Communications in Mathematics and Applications
Vol. 16, No. 3, pp. 923–927, 2025
ISSN 0975-8607 (online); 0976-5905 (print)
Published by RGN Publications
DOI: 10.26713/cma.v16i3.3215

http://www.rgnpublications.com

Research Article

Construction of Regular Hadamard Matrices From Circulant Hadamard Matrices and Ryser's Conjecture

Pankaj Kumar Manjhi* and Jitendra Kumar

University Department of Mathematics, Vinoba Bhave University, Hazaribag, Jharkhand, India
***Corresponding author:** 19pankaj81@gmail.com

Received: May 30, 2025 **Revised:** June 25, 2025 **Accepted:** July 14, 2025

Abstract. This article presents a simplified proof of Ryser's conjecture by building upon and extending the modular arithmetic framework introduced by Luis Henri Gallardo (On Ryser's conjecture: modulo 2 approach, *Applied Mathematics E-Notes* **21** (2021), 220 – 224), specifically leveraging the modulo 2 approach. The methodology highlights an accessible and robust pathway to understanding the conjecture's constraints, providing new insights into the structural properties of circulant and regular Hadamard matrices.

Keywords. Hadamard matrix, Partial Hadamard matrix, Circulant matrix

Mathematics Subject Classification (2020). 05B15, 05B20, 05B30

1. Introduction

A *Hadamard matrix* is a square matrix H of order n with entries from $\{\pm 1\}$ satisfying the relation $HH^\top = nI_n$, where I_n denotes the identity matrix of order n. A special class of Hadamard matrices, called *circulant Hadamard matrices*, consists of matrices of the form $H = \text{circ}(h_1, h_2, \dots, h_n)$, where each row is obtained by a cyclic right shift of the preceding row.

The known circulant Hadamard matrices are limited to the following ten:

$H_1 = \text{circ}(1)$, $H_2 = -H_1$,

$H_3 = \text{circ}(1, -1, -1, -1)$, $H_4 = -H_3$,

$H_5 = \mathrm{circ}(-1,1,-1,-1), \quad H_6 = -H_5,$

$H_7 = \mathrm{circ}(-1,-1,1,-1), \quad H_8 = -H_7,$

$H_9 = \mathrm{circ}(-1,-1,-1,1), \quad H_{10} = -H_9.$

In 1963, Ryser [9] conjectured that *there exists no circulant Hadamard matrix of order* $n > 4$. Since then, this conjecture has attracted considerable attention and has been approached using various techniques. One of the earliest significant results was provided by Brualdi in 1965 [1], who proved the conjecture for the case in which all eigenvalues of a circulant Hadamard matrix are real.

Numerous studies have further explored the conjecture from both algebraic and combinatorial perspectives (see, e.g., Erdös [3], Leung *et al*. [6], Schmidt [10], and Turyn [12]). In particular, Gallardo [4] extended Brualdi's result by demonstrating the nonexistence of circulant Hadamard matrices of order $n > 4$ under certain modular congruence conditions modulo 2. Gallardo's approach utilizes modular properties of an associated circulant weighing matrix of order $\frac{n}{2}$, offering new insight into this longstanding open problem.

2. Regular and Circulant Hadamard Matrices

2.1 Definitions and Known Results

Definition 2.1. A Hadamard matrix H of order n is said to be *r-regular* if all of its row and column sums are equal to r. A *regular Hadamard matrix* is an r-regular Hadamard matrix for some integer r.

For foundational results, the reader is referred to Hedayat and Wallis [5], Mcisncr [8], and Turyn [11].

Lemma 2.1. *Let H be a circulant Hadamard matrix of order $n \geq 1$. Then, $n = 4h^2$ for some positive integer h. Moreover, if H is circulant, then h is odd. Furthermore, either H or $-H$ is $2h$-regular (the other being $-2h$-regular). When H is $2h$-regular, each row contains $2h^2 + h$ positive entries and $2h^2 - h$ negative entries. If H is $-2h$-regular, the counts of positive and negative entries are reversed.*

