-2I_4]^{-1}=\frac{1}{4}\begin{bmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{bmatrix}.$$

위 행렬은 Circulant Jacket 행렬이 된다.

이차방정식 $\alpha^2+(\mathrm{n}-2)\alpha+1=0$에서 근(根) a_n은

$$\alpha_n=\frac{-(\mathrm{n}-2)\pm\sqrt{(\mathrm{n}-2)^2-4}}{2},\ n\geq 4\ .$$

Identity 행렬과 1로된 Jacket 행렬을 더하면 Circulant Jacket 행렬이다.

이 때, $P=(\alpha_n-1)\mathrm{I}_n+J_n$. 이 때, $\alpha_4=-1$이다. 즉,

$$I_4=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix},\quad J_4=\begin{bmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{bmatrix}.$$

Circulant Jacket 행렬 P는 다음과 같다.

$$P=\begin{bmatrix}-1&1&1&1\\1&-1&1&1\\1&1&-1&1\\1&1&1&-1\end{bmatrix}.$$

$9\times 9\ J_9-2I_9$ 행렬과 역행렬은 다음과 같다.

$$[J_9-2I_9]=\begin{bmatrix}-1&1&1&1&1&1&1&1&1\\1&-1&1&1&1&1&1&1&1\\1&1&-1&1&1&1&1&1&1\\1&1&1&-1&1&1&1&1&1\\1&1&1&1&-1&1&1&1&1\\1&1&1&1&1&-1&1&1&1\\1&1&1&1&1&1&-1&1&1\\1&1&1&1&1&1&1&-1&1\\1&1&1&1&1&1&1&1&-1\end{bmatrix}.$$

$$[J_9-2I_9]^{-1}=\frac{1}{9}\begin{bmatrix}-1&1&1&1&1&1&1&1&1\\1&-1&1&1&1&1&1&1&1\\1&1&-1&1&1&1&1&1&1\\1&1&1&-1&1&1&1&1&1\\1&1&1&1&-1&1&1&1&1\\1&1&1&1&1&-1&1&1&1\\1&1&1&1&1&1&-1&1&1\\1&1&1&1&1&1&1&-1&1\\1&1&1&1&1&1&1&1&-1\end{bmatrix}.$$

는 모두 MHJ$(5k+4,5)$행렬이다.

예제 4.3 : $n\equiv 10k+8, k\geq 0$인 경우 n=8, 18, 28, …에 대한 행렬 J_n-2I_n은 다음과 같다.

$$H_2\otimes(J_4-2I_4)=\begin{bmatrix}-1&1&1&1&-1&1&1&1\\1&-1&1&1&1&-1&1&1\\1&1&-1&1&1&1&-1&1\\1&1&1&-1&1&1&1&-1\\-1&1&1&1&1&-1&-1&-1\\1&-1&1&1&-1&1&-1&-1\\1&1&-1&1&-1&-1&1&-1\\1&1&1&-1&-1&-1&-1&1\end{bmatrix}.\quad(11)$$

과 $H_2\otimes(J_9-2I_9)$는 모두 MHJ$(10k+8,5)$행렬이다.

결과 4.2 : ([15], 정리 3.1참조) MHJ(6,5)행렬과 MHJ(11,5)행렬은 존재하지 않는다.

증명 : 정리 3.1로부터 $m=5$와 n=6, 11의 경우는 $n\geq 16$의 조건에 위배되기 때문에 존재하지 않음을 알 수 있다. □

따라서 $n\equiv 1, 2$ 또는 6(mod 10)인 경우의 MHJ$(n,5)$ 행렬을 구성하는 것이 실제로 풀어야할 문제이다. 흥미로운 modular Hadamard 행렬의 예를 얻기 위해 [5], [13], [14], [15]에서 사용되었던 결합설계(combinatorial design)를 이용할 수 있다. 그러나 조금 진전된 단계로서 다음과 같은 modular block 설계를 택할 수 있다.

정의 4.1 : ([12] 참고) $m,v\geq 2$ 는 정수라 놓는다. 만약 $DD^T\equiv(k-\lambda)I+\lambda J\pmod m$과 $DJ\equiv JD\equiv kJ\pmod m$의 조건을 만족하는 정수 k와 λ가 주어질 때,

원소가 0 또는 1인 $v\times v$ 행렬 D는 m-modular 이다.

