논문 18-43-06-03 The Journal of Korean Institute of Communications and Information Sciences '18-06 Vol.43 No.06
https://doi.org/10.7840/kics.2018.43.6.902

페일리형 하다마드 행렬의 고유값 분해

송 민 규◆, 송 홍 엽°

Eigenvalue Decomposition of Paley-Type Hadamard Matrices

Min Kyu Song◆, Hong-Yeop Song°

요 약

본 논문은 (p^k+1)차 또는 $2(p^k+1)$차 페일리형 하다마드 행렬의 고유값 분해를 결정한다. 이는, 페일리형 하다마드 행렬 생성의 근간이 되는 p^k차 야콥스탈 행렬과 (p^k+1)차 페일리 행렬의 고유값 분해를 토대로 계산된다. 또한, 페일리형 하다마드 행렬의 고유값 분해 계산방법을 이용하여, 임의의 순회형 하다마드 행렬의 고유값 분해를 계산한다. 이 결과들은, 페일리형 하다마드 행렬과 순회형 하다마드 행렬의 고유값 분해를 완벽히 기술하는 최초의 연구 결과이다. 본 논문에서 결정한 모든 고유값 분해에서 나타나는 고유벡터들은 항상 서로 직교한다.

Key Words : eigenvalues, eigenvectors, Hadamard matrices, Paley-type, cyclic-type

ABSTRACT

In this paper, we determine explicitly the eigenvalue decomposition of Paley-type Hadamard matrices of order p^k+1 or $2(p^k+1)$, where p is an odd prime and k is a positive integer. For this, we also determine those of Paley matrices of order p^k+1 using those of Jacobsthal matrices of order p^k. Some of these results directly applies to any cyclic-type Hadamard matrices. Those results are the first complete description of eigenvalue decompositions of Paley-type or cycic-type Hadamard matrices. All the eigenvector matrices we determined here turned out to be unitary matrices.

Ⅰ. 서 론

하다마드 행렬 (n차) H는 $HH^T=nI_n$를 만족하는 ± 1로 이루어진 크기 $n\times n$의 정방행렬이다. ± 1로 이루어진 직교행렬이라는 특성으로 인해, 하다마드 행렬은 다양한 분야에서 폭넓게 사용된다. 예를 들어, 디지털 통신 시스템에서는 하다마드 행렬의 각 행이 서로 직교한다는 특성을 이용해 코드분할다중접속(CDMA)의 확산코드[7,13,29], 파일럿 신호[22], 그리고 오류정정부호[7,29] 등에 사용된다. 신호처리 분야에서는 신호와 이미지의 표현/압축에 사용된다.[29] 또한, 하다마드 행렬을 이용한 암호화 기법들도 고려된다.[15,24]

하다마드 행렬은 그 차수가 4의 배수인 경우에 대해서만 존재한다는 것이 잘 알려져 있으며, 이를 생성하는 대표적인 방법으로는 아래의 네 가지가 있다[7,29]:

1) 2^t차 실베스터형 하다마드 행렬.[26] (여기서, t는 양의 정수)
2) $q+1$차 또는 $2(q+1)$차 페일리형 하다마드 행렬.[19] (여기서, q는 임의의 홀수 소수의 거듭제곱)

※ 이 성과는 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2017R1A2B4011191).
◆ First Author : (ORCID:0000-0002-5481-9180)Yonsei University School of Electrical and Electronic Engineering, mk.song@yonsei.ac.kr, 학생회원
° Corresponding Author : (ORCID:0000-0001-8764-9424)Yonsei University School of Electrical and Electronic Engineering, hysong@yonsei.ac.kr, 종신회원
논문번호 : KICS2018-03-002, Received March 14 2018; Revised May 21, 2018; Accepted June 1, 2018

3) 윌리암슨형 하다마드 행렬.[30]
4) 순회 하다마드 수열로부터 생성되는 순회형 (cyclic-type) 하다마드 행렬.[7,8,14,23]

하다마드 행렬의 응용 분야에서, 일반적으로, 월시 함수와의 밀접한 연관성 때문에 2^t차 실베스터형 하다마드 행렬이 주로 고려된다. 하지만, 2의 거듭제곱이 아닌 차수의 하다마드 행렬 또는 다른 특성의 하다마드 행렬이 필요한 경우, 그 외의 하다마드 행렬들을 고려한다. 특히, 페일리형 하다마드 행렬의 경우, 수학적으로 용이한 생성과 다양한 차수에서 존재한다는 특징으로, 2의 거듭제곱이 아닌 차수가 요구 될 때 유용하다. 이에 기반하여, 페일리형 하다마드 행렬은 CDMA 시스템의 확산코드[13], MIMO 채널에서의 파일럿 신호 설계[22], 비밀 공유 기법[15], 블록암호 설계[24] 등에서 고려되었다. 순회형 하다마드 행렬 또한 다양한 형태로 고려되어 왔다. 그 대표적인 예로써, 1997년 제안된 Cohn과 Lempel의 최대주기수열(maximal length sequence)로 얻어진 순회형 하다마드 행렬의 최대주기수열 변환(maximal length sequence transform, m-transform)은[3], 통신 시스템과 신호처리 등에 다양하게 적용되었다.[2,12,25] 참고로, 길이 2^t-1인 최대주기수열로부터 생성된 순회형 하다마드 행렬은 2^t차 실베스터형 하다마드 행렬과 하다마드 보존 변환(Hadamard preserving operation)에 대해 동치이다.[3]

