RAD HRVATSKE AKADEMIJE ZNANOSTI I UMJETNOSTI
MATEMATIČKE ZNANOSTI

A. Domic and L. H. Gallardo

On Ryser's conjecture

Manuscript accepted for publication

This is a preliminary PDF of the author-produced manuscript that has been peer-reviewed and accepted for publication. It has not been copy-edited, proofread, or finalized by Rad HAZU Production staff.

ON RYSER'S CONJECTURE

ANTUN DOMIC, LUIS H. GALLARDO

ABSTRACT. We provide new sufficient conditions under which Ryser's conjecture holds.

1. INTRODUCTION

Let A be a square matrix of order n with real coefficients. We denote by A^t the transpose of the matrix A. For any pair of rows R_i, R_j of A, we denote by $\langle R_i, R_j \rangle$ the usual scalar product. A *circulant* matrix $A := \mathrm{circm}(a_1, \dots, a_n)$ of order n is a matrix of order n whose first row is $[a_1, \dots, a_n]$ and in which each row after the first is obtained by a cyclic shift of its predecessor by one position. For example, the second row R_2 of A is $[a_n, a_1, \dots, a_{n-1}]$. With $\pi := \mathrm{circm}(0, 1, 0, \dots, 0)$, one has that R_2 is the first row of πA.

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 orthogonal. A *circulant Hadamard* matrix of order n is a circulant matrix that is also Hadamard. Besides the two trivial matrices of order 1, $H_1 := \mathrm{circm}(1)$ and $H_2 := -H_1$, the remaining 8 known circulant Hadamard matrices are $H_3 := \mathrm{circm}(1, -1, -1, -1), H_4 := -H_3, H_5 := \mathrm{circm}(-1, 1, -1, -1), H_6 := -H_5, H_7 := \mathrm{circm}(-1, -1, 1, -1), H_8 := -H_7, H_9 := \mathrm{circm}(-1, -1, -1, 1), H_{10} := -H_9$.

No other circulant Hadamard matrices are known. Ryser conjectured in 1963 (see [19], [1, p. 97]) that no such matrices exist when $n > 4$. Previous work on the conjecture include [2, 3, 6, 7, 8, 9, 11, 13, 15, 16, 20].

If $H = \mathrm{circm}(h_1, \dots, h_n)$ is a circulant Hadamard matrix of order n, then its *representer* polynomial is

$$R(x) := h_1 + h_2 x + \cdots + h_n x^{n-1}.$$

2010 *Mathematics Subject Classification.* 11B30, 15B34, 11C20.

Key words and phrases. Circulant matrices, Hadamard matrices, Eigenvalues, Eigenvectors, Gram matrices.

Let $H = \operatorname{circm}(h_1, \ldots, h_n)$ be a circulant Hadamard matrix of order $n \geq 4$. Define

$$E_1 := \operatorname{circm}(h_1, h_3, h_5, \ldots, h_{n-1}), \quad E_2 := \operatorname{circm}(h_2, h_4, h_6, \ldots, h_n).$$

When $n = 4$, both E_1 and E_2 have rank equal to 1 (as their determinant is 0, see the matrices $H_3, \ldots, H_{10}$).

Two other interesting properties of E_1 and E_2 when $n = 4$ are the following:

Remark 1.1. Let $K_1 := \frac{E_1+E_2}{2}$ and $K_2 := \frac{E_1-E_2}{2}$. Then:

(a) K_1 and K_2 are projections.
(b) K_1 and K_2, reduced modulo 2, are symmetric orthogonal matrices.

Property (b) in Remark 1.1 is significant because of a result of McWilliams [12, Corollary 1.8] (see also Lemma 2.1) which states that for $n > 2$, the orthogonal group $\mathbb{O}(n, \mathbb{F}_2)$ intersected with the set of symmetric matrices, consists only of the identity matrix. In other words, $n = 4$ is the only case in which (b) holds.

When a circulant Hadamard matrix of order $n \geq 4$ is such that both E_1 and E_2 are non-singular, it follows from [9] and our Lemma 2.8 (see Section 2) that n must equal 4. The rank-1 property that we consider in the present paper is the first natural case to study in order to make progress on the open case when at least one of E_1, E_2 is singular.

