© Algebra and Discrete Mathematics
Volume **33** (2022). Number 1, pp. 30–37
DOI:10.12958/adm1791

RESEARCH ARTICLE

Ryser's conjecture under linear constraints

L. H. Gallardo

Communicated by V. A. Artamonov

Abstract. There are no nontrivial circulant Hadamard matrices provided that the entries satisfy some linear relations.

Introduction

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

If $H = \mathrm{circ}(h_1, \ldots, h_n)$ is a circulant Hadamard matrix of order n then its *representer* polynomial is the polynomial $R(x) := h_1 + h_2 x + \cdots + h_n x^{n-1}$.

No one has been able, despite several deep computations (see [12]), to discover any other circulant Hadamard matrix. Ryser proposed in 1963 (see [2, p. 97], [16]) the conjecture of the non-existence of these matrices when $n > 4$. Ryser's conjecture has since attracted many attention [1, 3–7, 9–13, 15, 18].

2020 MSC: 11R18, 15B34, 11A07.

Key words and phrases: circulant matrices, Hadamard matrices, sums of roots of unity, unit circle, cyclotomic fields.

Schmidt and Leung results [9–11] helped Logan and Mossinghoff [12] to obtain the nice result that up to order $4 \cdot 10^{30}$ there are only 4489 undecided values of n (thus the Conjecture holds for very large orders). In this paper we are not able to obtain any progress on new values of n for which the Conjecture holds. Our approach is much more modest, we will work, instead, on a simple generalization of some results of Brualdi, detailed below.

We are aware of only two results in which the Conjecture is proved for an infinity of n's. Brualdi [1] proved the conjecture in 1965 for every n provided H is symmetric, and Turyn [18] proved the conjecture for all n's of the form $n = 4p^{2m}$ where p is an odd prime number and m is a positive integer.

We may think of the result of Brualdi as proving that the existence of a circulant Hadamard matrix $H := \mathrm{circ}(h_1, \ldots, h_n)$ of order $n \geqslant 4$, such that the entries h_j satisfy the following set of $n/2 - 1$ (by Lemma 1 $n = 4h^2$ with h odd) linear equations

$$h_{n-k} - h_{k+2} = 0, \text{ for } k = 0, \ldots n/2 - 2, \tag{1}$$

implies that $n = 4$.

The conjecture being very difficult, we have only tried to find some simple sufficient conditions. For example, in most of our preceding papers (c.f. the bibliography), we focused, mainly, in the behavior of the eigenvalues of a possible circulant Hadamard matrix H of order n (or its orthogonal version $K := H/\sqrt{n}$). Our new contribution in the present paper is based in working directly with congruences on the entries of the first row of H (or of some appropriate sub-matrix of H), in a more general way than in the special case [5]. There, we asked that $C := A(H) + B(H)/2$ be *symmetric*. Some details on the matrix C are showed below. For more, see Lemma 3, as well as the first few lines of the proof of Theorem 1. On the other hand, in the present paper, our conditions ask for a more general kind of *symmetry* on the matrix C.

Thus, in the present paper, we assume that the entries of a possible circulant Hadamard H with more that 4 rows, satisfy some linear relations, and that the matrix C satisfy some symmetric property (see Condition 1). Then we build a contradiction. These contradiction proves the non-existence of H. This explains why we are unable to obtain new values of n for which there is no circulant Hadamard matrices of order n.

More precisely, in the present paper, we will require a condition analogue to (1) stated in terms of entries of special sub-matrices of H. We replace the set of equations (1), by a set of $n/4 - 1$ congruences modulo 2,

depending on some of the entries of a circulant matrix of order $n/2$ associated to H, namely $C := (A + B)/2$, where A and B are $n/2 \times n/2$ block sub-matrices of H defined (see details in Lemma 3) by

$$H = \begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

Write $C := \mathrm{circ}(c_1, \ldots, c_{n/2})$. Observe that (see Lemma 4) C has exactly $n/4$ nonzero entries c_{t_j} in its first row, with $1 \leqslant t_1 < t_2 < \cdots < t_{h^2} \leqslant 2h^2$. Put $D := \{c_{t_k} \mid 2 \leqslant k \leqslant h^2\}$. Recall that by Lemma 1, $n = 4h^2$ with h odd.