직교행렬이라는 특성을 바탕으로 하다마드 행렬은 직교변환(orthogonal transform)으로 다양한 분야에서 사용된다.[1,10,29] 직교변환에서, 이들의 정확한 고유값과 고유벡터를 찾는 것은 직교변환 행렬의 특성을 이해함에 있어서 중요하다. 따라서, 이산 퓨리에 변환[5,27], 이산 하티 변환[20], 이산 하다마드 변환[6,28,29] 등과 같은 다양한 직교 변환 행렬의 정확한 고유값과 (직교하는) 고유벡터를 찾는 연구가 진행되었다. 이러한 직교변환 행렬의 고유값 분해에 대한 연구 결과는 이산 분수차 퓨리에 변환(discrete fractional Fourier transform)[9], 이산 분수차 하다마드 변환(discrete fractional Hadamard transform)[20] 등의 기존의 직교 변환들을 확장하고, 응용함에 있어 중요한 역할을 수행 해왔다.

하다마드 행렬을 오류정정부호로써 사용할 때, 이산 하다마드 변환은 오류정정부호의 디코더로써 사용된다. 따라서, 실베스터형 하다마드 행렬의 특정 행 또는 열의 부호가 바뀌거나 행과 열의 순서가 뒤섞이는 경우 변화하는 고유값 분해에 대한 연구도 진행되었다.[16-17] 참고로, 실베스터형 하다마드 행렬은 고유치 분해가 결정된 유일한 하다마드 행렬이다.[16] 따라서, 위에서 언급한 이산 분수차 하다마드 변환 또한 실베스터형 하다마드 행렬의 확장만이 알려져 있다.

본 논문은, 페일리형 하다마드 행렬의 정확한 고유값 분해를 계산한다. 또한, 이로부터, 임의의 순회형 하다마드 행렬의 고유값 분해를 계산한다. 이는, 페일리형 하다마드 또는 순회형 하다마드 행렬의 고유값 분해 결정에 대한 최초의 연구결과이다. 모든 결정된 고유값 분해에서, 모든 고유벡터들은 서로 직교한다.

본 논문은 다음과 같은 표기법을 사용한다:

- p는 임의의 홀수 소수
- $q=p^k$는 소수 p의 k 거듭제곱 (여기서, k는 양의 정수)
- I_n (또는 0_n)은 n차 단위행렬 (또는 영행렬)
- J_n은 모든 원소가 1인 n차 정방행렬
- $\mathbf{1_n}$ (또는 $\mathbf{0_n}$)은 모든 원소가 1인 (또는 0인) 길이 n인 벡터
- $j=\sqrt{-1}$이고, ω_n은 복소평면 상의 n-차 단위근
- $\Omega_n=\mathrm{diag}(1,\omega_n,...,\omega_n^{n-1})$는 $1,\omega_n,...,\omega_n^{n-1}$을 대각원소로 갖는 n차 대각행렬
- $F_n=\frac{1}{\sqrt{n}}(\omega_n^{i,j})$는 n차 퓨리에 행렬
- $\mathbb{Z}_q$와 $\mathbb{F}_q$는 각각 q진 정수환과 크기 q인 유한체
- Ψ는 $\mathbb{Z}_q$에서 $\mathbb{F}_q$로의 1-1 대응 함수 (본문의 정의 2 참조)
- $Q=Q_\Psi$는 Remark 1의 Ψ에 의해 정의된 q차 야콥스탈 행렬

Ⅱ. 야콥스탈 행렬의 고유값 분해

정의 1. (야콥스탈 행렬[18]) 함수 f를 $f(0)=0$인 $\mathbb{Z}_q$에서 $\mathbb{F}_q$로의 전단사함수라 하자. 함수 f로 정의되는 야콥스탈 행렬 (jacobsthal matrix) $Q_f=(\sigma_{s,t})$는 q차 정방행렬로, 여기서, s행 t열의 원소 $\sigma_{s,t}$는 $\sigma_{s,t}=\chi(f(s)-f(t))$ 로 정의한다. 여기서, $\chi(\cdot)$은 $\mathbb{F}_q$상의 제곱 지표(quadratic character)로, 편의상 $\chi(0)=0$으로 한다.

홀수 소수의 거듭제곱 q에 대해서, 유한체 $\mathbb{F}_q$에는 항상 제곱잉여(quadratic residue)와 비제곱잉여(quadratic non-residue)가 각각 $\frac{q-1}{2}$개 존재한다. 이

로부터,

$$Q_f \mathbf{1}_q = \mathbf{0}_q \tag{1}$$

임을 쉽게 알 수 있다.

정의 2. $\mathbb{F}_q$의 원시원소 α에 대해서, $\mathbb{Z}_q$에서 $\mathbb{F}_q$로의 함수 Ψ를

$$\Psi(i) = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{k-1}\alpha^{k-1} = \sum_{z=0}^{k-1} c_z \alpha^z$$

와 같이 정의하자. 여기서, $i = \sum_{z=0}^{k-1} c_z p^z$이고, 모든 $z = 0, 1, ..., k-1$에 대해서 $c_z < p$이다.