In this paper we prove two results. Essentially, the first shows that for circulant Hadamard matrices of order n, the rank-1 property and properties (a) and (b) in Remark 1.1 hold for $n = 4$ and do not hold when $n > 4$. Our second main result, which follows from a simple characterization of circulant matrices of rank ≤ 2 together with the Plotkin bound for codewords, proves the more general statement that there is no circulant Hadamard matrix of order > 4 in which either one of the submatrices E_1, E_2 has rank 1 while the other has arbitrary rank, or both have rank 2.

More precisely, in this paper we prove the following two theorems.

Theorem 1.2. *Let $H = \operatorname{circm}(h_1, \ldots, h_n)$ be a circulant Hadamard matrix of order $n \geq 4$. Let $E_1 := \operatorname{circm}(h_1, h_3, h_5, \ldots, h_{n-1})$ and $E_2 := \operatorname{circm}(h_2, h_4, h_6, \ldots, h_n)$. We denote by R_j, respectively S_j, the rows of E_1 and E_2, for $j = 1, \ldots, n/2$. Let $G_1 := E_1 E_1^*$ and $G_2 := E_2 E_2^*$ be the Gram matrices of E_1 and E_2. Assume that one of the following conditions holds:*

(a) $\operatorname{rank}(E_1) = 1 = \operatorname{rank}(E_2)$;
(b) *all entries of G_1 and G_2 have the same absolute value;*
(c) *R_1 and R_2 are linearly dependent over $\mathbb{Q}$, and S_1 and S_2 are linearly dependent over $\mathbb{Q}$;*
(d) $|\langle R_1, R_2 \rangle| = |\langle R_1, R_1 \rangle|$, *and* $|\langle S_1, S_2 \rangle| = |\langle S_1, S_1 \rangle|$.

Then $n = 4$.

REMARK 1.3. All statements (a), (b), (c), and (d) of the theorem hold when $n = 4$. Moreover, for any entry e of G_1 or G_2, we have $|e| = 2 = n/2$.

REMARK 1.4. Our results also cover the recent generalization of the circulant Hadamard conjecture [5] by Goyeneche and Turek, since a generalized circulant Hadamard matrix $H(d) := \mathrm{circm}(d, h_2, \ldots, h_n)$ satisfying our hypotheses necessarily has $|d| = 1$.

Our second main result is as follows:

THEOREM 1.5. *With the notation of Theorem 1.2, there is no circulant Hadamard matrix H of order $n > 4$ of either of the following two types:*

(a) *one of E_1, E_2 has rank 1;*
(b) *both E_1 and E_2 have rank 2.*

The needed preliminaries for the proofs are given in Section 2. The proof of Theorem 1.2 is presented in Section 3. The proof of Theorem 1.5 is presented in Section 4.

2. Preliminaries

The following is a result of MacWilliams [12]. It was already used in [10, Theorem 1].

LEMMA 2.1. *The only circulant, symmetric, and orthogonal matrix over the binary field $\mathbb{F}_2$ of order $n > 2$ is the identity matrix I_n.*

The following lemma gives some properties of certain circulant matrices.

LEMMA 2.2. *Let $C := \mathrm{circm}(c_1, \ldots, c_{2k})$ be a circulant matrix of order $2k$ such that the first two rows R_1 and R_2 of C are linearly dependent over $\mathbb{Q}$, and such that $c_j^2 = 1$ for all $j = 1, \ldots, 2k$. Then there exist $a, b \in \{-1, 1\}$ such that for all $s = 1, \ldots, k$ we have $c_{2s-1} = a$ and $c_{2s} = b$. Moreover, exactly one of the following cases holds:*

(a) *$R_1 = R_2$, and $c_1 = c_2 = \cdots = c_{2k} = a = b$.*
(b) *$R_1 = -R_2$, $c_1 = c_3 = \cdots = c_{2k-1} = a$, $c_2 = c_4 = \cdots = c_{2k} = b$, and $a \neq b$.*

Moreover, if case (b) holds, then

$$c_1 + c_2 + \cdots + c_{2k} = 0.$$

PROOF. Since R_2 is a multiple of R_1 and each entry of C is ± 1, there are two cases to consider: (1) $R_1 = R_2$ and (2) $R_1 = -R_2$.

