



순환 부분 하다마드 행렬에 관한 조사

채상원, 김강산, 송홍엽
연세대학교

2024 한국통신학회 동계종합학술발표회



목차

- 서론
 - 순환 부분 하다마드 행렬
- 본론
 - 순환 부분 하다마드 행렬과 관련 이론
 - 실험 및 결과
 - 수열 생성법
- 결론



서론

- 서론
 - 순환 부분 하다마드 행렬
- 본론
 - 순환 부분 하다마드 행렬과 관련 이론
 - 실험 및 결과
 - 수열 생성법
- 결론



순환 행렬

- 순환 행렬 (Circulant Matrix) 은 각 행이 바로 위 행에서 오른쪽으로 한 요소만큼 순환한 정사각 행렬임.

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}$$



하다마드 행렬

- 하다마드 행렬 (Hadamard Matrix) 은 모든 요소가 ± 1 이고 모든 행(열)이 서로 직교하는 정사각 행렬임.

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

- 모든 행(열)이 서로 직교하기에, 신호 코딩, 변조 및 대역 확산 등에 이용됨[1].

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



하다마드 행렬의 파생 행렬들

- 부분 하다마드 행렬 (Partial Hadamard Matrix) [3, 4], 준 하다마드 행렬 (Quasi Hadamard Matrix) [9] 등 다양한 하다마드 행렬의 파생 행렬들이 연구됨.

$$PH = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & +1 & -1 & -1 \end{bmatrix}$$

$$QH = \begin{bmatrix} +1 & +1 & +1 & +1 & +1 \\ +1 & +1 & +1 & -1 & -1 \\ +1 & +1 & -1 & +1 & -1 \\ +1 & -1 & +1 & +1 & -1 \\ +1 & -1 & -1 & -1 & +1 \end{bmatrix}$$

[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.

[9] Ki-Hyeon Park and Hong-Yeop Song, "Quasi-Hadamard Matrix," The 2010 IEEE International Symposium on Information Theory (ISIT 2010), Austin, Texas, USA, June 13-18, 2010.



순환 부분 하다마드 행렬

- 부분 하다마드 행렬은 모든 요소가 ± 1 이고 모든 행이 서로 직교하는 행렬임.
- 순환 부분 하다마드 행렬 (Circulant Partial Hadamard Matrix) 은 순환 행렬이면서 부분 하다마드 행렬임.
- 본 논문은 주어진 열의 개수에 대해 최대의 행의 개수를 갖는 순환 부분 하다마드 행렬의 예시를 제시함.
- 또한 순환 부분 하다마드 행렬과 관련된 이론을 소개함.



본론

- 서론
 - 순환 부분 하다마드 행렬
- 본론
 - 순환 부분 하다마드 행렬과 관련 이론
 - 실험 및 결과
 - 수열 생성법
- 결론



순환 부분 하다마드 행렬과 수열의 관계

- $m \times n$ 크기의 순환 부분 하다마드 행렬은 수열을 통해 나타낼 수 있음.

$$a = (+1, +1, -1, +1, -1, -1, -1, -1),$$

$$A = \text{circ}_4(a) = \begin{bmatrix} +1 & +1 & -1 & +1 & -1 & -1 & -1 & -1 \\ -1 & +1 & +1 & -1 & +1 & -1 & -1 & -1 \\ -1 & -1 & +1 & +1 & -1 & +1 & -1 & -1 \\ -1 & -1 & -1 & +1 & +1 & -1 & +1 & -1 \end{bmatrix}$$

이 때 $\text{circ}_m(\cdot)$ 는 원소를 0번부터 $m - 1$ 번까지 오른쪽으로 순환이동한 m 개의 행을 갖는 행렬임.



순환 하다마드 행렬의 존재성

- 정사각 순환 하다마드 행렬은 하다마드-동치 아래 단 두 개만 알려져 있음:

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

- 이는 완벽 수열의 존재성 및 Circulant Hadamard Conjecture와 관련 있음 [5].
- Circulant Hadamard Conjecture에 따르면 $n > 4$ 크기에서 순환 하다마드 행렬은 존재하지 않음.