위의 함수 Ψ를 이용하여 정의한 야콥스탈 행렬 Q_Ψ를 생각해자. 이 때, $q = p$인 경우, $\Psi(i) = i$가 된다. 따라서, 이 경우, 생성된 야콥스탈 행렬은 순환 행렬(circulant matrix)가 된다.

Remark 1. Q_Ψ와 Q_f를 각각 정의 2의 함수 Ψ와 임의의 함수 f로부터 정의 1에 따라 생성된 두 야콥스탈 행렬이라 하자. 이 때, 함수 Ψ와 f가 모두 단전사 함수이기 때문에, 모든 $x \in \mathbb{Z}_q$에 대해서 $g(\Psi(x)) = f(x)$인 함수 g가 항상 존재 한다. 만일 Q_Ψ가 $Q_\Psi = S\Lambda S^H$와 같이 대각화된다면,

$$Q_f = P_g Q_\Psi P_g^T = P_g S Q_\Psi S^H P^T = P_g S Q_\Psi (PS)^H$$

와 같이 쉽게 Q_f의 대각화를 얻을 수 있다. (여기서, P_g는 g에 대응되는 순열 행렬이다.) 따라서, Q_Ψ의 정확한 고유값 분해를 파악함으로써, 동일한 차수의 모든 야콥스탈 행렬의 고유값 분해를 알 수 있다.

따라서, 본 논문의 나머지 부분에서는, 정의 2의 함수 Ψ에 초점을 맞춰 야콥스탈 행렬의 고유값 분해를 논하도록 한다. 또한, 함수 Ψ로부터 생성된 야콥스탈 행렬 Q_Ψ를 편의상 Q로 표기한다. 아래의 예제 1은 함수 Ψ로부터 생성된 행렬 Q_Ψ가 갖는 특별한 구조를 보여준다.

예제 1. 홀수 소수 $p = 3$과 그의 거듭제곱 $q = p^2 = 9$에 대해, α를 $\mathbb{F}_q$상의 원시원소라 하자. $\mathbb{Z}_q$상의 임의의 원소 i에 대해, $\Psi(i) = (i - 3\left\lfloor \frac{i}{3} \right\rfloor) + \left\lfloor \frac{i}{3} \right\rfloor \alpha$이다. 이를 이용하여, 9차 야콥스탈 행렬 Q을 생성하면 다음과 같다:

$$Q = \begin{bmatrix} 0\,1\,1 & --1-1- \\ 1\,0\,1 & 1----1 \\ 1\,1\,0 & -1-1-- \\ -1- & 0\,1\,1 & --1 \\ --1 & 1\,0\,1 & 1-- \\ 1-- & 1\,1\,0 & -1- \\ --1-1- & 0\,1\,1 \\ 1----1 & 1\,0\,1 \\ -1-1-- & 1\,1\,0 \end{bmatrix} := \begin{bmatrix} B_0 B_1 B_2 \\ B_2 B_0 B_1 \\ B_1 B_2 B_0 \end{bmatrix}.$$

위의 야콥스탈 행렬 Q는 최소다항식 $x^2 + x + 2$의 근 α를 가지고 생성되었으며, "$-$" 기호는 -1을 의미한다.

- Q를 겹치지 않는 크기 3×3인 부분행렬 (또는 블록) 9개로 분할하면, 각각의 부분행렬들은 순환 행렬이다.
- 위에서 분할된 부분행렬 각각을 하나의 원소로 보면, Q를 순환 행렬로 생각할 수 있다. 이러한 행렬을 일컬어 블록 순환 행렬(block circulant matrix)라 한다.
- 위의 두 사실을 모두 만족하는 행렬을 일컬어 순환 블록들의 블록 순환 행렬이라 한다. 즉, Q는 순환 블록들의 블록 순환 행렬이다.

위의 예제를 일반화 한 것을 일컬어 멀티 레벨(multi-level) 순환 행렬이라 한다.[4] 이때, 1-레벨 순환 행렬은 보통의 순환 행렬이고, 2-레벨 순환 행렬은 순환 블록들의 블록 순환 행렬이다. 일반적으로, p^k차 k-레벨 순환 행렬은 다음과 같이 정의할 수 있다[4]:

정의 3. A를 어떤 $q = p^k$차 정방행렬이라 하자. 모든 $t = 1, 2, ..., k$에 대해서, A의 모든 분할된 $p^{2(k-t)}$개의 p^t차 정방 부분행렬이 p^{t-1}차 블록 순환 행렬이면, 행렬 A를 k-레벨 순환 행렬이라 한다.

위의 정의에서, $t = 1$일 때, 모든 p차 부분행렬은 1차 블록(단일 원소로 이루어진 행렬)의 블록 순환 행렬이 된다. 즉, 모든 p차 부분행렬이 보통의 순환행렬이 된다. 또한, 임의의 $k > 1$에 대해서, k-레벨 순환 행렬은 $(k-1)$-레벨 순환 행렬이기도 하다. 위의 정의에 따라서, $q = p^k$차 야콥스탈 행렬 Q가 k-level 순

환 행렬이다.

k-level 순환 행렬의 고유값 분해는 보통의 순환 행렬의 고유값 분해로부터 쉽게 유도 할 수 있다 [4]: $A=(a_{i,j})$를 n차 순환 행렬이라 하면, A의 고유값 분해는

$$A=F_n\Lambda_A F_n^H$$

와 같이 주어진다. 여기서, $\Lambda_A=\sum_{l=0}^{n-1}a_{0,l}\Omega_n^l$이다. 위 사실을 이용하여 [4]에서 소개된 3-level 순환 행렬의 고유값 분해를 수행하는 방법은 쉽게 임의의 k-level 순환 행렬로 확장될 수 있다. 이를 본 논문에서 고려하는 $q=p^k$차 야콥스탈 행렬 Q에 적용하면 다음과 같은 결과를 얻을 수 있다. 여기서, 한 가지 자명한 사실은 얻어진 q개의 고유벡터들은 모두 단위벡터이며, 서로 직교한다는 것이다.

