순환 부분 하다마드 행렬에 관한 조사

채상원, 김강산, 송홍엽

연세대학교

{sw.chae, gs.kim, hysong}@yonsei.ac.kr

A Search of the Circulant Partial Hadamard Matrices

Sangwon Chae, Gangsan Kim, and Hong-Yeop Song

Yonsei Univ.

요 약

본 논문은 순환 부분 하다마드 행렬 및 성질과 관련 이론을 소개한다. m이 최댓값일 때의 (m,n) 중 일부 파라미터에 대하여 순환 부분 하다마드 행렬을 생성하는 잘 알려진 방법을 소개한다. $m\times n$ 크기의 순환 부분 하다마드 행렬에서 $n\le 44$에 대해 m의 최댓값을 조사한다.

Ⅰ. 서론

하다마드 행렬은 모든 요소가 $+1$ 또는 -1이고 모든 행이 서로 직교하는 정사각행렬이다. 이러한 직교 성질로부터 디지털 통신 신호 코딩 및 변조와 같은 여러 분야에서 널리 사용된다[1]. 하다마드 행렬 중, 하나의 행을 한 요소씩 순환이동시켜서 모든 행을 구성할 수 있는 순환 하다마드 행렬은 이상적인 통신 신호인 완벽 수열의 존재성과 관련이 있다[2]. 그러나 순환 하다마드 행렬인 행렬은 크기 $n>4$ 이상에서 알려지지 않았다[3]. 이와 관련하여 정사각형이 아닌, 순환 행렬이면서 부분 (partial) 하다마드 행렬인 순환 부분 하다마드 행렬에 관한 연구가 있었다[3, 4]. 본 논문에서는 주어진 열의 개수에 대해 최대의 행의 개수를 갖는 순환 부분 하다마드 행렬의 예시를 제시하고, 행렬과 관련된 이론을 소개한다.

Ⅱ. 본론

순환 부분 하다마드 행렬을 $A=(a_{ij})$라고 하자. 이때 행렬 A는 다음을 만족한다[3].

- 아래 행이 바로 위 행에서 오른쪽으로 한 요소만큼 순환이동한 행이다. 이를 길이 n의 수열 $a=(a_0,a_1,...,a_{n-1})$를 통해 다음과 같이 나타낼 수 있다.

$$A=\mathrm{circ}_m(a)=\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1}\\ a_{n-1} & a_0 & \cdots & a_{n-2}\\ \vdots & \vdots & \ddots & \vdots\\ a_{n-m+1} & a_{n-m+2} & \cdots & a_{n-m}\end{bmatrix},$$

  이때 $\mathrm{circ}_m(\cdot)$은 안의 원소를 0번부터 $m-1$번까지 오른쪽으로 순환이동한 m개의 행을 갖는 행렬이다$(m\le n)$.
- 모든 원소는 ± 1이다.
- 모든 행이 서로 직교하므로 $AA^T=nI_m$이다.

여기서 $m=n$인 정사각 순환 하다마드 행렬은 하다마드-동등 아래에서

$$H_1=[1],\quad H_4=\begin{bmatrix} 1 & -1 & -1 & -1\\ -1 & 1 & -1 & -1\\ -1 & -1 & 1 & -1\\ -1 & -1 & -1 & 1\end{bmatrix}$$

외에는 알려지지 않았다. 이는 $m=n>4$에 대한 순환 하다마드 행렬은 없다는 Circulant Hadamard Conjecture의 반례가 발견되지 않았다고 알려져 있다[3]. Circulant Hadamard Conjecture가 사실일 경우 $n>4$에 대하여 순환 부분 하다마드 행렬의 행의 개수는 $m\le n/2$이다[8].

순환 부분 하다마드 행렬 A를 구성하는 주기 n인 수열 a의 자기상관함수를 다음과 같이 정의할 수 있다:

$$R_a(l)=\sum_{i=0}^{n-1}a_i a_{i+l(\mathrm{mod}\,n)},\ 0\le l<n.$$

$R_a(l)\equiv n\,(\mathrm{mod}\,4)$임이 알려져 있으므로, $m\ge 2$인 순환 부분 하다마드 행렬이 될 수 있는 행렬을 구성하는 수열 a의 길이는 $n\equiv 0\,(\mathrm{mod}\,4)$이다[5].

