Applied Mathematics E-Notes, 21(2021), 220-224 © ISSN 1607-2510
Available free at mirror sites of http://www.math.nthu.edu.tw/∼amen/

On Ryser's Conjecture: Modulo 2 Approach*

Luis Henri Gallardo†

Received 12 April 2020

Abstract

We prove the nonexistence of circulant Hadamard matrices H of order $n > 4$ under the truth of some congruences (mod 2) extending a result of Brualdi. The new idea consists of exploiting modular properties of a related circulant weighing matrix of order $n/2$.

1 Introduction

A matrix of order n is a square matrix with n rows. A *circulant* matrix $A = \text{circ}(a_1, \dots, a_n)$ of order n is a matrix of order n of first row $[a_1, \dots, a_n]$ in which each row after the first is obtained by a cyclic shift of its predecessor by one position. For example, the second row of A is $[a_n, a_1, \dots, a_{n-1}]$. As usual, J is the matrix of order n with all its entries equal to 1 (i.e., $J = circ(1, \dots, 1)$). A *Hadamard* matrix H of order n is a matrix of order n with entries in $\{-1, 1\}$ such that $\frac{H}{\sqrt{n}}$ is an orthogonal matrix. A *circulant Hadamard* matrix of order n is a circulant matrix that is Hadamard. The 10 known circulant Hadamard matrices are $H_1 = \text{circ}(1), H_2 = -H_1, H_3 = \text{circ}(1, -1, -1, -1), H_4 = -H_3, H_5 = \text{circ}(-1, 1, -1, -1), H_6 = -H_5$, $H_7 = \text{circ}(-1, -1, 1, -1), H_8 = -H_7, H_9 = \text{circ}(-1, -1, -1, 1), H_{10} = -H_9$.

If $H = \text{circ}(h_1, \dots, h_n)$, is a circulant Hadamard matrix of order n then its *representer* polynomial is the polynomial $R(x) = h_1 + h_2x + \cdots + h_nx^{n-1}$.

No one has been able, despite several deep computations (see [9]), to discover any other circulant Hadamard matrix. Ryser [2, p. 97], [15] proposed in 1963 the conjecture of the non-existence of these matrices when $n > 4$. Preceding work on the conjecture includes [3, 4, 6, 7, 8, 11, 13, 14, 16].

Ryser's conjecture (there is no circulant Hadamard matrices of order > 4) has been studied by several different methods. Brualdi [1] proved in 1965 the first special, and important, case of the conjecture, in which all eigenvalues of a circulant Hadamard matrix $H = circ(h_1, \dots, h_n)$ of order $n > 4$, are real; i.e., we assume that H is symmetric. We relax in this paper the symmetry condition, by asking just a condition of symmetry modulo 2 of a related matrix.

Assume the existence of a circulant Hadamard matrix H of order $n > 4$. The present paper proves that this is impossible when the matrix $H_2 = (H + J)/2$ reduced modulo 2 is a symmetric matrix. It is also impossible when an $n/4 \times n/4$ related matrix reduced (mod 2) is symmetric. The result follows, essentially, from a result of MacWilliams [10, Corollary 1.8] (see Lemma 5).

In order to be more precise, we define some sub-matrices of a given circulant matrix of even order. Let M be a circulant matrix of even order $2k$. Observe that M, having even order $2k$, can be partitioned in four blocks M_1, M_2, M_3, M_4, each of size $k \times k$, as follows

$$M = \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix}.$$

Since M is circulant, we have $M_4 = M_1$, and $M_3 = M_2$. We are thus associating to the $2k \times 2k$ circulant matrix M the square $k \times k$ matrices M_1 and M_2 (see exact details in Lemma 4), in order to have

$$M = \begin{bmatrix} M_1 & M_2 \\ M_2 & M_1 \end{bmatrix}.$$

*Mathematics Subject Classifications: 11C20, 15B34, 11A07, 15B33.

†Univ. Brest, UMR CNRS 6205, Laboratoire de Mathématiques de Bretagne Atlantique, 6, Av. Le Gorgeu, C.S. 93837, Cedex 3, F-29238 Brest, France

Our main result is as follows:

Theorem 1 *There is no circulant Hadamard matrix H of order $n > 4$ provided*

(a) the matrix $S_2 = (H+J)/2 \pmod 2$ is symmetric, or

(b) both matrices C and D, defined below, are symmetric.