보조정리 1. (야콥스탈 행렬의 고유값 분해) Q를 $q=p^k$차 야콥스탈 행렬, $\beta=(\beta_0,\beta_1,...,\beta_{p^k-1})$을 Q의 첫 행이라 하자. Q는 유니타리 행렬

$$S_Q=F_p\otimes F_p\otimes\cdots\otimes F_p:=\bigotimes_{z=}^{k}F_p$$

에 의해 대각화된다. 여기서, $A\otimes B=(a_{i,j}B)$는 행렬 A와 B의 크로넥커 곱(Kronecker product)를 의미한다. 즉,

$$Q=S_Q\Lambda_Q S_Q^H \tag{2}$$

이다. 이 때, 대각행렬 Λ_Q는, $\theta=\sum_{e=0}^{p-1}l_e\alpha^e$에 대해서,

$$\Lambda_Q=\sum_{l_0=0}^{p-1}\sum_{l_1=0}^{p-1}\cdots\sum_{l_{k-1}=0}^{p-1}\beta_{\Psi^{-1}(\theta)}(\Omega_p^{l_0}\otimes\Omega_p^{l_1}\otimes\cdots\otimes\Omega_p^{l_{k-1}}) \tag{3}$$

과 같이 주어진다.

Ⅲ. 페일리형 하다마드 행렬의 고유값 분해

q차 야콥스탈 행렬 Q에 대해서, $q+1$차 페일리 행렬 C는

$$C=\begin{bmatrix}0 & \mathbf{1}_q^T\\ \pm\mathbf{1}_q & Q\end{bmatrix}$$

와 같이 정의한다. 여기서, $\pm\underline{1}_q$은 부호는 q를 4로 나눈 나머지가 1인 경우 양의 부호를, 3인 경우 음의 부호를 갖는다.[18-19] $QQ^T=qI_q+J_q$라는 사실로부터 페일리형 하다마드 행렬은 다음과 같이 생성된다.

1) $q\equiv 3\ (\mathrm{mod}4)$ 의 경우,

$$H=C+I_{q+1} \tag{4}$$

은 $(q+1)$차 페일리형 하다마드 행렬이다.

2) $q\equiv 1\ (\mathrm{mod}4)$ 의 경우,

$$H=\begin{bmatrix}C+I_{q+1} & C-I_{q+1}\\ C-I_{q+1} & -C-I_{q+1}\end{bmatrix}$$

은 $2(q+1)$차 페일리형 하다마드 행렬이다.[18-19] 하지만, 본 논문에서는 위의 $2(q+1)$차 페일리형 하다마드 행렬과 동치인 하다마드 행렬

$$H=\begin{bmatrix}C-I_{q+1} & C+I_{q+1}\\ C+I_{q+1} & C-I_{q+1}\end{bmatrix} \tag{5}$$

를 고려한다. 참고로, 이 행렬은 꼬인 블록 순환 행렬 (skew block circulant matrix)이다.

보조정리 2. (페일리 행렬의 고유값 분해) C를 $q+1$차 페일리 행렬, $Q=S_Q\Lambda_Q S_Q^H$을 보조정리 1에 나타난 q차 야콥스탈 행렬 Q의 고유값 분해라 하자. 그리고, $\tilde{S}_Q$와 $\tilde{\Lambda}_Q$를 각각 S_Q와 Λ_Q의 $(q-1)$차 우하단 정방 부행렬이라 하자. 그러면,

$$C=S_C\Lambda_C S_C^H$$

으로 대각화되며, 이때, S_C와 Λ_C는 다음과 같다.

1) $q\equiv 3\ (\mathrm{mod}4)$ 의 경우,

$$S_C=\frac{1}{\sqrt{2}}\begin{bmatrix}j\sqrt{q}-j\sqrt{q} & \mathbf{0}_{q-1}^T\\ 1 \quad 1 & \sqrt{2}\mathbf{1}_{q-1}^T\\ \mathbf{1}_{q-1} \quad \mathbf{1}_{q-1} & \sqrt{2q}S_Q\end{bmatrix}$$

이며, 대각행렬 Λ_C의 처음 두 대각원소는 $-j\sqrt{q}$, $j\sqrt{q}$이고, Λ_C의 $q-1$차 우하단 정방 부행렬은 $\tilde{\Lambda}_Q$와 같다.

2) $q \equiv 1 \pmod 4$ 의 경우,

$$S_C = \frac{1}{\sqrt{2}} \begin{bmatrix} \sqrt{q} & -\sqrt{q} & \mathbf{0}_{q-1}^T \\ 1 & 1 & \sqrt{2}\,\mathbf{1}_{q-1}^T \\ \mathbf{1}_{q-1} & \mathbf{1}_{q-1} & \sqrt{2q}\,S_Q \end{bmatrix}$$

이며, 대각행렬의 처음 두 대각원소는 $\sqrt{q}$, $-\sqrt{q}$이고, Λ_C의 $q-1$차 우하단 정방 부행렬은 $\tilde{\Lambda}_Q$와 같다.

