MATHEMATICAL COMMUNICATIONS
Math. Commun. **24**(2019), 235–244

Ryser's conjecture under eigenvalue conditions

Luis H. Gallardo*

Department of Mathematics, University of Brest, 6 Avenue Victor Le Gorgeu, C. S. 93 837, 29 238 Brest Cedex 3, France

Received December 13, 2018; accepted May 20, 2019

Abstract. We prove the nonexistence of a circulant Hadamard matrix H of order n, under technical conditions on the eigenvalues of H, when n has only two odd prime divisors and in the general case.

AMS subject classifications: 11R18, 15B34, 11A24, 11A07, 11B30

Key words: Hadamard matrices, circulant matrices, eigenvalues, cyclotomic polynomials, congruences

1. 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 of first row $[a_1, \ldots, a_n]$, 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 $[a_n, a_1, \ldots, a_{n-1}]$. 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. A *circulant Hadamard* matrix of order n is a circulant matrix that is Hadamard. The 10 known circulant Hadamard matrices are: $H_1 := \mathrm{circ}(1), H_2 := -H_1, H_3 := \mathrm{circ}(1, -1, -1, -1), H_4 := -H_3, H_5 := \mathrm{circ}(-1, 1, -1, -1), H_6 := -H_5$, $H_7 := \mathrm{circ}(-1, -1, 1, -1), H_8 := -H_7, H_9 := \mathrm{circ}(-1, -1, -1, 1)$, and $H_{10} := -H_9$.

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

Despite several deep computations (see [3]) no one has been able to discover any other circulant Hadamard matrix. In 1963, Ryser proposed (see [19], [6, p. 97]) the conjecture of the non-existence of these matrices when $n > 4$. Previous work on the conjecture includes [7, 8, 9, 10, 12, 13, 14, 15, 17, 20, 22].

Ryser's conjecture (there are no circulant Hadamard matrices of order> 4) has been studied by several different methods. The first special case done (by Brualdi [4] in 1965) assumed that all eigenvalues of $H := circ(h_1, \ldots, h_n)$, a circulant Hadamard matrix of order $n > 4$, were real; i.e., that H is symmetric. Below, $\omega(k)$ counts the number of distinct prime divisors of the positive integer k.

Besides Brualdi's result, all other known results are only partial results for particular n's obtained by deep methods. For example, the known case $\omega(n) = 2$ is a consequence of some results of Turyn [22]. More precisely, Turyn proved that if $n > 4$, then $n = 4h^2$ with odd h and h must have more than two distinct prime

*Corresponding author. *Email address:* Luis.Gallardo@univ-brest.fr (L. H. Gallardo)

factors, so that n must have the following form $n = 4p_1^{2a_1}p_2^{2a_2}\cdots p_s^{2a_s}$ with $s \geq 2$, and, say, $p_1 < p_2$ two odd prime numbers. In particular, n cannot be a power of 2, n cannot be a power of 3, and n cannot be a product of powers of 2 by powers of 3. This latter result was also reproved by Schmidt and Smith [20] as a special case of their more general results.

Moreover, when $\omega(n) = 3$, i.e., when $n = 4p_1^{2a_1}p_2^{2a_2}$ as before with $s = 2$, it is known that the odd prime divisors p_1, p_2 of n must be Wieferich's pairs, i.e, $p_1^{p_2-1} \equiv 1 \pmod{p_2^2}$ and $p_2^{p_1-1} \equiv 1 \pmod{p_1^2}$. These results allowed some computer calculations, from which the result essentially follows for increasing numerical values of n. However, these methods seems to be unable to produce general proofs (say, a proof of the conjecture for an infinity of n's with $\omega(n) \geq 3$).

It is worth reporting that Schmidt and Leung (see, e.g., [13, 15]) obtained the best known results about this problem. Their approach uses sophisticated technical results about group rings, characters and cyclotomic fields. Their main results might be roughly described as: (a) results that reduce the number of cases to consider in order to prove the full conjecture, and (b) results that can be used further to practical important things as to exclude specific numerical values of n as possible candidates to be the order of a possible circulant Hadamard matrix H. The reason why (b) is possible is that in the above results the possible prime divisors of n play an important role.