In case (1), comparing the first entries of R_1 and R_2 gives $c_{2k} = c_1$, and comparing the remaining entries shows that $c_1 = c_2 = c_3 = \cdots = c_{2k-1}$. Thus all entries of R_1 are equal, say to $a \in \{-1, 1\}$. Hence case (a) holds.

In case (2), a similar argument shows that (b) holds. Then $a \neq b$, so that $\{a, b\} = \{-1, 1\}$. Hence,

$$c_1 + c_2 + \cdots + c_{2k} = (a + b)k = 0.$$

□

The following lemma gives some properties of certain circulant matrices of rank 2.

LEMMA 2.3. *Let $D := \operatorname{circm}(d_1, \ldots, d_{2k})$ be a circulant matrix of order $2k \geq 6$ and rank 2 such that $d_j^2 = 1$ for all $j = 1, \ldots, 2k$. Assume that the first two rows of D,*

$$v = (d_1, d_2, d_3, \ldots, d_{2k-2}, d_{2k-1}, d_{2k}),$$

and

$$w = (d_{2k}, d_1, d_2, \ldots, d_{2k-3}, d_{2k-2}, d_{2k-1}),$$

are $\mathbb{Q}$-linearly independent. Let $u = av + bw$ be any row of D, where $a, b \in \mathbb{Q}$. Assume that

$$s := d_1 + d_2 + \cdots + d_{2k-1} + d_{2k} \neq 0.$$

Then $a + b = 1$.

PROOF. For simplicity (the proof in the general case is similar), we may assume that u is the third row of D, so that

$$u = (d_{2k-1}, d_{2k}, d_1, \ldots, d_{2k-4}, d_{2k-3}, d_{2k-2}). \tag{2.1}$$

Since $u = av + bw$, with indices taken modulo $2k$, we have for all $j = 1, \ldots, 2k$:

$$d_j = a\, d_{j+2} + b\, d_{j+1}. \tag{2.2}$$

Summing over all j in (2.2) gives

$$s = a\, s + b\, s. \tag{2.3}$$

As $s \neq 0$, equation (2.3) implies that $a + b = 1$, as claimed. □

LEMMA 2.4. *Let $h_k, h_\ell, h_m \in \{-1, 1\}$. Assume that for some rational numbers $a, b \in \mathbb{Q}$ satisfying*

$$a + b = 1, \tag{2.4}$$

we have

$$h_k = a\, h_\ell + b\, h_m. \tag{2.5}$$

Then either

$$h_k = h_\ell = h_m, \tag{2.6}$$

or

$$(a, b) \in \{(0, 1), (1, 0)\}. \tag{2.7}$$

PROOF. Assume first that $ab \neq 0$. It suffices to prove that $h_\ell = h_m$, since if this holds then (2.5) and (2.4) give

$$h_k = (a+b)h_\ell = h_\ell. \tag{2.8}$$

To prove $h_\ell = h_m$, assume without loss of generality that

$$h_\ell = 1, \quad h_m = -1. \tag{2.9}$$

From (2.5) we obtain

$$h_k = a - b. \tag{2.10}$$

If $h_k = 1$, then together with (2.4) we find $b = 0$, a contradiction to $ab \neq 0$. Similarly, if $h_k = -1$ we find $a = 0$, again a contradiction. Thus $h_\ell = h_m$.

If $ab = 0$, then (2.4) implies (2.7). □

LEMMA 2.5. *Let $C = \operatorname{circm}(c_1, \ldots, c_{2k})$ be a circulant matrix with entries in $\{-1, 1\}$, of order $2k \geq 6$, such that the first row of C is equal to the third. Let $s = c_1 + \cdots + c_{2k}$. Then*

$$s \in \{0, 2k, -2k\}.$$

PROOF. Comparing the first and third rows of C gives $c_j = c_{j-2}$ for all j (indices modulo $2k$). Hence, all odd-indexed c_j are equal to some $c \in \{-1, 1\}$, and all even-indexed c_j are equal to some $d \in \{-1, 1\}$. Therefore, $s = k(c+d)$, which yields $s \in \{0, 2k, -2k\}$. This proves the claim. □

We recall that a *regular* Hadamard matrix H is a Hadamard matrix whose row and column sums are all equal to some integer s. We then say that H is *s-regular.*

The following two lemmas are well known; see, e.g., [4, p. 1193], [14, p. 234], [20, pp. 329–330].