또한, 위 두 경우에서, 모든 q개의 고유벡터들은 서로 직교한다.

증명: $q \equiv 1 \pmod 4$ 와 $q \equiv 3 \pmod 4$ 인 경우 모두 동일한 방법으로 고유값 분해가 유도된다. 따라서, 본 증명에서는 $q \equiv 3 \pmod 4$ 일 때만을 보이고자 한다.

$q \equiv 3 \pmod 4$ 의 경우에서, λ를 $\mathbf{1}_q$가 아닌 고유벡터 $\boldsymbol{v}$에 대응되는 q차 야콥스탈 행렬 Q의 고유값이라 하자. 식 (1)로부터,

$$C\begin{bmatrix} 0 \\ \boldsymbol{v} \end{bmatrix} = \begin{bmatrix} 0 & \mathbf{1}_q^T \\ -\mathbf{1}_q & Q \end{bmatrix} \begin{bmatrix} 0 \\ \boldsymbol{v} \end{bmatrix} = \lambda \begin{bmatrix} 0 \\ \boldsymbol{v} \end{bmatrix}$$

임을 쉽게 알 수 있다. 즉, $[0\,\boldsymbol{v}^T]^T$이 C의 고유벡터이고, 그에 대응하는 고유값은 λ이다. 이 사실로부터, C의 $q-1$개의 고유벡터와 고유값을 찾을 수 있다. 보조정리 1에서 구한 Q의 고유벡터 모두 서로 직교하므로, 이 $q-1$개의 고유벡터 역시 서로 직교한다. 나머지 두 고유값과 그에 대응하는 고유벡터를 찾기 위해, 다음의 방정식을 고려하자:

$$C\begin{bmatrix} x \\ \mathbf{1}_q \end{bmatrix} = \begin{bmatrix} 0 & \mathbf{1}_q^T \\ -\mathbf{1}_q & Q \end{bmatrix} \begin{bmatrix} x \\ \mathbf{1}_q \end{bmatrix} = \begin{bmatrix} q \\ -x\mathbf{1}_q \end{bmatrix} = \lambda \begin{bmatrix} x \\ \mathbf{1}_q \end{bmatrix}.$$

위를 정리하면, $q = x\lambda$와 $-x = \lambda$를 얻을 수 있고, 이 방정식은 $(x,\lambda) = (j\sqrt{q}, -j\sqrt{q})$ 또는 $(-j\sqrt{q}, j\sqrt{q})$를 해로 갖는다. 이렇게 구한 해가 되는 λ가 나머지 두 고유값이고, 그에 대응되는 x를 대입하여 얻은 $[x\,\mathbf{1}_q^T]^T$가 각각의 고유값에 대응되는 고유벡터가 된다. 이 두 고유벡터와 이전에 찾은 $q-1$개의 고유벡터들이 서로 직교한다는 사실은 쉽게 확인할 수 있다.

정리1. (페일리형 하다마드 행렬의 고유값 분해) $C = S\,{}_C\Lambda_C S_C^H$를 보조정리 2에서 얻은 페일리 행렬 C의 고유값 분해라 하자. 그리고, q에 따라 페일리형 하다마드 행렬 H가 식 (4) 또는 (5)의 형태라 하자.

1) $q \equiv 3 \pmod 4$ 의 경우, H의 고유값 분해는 다음과 같다:

$$H = S_C(\Lambda_C + I_{q+1})S_C^H. \tag{6}$$

2) $q \equiv 1 \pmod 4$ 의 경우, H의 고유값 분해는

$$H = S_h\left(\sum_{l=0}^{1}(-j)^l \Omega_2^l \otimes (\Lambda_C + (-1)^{l+1} I_{q+1})\right)(S_h)^H \tag{7}$$

이며, 이때, $\Omega_2 = \mathrm{diag}(1,-1)$이고,

$$S_h = \frac{1}{\sqrt{2}} \begin{bmatrix} S_C & S_C \\ -jS_C & jS_C \end{bmatrix}$$

이다. 위의 두 가지 경우 모두에서, 모든 고유벡터는 단위벡터이며, 서로 직교 한다.

증명: $I_{q+1} = S_C S_C^H$로부터, $q \equiv 3 \pmod 4$ 의 경우에 대한 증명은 자명하다. $q \equiv 1 \pmod 4$ 의 경우, [11]의 기법을 이용하여 꼬인 순환 행렬을 순환 행렬로 변환함으로써, 고유값 분해를 쉽게 얻을 수 있다.

$$A = \begin{bmatrix} 1 & 0 \\ 0 & -j \end{bmatrix}$$

라 하고, $A' = A \otimes I_{q+1}$라 하자. 식 (5)에 주어진 $2(q+1)$차 페일리형 하다마드 행렬을

$$A'^H H A' = \begin{bmatrix} C - I_{q+1} & -j(C + I_{q+1}) \\ -j(C + I_{q+1}) & C - I_{q+1} \end{bmatrix}$$