Our condition follows.

Condition 1. One has $t_1 = 1$, $c_{t_1} = -1$, and $c_{h^2+1} = 0$. Moreover, if $n > 4$, then for each of the $h^2 - 1$ elements $c_{t_k} \in D$ we have

(a)
$$\{t_k + h^2 \mid 1 < t_k \leqslant h^2\} = \{t_m \mid h^2 + 1 \leqslant t_m \leqslant 2h^2\}. \tag{2}$$

(b) Let $G_1 := \{k \mid 2 \leqslant k \leqslant h^2, 1 < t_k \leqslant h^2, \text{ and } c_{t_k} = c_{t_k+h^2}\}$. One has

$$\sharp G_1 \geqslant h(h-1)/2. \tag{3}$$

Part (a) of our condition ask roughly for a kind of *symmetric repartition*, relative to the entry in position h^2 of the nonzero entries of the first row of the circulant matrix C, that has order $2h^2$. For example, taking $t_1 = 2$, and assuming that $t_1 \leqslant h^2$, we ask in (2) that $c_{h^2+2} \in \{-1, 1\}$.

Since all h_j's are in $\{-1, 1\}$ and for all $k = 1, \ldots, 2h^2$, one has $c_k = (h_k + h_{k+n/2})/2$, so that $c_{t_k} \in \{-1, 1\}$, we may think of (a) as linear conditions on some of the h_j's, the entries of H.

Condition 1 already hold (trivially) for the known circulant Hadamard matrix H_9, for which the corresponding C, say C_9, is equal to $\mathrm{circ}(-1, 0)$. We might think that we prove that the matrix H_9 is the unique circulant Hadamard matrix with these properties.

More precisely, our main result is the following:

Theorem 1. *Let $H = \mathrm{circ}(h_1, \ldots, h_n)$ be a circulant Hadamard matrix of order $n \geqslant 4$. Then $n = 4$, provided that Condition 1 hold.*

Unfortunately, Condition 1 do not allow one to obtain new specific values of n for which Ryser's conjecture holds.

The necessary tools for the proof of the theorem are given in section 1. The proof of Theorem 1 is presented in section 2. For a matrix M with complex entries, we let M^* denote the transpose conjugate matrix of M.

Also, we let I_k denote the identity matrix of order k. For a finite set S, we let $\sharp S$ denote the number of elements of S.

1. Tools

The following is well known. See, e.g., [8, p. 1193], [14, p. 234], [18, pp. 329-330] for the first lemma and [2, p. 73] for the second.

Lemma 1. *Let H be a regular Hadamard matrix of order $n \geqslant 4$, i.e., a Hadamard matrix whose row and column sums are all equal. Then $n = 4h^2$ for some positive integer h. Moreover, the row and column sums are all equal to $\pm 2h$ and each row has $2h^2 \pm h$ positive entries and $2h^2 \mp h$ negative entries. If H is circulant then h is odd.*

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

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

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

Lemma 3. *Let M be a circulant matrix of even order n and with first row $R_1 = [m_1, \ldots, m_n]$. Then*

(a)
$$M = \begin{bmatrix} A(M) & B(M) \\ B(M) & A(M) \end{bmatrix}$$
where $A(M), B(M)$ are the matrices of order $\frac{n}{2}$, with subscripts (mod n), defined by $A(M) = (a_{i,j})$, $B(M) = (b_{k,\ell})$, where $i, j, k, \ell = 1, \ldots, n/2$, and $a_{i,j} = m_{j-i+1}$, $b_{k,\ell} = m_{\ell+n/2-k+1}$.

(b) *The matrix $A(M) + B(M)$ is circulant.*

The following lemma counts useful things and is important for the proof of the theorem.