표 1은 주어진 4의 배수 $n\le 44$에 대해 최대 m을 갖는 순환 부분 하다마드 행렬을 컴퓨터 프로그램으로 조사한 결과 및 그에 해당하는 첫 번째 행을 수열로 나타냈다. 각 n에서 표 1에 기재된 m보다 큰 값이 존재하지 않음을 확인하였다. $m=n/2$이 존재하는 경우, 하나의 예시만 찾으면 되므로 비교적 빠르게 찾을 수 있었다. 하지만 $m=n/2$이 존재하지 않는 경우, 존재하지 않음을 확인하기 위해 모든 경우의 수를 확인해야 하므로 오랜 시간이 예상되어 $n=44$ 경우까지 조사했다.

$m=n/2$이 존재하는 경우, 홀수인 소수 또는 그 거듭제곱 p에 대하여 $n=2(p+1)$인 수열 a의 생성법은 [6, 7]에서 제안되었다. 해당 방법을 통해 생성할 수 없는 경우는 표 1에서 $n=32,44$이며, 이 n에 대하여 $n/2\times n$ 순환 부분 하다마드 행렬이 존재하지 않음을 확인하였다.

Ⅲ. 결론

본 논문에서는 $m\times n$ 순환 부분 하다마드 행렬에서 $n\equiv 0(\mathrm{mod}\,4)$에서 각각의 $n\le 44$에 대한 최대 m 값을 도출하였다. 그리고 $n\le 44$까지 최대 m값이 $n/2$인 모든 n에 대하여 [6, 7]에서 제시된 방법으로

n	$m_{\max}$	순환 부분 하다마드 행렬의 예시	검색 시간
4	4	$+---$	-
8	4	$++-+----$	0s
12	6	$++--+-+-----$	0s
16	8	$++-+-+++--+-----$	0s
20	10	$+-++--++++-+---+----$	0.04s
24	12	$+--+-+++-+-+$ $+------+++---$	0.12s
28	14	$--++--+-+--+++$ $++--+-+-+-+----$	2.07s
32	14	$+++++++--+-+--++$ $-----+-+-+-+-++--$	117.63s
36	18	$++-----+---+-+--+-$ $--++++++--++-+-++-+$	8.66s
40	20	$+--+--+++---+-++++++$ $-++-++---+++-+-+----$	118.71s
44	18	$-+-++-+++--+--+-+---+-$ $-+-+++---+--------++++--$	105253s

표 1. n에 대해 최대 m을 갖는 순환 부분 하다마드 행렬의 예시

$n/2 \times n$ 크기인 순환 부분 하다마드 행렬을 생성할 수 있음을 확인했다. 또한 해당 방법으로 생성할 수 없는 길이 $n = 32, 44$에서 $m < n/2$을 확인하였다. 추가적으로 다음과 같은 추론을 생각할 수 있다.

추론1. 모든 4의 배수 n에 대하여 $m_{\max}$는 항상 짝수이다.

추론2. 홀수인 소수 또는 그 거듭제곱 p에 대하여 $2(p+1)$꼴이 아닌 5 이상의 n에 대하여 항상 $m_{\max} < n/2$이다.

ACKNOWLEDGMENT

이 (성과)는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.RS-2023-00209000).

참 고 문 헌

[1] X. Huang, “Complementary Properties of Hadamard Matrices,” *2006 International Conference on Communications, Circuits and Systems*, Guilin, China, pp. 588-592, 2006.

[2] D. Jungnickel and A. Pott, “Perfect and almost perfect sequences,” *Discrete Applied Mathematics*, vol. 95, no. 1 - 3, pp. 331 - 359, 1999.

[3] R. Craigen, G. Faucher, R. M. Low, and T. Wares, “Circulant partial Hadamard matrices,” *Linear Algebra and Its Applications*, vol. 439, no. 11, pp. 3307 - 3317, 2013.

[4] M. Pankaj K. and R. Mahendra K., “On Circulant Partial Hadamard Matrices,” *Applied Linear Algebra, Probability and Statistics*, Springer Nature Singapore, pp. 425-433, 2023.

[5] X. Niu, H. Cao, and K. Feng, “Binary periodic sequences with 2-level autocorrelation values,” *Discrete Mathematics*, Volume 343, Issue 3, 2020.

[6] G. Kim and H. -Y. Song, “Almost perfect sequence family with perfect crosscorrelation,” *2020 International Symposium on Information Theory and Its Applications (ISITA)*, Kapolei, HI, USA, pp. 456-459, 2020.

[7] Y. Nogami, K. Tada, and S. Uehara, “A Geometric Sequence Binarized with Legendre Symbol over Odd Characteristic Field and Its Properties,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, pp. 2336-2342, 2014.

[8] P. Fan and M. Darnell, *Sequence Design for Communications Applications*, Somerset, England: Research Studies Press, 1996.