즉, 각 행과 열에서 1의 수가 k(mod m)개와 일치하고, 두 개의 서로 다른 행 사이에 수직쌍$[1,1]^T$의 수가 λ(mod m)개와 일치할 때, D는 m-modular 대칭설계라는 의미이다. 따라서 어떠한 대칭 (v,k,λ) 설계이든 모든 $m>1$인 경우에 대해 $(v,k,\lambda;m)$ 설계에 해당한다. 다른 예는 modular 차집합(difference set)[12]로부터 얻을 수 있다. 그러나 modular 차집합으로부터 생성된 modular 조합 설계는 행과 열에 같은 1의 개수를 갖기 때문에 제안된 개념의 특수한 경우를 구성할 수 있다. 대칭 설계에 관한 일반 이론은 [1]에 제시되어 있다. 예제를 들면,

예제 4.4 : A(3,2,1) 설계

$$D=\begin{bmatrix}0&1&1\\1&0&1\\1&1&0\end{bmatrix}.$$

$DJ=2J$ 및

$$DD^T=I+J=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}+\begin{bmatrix}1&1&1\\1&1&1\\1&1&1\end{bmatrix}. \quad (12)$$

예제 4.5 : A(7,2,1) 설계

$$D=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\\1&0&1&0&0&0&1\end{bmatrix}.$$

$DJ=3J$ 및 $DD^T=2I+J.$ (13)

예제 4.6 : 행벡터 [1 0 1 1 0 0 0 1 0 0 0 0 0 0]의 순환치환(cyclic permutation)에 의해 생성되는 (13,4,1) 설계 R에 대해 생각해본다. 다음은 (26,1,2;5)는

$$\begin{bmatrix}R & J-I\\ J-I & J-R^T\end{bmatrix}.$$

$n\geq 2$라 놓고 정규화된 MHJ(n,m)에 대해 생각해보면, 첫 번째 행과 열을 제거해 H의 핵(core)을 얻는다. 약간의 가정을 추가하면 다음과 같은 특수 파라미터를 갖는 H의 핵으로부터 m-modular 설계를 얻을 수 있다.

정리 4.1 : $m,n\geq 3,(m,n)=1$ 이라 놓는다. 만약 핵을 C로 표시할 때 H가 정규화된 MHJ(n,m)이라면 $D=(C+J)/2$는 $(n-1,2^{\varphi(m)-1}(n-2),2^{\varphi(m)-2}(n-4);m)$.

증명 : 먼저 정리 3.1에 의해 m은 자연 홀수이다. $(m,n)=1$ 이므로 $HH^T\equiv H^TH\equiv nI$ 이다. 특히 H의 열은 쌍으로 직교이다. 즉 $CJ\equiv JC\equiv -J$(mod m)이고 따라서 $2DJ\equiv 2JD\equiv JC+J^2\equiv(n-2)J$ (mod m)임을 알 수 있다.

두 번째로 $CC^T\equiv nI-J$(mod m)이기 때문에 따라서 $4DD^T=(C+J)(C+J)^T=CC^T+JC^T+CJ+(n-1)J\equiv nI+(n-4)J$(mod m)이다.

결국 이 정리는 $2DJ$와 $4DD^T$에 $2^{\varphi(m)-1}$과 $2^{\varphi(m)-2}$을 각각 곱하여 얻어진 결과임을 알 수 있다.

결합설계는 제안기법에 아주 유용한 방법이다. 따라서 다음과 같은 간단한 정리를 제시할 수 있다.

정리 4.2 : ([15]의 정리 2.5 참고) D를 $(v,k,\lambda;m)$설계라 놓으면, $v\equiv 4(k-\lambda)$(mod m)인 경우 행렬 $2D-J$는 MHJ(v,m)이다.

증명 : $(2D-J)(2D-J)^T\equiv 4(k-\lambda)I+(v-4k+4\lambda)I\equiv vI$(mod m).

예제 4.7 : $D=J-I$이 $(v,v-1,v-2)$ 설계라 놓는다. $v-4k+4\lambda=v-4(v-1)+4(v-2)=v-4\equiv 0$(mod 5) 이면 $v=5k+4$일 때 $2D-J=J-2I$는 MHJ$(5k+4,5)$이다.

예제 4.8 : $(16,6,2)$ 설계, D_{16} 은 존재한다. 따라서 $v-4k+4\lambda=16-4\cdot 6+4\cdot 2\equiv 1-4+3\equiv 0$ (mod 5)이기 때문에 MHJ(16,5)가 존재한다.

$(21,5,1)$ 설계, D_{21}은 존재한다. 따라서 $v-4k+4\lambda=21-4\cdot 5+4\cdot 1\equiv 1-0+4\equiv 0$(mod 5)이기 때문에 MHJ(21,5)가 존재한다.