Write H as

$$H = \begin{bmatrix} H_1 & H_2 \\ H_2 & H_1 \end{bmatrix}$$

where the $n/2 \times n/2$ matrices H_1 and H_2 are defined in Lemma 4 applied to H. Put $T = (H_1 + H_2)/2$. Observe that T is circulant, and define $n/4 \times n/4$ matrices T_1 and T_2 as above, by using again Lemma 4, this time applied to T. Namely, write T as

$$T = \begin{bmatrix} T_1 & T_2 \\ T_2 & T_1 \end{bmatrix}.$$

Finally, we define $C = T_1 \pmod 2$, and $D = T_2 \pmod 2$.

Section 2 contains the main tools necessary for the proof of the theorem. Section 3 contains the proof of Theorem 1. Throughout the paper, we let A^* denote the transpose conjugate of a matrix A, and the identity matrix of order k is denoted by I_k. We let $\mathbb{F}_2 = \{0, 1\}$ denote, as usual, the binary finite field. A binary matrix is a matrix with all its entries in $\mathbb{F}_2$.

2 Tools

The following is well known. See, e.g., [5, p. 1193], [12, p. 234], [16, pp. 329-330] for the first lemma and [2, p. 73] for the second.

First of all, we recall the notion of regular Hadamard matrix.

Definition 1 *An r-regular Hadamard matrix is a Hadamard matrix whose row and column sums are all equal to r. A regular Hadamard matrix is an r-regular Hadamard matrix for some integer r.*

Lemma 1 *Let H be a regular Hadamard matrix of order $n \geq 4$. 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 is $(-2h)$-regular) and each row has $2h^2 + h$ positive entries and $2h^2 - h$ negative entries, when H is $2h$-regular; respectively, has $2h^2 - h$ positive entries and $2h^2 + h$ negative entries, when H is $(-2h)$-regular.*

Lemma 2 *Let H be a circulant Hadamard matrix of order $n \geq 1$, let $w = \exp(2\pi i/n)$, and let $R(x)$ be its representer polynomial. Then, the set of all eigenvalues of H, consists of the set of all $R(v)$ where $v \in \{1, w, w^2, \ldots, w^{n-1}\}$. Moreover, one has*

$$|R(v)| = \sqrt{n}.$$

More generally, and in more detail (see [2]), one has

Lemma 3 *Let $C = circ(c_1, \ldots, c_n)$ be a circulant matrix of order $n > 0$ with* representer *polynomial $P(t) = c_1 + c_2 t + \ldots + c_n t^{n-1}$. Let ω be the primitive complex n-th root of unity with smaller positive argument. The matrix C is diagonalizable and $C = F^* \Delta F$ where $\Delta = diag(P(1), P(w), \ldots, P(w^{n-1})$ is a diagonal matrix containing the eigenvalues of C, and $F^* = \left(\frac{\omega^{(i-1)(j-1)}}{\sqrt{n}}\right)$ is the conjugate of the Fourier matrix. Moreover, F is unitary.*

The following is well known, useful, and easy to check:

Lemma 4 *Let M be a circulant matrix of even order n and with first row $R_1 = [m_1, \ldots, m_n]$. Then*

(a)

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

where M_1, M_2 are the matrices of order $\frac{n}{2}$ defined by $M_1 = (a_{i,j})$, $M_2 = (b_{k,\ell})$, where $i, j, k, \ell = 1, \ldots, n/2$, and $a_{i,j} = m_{j-i+1}$, $b_{k,\ell} = m_{\ell+n/2-k+1}$, subscripts $\pmod{n}$.

(b) The matrix $M_1 + M_2$ is circulant.

The following result of MacWilliams [10] is crucial.

Lemma 5 *The only circulant, symmetric, and orthogonal matrix, over the binary field $\mathbb{F}_2$, of given order n, is the identity matrix I_n.*

The following "counting" lemma is important for the proof of the second part of the theorem.

Lemma 6 *Let H be a $\sqrt{n}$-regular circulant Hadamard matrix of order $n > 1$. Let H_1 and H_2 be the $n/2$ square matrices defined in Lemma 4 applied to H. Let $M = \frac{H_1+H_2}{2}$. Let a = number of 0's in the first row of the circulant matrix M. Let b = number of 1's in the first row of M, and let c = number of -1's in the first row of M. Then*

(i) $a = \frac{n}{4}$,

(ii) $b = \frac{n+2\sqrt{n}}{8}$,

(iii) $c = \frac{n-2\sqrt{n}}{8}$.