The present paper is much more modest; our results are obtained by using elementary methods, and we are (unfortunately) not specialists in this subject, so that we are only able to contribute to part (a) of the above discussion. More precisely, we believe that our results in the present paper may be useful to reduce the number of cases to consider in order to advance to the proof of the full conjecture. However, our results cannot contribute to the second, more concrete and important, part (b). Besides perhaps in Lemma 1, that might be an interesting more general contribution, the exact reason of the lack of results of type (b) is as follows: Condition 1 does not depend only on the prime divisors of n , so that our first two theorems cannot contribute to (b). Moreover, our latter theorem cannot contribute to (b) since in both hypothesis in Theorem 3 the prime divisors of h are not used.

We describe now our results. Our general approach is (a) to assume that a possible circulant Hadamard matrix H of order n exists, (b) to consider cases in which some conditions on the eigenvalues of H matrix imply contradictions.

The first part of our results is about the case $\omega(n) = 3$. The second part is about the general case $\omega(n) \geq 2$.

The technical condition required in the case $\omega(n) = 3$ reads:

Condition 1. *Let H be a circulant Hadamard matrix of order $n = 4p^{2a}q^{2b}$, where $p \neq q$ are odd prime numbers, and a, b are positive integers. Let $R(x)$ be the representer polynomial of H. One has*

$$d < \varphi(n)/2,$$

where $d = \deg(R(x) \pmod{\Phi_n(x)})$, $\Phi_n(x)$ is the n-th cyclotomic polynomial and φ is Euler's function.

Our first result comes from known properties of the cyclotomic polynomial $\Phi_n(x)$, when n has only two distinct odd prime divisors [21], together with a variant of our argument used in [7]:

Theorem 1. *There is no circulant Hadamard matrix that satisfies Condition 1 when a, b are large enough. Large enough means that a, b satisfy*

$$p^a q^b > (p+q-1)(pq)! \exp(pq) + 1.$$

Remark 1. *Lemma 5 that gives the crucial upper bound for the proof of Theorem 1 does* not *depend on Condition 1; thus, besides being new, it might have an interest in itself.*

It appears that our method above cannot deal with small exponents. Thus, besides Condition 1, more conditions are expected in the smallest case $a = 1$ and $b = 1$:

Theorem 2. *There is no circulant Hadamard matrix H that satisfies Condition 1 when $a = b = 1$, provided that*

$$\{R(\omega^t) : 1 \le t \le n,\ R(\omega^t) \notin \mathbb{R}\} = \{R(\omega^k) : 1 \le k \le n,\ \gcd(k,n) = 1\} \qquad (1)$$

if H has some non-real eigenvalue.

We checked by a simple computation that 4 of the 8 circulant Hadamard 4×4 matrices, namely, H_5, H_6, H_9 and H_{10}, all satisfy Condition (1).

More generally, for any possible n, not just for an n with $\omega(n) = 3$, some conditions on the eigenvalues of H guarantee the non-existence.

Theorem 3. *There is no circulant Hadamard matrix H of order $n = 4h^2$, where $h > 1$ is an odd number, provided both conditions below hold:*

(a) $\mathrm{Tr}(H^2) = 0$, *where* Tr *means the trace.*

(b) $A := \frac{H+H^*}{2}$ *is positive-semidefinite, where H^* is the transpose conjugate (transpose here) of H.*

We checked by a computation that for 2 of the 8 circulant Hadamard matrices with $n = 4$, namely, for H_6 and for H_{10}, both conditions on Theorem 3 hold.

The main tools necessary for the proofs are given in Section 2. The proofs of Theorem 1, Theorem 2, and Theorem 3 are given in Section 3, Section 4, and Section 5, respectively.

2. Tools

The following result attributed to Migotti (in 1883) in [21] is important for our work.

Lemma 1. *The cyclotomic polynomial $\Phi_{mn}(x)$ has all its coefficients in $\{-1, 0, 1\}$.*

A special useful case we require is

Lemma 2. *Let $h = p_1^{r_1} p_2^{r_1}$ be a positive integer with two distinct odd prime factors $p_1 \neq p_2$. Then*

$$\Phi_{4h^2}(t) = \Phi_{p_1 p_2}(-t^{2{p_1}^{2r_1-1}{p_2}^{2r_2-1}}).$$

Thus from Lemmas 1 and 2 one has:

Lemma 3. *The cyclotomic polynomial $\Phi_{4p^{2a}q^{2b}}(x)$ has all its coefficients in $\{-1, 0, 1\}$, where $p \neq q$ are two odd prime numbers.*

The following lemma of Agou [1, 2] is crucial.