Lemma 4. *Let H be a circulant Hadamard matrix of order $n > 1$. Let A and B be the $n/2$ square matrices defined in Lemma 3. Let $M := \frac{A+B}{2}$. 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, up to change H by $-H$, that would permute b and c one has*

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

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

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

Proof. Since $H/\sqrt{n}$ is orthogonal one has from Lemma 3: $AA^* + BB^* = nI_{n/2}$ and $AB^* + BA^* = 0$. It follows then that

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

One has

$$M = circ\left(\frac{h_1 + h_{n/2+1}}{2}, \ldots, \frac{h_{n/2} + h_n}{2}\right). \tag{5}$$

Observe, from (4), 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

$$n/4 = b + c. \tag{6}$$

Compute now the sum S of all entries in row 1 of M:

$$S = \sum_{i=1}^{n/2} \frac{h_i + h_{n/2+i}}{2} = \frac{1}{2}\sum_{i=1}^{n} h_i = \frac{\sqrt{n}}{2}. \tag{7}$$

But $S = b - c$ since zeros do not contribute to the sum, thus it follows from (7) that

$$b - c = \frac{\sqrt{n}}{2}. \tag{8}$$

From (6) and (8) we get (b) and (c). Since the total number of entries in the first row of M is equal to $n/2$ we have

$$n/2 = a + b + c, \tag{9}$$

thereby obtaining also (a). This finishes the proof of the lemma. □

The next lemma (see [17, Lemma 8.6]) is frequently used in the theory of group representations.

Lemma 5. *Let $c_1, \ldots, c_r$ be r complex numbers of absolute value 1. If $|c_1 + \cdots + c_r| = r$, then $c_1 = \cdots = c_r$.*

2. Proof of Theorem 1

Assume that $n > 4$. Observe that H is regular since H is circulant. In particular, Lemma 1, implies that $n = 4h^2$ for some positive odd integer

$h > 1$, so that n is even. Write $H = \mathrm{circ}(h_1, \ldots, h_n)$ and let $R(x)$ be the representer polynomial of H. Let $C := (A(H) + B(H))/2$ obtained from Lemma (3) applied to $M := H$. Thus C is a circulant matrix of order $2h^2$ with all its entries in $\{-1, 0, 1\}$. Moreover, by block multiplication we deduce from $HH^* = I_n$ that, with $A := A(H)$ and $B := B(H)$, one has

$$AA^* + BB^* = 4h^2 I_{2h^2},\ AB^* + BA^* = 0. \tag{10}$$

By adding both equations in (10) we get

$$CC^* = h^2 I_{2h^2}. \tag{11}$$

Let $S(x)$ be the representer polynomial of $C = \mathrm{circ}(c_1, \ldots, c_{2h^2})$. By Condition 1 we can assume that $c_1 = -1$, and that $c_{h^2+1} = 0$. Put $\omega := \exp(2\pi i/2h^2) = \exp(\pi i/h^2)$. By Lemma 2 and (11) one has $S(\omega) = ha$ where a is a complex number on the unit circle, i.e.,

$$|a| = 1. \tag{12}$$

In other words we have

$$ha = c_1 + c_2\omega + \cdots + c_{2h^2}\omega^{2h^2-1}. \tag{13}$$

Lemma (4) implies that there are h^2 values of $j = 1, \ldots, 2h^2$ such that $c_j = 0$. Put $z_1 := c_1$ and let denote by z_{t_j} with $j = 2, \ldots, h^2$ the remaining (nonzero) terms in the right hand side of (13). In other words: we have $1 < t_2 < \cdots < t_{h^2} \leqslant 2h^2$, with $z_{t_j} := c_{t_j}\omega^{t_j-1}$.

Observe that $c_{h^2+1} = 0$ means that for all $k = 2, \ldots, h^2$ one has $t_k - 1 \neq h^2$. Thus, from (2), $\omega^{h^2} = -1$, and $c_{h^2+1} = 0$, we get

$$ha = z_1 + \sum_{k=2}^{h^2} (c_{t_k} - c_{t_k+h^2})\omega^{t_k-1}. \tag{14}$$

Put $L := \{k \mid 1 < t_k \leqslant h^2\}$, and $d := \sharp L$. By (2) one sees that

$$d = (h^2 - 1)/2. \tag{15}$$

Put $G_2 := L \backslash G_1$. By (3) and(15) it follows that $\sharp G_2 \leqslant (h-1)/2$. From Condition 1 (b) one sees that (14) becomes

$$ha = -1 + 2 \cdot \sum_{k \in G_2} z_{t_k}. \tag{16}$$

In more detail: since $k \in G_2 \iff c_{t_k+h^2} \neq c_{t_k}$, and both c_{t_k} and $c_{t_k+h^2}$ are ± 1, one has $-c_{t_k+h^2} = c_{t_k}$.