Lemma 2.2. *Let $\omega = e^{2\pi i/n}$, and let $R(x)$ be the representer polynomial of a circulant matrix H. Then the eigenvalues of H are given by the set $\{R(\omega^k) : 0 \leq k \leq n-1\}$, and each satisfies*

$$|R(\omega^k)| = \sqrt{n}.$$

Lemma 2.3. *Let $C = \mathrm{circ}(c_1, c_2, \ldots, c_n)$ be a circulant matrix of order $n > 0$, with representer polynomial $P(t) = c_1 + c_2 t + \cdots + c_n t^{n-1}$. Let ω be a primitive n-th root of unity with the smallest positive argument. Then, C is diagonalizable, and can be expressed as*

$$C = F^* \Lambda F,$$

where $\Lambda = \mathrm{diag}(P(1), P(\omega), \ldots, P(\omega^{n-1}))$ contains the eigenvalues of C, and F^* is the conjugate transpose of the Fourier matrix $F = \left(\frac{1}{\sqrt{n}}\omega^{(i-1)(j-1)}\right)$. Moreover, F is a unitary matrix.

2.2 Main Contribution

We now present our central result establishing a structural transformation from a circulant Hadamard matrix to a regular Hadamard matrix.

Lemma 2.4. *Let $H = \text{circ}(h_1, h_2, \dots, h_n)$ be a circulant Hadamard matrix of order $n = 4h^2$, with row and column sum $\pm 2h$. Then, there exists a regular Hadamard matrix of the form*

$$M = \begin{bmatrix} M_1 & M_2 \\ M_2 & r(M_1) \end{bmatrix}$$

of order n, where

(i) $M_1 = \text{circ}(h_1, h_3, h_5, \dots, h_{n-1})$,

(ii) $M_2 = \text{circ}(h_2, h_4, h_6, \dots, h_n)$, *and*

(iii) $r(M_1)$ *is the matrix obtained by reversing the cyclic order of each row of* M_1.

Proof. Let S_i, K_i, L_i, and R_i denote the i-th rows of M_1, M_2, $r(M_1)$, and H, respectively. Since H is Hadamard, it satisfies

$$\langle R_i, R_j \rangle = 0, \quad \text{for } i \neq j, \tag{2.1}$$

$$\langle R_i, R_i \rangle = n. \tag{2.2}$$

We now compute

$$MM^T = \begin{bmatrix} M_1 & M_2 \\ M_2 & r(M_1) \end{bmatrix} \begin{bmatrix} M_1^T & M_2^T \\ M_2^T & r(M_1)^T \end{bmatrix} = \begin{bmatrix} M_1M_1^T + M_2M_2^T & M_1M_2^T + M_2r(M_1)^T \\ M_2M_1^T + r(M_1)M_2^T & M_2M_2^T + r(M_1)r(M_1)^T \end{bmatrix}.$$

Using equations (2.1) and (2.2), and noting the indexing shift patterns of the circulant structure, we get

$$\begin{aligned} M_1M_1^T + M_2M_2^T &= nI_{\frac{n}{2}}, \\ M_1M_2^T + M_2r(M_1)^T &= O_{\frac{n}{2}}, \\ M_2M_1^T + r(M_1)M_2^T &= O_{\frac{n}{2}}, \\ M_2M_2^T + r(M_1)r(M_1)^T &= nI_{\frac{n}{2}}. \end{aligned}$$

Thus,

$$MM^T = \begin{bmatrix} nI_{\frac{n}{2}} & O_{\frac{n}{2}} \\ O_{\frac{n}{2}} & nI_{\frac{n}{2}} \end{bmatrix} = nI_n,$$

which completes the proof. □

Theorem 2.1. *There does not exist any regular Hadamard matrix of the form*

$$M = \begin{bmatrix} M_1 & M_2 \\ M_2 & r(M_1) \end{bmatrix}$$

of order $n > 4$.

Proof. Suppose, for contradiction, that such a matrix M exists for $n > 4$. Then, by Lemma 2.4, there must exist a circulant Hadamard matrix $H = \text{circ}(h_1, h_2, \dots, h_n)$ satisfying $HH^T = nI_n$.