와 같이 변환하면, 그 결과는 블록 순환 행렬이 된다. 이때, $C \pm I_{q+1} = S_C(\Lambda_C \pm I_{q+1})S_C^H$임을 이용하여,

$$\begin{aligned} &A'^H H A' \\ &= \begin{bmatrix} C - I_{q+1} & 0_{q+1} \\ 0_{q+1} & C - I_{q+1} \end{bmatrix} - j\begin{bmatrix} 0_{q+1} & C + I_{q+1} \\ C + I_{q+1} & 0_{q+1} \end{bmatrix} \\ &= M\left[\sum_{l=0}^{1}(-j)^l \Omega_2^l \otimes (\Lambda_C + (-1)^{l+1} I_{q+1})\right] M^H \end{aligned}$$

와 같이 대각화 할 수 있다. 여기서, $M=F_2\otimes S_C$, $\Omega_2=\mathrm{diag}(1,-1)$ 이다. $H=A'(A'^HHA')A'^H$임을 이용하면, 최종적으로, 식 (7)의 $2(q+1)$차 페일리형 하다마드 행렬의 고유값 분해를 얻게 된다. 모든 고유벡터가 서로 직교함은 $I_{q+1}=S_CS_C^H$로부터 쉽게 확인이 가능하다.

$q=p\equiv 3\ (\mathrm{mod}4)$ 의 경우, 식 (4)에 있는 페일리형 하다마드 행렬은 첫 번째 행을 제외한 모든 행의 원소에 -1을 곱함으로써 순회형 하다마드 행렬로 쉽게 변환된다. 사실, $q=p\equiv 3\ (\mathrm{mod}4)$ 차 야콥스탈 행렬의 임의의 행에서 오직 하나 존재하는 "0"을 "-1"로 변환하면, 그 결과는 잘 알려진 제곱잉여수열(quadratic residue sequence)가 된다. 사실, 이 제곱잉여수열은 순회형 하다마드 행렬을 생성하는 순회 하다마드 수열(cyclic Hadamard sequence)의 하나의 예이다.[5] 참고로, n차 순회형 하다마드 행렬은, 길이 $n-1$인 순회 하다마드 수열이 존재할 때, 그 수열의 모든 (주기적) 순환 천이로 생성된 행렬에 $+1$들을 좌측과 상단에 추가적으로 배열함으로써 생성 된다.

순회 하다마드 수열의 잘 알려진 예로써, 이진 최대주기수열, GMW 수열, 제곱잉여수열, 쌍둥이 소수(twin prime) 수열, 그리고 홀의 6차 잉여 수열(Hall's sextic residue sequence) 등이 있다.[7-8],[14],[23] 이러한 길이 $n-1$인 순회 하다마드 수열들은 -1과 1을 각각 정확히 $n/2$번, $(n-2)/2$ 갖는다. 순회 하다마드 수열로부터 생성되는 순회형 하다마드 행렬의 고유값 분해는 보조정리 2의 증명 방법을 이용하여 다음을 얻을 수 있다:

따름정리 1. (순회형 하다마드 행렬의 고유값 분해) H를 순회 하다마드 수열 $\gamma=(\gamma_0,\gamma_1,...,\gamma_{n-2})$로부터 생성된 n차 순회형 하다마드 행렬이라 하자. 즉,

$$H=\begin{bmatrix}1 & \mathbf{1}_{n-1}^T\\ \mathbf{1}_{n-1} & \mathrm{circ}(\gamma)\end{bmatrix}$$

라 하자. 이때, 순회형 하다마드 행렬 H는

$$H=S_h\Lambda_h(S_h)^H$$

의 고유값 분해를 갖으며, $\tilde{F}_{n-1}$을 $n-1$차 퓨리에 행렬의 우하단 $n-2$차 정방 부행렬이라 할 때,

$$S_h=\begin{bmatrix}\frac{1+\sqrt{n}}{\sqrt{2n+2\sqrt{n}}} & \frac{1-\sqrt{n}}{\sqrt{2n-2\sqrt{n}}} & \mathbf{0}_{n-2}^T\\ \frac{1}{\sqrt{2n+2\sqrt{n}}} & \frac{1}{\sqrt{2n-2\sqrt{n}}} & \frac{1}{\sqrt{n-1}}\mathbf{1}_{n-2}^T\\ \frac{1}{\sqrt{2n+2\sqrt{n}}}\mathbf{1}_{n-2} & \frac{1}{\sqrt{2n-2\sqrt{n}}}\mathbf{1}_{n-2} & \tilde{F}_{n-1}\end{bmatrix}$$

이고,

$$\Lambda_h=\mathrm{diag}(\lambda_0=\sqrt{n},\lambda_1=-\sqrt{n},\lambda_2,\lambda_3,...,\lambda_{n-1})$$

이다. 여기서, $i=2,3,...,n-1$에 대해서,

$$\lambda_i=\sum_{z=0}^{n-2}\gamma_z\omega_{n-1}^{(i-1)z} \tag{8}$$

이다. 위의 고유값 분해에서 고유벡터들은 모두 단위벡터이며, 서로 직교한다.

Remark 2. 모든 n차 순회형 하다마드 행렬은 다음의 특성을 갖는다.

1) 모든 n차 순회형 하다마드 행렬은 $n-1$차 퓨리에 행렬의 고유벡터와 밀접한 관련이 있는 고유벡터들로 대각화된다.

2) 모든 n차 순회형 하다마드 행렬은 항상 $\sqrt{n}$과 $-\sqrt{n}$을 고유값으로 갖는다.