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



자기상관함수와 순환 부분 하다마드 행렬의 크기

- 순환 부분 하다마드 행렬을 구성하는 주기 n 인 수열 a 의 자기상관함수

$$R_a(l) = \sum_{i=0}^{n-1} a_i a_{i+l \pmod n}$$

에 대해

- $R_a(l)$ 은 짝함수이므로 m 은 순환의 방향과는 관계 없음.
- $R_a(l)$ 이 짝함수이고 Circulant Hadamard Conjecture가 참이라면 $n > 4$ 에서 $m > n/2$ 인 순환 부분 하다마드 행렬은 존재하지 않음.
- $R_a(l) \equiv n \pmod 4$ 이므로, $m \geq 2$ 의 순환 부분 하다마드 행렬을 생성할 수 있는 수열 a 의 길이는 $n \equiv 0 \pmod 4$ 임.



실험 방법

- 실험에 사용된 컴퓨터와 프로그램:
 - Windows 11 23H2
 - Ryzen 9 7900X (12c 24t, 5.1GHz)
 - C17 with OpenMP
- 각 n 에서 표 1에 기재된 m 보다 큰 값이 존재하지 않음을 확인함.
- 표 1에서 $m_{\max} = n/2$ 의 경우, 하나의 예시만 찾으면 되므로 비교적 빠르게 찾을 수 있지만 $m_{\max} < n/2$ 의 경우, $m = n/2$ 이 존재하지 않음을 확인하기 위해 모든 경우의 수를 확인해야 하므로 비교적 오랜 시간이 걸림.



실험 결과

- 표 1은 컴퓨터 프로그램으로 주어진 4의 배수 $n \leq 44$ 에서 최대 m 을 찾고, 해당 크기를 갖는 순환 부분 하다마드 행렬의 예시를 보임.

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	- + - + + - + + + - - + - - + - + - - - + - - + - + + + - - - + - - - - - - - + + + - -	29.23h



수열 생성법

- $m = n/2$ 인 경우에 대해 홀수인 소수 또는 그 거듭제곱 p 에 대해 $n = 2(p + 1)$ 인 수열 a 의 생성법은 [6, 7, 10]에서 제안함.

$$a_i = \begin{cases} 1, & \text{Tr}(\alpha^i) = 0 \\ (\text{Tr}(\alpha^i) / p), & \text{otherwise} \end{cases}$$

여기서 $i = 0, 1, \dots, n - 1$ 이고, $(\cdot / p)$ 는 르장드르 기호이며, α 는 extension field F_{p^2} 의 원시 원소임.

[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.

[10] Gangsan Kim and Hong-Yeop Song, "Some properties of NTU sequences," The International Symposium on Information Theory and Its Applications 2018 (ISITA 2018), Singapore, Oct. 28-31, 2018.



수열 생성법

- 해당 방법을 사용할 수 없는 길이는 표 1에서 $n = 32, 44$ 이며, 해당 길이에 대해 $n/2 \times n$ 순환 부분 하다마드 행렬이 존재하지 않음을 확인함.

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	- + - + + - + + + - - + - - + - + - - - + - - + - + + + - - - + - - - - - - - + + + - -	29.23h



결론

- 서론
 - 순환 부분 하다마드 행렬
- 본론
 - 순환 부분 하다마드 행렬과 관련 이론
 - 실험 및 결과
 - 수열 생성법
- 결론



결론

- 본 논문에서는 $m \times n$ 순환 부분 하다마드 행렬에서 $n \equiv 0 \pmod{4}$ 에서 각각의 $n \leq 44$ 에 대한 최대 m 값을 도출함.
- $n \leq 44$ 에서 $m_{\max} = n/2$ 을 만족하는 모든 n 에 대하여 [6, 7, 10]에서 제시된 방법으로 $n/2 \times n$ 크기의 순환 부분 하다마드 행렬을 생성할 수 있음을 확인함.



결론

- 아래의 추론을 생각해볼 수 있음.
- **추론 1.** 모든 4의 배수 n 에 대해 $m_{\max}$ 는 항상 짝수임.
 - 4의 배수가 아닌 n 에 대해서 $m_{\max} = 1$ 임.
- **추론 2.** 홀수인 소수 또는 그 거듭제곱 p 에 대해 $2(p + 1)$ 꼴이 아닌 5 이상의 n 에 대해 항상 $m_{\max} < n/2$ 임.



THE END

CCL

감사합니다.