According to Gallardo's result in [4], we have

$$\left(\frac{H+J}{2}\right)\left(\frac{H+J}{2}\right)^T \bmod 2 \neq I_n,$$

which implies

$$\frac{HH^T}{4} + \frac{HJ^T + JH^T}{4} + \frac{JJ^T}{4} \bmod 2 \neq I_n.$$

Since $HH^T = nI_n$ and $JJ^T = nJ$, we get

$$\frac{MM^T}{4} + (h+h^2)J \bmod 2 \neq I_n$$

this leads to

$$\frac{MM^T}{4} \bmod 2 \neq I_n,$$

$$\frac{nI_n}{4} \bmod 2 \neq I_n,$$

$$h^2 I_n \bmod 2 \neq I_n.$$

This is only possible if h is even, contradicting the result that h must be odd for circulant Hadamard matrices. Hence, no such regular Hadamard matrix M of order $n > 4$ exists. □

3. Conclusion

In this article, two significant results have been established. First, a special class of regular Hadamard matrices of the form

$$M = \begin{bmatrix} M_1 & M_2 \\ M_2 & r(M_1) \end{bmatrix}$$

has been constructed, which incorporates circulant matrices. The matrices M_1 and M_2 are designed so that each contains exactly $\frac{n}{2}$ elements in their generating rows. These elements correspond respectively to the odd-positioned and even-positioned entries of a circulant Hadamard matrix H of order n. The matrix $r(M_1)$ is obtained by applying a backward cyclic shift to each row of M_1, which ensures the required structural symmetry in the construction.

Secondly, certain properties regarding the order of this special type of regular Hadamard matrix M have been investigated and established. Moreover, as an application of the theoretical results, the article utilizes Ryser's conjecture together with the approach of Luis Henri Gallardo to demonstrate the construction of regular Hadamard matrices of order not exceeding 4.

These results contribute to the structural understanding of regular Hadamard matrices and provide a constructive framework that may be useful for further investigations on circulant and related classes of Hadamard matrices.

Competing Interests

The authors declare that they have no competing interests.

Authors' Contributions

All the authors contributed significantly in writing this article. The authors read and approved the final manuscript.

References

[1] R. A. Brualdi, A note on multipliers of difference sets, *Journal of Research of the National Bureau of Standards-B. Mathematics and Mathematical Physics* **69B**(1-2) (1965), 87 – 89.

[2] P. J. Davis, *Circulant Matrices*, 2nd edition, AMS Chelsea Publishing: An Imprint of the American Mathematical Society, New York, 240 pages (1994).

[3] P. Erdös, On the coefficients of the cyclotomic polynomial, *Bulletin of the American Mathematical Society* **52** (1946), 179 – 184, DOI: 10.1090/S0002-9904-1946-08538-9.

[4] L. H. Gallardo, On Ryser's conjecture: modulo 2 approach, *Applied Mathematics E-Notes* **21** (2021), 220 – 224, https://www.math.nthu.edu.tw/~amen/2021/AMEN-200412.pdf.

[5] A. Hedayat and W. D. Wallis, Hadamard matrices and their applications, *The Annals of Statistics* **6**(6) (1978), 1184 – 1238, DOI: 10.1214/aos/1176344370.

[6] K. H. Leung, S. L. Ma and B. Schmidt, New Hadamard matrices of order $4p^2$ obtained from Jacobi sums of order 16, *Journal of Combinatorial Theory, Series A* **113**(5) (2006), 822 – 835, DOI: 10.1016/j.jcta.2005.07.011.

[7] P. K. Manjhi, On permutation groups and Fourier matrices, *International Journal for Research in Engineering Application & Management* **04**(04) (2018), 197 – 200, URL: http://ijream.org/papers/IJREAMV04I0440039.pdf.

[8] D. B. Mcisncr, On a construction of regular Hadamard matrices, *Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Serie 9* **3**(4) (1992), 233 – 240, URL: http://www.bdim.eu/item?fmt=pdf&id=RLIN_1992_9_3_4_233_0.

[9] H. J. Ryser, *Combinatorial Mathematics*, The Carus Mathematical Monographs, Vol. 14, The Mathematical Association of America, xiv + 154 pages (1963).

[10] B. Schmidt, Cyclotomic integers and finite geometry, *Journal of the American Mathematical Society* **12** (1999), 929 – 952, DOI: 10.1090/S0894-0347-99-00298-2.

[11] R. J. Turyn, Character sums and difference sets, *Pacific Journal of Mathematics* **15**(1) (1965), 319 – 346, DOI: 10.2140/pjm.1965.15.319.

[12] R. Turyn, Sequences with small correlation, in: *Error Correcting Codes: Symposium Proceedings*, H. B. Mann (editor), John Wiley & Sons Inc., New York, pp. 195 – 228 (1968).