By (12) $|a| = 1$, and for each j one has $|z_{t_j}| = 1$. Thus, we apply the triangle inequality to (16). From (3) we get

$$h = |ha| \leqslant 1 + 2 \cdot \sharp G_2 \leqslant h. \tag{17}$$

Therefore, (17) implies that

$$\sharp G_2 = (h-1)/2. \tag{18}$$

Put $S := \sum_{k \in G_2} z_{t_k}$. Since $|z_{t_k}| = 1$, (18) implies that

$$|S| \leqslant (h-1)/2. \tag{19}$$

But, (16) says that $S = (ha+1)/2$. Thus

$$|S| = |ha+1|/2 \geqslant (1/2) \cdot ||ha| - |1|| = (h-1)/2 \tag{20}$$

since $|a| = 1$.

From (19) and (20) one gets

$$|S| = (h-1)/2. \tag{21}$$

From (18) and (21) we obtain that Lemma 5, applied to the set $\{z_{t_k} \mid k \in G_2\}$ with $r := (h-1)/2$ implies that

$$z_{t_k} = z_{t_\ell} \text{ for all } k \neq \ell \in G_2. \tag{22}$$

Thus (22) and (18) implies that $h = 3$. But, it is known [12] that there are no circulant Hadamard matrices of order 36.

Thus our assumption $n > 4$ fails, and we have then

$$n = 4. \tag{23}$$

This finishes the proof of Theorem 1 and the conjecture is settled, under Condition 1.

References

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

[2] P. J. Davis, *Circulant matrices*, 2nd ed., New York, NY: AMS Chelsea Publishing, xix, 1994.

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

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

[5] L. Gallardo, *On a special case of a conjecture of Ryser about Hadamard circulant matrices*, Appl. Math. E-Notes **12**, 2012, pp.182-188.

[6] L. H. Gallardo, *New duality operator for complex circulant matrices and a conjecture of Ryser*, Electron. J. Combin. **23**, N.**1**, Paper 1.59, 2016, 10 pp.

[7] L. H. Gallardo, *Ryser's conjecture under eigenvalue conditions*, Math. Commun. **24**, 2019, N.**2**, pp.233-242.

[8] A. Hedayat, W. D. Wallis, *Hadamard matrices and their applications*, Ann. Statist. **6**, N.**6**, 1978, pp.1184-1238.

[9] K. H. Leung, B. Schmidt, *The field descent method*, Des. Codes Cryptogr. **36**, N.**2**, 2005, pp.171-188.

[10] K. H. Leung, B. Schmidt, *New restrictions on possible orders of circulant Hadamard matrices*, Des. Codes Cryptogr. **6**4, N.**1-2**, 2012, pp.143-151.

[11] K. H. Leung, B. Schmidt, *The anti-field-descent method*, J. Combin. Theory Ser. A **1**39, 2016, pp.87-131.

[12] B. Logan, M. J. Mossinghoff, *Double Wieferich pairs and circulant Hadamard matrices*, J. Comb. Math. Comb. Comput. **101**, 2017, pp.145-156.

[13] 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, pp.201-208.

[14] D. B. Meisner, *On a construction of regular Hadamard matrices*, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei, **9**, Mat. Appl. **3**, N.**4**, 1992, pp.233-240.

[15] Y. Y. Ng, *Cyclic Menon Difference Sets, Circulant Hadamard Matrices and Barker sequences*, Master Thesis, The University of Hong Kong, December 1993.

[16] 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., New York 1963.

[17] J.-P. Serre, *Finite Groups: An Introduction*. Surveys of Modern Mathematics, No. 10. International Press, Somerville, MA; Higher Education Press, Beijing, 2016.

[18] R. J. Turyn, *Character sums and difference sets*, Pac. J. Math. **15** 1965, pp.319-346.

Contact information

Luis H. Gallardo Université de Bretagne Occidentale, UMR CNRS 6205, Laboratoire de Mathématiques de Bretagne Atlantique, 6, Av. Le Gorgeu, C.S. 93837, Cedex 3, F-29238 Brest, France
E-Mail(*s*): Luis.Gallardo@univ-brest.fr

Received by the editors: 02.04.2021
and in final form 27.05.2021.