LEMMA 2.6. *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 being $(-2h)$-regular). In the $2h$-regular case, each row has $2h^2 + h$ positive entries and $2h^2 - h$ negative entries; in the $(-2h)$-regular case, each row has $2h^2 - h$ positive entries and $2h^2 + h$ negative entries.*

LEMMA 2.7. *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:*

(a) *All eigenvalues $R(s)$ of H, where $s \in \{1, w, w^2, \ldots, w^{n-1}\}$, satisfy*
$$|R(s)| = \sqrt{n}.$$

(b) *The vector $v := [1, \ldots, 1] \in \mathbb{R}^n$ is an eigenvector of H with associated eigenvalue λ, where either $\lambda = \sqrt{n}$ or $\lambda = -\sqrt{n}$. If $\lambda = -\sqrt{n}$, then v is an eigenvector of $-H$ with associated eigenvalue $-\lambda = \sqrt{n}$.*

The following lemma is important for the proof of the theorems.

Lemma 2.8. *Let* $H := \mathrm{circm}(h_1, \ldots, h_n)$ *be a circulant Hadamard matrix, let* $E_1 := \mathrm{circm}(h_1, h_3, h_5, \ldots, h_{n-1})$*, and* $E_2 := \mathrm{circm}(h_2, h_4, h_6, \ldots, h_n)$*. Then*

$$\sum_{\substack{j\neq 1\\ 1\leq j\leq n/2}} \langle R_1, R_j\rangle + \sum_{\substack{j\neq 1\\ 1\leq j\leq n/2}} \langle S_1, S_j\rangle = \sum_{\substack{j\neq 1\\ 1\leq j\leq n}} \langle T_1, T_j\rangle = 0, \tag{2.11}$$

where R_j*,* S_j*, and* T_j *denote the* j*-th row of* E_1*,* E_2*, and* H*, respectively.*

Proof. The result follows from the equality

$$\langle R_1, R_j\rangle + \langle S_1, S_j\rangle = \langle T_1, T_{2j-1}\rangle, \tag{2.12}$$

since two distinct rows of H are orthogonal. □

Lemma 2.9. *Let* $H := \mathrm{circm}(h_1, \ldots, h_n)$ *be a circulant Hadamard matrix, let* $E_1 := \mathrm{circm}(h_1, h_3, h_5, \ldots, h_{n-1})$*, and* $E_2 := \mathrm{circm}(h_2, h_4, h_6, \ldots, h_n)$*. Let*

$$\lambda_1 := h_1 + h_3 + \cdots + h_{n-1}, \quad \lambda_2 := h_2 + h_4 + \cdots + h_n,$$

be the real eigenvalues of E_1 *and* E_2 *associated with the eigenvector* $v_0 := [1, \ldots, 1] \in \mathbb{R}^{n/2}$*. Then* $\lambda_1\lambda_2 = 0$*, so that we may assume, without loss of generality (possibly replacing* H *by* πH*), that*

$$h_1 + h_3 + \cdots + h_{n-1} = 0, \quad |h_2 + h_4 + \cdots + h_n| = \sqrt{n}. \tag{2.13}$$

Proof. With the same notation as in Lemma 2.8, put

$$a := \sum_{\substack{j\neq 1\\ 1\leq j\leq n/2}} \langle R_1, R_j\rangle, \quad b := \sum_{\substack{j\neq 1\\ 1\leq j\leq n/2}} \langle S_1, S_j\rangle.$$