Proof. Since $H/\sqrt{n}$ is orthogonal, by Lemma 4, we have $H_1{H_1}^* + H_2{H_2}^* = nI_{n/2}$, and $H_1{H_2}^* + H_2{H_1}^* = 0$. Then, it follows that

$$MM^* = (n/4)I_{n/2}. \tag{1}$$

One has

$$M = circ\left(\frac{h_1 + h_{n/2+1}}{2}, \ldots, \frac{h_{n/2} + h_n}{2}\right).$$

Observe, from (1), that $n/4$ equals the sum of squares of all entries in row 1 of M, and that an entry $\frac{h_i+h_{n/2+i}}{2} = 0$ does not contribute to the sum of squares, while the other entries, i.e., the nonzero ones, each contribute by 1 to the same sum. In other words one has

$$n/4 = b + c. \tag{2}$$

Since H is $\sqrt{n}$-regular, and $2\sqrt{n} > 0$, we have that M is S-regular, with $S > 0$. Compute now S, i.e., compute the sum of all entries in row 1 of M:

$$S = \sum_{i=1}^{n/2} \frac{h_i + h_{n/2+i}}{2} = \frac{1}{2}\sum_{i=1}^{n} h_i = \frac{\sqrt{n}}{2}. \tag{3}$$

But $S = b - c$, since zeros do not contribute to the sum, thus it follows from (3) that

$$b - c = \frac{\sqrt{n}}{2}. \tag{4}$$

From (2) and (4) we get (ii) and (iii). Since the total number of entries in the first row of M is equal to $n/2$, we have

$$n/2 = a + b + c,$$

thereby obtaining also (i). This finishes the proof of the lemma. ■

3 Proof of Theorem 1

Proof. Assume, on the contrary, the existence of a circulant Hadamard matrix $H = circ(h_1, \ldots, h_n)$ where $n > 4$, such that

(a) for $C_1 = (H + J)/2$, the matrix $S_2 = C_1 \pmod 2$ is symmetric. Put $I = I_n$. By Lemma 1, $n = 4h^2$ with odd $h > 1$, and we can assume that all the row sums of H equal $2h$ (i.e, H is $2h-$regular). Observe that $HH^* = 4h^2 I$, $HJ = JH^* = 2hJ$, and $J^2 = nJ$. Thus

$$C_1 C_1^* = HH^*/4 + (HJ + JH^*)/4 + J^2/4 = h^2 I + (h + h^2)J. \tag{5}$$

Since h is odd, it follows then from (5) that $S_2 S_2^* = I$, as a matrix over $\mathbb{F}_2$. In other words, S_2 is an orthogonal matrix of order n over $\mathbb{F}_2$. Thus, since we assumed that S_2 is symmetric, Lemma 5 implies that $S_2 = I$. In particular, the number of 1's in the first row of S_2 is equal to 1. But, by definition of S_2, this says that C_1 (a $\{0, 1\}$ matrix), and thus H, has also only a single 1 in its first row. By Lemma 1, and since H is $2h-$regular, we know that the number of these 1's is equal to $2h^2 + h$. We conclude that $2h^2 + h = 1$. This is impossible since $h > 1$. This contradiction proves the result.

(b) Put $E = C + D$. Thus E is symmetric. Apply Lemma 4 to $M = H$ to get matrices $A_1 = H_1, B_1 = H_2$ of order $2h^2$ for which $T = (H_1 + H_2)/2$ is a circulant $\{-1, 0, 1\}$ matrix. Apply again Lemma 4, this time to $M = T$, to get matrices $A_2 = T_1, B_2 = T_2$ of order h^2 for which $L = (A_2 + B_2)$ is a circulant matrix with entries in $\{-2, -1, 0, 1, 2\}$. Thus $C = A_2 \pmod 2$, and $D = B_2 \pmod 2$. Since $HH^* = nI_n$, we get by block multiplication