예제 2. 전술한 바와 같이, 최대주기수열과 제곱잉여수열은 잘 알려진 순회형 하다마드 수열이다. 주기가 2^t-1인 최대주기수열 $m=(m_0,m_1,...,m_{2^t-2})$의 i번째 원소는

$$m_i=(-1)^{\mathrm{Tr}_1^t(\alpha^i)}$$

와 같이 정의한다. 여기서, α는 $\mathbb{F}_{2^t}$의 원시원소이고, $\mathrm{Tr}_1^t(\cdot)$는 $\mathbb{F}_{2^t}$에서 $\mathbb{F}_2$로의 트레이스(trace) 함수 이다. $p\equiv 3\ (\mathrm{mod}4)$를 만족하는 홀수 소수 p를 주기로 갖는 제곱잉여수열 $r=(r_0,r_1,...,r_{p-1})$의 0번째 원소 r_0는 -1이며, i번째 원소는 $r_i=\chi(i)$로 정의한다. 여기서, 정의 1에서와 같이 $\mathbb{F}_q$상의 제곱 지표이다. 길이 31인 최대주기수열과 제곱잉여수열은 순회 하다마드 수열 관점에서 비동치로 알려져 있다.[8,13] 길이 31인 최대주기수열 m과 제곱잉여수열 r로부터 생성

한 두 순회형 하다마드 행렬

$$H_m = \begin{bmatrix} 1 & \mathbf{1}_{n-1}^T \\ \mathbf{1}_{n-1} & \mathrm{circ(m)} \end{bmatrix} \text{와 } H_r = \begin{bmatrix} 1 & \mathbf{1}_{n-1}^T \\ \mathbf{1}_{n-1} & \mathrm{circ(r)} \end{bmatrix}$$

는 모두

$$\begin{bmatrix} \frac{1+\sqrt{32}}{\sqrt{64+2\sqrt{32}}} & \frac{1-\sqrt{n}}{\sqrt{64-2\sqrt{32}}} & \mathbf{0}_{30}^T \\ \frac{1}{\sqrt{64+2\sqrt{32}}} & \frac{1}{\sqrt{64-2\sqrt{32}}} & \frac{1}{\sqrt{31}}\mathbf{1}_{30}^T \\ \frac{1}{\sqrt{64+2\sqrt{32}}}\mathbf{1}_{30} & \frac{1}{64-2\sqrt{32}}\mathbf{1}_{30} & \tilde{F}_{31} \end{bmatrix}$$

에 의해 대각화 된다. 또한 두 순회형 하다마드 행렬은 $\pm 4\sqrt{2}$를 두 개의 공통된 고유값으로 갖는다. 나머지 30개의 고유값들은 식 (9)를 이용하여 계산할 수 있다.

Ⅳ. 결 론

본 논문에서는, 최초로 페일리형 하다마드 행렬과 순회형 하다마드 행렬의 고유값 분해를 계산하였다. 계산된 고유벡터들은 모두 단위 벡터로, 서로 직교한다. 본 논문에서 계산한 고유벡터들은 모두 퓨리에 행렬의 고유벡터들과 밀접한 연관이 있다. 또한, 동일 차수의 순회형 하다마드 행렬은 모두 갖은 고유벡터 집합을 갖으며, 공통된 고유값의 개수 또한 최소 두 개 이상이다. [15]에서 고려한 바와 같이, 페일리형 하다마드 행렬 또는 순회형 하다마드 행렬과 동치인 다른 하다마드 행렬의 고유값 분해를 계산하는 것은 하다마드 행렬에 대한 보다 깊은 이해 및 응용을 위해서 흥미로운 연구 주제일 것이다.

References

[1] N. Ahmed and K. R. Rao, *Orthogonal Transforms for Digital Signal Processing*, Springer Verlag, 1975.

[2] D. Borio, "M-sequence and secondary code constraints for GNSS signal acquisition," *IEEE Trans. Aerospace and Electron. Syst.*, vol. 47, no. 2, pp. 928-945, Apr. 2011.

[3] M. Cohn and A. Lempel, "On fast m-sequence transforms (corresp.)," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 153-137, Jan. 1977.

[4] P. J. Davis, *Circulant matrices*, 2nd Ed., Shelsea Publishing, 1979.

[5] B. W. Dickinson and K. Steiglitz, "Eigenvectors and functions of the discrete Fourier transform," *IEEE Trans. Acousics., Speech, and Signal Process.*, vol. 30, no. 1, pp. 25-31, Feb. 1982.

[6] C. R. Givens, "Some observations on eigenvectors of Hadamard matrices of order 2^n," *Linear algebra and its applications*, vol. 56. pp. 245-250, Jan. 1984.

[7] S. W. Golomb and G. Gong, *Signal design for good correlation: for wireless communication, cryptography, and radar*, Cambridge Univ. Press, 2005.

[8] S. W. Golomb, "On the classification of cyclic Hadamard sequences," *IEICE Trans. Fundamentals of Electronics, Commun. and Computer Sci.*, vol. 89, no. 9, pp. 2247-2253, Sept. 2006.

[9] M. T. Hanna, N. P. A. Sief, and W. A. E. M. Ahmed, "Hermite-Gaussian-like eigenvectors of the discrete Fourier transform matrix based on the singular-value decomposition of its orthogonal projection matrices," *IEEE Trans. Cir. and Syst. I: Regular Papers*, vol. 51, pp. 2245-2254, Nov. 2004.