Since $h_j^2 = 1$ for all j, we have

$$\langle R_1, R_1\rangle = \frac{n}{2} = \langle S_1, S_1\rangle.$$

Thus,

$$a + \frac{n}{2} = \langle R_1, \sum_{1\leq j\leq n/2} R_j\rangle = \langle R_1, \lambda_1 v_0\rangle = \lambda_1^2,$$

and

$$b + \frac{n}{2} = \langle S_1, \sum_{1\leq j\leq n/2} S_j\rangle = \langle S_1, \lambda_2 v_0\rangle = \lambda_2^2.$$

By Lemma 2.8 we have $a + b = 0$. Adding the two equations above gives

$$\lambda_1^2 + \lambda_2^2 = n.$$

Moreover, Lemma 2.7 implies

$$\lambda_1 + \lambda_2 = h_1 + h_2 + \cdots + h_n \in \{\sqrt{n}, -\sqrt{n}\}.$$

These two relations together yield $\lambda_1\lambda_2 = 0$, as claimed. □

In order to prove our second theorem, we recall a special case of the Plotkin bound (see [17], [18]) as well as a simple corollary of it involving Hadamard matrices.

Lemma 2.10 (Plotkin bound, special case). *Let $V = \mathbb{F}_2^k$, and let C be a finite subset of a subspace W of dimension m. Let d be the minimum distance in C, namely*

$$d = \min_{\substack{x,y\in C\\ x\neq y}} H(x,y),$$

where $H(x,y)$ denotes the Hamming distance between x and y, i.e., the number of coordinates equal to 1 in $x+y$. Let $A_2(m,d)$ be the maximum size of a subset S of some m-dimensional subspace of V having minimum distance d. If d is even and $2d > m$, then

$$A_2(m,d) \leq 2\left\lfloor \frac{d}{2d-m} \right\rfloor.$$

Lemma 2.11. *Let $H = (H_{i,j})$ be a Hadamard matrix of order $n > 2$. If a submatrix L of H of size $a \times b$ contains only 1's (or only -1's), then $ab \leq n$.*

Proof. Without loss of generality, assume that all entries of L are equal to 1. Let $1 \leq i_1, \ldots, i_a \leq n$ and $1 \leq j_1, \ldots, j_b \leq n$ be indices such that the entries $(L_{r,s})$ of L, with $1 \leq r \leq a$ and $1 \leq s \leq b$, satisfy

$$L_{r,s} = H_{i_r, j_s}.$$

Let $R_{i_1}, \ldots, R_{i_a}$ be the corresponding rows of H, and $T_{j_1}, \ldots, T_{j_b}$ the corresponding columns of H. Put $C = \{R_{i_1}, \ldots, R_{i_a}\}$.

For any pair of rows R_{i_h}, R_{i_k} in C (say R_{i_1}, R_{i_2}), define: (a) $x_{1,2}$ as the number of columns T_k with $k \notin \{j_1, \ldots, j_b\}$ in which $H_{i_1,k} = H_{i_2,k}$; (b) $y_{1,2}$ as the number of such columns in which $H_{i_1,k} \neq H_{i_2,k}$. Thus,

$$x_{1,2} + y_{1,2} = n - b, \tag{2.14}$$

while the orthogonality of R_{i_1} and R_{i_2} implies

$$b + x_{1,2} - y_{1,2} = \langle R_{i_1}, R_{i_2} \rangle = 0. \tag{2.15}$$

From (2.14) and (2.15) we obtain

$$y_{1,2} = \frac{n}{2}. \tag{2.16}$$

In other words,

$$H(R_{i_1}, R_{i_2}) = \frac{n}{2}, \tag{2.17}$$

since all entries of L are equal to 1.

We have thus proved that the minimum Hamming distance d in C satisfies

$$d = \frac{n}{2}. \tag{2.18}$$

Let $m = n - b$. Observe that the set C has a elements. With the notation of Lemma 2.10, we have by definition of $A_2(m, d)$ that

$$A_2(m,d) \geq a \tag{2.19}$$

by choosing the subset $S = C$. Since H is Hadamard and $n > 2$, the order n is a multiple of 4. Hence (2.18) implies that d is even. Moreover, $2d = n > m = n - b$, so that (2.19) and Lemma 2.10 imply

$$a \leq 2 \left\lfloor \frac{n/2}{b} \right\rfloor. \tag{2.20}$$

Multiplying (2.20) by b, we obtain

$$ab \leq 2b \left\lfloor \frac{n/2}{b} \right\rfloor \leq n. \tag{2.21}$$

This proves the result. □

3. Proof of Theorem 1.2

Proof. We claim that it suffices to prove that (c) implies $n = 4$ and that (d) implies $n = 4$. To justify this, we prove the following statements:

(1) If (a) holds, then (c) holds;
(2) If (b) holds, then (d) holds.