Lemma 4. *Let R be a ring with 1. Let $S = x^n - s_1 x^{n-1} - \cdots - s_n \in R[x]$ be a polynomial of degree $n > 0$. Let $k > 0$ be a positive integer. Let $T = \sum_{j=0}^{n-1} t_{k,j} x^j$ be the remainder of the Euclidean division (long division) of the monomial $M = x^{k+n-1}$ by the polynomial S in $R[x]$. Then for $j = 0, \ldots, n-1$ one has*

$$t_{k,j} = \sum_{\substack{u_1+2u_2+\cdots+nu_n=k+n-j-1,\\ u_i \geq 0, i=1,\ldots,n}} \left(\frac{(u_1 + \cdots + u_n - 1)!}{u_1! \cdots u_n!} \sum_{t=0}^{j} u_{n-t} \right) s_1^{u_1} \cdots s_n^{u_n}.$$

For $j = 0$ we get

$$t_{k,0} = s_n \left(\sum_{\substack{u_1+2u_2+\cdots+nu_n=k-1,\\ u_i \geq 0, i=1,\ldots,n}} \frac{(u_1 + \cdots + u_n)!}{u_1! \cdots u_n!} s_1^{u_1} \cdots s_n^{u_n} \right)$$

if $k \geq 1$ and

$$t_{k,0} = 0$$

if $-n + 1 \leq k - 1 < 0$ (provided $n > 1$) and assuming that $0^0 = 1$.

We proceed then to prove the following lemma that is key to the proof of Theorem 1.

Lemma 5. *Let H be a circulant Hadamard matrix of order $n = 4p^{2a}q^{2b}$, where $p \neq q$ are prime numbers and a, b are non-negative integers. Let $R(x)$ be the representer polynomial of H. Let $S(x)$ be the remainder of the Euclidean division of $R(x)$ by the cyclotomic polynomial $\Phi_n(x)$. Let $d > 0$ be a positive integer such that $d \leq \deg(S)$. Let $C(d, S)$ be the coefficient of the monomial x^d that appears in $S(x)$. Then*

$$|C(d, S)| \leq 2(p + q - 1)(pq)! \exp(pq) + 2.$$

Proof. Let

$$l := n/(2pq). \tag{2}$$

Write $\Phi_n(x) = x^{\varphi(n)} - \sum_{j=1}^{\varphi(n)} c_j x^{\varphi(n)-j}$. By Lemma 2, $\Phi_n(x) = \Phi_{pq}(-x^l)$ so that $c_j = 0$ for all j not a multiple of l. More precisely,

$$c_j = 0 \text{ for all } j \neq vl, \text{ where } 0 \leq v \leq K := \varphi(pq) = (p-1)(q-1). \tag{3}$$

Let $\omega \in \mathbb{C}$ be an n-th primitive root of 1. Since $\omega^{n/2} = -1$, so that $\omega^{n/2+i} = -\omega^i$ one can write $R(\omega) = r_0 + r_1\omega + \cdots + r_{n/2-1}\omega^{n/2-1}$, where each $r_j \in \{-2, 0, 2\}$ by Lemma 3. Define then the *reduced representer* polynomial $V(x)$ of H by $V(x) := \sum_{j=0}^{n/2-1} r_j x^j$. Clearly, $S(x)$ is also the remainder of the Euclidean division of $V(x)$ by $\Phi_n(x)$. Put $M_k := x^{k+\varphi(n)-1}$, for each $k \in \{1, \ldots, n/2 - \varphi(n)\}$. Therefore, defining $V_1(x)$ by

$$V(x) = r_0 + r_1 x + \cdots + r_{\varphi(n)-1}x^{\varphi(n)-1} + V_1(x)$$

one has

$$C(d, S) = r_d + \sum_{k=1}^{n/2-\varphi(n)} r_{k+\varphi(n)-1}t_{k,d},$$

where $t_{k,d}$ is the remainder of the Euclidean division of the monomial M_k of $V_1(x)$ by $\Phi_n(x)$.