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

[11] H. Karner, J. Schneid, and C. W. Ueberhuber, "Spectral decomposition of real circulant matrices," *Linear Algebra and Its Appl.*, vol. 367, pp. 301-311, Jul. 2003.

[12] H. Kashiwagi, M. Liu, H. Harada, and T. Yamaguchi, "M-transform and its application to system identification," *Trans. Soc. Instrument and Control Eng.*, vol. 34, pp. 1785-1790, Dec. 1998.

[13] M. M. Khairy and E. Geraniotis, "Effect of time-jitter on CDMA networks with orthogonal and quasi-orthogonal sequences," in *Proc. IEEE Int. Symp. Comput. and Commun.*, pp. 260-264, Alexandria, Jul. 1997.

[14] J.-H. Kim and H.-Y. Song, "Existence of cyclic Hadamard difference sets and its relation to binary sequences with ideal autocorrelation," *J. Commun. and Netw.*, vol. 1, no. 1, pp. 14-18, Mar. 1999.

[15] C. Koukouvinos, D. E. Simos, and Z. Varbanov, "Hadamard matrices, designs and their secret-sharing schemes," *LNCS*, vol. 6742, pp. 216-229, Jun. 2011.

[16] S.-R. Lee, J.-S. No, and K.-M. Sung, "Eigenvalues of non-sylvester Hadamard matrices constructed by monomial permutation matrices," *J. KICS*, vol. 31, no. 4C, pp. 434-440, Apr. 2006.

[17] S.-R. Lee, J.-S. No, E.-H. Shin, and H. Chung, "On eigenvalues of row-inverted Sylvester Hadamard matrices," *Results in Math.*, vol. 54, no. 1, pp. 117-126, Aug. 2009.

[18] J. H. van Lint and R. M. Wilson, *A course in combinatorics*, Cambridge Univ. Press, 1994.

[19] R. Paley, "On orthogonal matrices," *J. Math. and Physics*, vol. 12, no. 1, pp. 311-320, Apr. 1933.

[20] S. C. Pei, C. C. Tseng, M. H. Yeh, and J. J. Shyu, "Discrete fractional Hartley and Fourier transforms," *IEEE Trans. Cir. and Syst. II: Analog and Digital Sign. Process.*, vol. 45, no. 6, pp. 665-675, Jun. 1998.

[21] S. C. Pei and M. H. Yeh, "Discrete fractional Hadamard transform," in *Proc. 1999 IEEE Int. Symp. Cir. and Syst.*, pp. 179-182, Orlando, May 1999.

[22] M. F. Siyau, S. L. Ling, O. Onalaja, and M. Ghavami, "MIMO channel estimation and tracking using a novel pilot expansion technique with Paley-Hadamatd codes for future generation fast speed communications," in *Proc. 2nd Int. Conf. Future Generation Commun. Technol.*, pp. 48-53, London, Nov. 2013.

[23] H.-Y. Song and S. W. Golomb, "On the existence of cyclic Hadamard difference sets," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1266-1268, Jul. 1994.

[24] D. R. Stinson, "Something about all or nothing (Transforms)," *Designs, codes and cryptography*, vol. 22, pp. 133-138, Mar. 2001.

[25] E. E. Sutter, "The fast m-transform: a fast computation of cross-correlations with binary m-sequences," *SIAM J. Computing*, vol. 20, no. 4, pp. 686-694, Aug. 1991.

[26] J. J. Sylvester, "Thoughts on inverse orthogonal matrices, simultaneous signsuccessions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-works, and the theory of numbers," *The London, Edinburgh, and Dublin Philosophical Mag. and J. Sci.*, vol. 34, no. 232, pp. 461-475, Dec. 1867.

[27] R. Yarlagadda, "A note on the eigenvector of DFT matrices," *IEEE Trans. Acousics., Speech, and Sign. Process.*, vol. 5, no. 6, pp. 586-589, Dec. 1977

[28] R. Yarlagadda and J. Hershey, "A note on the eigenvectors of Hadamard matrices of order 2^n," *Linear Algebra and Its Appl.*, vol. 45, pp. 43-53, Jun. 1982.

[29] R. Yarlagadda and J. Hershey, *Hadamard matrix analysis and synthesis: with applications to communications and signal/image processing*, Kluwer Academic Publisher, 1997.

[30] J. Williamson, "Hadamard's determinant theorem and the sum of four squares," *Duke Math. J.*, vol. 11, no. 1, pp. 65-81, Mar. 1944.

송 민 규 (Min Kyu Song)

2011년 2월 : 건국대학교 전자공학과 졸업

2013년 2월 : 연세대학교 전기전자공학과 석사

2014년 3월~현재 : 연세대학교 전자공학과 박사과정

<관심분야> 통신공학, 정보이론, 부호이론

송 홍 엽 (Hong-Yeop Song)

1984년 2월 : 연세대학교 전자공학과 졸업
1986년 5월 : University of Southern California Dept. of EE. System 석사
1991년 12월 : University of Southern California Dept. of EE. System 박사
1992년 1월~1993년 12월 : University of Southern California 박사 후 연구원
1994년 1월~1995년 8월 : Qualcomm, San Diego, Senior Engineer
1995년 9월~현재 : 연세대학교 전기전자공학과 전임교수
<관심분야> 통신공학, 정보이론, 부호이론