Assume that (a) holds. Observe that R_1 and R_2 are both nonzero and that there exists a nonzero real number a such that

$$R_1 = a\, R_2. \tag{3.22}$$

From (3.22), comparing the first coordinates, we obtain $a = \frac{h_1}{h_{n-1}} \in \{-1, 1\}$. Hence $a \in \mathbb{Q}$, and therefore R_1 and R_2 are linearly dependent over $\mathbb{Q}$. Similarly, S_1 and S_2 are linearly dependent over $\mathbb{Q}$. This proves that (a) implies (c).

Assume that (b) holds. Then the absolute values of the entries $(1, 1)$ and $(1, 2)$ of G_2 are equal, that is,

$$|\langle S_1, S_1\rangle| = |\langle S_1, S_2\rangle|. \tag{3.23}$$

Similarly,

$$|\langle R_1, R_1\rangle| = |\langle R_1, R_2\rangle|. \tag{3.24}$$

It follows from (3.23) and (3.24) that (b) implies (d).

We now prove that (c) implies $n = 4$. By Lemma 2.6, we have $n = 4h^2$ for some positive integer h. By Lemma 2.9, we may assume that the $2h^2$ entries of E_1 sum to 0, that is,

$$h_1 + h_3 + \cdots + h_{n-1} = 0. \tag{3.25}$$

It follows from (3.25) that E_1 has exactly h^2 entries equal to 1 and h^2 entries equal to -1. Replacing H by $-H$ if necessary, we may assume that H is $2h$-regular. Hence, using (3.25), we deduce that

$$h_2 + h_4 + \cdots + h_n = 2h. \tag{3.26}$$

Since by Lemma 2.6, the first row of H contains exactly $2h^2 + h$ entries equal to 1, and h^2 of them already appear in E_1, it follows that E_2 has $h^2 + h$ entries equal to 1 in its first row S_1. Similarly, S_1 has $h^2 - h$ entries equal to -1.

On the other hand, by Lemma 2.2 (a), applied to $C = E_2$ with $k = h^2$, all $2h^2$ entries of S_1 are equal to some $a \in \{-1, 1\}$. Hence:

(i) If $a = 1$, then all $2h^2$ entries of S_1 are equal to 1, so that

$$2h^2 = h^2 + h, \tag{3.27}$$

which implies $h^2 = h$, and hence $h = 1$.

(ii) If $a = -1$, then all $2h^2$ entries of S_1 are equal to -1, so that

$$2h^2 = h^2 - h, \tag{3.28}$$

which is impossible.

It remains to consider case (b) of Lemma 2.2, applied to $C = E_2$ with $k = h^2$. This case cannot occur, since it would imply that

$$h_2 + h_4 + \cdots + h_n = 0, \tag{3.29}$$

which contradicts (3.26). This proves that (c) implies $n = 4$.

We now show that (d) implies (c). Assume that (d) holds. Observe that

$$|\langle R_2, R_2\rangle| = \frac{n}{2} = |\langle R_1, R_1\rangle|. \tag{3.30}$$

It follows from (d) and (3.30) that

$$|\langle R_1, R_2\rangle|^2 = |\langle R_1, R_1\rangle| \cdot |\langle R_2, R_2\rangle|. \tag{3.31}$$

Thus equality holds in the Cauchy–Schwarz inequality, and therefore R_1 and R_2 are linearly dependent over $\mathbb{R}$. As in (3.22), it follows that they are in fact linearly dependent over $\mathbb{Q}$. Similarly, S_1 and S_2 are linearly dependent over $\mathbb{Q}$. This proves the claim.