$(101,25,6)$ 설계, D_{101}은 존재한다. 따라서 $v-4k+4\lambda=101-4\cdot 25+4\cdot 6\equiv 101-100+24\equiv 0$(mod 5)이기 때문에 MHJ(101,5)가 존재한다.

(16,6,2)설계는 다음 행렬과 같다.

$[D_{16}] =$

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

따라서 MHJ(16,5)는 다음 행렬과 같이 나타 낼 수 있다.

[MHJ(16,5)]=

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

$$[\mathrm{MHJ}(16,5\ )]^{-1}=\frac{1}{16}$$

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

즉 [MHJ(16,5)]와 [MHJ(16,5)]$^{-1}$은 크기만 다를 뿐 같은 행렬이기 때문에 송신과 수신이 일치한다는 장점이 있다.

그러나 결합 설계를 얻어내는 것이 쉽지가 않아서 정리 4.2의 응용은 다소 제한되어 있다. 보다 강력한 설계 방법을 얻기 위해 다음과 같은 두 개의 m-modular 구성방법을 결합한다.

정의 4.2 : D_1과 D_2 를 각각 $(v_1,k_1,\lambda_1;m)$ 과 $(v_2,k_2,\lambda_2;m)$의 설계라 하자. 그러면 $D_1 \oplus D_2$ 로 표시되는 이들의 직합은 사이즈가 v_1+v_2 인 다음과 같은 블록행렬이다.

$$\begin{bmatrix} D_1 & J \\ J^T & D_2 \end{bmatrix}.$$

modular 설계의 직합은 일반적인 직합이 아님을 잊지 말아야한다. 그럼에도 불구하고 두 modular 설계의 직합이 modular Hadamard 행렬에 이르는 경우에 대해 설명이 필요하다.

정리 4.3 : $v_1, v_2 \geq 2$ 라 놓으면 D_1과 D_2 는 각각 $(v_1,k_1,\lambda_1;m)$ 과 $(v_2,k_2,\lambda_2;m)$ 의 설계라 할 수 있다. 따라서 $2(D_1 \oplus D_2) - J$ 는 다음을 만족하면 MHJ $(v_1+v_2, m\ )$이다.

$$v_2 \equiv -v_1 + 4k_1 - 4\lambda_1 \ (\mathrm{mod}\ m), \tag{14}$$

$$2k_2 \equiv 2k_1 - 4\lambda_1 (\mathrm{mod}\ m), \tag{15}$$

$$4\lambda_2 \equiv -4\lambda_1 (\mathrm{mod}\ m). \tag{16}$$

증명 : 이 공식들은 행렬 $2(D_1 \oplus D_2) - J$ 의 행들이 직교한다는 조건과, $v_1, v_2 \geq 2$ 이고 $m > 1$인 경우에 대해 행렬 J 와 I 가 선형적으로 직교한다는 사실로부터 직접 도래되었다. 따라서 다음 사실이 유지되어야 한다는 것을 쉽게 알 수 있다.

$$v_1 + v_2 - 4k_1 + 4\lambda_1 \equiv 0 \ (\mathrm{mod}\ m),$$
$$v_1 + v_2 - 4k_2 + 4\lambda_2 \equiv 0 \ (\mathrm{mod}\ m),$$
$$v_1 + v_2 - 2k_1 - 2\lambda_2 \equiv 0 \ (\mathrm{mod}\ m).$$

결국 원하는 결과는 약간의 조정을 통해 달성된다.

이해를 돕기 위해 다음과 같은 예제를 더 제시한다.

예제 4.9 : 여기서 MHJ(86,5) 행렬을 구성해보자. 먼저 정리 4.3에 의해 MHJ(51,5)로 주어지는 $2((16,6,2) \oplus (35,17,8)) - J$ 에 대해 생각해보면, 이 행렬의 핵은 정규화 된 후 정리 4.1에 의해 $(50,2,3;5)$가 된다. 마지막으로 $2((36,21,12) \oplus (50,2,3;5)) - J$를 이용하면 원하는 MHJ(86,5) 행렬을 얻게 된다.

이제 MHJ$(n,5)$을 구성해본다.

제안 4.1 : 필요충분조건 $n \neq 6,11$ 을 만족하면 차수 $n \equiv 1(\mathrm{mod}\ 5)$인 MHJ$(n,5)$행렬이 존재한다.