$$A_1 A_1^* + B_1 B_1^* = 4h^2 I_{2h^2},\ A_1 B_1^* + B_1 A_1^* = 0 \tag{6}$$

so that, by adding both equations in (6) we get

$$TT^* = h^2 I_{2h^2}. \tag{7}$$

Remember that we have

$$D = D^*,\ C = C^*. \tag{8}$$

Put $U = T \pmod 2$. Reducing (7) $\pmod 2$ one sees that U is orthogonal. Thus, it follows from the definition of T, and from (8), that U is also symmetric. Therefore, a new application of Lemma 5 gives

$$U = I_{2h^2}. \tag{9}$$

But (9) contradicts Lemma 6 since the number of entries equal to -1 or to 1 in the first row of T (and thus, the number of 1's in the first row of U) is (with the notation of the lemma) equal to $b + c = h^2 \geq 9$, and not equal to 1, as is in the matrix I_{2h^2}. This contradiction proves the result.

■

Remark 1 *Concerning the proof of part (b) of the theorem. Asking that $E = C + D$ be symmetric, instead of asking that both C and D be symmetric, (in the hypothesis of the theorem), seems too weak, in order to get the same result. Moreover, when both C and D are assumed to be symmetric, it is possible to prove, using again MacWilliams result, that one has $E = I_{h^2}$ (i.e., that we have $C = I_{h^2} + D$). However, this alone do not seems to give a contradiction. Thus, we obtained the contradiction (that proved part (b) of the Theorem) by focusing on the $2h^2 \times 2h^2$ matrix T, instead.*

Acknowledgment. We are grateful to the referee for very careful reading and suggestions. We particularly appreciated the suggestions about clarifying the statement (and proof!) of the theorem, in our older draft. Thanks to his (her) work, the actual paper is substantially better.

References

[1] R. A. Brualdi, A note on multipliers of difference sets, J. Res. Nat. Bur. Standards Sect. B, 69(1965), 87–89.

[2] P. J. Davis, Circulant Matrices, 2^{nd} ed., New York, NY: AMS Chelsea Publishing, xix, 250 p., 1994.

[3] R. Euler, L. H. Gallardo and O. Rahavandrainy, Sufficient conditions for a conjecture of Ryser about Hadamard Circulant matrices, Lin. Alg. Appl., 437(2012), 2877–2886.

[4] R. Euler, L. H. Gallardo and O. Rahavandrainy, Combinatorial properties of circulant Hadamard matrices, A panorama of mathematics: pure and applied, Contemp. Math. 658, 9–19, Amer. Math. Soc., Providence, RI, 2016.

[5] A. Hedayat and W. D. Wallis, Hadamard matrices and their applications, Ann. Statist., 6(1978), 1184–1238.

[6] L. Gallardo, On a special case of a conjecture of Ryser about Hadamard circulant matrices, Appl. Math. E-Notes, 12(2012), 182–188.

[7] L. H. Gallardo, New duality operator for complex circulant matrices and a conjecture of Ryser, Electron. J. Combin., 23(2016), Paper 1.59, 10 pp.

[8] L. H. Gallardo, Ryser's conjecture under eigenvalue conditions, Math. Commun., 24(2019), 233–242.

[9] B. Logan and M. J. Mossinghoff, Double Wieferich pairs and circulant Hadamard matrices, J. Comb. Math. Comb. Comput., 101(2017), 145–156.

[10] F. J. MacWilliams, Orthogonal circulant matrices over finite fields, and how to find them, J. Combinatorial Theory Ser. A, 10(1971), 1–17.

[11] M. Matolcsi, A Walsh-Fourier approach to the circulant Hadamard conjecture, Algebraic design theory and Hadamard matrices, Springer Proc. Math. Stat., 133, Springer, Cham, (2015), 201–208.

[12] D. B. Meisner, On a construction of regular Hadamard matrices, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei, Mat. Appl. 3, 9(1992), 233–240.

[13] Y. Y. Ng, Cyclic Menon Difference Sets, Circulant Hadamard Matrices and Barker Sequences, Master Thesis, The University of Hong Kong, 36 pp., December 1993.

[14] K. H. Leung, B. Schmidt, New restrictions on possible orders of circulant Hadamard matrices, Designs, Codes and Cryptography 64(2012), 143–151.

[15] H. J. Ryser, Combinatorial Mathematics. The Carus Mathematical Monographs, No. 14 Published by the Mathematical Association of America; distributed by John Wiley and Sons, Inc., xiv+154 pp., New York 1963.

[16] R. J. Turyn, Character sums and difference sets, Pac. J. Math., 15(1965), 319–346.