Since (d) implies (c) and (c) implies $n = 4$, we conclude that (d) implies $n = 4$. This completes the proof. □

4. Proof of Theorem 1.5

Proof. Assume, by contradiction, that H is a circulant Hadamard matrix with $n > 4$. By Lemma 2.9, we may assume that (2.13) holds. Moreover, replacing H by $-H$ if necessary, we may assume that $h_2 + h_4 + \cdots + h_n$ is positive. Namely, the following hold:

$$h_1 + h_3 + \cdots + h_{n-1} = 0, \tag{4.32}$$

and

$$h_2 + h_4 + \cdots + h_n = \sqrt{n}. \tag{4.33}$$

By Lemma 2.6, we have $n = 4h^2$. Let L be the submatrix of H formed by the intersection of rows $1, 5, \ldots, 4h^2 - 3$ and columns $1, 5, \ldots, 4h^2 - 3$.

Assume that $\operatorname{rank}(E_1) = 1$. Apply Lemma 2.2 to $C = E_1$. If case (a) of Lemma 2.2 holds, then

$$h_1 = h_3 = \cdots = h_{n-1}, \tag{4.34}$$

and (4.32) gives the contradiction $(n/2)\, h_1 = 0$. Hence case (b) of Lemma 2.2 holds, and thus

$$h_1 = h_5 = \cdots = h_{n-3} \in \{-1, 1\}. \tag{4.35}$$

It follows from (4.35) that L is a submatrix of H of size $h^2 \times h^2$ whose entries are all equal. Therefore, Lemma 2.11 implies that

$$h^2 \cdot h^2 \le 4h^2. \tag{4.36}$$

Thus $h^2 \le 4$. Since h is odd by Lemma 2.6, we obtain $h = 1$, hence $n = 4$, a contradiction.

Assume that $\operatorname{rank}(E_2) = 1$. Apply Lemma 2.2 to $C = E_2$. If case (b) of Lemma 2.2 holds, then

$$h_2 + h_4 + \cdots + h_n = 0, \tag{4.37}$$

which contradicts (4.33). Hence case (a) of Lemma 2.2 holds, and we obtain

$$h_2 = h_4 = \cdots = h_n = 1. \tag{4.38}$$

It follows that E_2 is a submatrix of H of size $2h^2 \times 2h^2$ whose entries are all equal to 1. By (4.38) combined with (4.33), we obtain

$$2 \cdot h^2 = 2 \cdot h \tag{4.39}$$

that is, $h = 1$ and $n = 4$, a contradiction.

This proves the theorem in case (a).

We now prove case (b). Assume that both E_1 and E_2 have rank 2. By Lemma 2.6, $n = 4h^2$ with h odd.

Let v, w be the first two rows of $E_2 = \operatorname{circm}(h_2, h_4, \ldots, h_{4h^2})$. We claim that v and w are linearly independent over $\mathbb{Q}$. Otherwise, applying Lemma 2.2 to $C = E_2$ yields

$$h_2 = h_4 = \cdots = h_{4h^2} = 1, \tag{4.40}$$

since case (b) of Lemma 2.2 is impossible by (4.33). From (4.40) and (4.33), we obtain

$$2h^2 = 2h, \tag{4.41}$$

that is, $h = 1$, a contradiction. This proves the claim.

Let u be the third row of E_2. Since v and w form a basis of the $\mathbb{Q}$-vector space generated by the rows of E_2, there exist $a, b \in \mathbb{Q}$ such that

$$u = av + bw. \tag{4.42}$$

Let $S = h_2 + h_4 + \cdots + h_{4h^2}$. Since, by (4.33), $S \neq 0$, Lemma 2.3 with $D = E_2$ and $s = S$ implies that

$$a + b = 1. \tag{4.43}$$

Let h_{2j} be any entry of u, with $j = 2h^2 - 1, 2h^2, 1, 2, \ldots, 2h^2 - 2$. By (4.42), we have

$$h_{2j} = ah_{2j+4} + bh_{2j+2}. \tag{4.44}$$

Assume that $ab \neq 0$. By Lemma 2.4, (4.44) implies

$$h_{2j} = h_{2j+4} = h_{2j+2} \tag{4.45}$$

for all such j. Thus all entries of v are equal. By (4.33), they must be equal to 1, and then (4.33) becomes (4.41), yielding again the contradiction $h = 1$. Therefore, $ab = 0$. By (4.43), the only possibilities in (4.42) are $w = u$ when $(a, b) = (0, 1)$ and $v = u$ when $(a, b) = (1, 0)$.