증명 : $n = 20k+16 = 4(5k+4)$이면 정리 3.4를 통해 차수가 $5k+4$ 인 행렬 $J-2I$ 를 4배하여 MHJ $(20k+16,5)$를 얻을 수 있다는 사실에 대해 관찰해본다. 이제 이 행렬들을, 보다 정확하게는, 파라미터가 $(20k+15,4,4;5)$ 인 5-modular 설계에 해당하는 행렬들을 사용한다. 정리 4.3을 참고하여 MHJ$(20k+41,5)$, MHJ$(20k+106,5)$, MHJ$(20k+31,5)$을 얻기 위해 각각 디자인 (26,1,2;5), (16,6,2)와 (91,81,72)를 직합한다. 첫 번째 modular 디자인은 예제 4.6에 제시되어 있고, 두 번째 디자인은 사이즈가 16인 Menon 디자인이며, 세 번째는 사이즈가 91인 투사면의 보(complement)이다[1].

마지막으로 저차수의 경우에 대해 알아본다. MHJ $(1,5)$는 1×1 행렬 $F_1 = [1]$ 이고, MHJ$(6,5)$와 MHJ $(6,11)$은 결과 4.2에 의해 존재하지 않는다. MHJ$(21,5)$와 MHJ$(26,5)$는 각각 (21,5,1) 디자인과 정리 4.2를 통해 예제 4.6에 제시된 (26,1,2;5)디자인으로부터 구성될 수 있다. MHJ$(46,5)$와 MHJ$(66,5)$는 정리 4.3을 통해 $(26,1,2;5)\oplus(20,2,3;5)$ 와 $(21,5,1)\oplus(45,33,24)$ 의 직합에 의해 구할 수 있다. 5-modular 디자인 (20,2,3;5)는 정리 4.1에 의해 MHJ$(21,5)$의 핵으로부터 얻을 수 있다. 마지막으로 MHJ$(86,5)$은 예제 4.8에서 구성되었다. □

제안 4.1로부터 MHJ$(5k+2,5)$행렬의 존재는 k가 짝수일 때 가능함을 알 수 있으며 k가 홀 수 일 때는 정리 3.2에 의해 존재가 불가능하다.

제안 4.2 : 모든 $n \equiv 2(\mathrm{mod}\ 10)$에 대해서 MHJ$(n,5)$ 행렬은 존재한다.

증명 : MHJ$(20k+2,5)$와 MHJ$(40k+12,5)$행렬은 정리 3.4를 통한 제안 4.1의 MHJ$(10k+1,5)$와 MHJ $(20k+6,5)$행렬을 각각 2배하여 얻어질 수 있다. 반면에 MHJ$(40k+32,5)$행렬은 정리 3.4를 통해 MHJ $(5k+4,5)$행렬을 8배하여 얻을 수 있다. □

지금까지 5-modular Hadamard 행렬의 존재에 대해 서술했고 다음과 같은 결과를 얻었다.

결과 3.3 : 결과 4.1과 제안 4.1, 제안 4.2로부터 필요충분조건 $n \neq 3,7$ 와 $n \neq 6,11$을 만족하면 MHJ$(n,5)$이 존재한다.

결과 3.4 : $k \geq 1$인 경우에 대해 $4k$차원의 5-modular Hadamard 행렬이 존재한다.

V. 결 론

본 논문에서는 modular 대칭 설계에 대해 소개하고 이를 이용하여 Hadamard 행렬 modular 5가 존재한다는 것을 증명했다. 그리고 n차 5-modular Hadamard 행렬의 필요충분조건이 $n \neq 3,7\ (\mathrm{mod}\ 10)$ 와 $n \neq 6,11$ 임을 증명했다. 특히 Hadamard 추측에 대한 5-modular 버전을 구했다. 따라서 5-modular Hadamard 행렬이 존재할 것이라는 추측이 사실임이 확인 되었다. 또한 본 논문에서 제시한 새로운 툴과 아이디어는 보다 큰 m값에 대해서도 MHJ(n,m)행렬의 존재를 결정하는데 크게 기여를 할 것임을 알게 되었다. 이 5-modular Hadamard 행렬은 massive MIMO에서 많은 안테나가 요구되고 있는 안테나 설계나 All-or-Nothing 암부호 설계에 이용할 수 있다.

참 고 문 헌

[1] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs,* Second Edition, Chapman and Hall/CRC, 2006.

[2] S. Eliahou and M. Kervaire, "A survey on modular Hadamard matrices," *Discrete Mathematics*, vol.302, pp.85-106, 2005.

[3] R. G. Gibson and J. Jedwab, "Quaternary Golay sequence pairs I: even length," *Des. Codes Cryptogr.,* vol.59, pp.131-146, 2011.

[4] R. L. Graham and N. J. A. Sloane, "On additive bases and harmonious graphs," *SIAM J. Alg. Disc. Meth.*, vol.1, pp.382-404, 1980.

[5] S. P. R. Hebbare and G. A. Patwardhan, "On some constructions of modular Hadamard matrices," *J. Combin. Theory A*, vol.20, pp.258-263, 1976.

[6] K. J. Horadam, *Hadamard matrices and their applications*, Princeton University Press, 2007.

[7] M. Kolountzakis and M. Matolcsi, "Complex

Hadamard matrices and the spectral set conjecture," *Collect. Math.*, Vol. Extra, pp.281-291, 2006.
[8] M. H. Lee, "A New Reverse Jacket Transform and Its Fast Algorithm," *IEEE Transactions on circuits and systems II,* vol.47, pp.39-47, 2000.
[9] M. H. Lee, Y. L. Borissov and S. M. Dodunekov, "Class of jacket matrices over Finite characteristic Fields," *Electronics Letters*, vol.46, pp.13, 2010.
[10] M.H. Lee and Y.L. Borissov, "A Proof of Non-Existence of Bordered Jacket Matrices of Odd Order Over Some Fields," *Electronics Letters*, Vol. 46, No. 5, March 2010.
[11] K. H. Leung and B. Schmidt, "New restrictions on possible orders of circulant Hadamard matrices," *Des. Codes Cryptogr.*, vol.64, pp.143-151, 2012.
[12] O. Marrero, "Modular Difference Sets," *Aequationes Math.*, vol.11, pp.143-153, 1974.
[13] O. Marrero, "Modular Hadamard matrices and related designs III," *A equationes Math.*, vol.13, pp.289-297, 1975.
[14] O. Marrero and A. T. Butson, "Modular Hadamard matrices and related designs," *Journal of Combinatorial Theory A*, vol.15, pp.257-269, 1973.
[15] O. Marrero and A. T. Butson, "Modular Hadamard matrices and related designs II," *Canadian J. Math.*, vol.XXIV, pp.1100-1109, 1972.
[16] M. J. Mossinghoff, "Wieferich pairs and Barker sequences," *Des. Codes Cryptogr.*, vol.53, pp.149-163, 2009.
[17] R. L. Rivest, "All-or-nothing encryption and the package transform," *in Biham, E. (Ed.) Fast software encryption, Lect. Notes Comp. Sci.*, vol.1267, pp.210-218, 1997.
[18] I. Z. Ruzsa, "Solving a linear equation in a set of integers I," *Acta Arithmetica,* vol.LXV.3, pp.259-282, 1993.
[19] H. J. Ryser, *Combinatorial Mathematics*, Wiley, New York, 1963.
[20] D.R. Stinson, "Something about All-or-Nothing (transforms)," *Des. Codes Cryptogr.*, vol.22, pp.133-138, 2001.
[21] Moon Ho Lee, *Jacket Matrices : Constructions and Its Applications for Fast Cooperative Wireless Signal Processing*, LAP LAMBERT Academic Publishing, Germany, 1 Dec 2012.
[22] Chang Hui Choe, *A Design of Cryptographic Algorithm and Key Agreement Protocol using Jacket Matrices with Their Element-wise Inverses*, Ph. D. Thesis, The Graduate School of Chonbuk National University, 2010.
[23] Moon Ho Lee, *A. Latif, Massive MIMO Channel Estimation using Circulant Jacket Matrix*, prepared, Book Chapter, 2013.

저 자 소 개

박 주 용(평생회원)
1982년 전북대학교 전자공학과 석사
1994년 전북대학교 전자공학과 박사
1991년 3월～2007년 2월 서남대학교 전자공학부 부교수
2007년 3월～현재 신경대학교 인터넷정보통신학과 부교수
<주관심분야 : 무선이동통신>

김 정 수(정회원)
1998년 전북대학교 정보통신공학과 석사
2003년 전북대학교 컴퓨터공학과 박사 졸업.
2002년 6월～현재 숭실사이버대학교 컴퓨터정보통신학과 부교수
<주관심분야 : 이동통신>

Ferenc Szollosi
2008년 Budapest University of Technology & Economics, Hungary, Mathematics 석사
2012년 Central European University, Hungary, Mathematics and Its Applications 박사

이 문 호(평생회원)-교신저자
1984년 전남대학교 전기공학과 박사, 통신기술사
1985년～1986년 미국 미네소타대학 전기과 포스트닥터
1990년 일본동경대학 정보통신공학과박사
1970년～1980년 남양MBC 송신소장
1980년 10월～2010년 2월 전북대학교 전자공학부 교수
2010년 2월～현재 WCU-2 연구책임교수
<주관심분야 : 무선이동통신>