Since w and u are consecutive rows of E_2, the same argument used above to prove that v and w are $\mathbb{Q}$-linearly independent shows that w and u are also $\mathbb{Q}$-linearly independent. Hence $w \neq u$, so this case is impossible. Therefore, $v = u$. By Lemma 2.5 with $C = E_2$ and $s = S$, we obtain

$$S \in \{0, 2h^2, -2h^2\}. \tag{4.46}$$

But by (4.33), $S = 2h$. Hence (4.46) implies again (4.41), yielding the contradiction $h = 1$.

This completes the proof. ∎

Acknowledgements.

We thank the referee for careful reading and for detailed suggestions that lead to a better presentation of the paper.

References

[1] P. J. Davis, *Circulant matrices*, 2nd ed., New York, NY: AMS Chelsea Publishing, xix, 250 p. 1994.

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

[3] R. Euler, L. H. Gallardo, 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.

[4] A. Hedayat, W. D. Wallis, *Hadamard matrices and their applications*, Ann. Statist. **6**, no. 6, 1978, 1184–1238.

[5] D. Goyeneche, O. Turek, *A generalization of circulant Hadamard and conference matrices*, Linear Algebra Appl. **569**, 2019, 241–265.

[6] J. Jedwab, S. Lloyd, *A note on the nonexistence of Barker sequences*, Des. Codes Cryptogr. **2**, no. 1, 1992, 93–97.
[7] L. Gallardo, *On a special case of a conjecture of Ryser about Hadamard circulant matrices*, Appl. Math. E-Notes **12**, 2012, 182-188.
[8] L. H. Gallardo, *New duality operator for complex circulant matrices and a conjecture of Ryser*, Electron. J. Combin. **23**, 2016, no. 1, Paper 1.59, 10 pp.
[9] L. Gallardo, *A real eigenvector of circulant matrices and a conjecture of Ryser*, Appl. Math. E-Notes **20**, 2020, 155-157.
[10] L. H. Gallardo, *On Ryser's Conjecture: Modulo* 2 *approach*, Appl. Math. E-Notes **21**, 2021, 220-224.
[11] L. H. Gallardo, *Under a mild condition, Ryser's Conjecture holds for every* $n := 4h^2$ *with* $h > 1$ *odd and non square-free*, Math. Commun. **26,1**, 2021, 1-8.
[12] F. J. MacWilliams, Orthogonal circulant matrices over finite fields, and how to find them, J. Combinatorial Theory Ser. A 10(1971), 1–17.
[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, 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, no. 4, 1992, 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, 36 pp.
[16] K. H. Leung, B. Schmidt, *New restrictions on possible orders of circulant Hadamard matrices*, Designs, Codes and Cryptography **64**, 2012, 143–151.
[17] M. Plotkin, *Binary Codes with Specified Minimum Distance*, Univ. Penn. Res. Div. Report 51-20 (1951), IRE Trans. Inform. Theory, **6**, (1960), 445–450.
[18] J. Quistorff, *Some remarks on the Plotkin bound*, Electron. J. Combin. Research paper **N6**, 2003, 8 pp.
[19] 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 xiv+154 pp
[20] R. J. Turyn, *Character sums and difference sets*, Pac. J. Math. **15** 1965, pp. 319–346.

Naslov

Prvi autor, drugi autor i treći autor

Sažetak. Hrvatski prijevod sažetka.

Antun Domic
Kepler Computing and Stanford University, U. S. A.
E-mail: domic@stanford.edu

Luis H. Gallardo
Univ. Brest
UMR CNRS 6205
Laboratoire de Mathématiques de Bretagne Atlantique,
F-29238 Brest
France
E-mail: Luis.Gallardo@univ-brest.fr