Since $d > 0$ and $Kl = \varphi(n)$, from Lemma 4 and our discussion above (see (3)) one has

$$t_{k,d} = \sum_{\substack{lu_l+2lu_{2l}+\cdots+Klu_{Kl}=k-1+\varphi(n)-d,\\ u_{il}\geq 0, i=1,\ldots,K}} \left(\frac{(u_l+\cdots+u_{Kl}-1)!}{u_l!\cdots u_{Kl}!}\sum_{t=0}^{d} u_{Kl-t}\right) c_l^{u_l}\cdots c_{Kl}^{u_{Kl}}. \quad (4)$$

Define then the integer X by

$$k + \varphi(n) - d - 1 = lX. \quad (5)$$

Therefore, $t_{k,d} = 0$ for all other possible k's for which $k+\varphi(n)-d-1$ is not divisible by l. In other words,

$$C(d, S) = r_d + \sum_{X_{min}}^{X_{max}} r_{lX+d+1-\varphi(n)}t_{k,d}, \quad (6)$$

where X_{min} (respectively, X_{max}) is the minimum (respectively, the maximum) of integers X's that satisfy (5) when k goes from 1 to $n/2 - \varphi(n)$.

Observe that

$$X_{max} - X_{min} \leq \frac{n/2-\varphi(n)}{l} = pq - (p-1)(q-1) = p + q - 1. \quad (7)$$

and that from (5) and (4) we get

$$t_{k,d} = \sum_{\substack{u_l+2u_{2l}+\cdots+Ku_{Kl}=X,\\ u_{il}\geq 0, i=1,\ldots,K}} \left(\frac{(u_l+\cdots+u_{Kl}-1)!}{u_l!\cdots u_{Kl}!}\sum_{t=0}^{d} u_{Kl-t}\right) c_l^{u_l}\cdots c_{Kl}^{u_{Kl}}. \quad (8)$$

We want to bound above $|t_{k,d}|$. In order to do that, observe first that for the whole range $v = 0, \ldots, K$ one has $c_{vl} \in \{-1, 0, 1\}$ by Lemma 3 so that $|c_l^{u_l}\cdots c_{Kl}^{u_{Kl}}| \leq 1$, we also have $\sum_{t=0}^{d} u_{Kl-t} \leq u_l + u_{2l} + \cdots + u_{Kl}$ so that

$$0 \leq \left(\frac{(u_l+\cdots+u_{Kl}-1)!}{u_l!\cdots u_{Kl}!}\sum_{t=0}^{d} u_{Kl-t}\right) \leq \frac{(u_l+\cdots+u_{Kl})!}{u_l!\cdots u_{Kl}!} \quad (9)$$

Trivially, for the whole range of v one has $u_{vl}! \geq 1$ since $u_{vl} \geq 0$. Thus from (8) and (9) we get

$$|t_{k,d}| \leq \sum_{\substack{u_l+2u_{2l}+\cdots+Ku_{Kl}=X,\\ u_{il}\geq 0, i=1,\ldots,K}} (u_l + \cdots + u_{Kl})! \tag{10}$$

Since $0 \leq u_l+\cdots+u_{Kl} \leq u_l+2u_{2l}+\cdots+Ku_{Kl} = X$, an upper bound of $|u_l+\cdots+u_{Kl}|$ will be the maximal possible X, say X_2 in the range of k, i.e., $1 \leq k \leq n/2 - \varphi(n)$. Thus from (5) one immediately has

$$lX_2 \leq (n/2 - \varphi(n)) + \varphi(n) - d - 1 \leq n/2. \tag{11}$$

Since $X \leq X_2$, by rewriting (11) and using (2) one gets

$$X \leq X_2 \leq n/(2l) = pq. \tag{12}$$

Put Θ the number of terms in the sum in (10). The u_{ml}'s in the sum of the right-hand side of (10) are non-negative integers such that

$$u_l + 2u_{2l} + \cdots + Ku_{Kl} = X,$$

thus $|u_l| \leq X$, $|u_{2l}| \leq X/2, \ldots, |u_{Kl}| \leq X/K$. By using (12) it follows that

$$\Theta \leq X^K/K! \leq exp(X) \leq exp(X_2) \leq exp(pq). \tag{13}$$

Thus from (10), and (12), (13), it follows that

$$|t_{k,d}| \leq \Theta \cdot X_2! \leq (pq)!exp(pq). \tag{14}$$

We are ready to prove the result. Observing that for any j, $|r_j| \leq 2$, from (6), (7), and (14) it follows that

$$|C(d,S)| \leq 2 + 2(p+q-1)(pq)!exp(pq).$$

This finishes the proof of the lemma. □

The following is well known. See, e.g., [11, p. 1193], [18, p. 234], [22, pp. 329-330] for the first lemma and [6, p. 73] for the second.

Lemma 6. *Let H be a regular Hadamard matrix of order $n \geq 4$, 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 and $2h^2 \mp h$ negative entries.*

Lemma 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 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, they satisfy*

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

More generally and for more details see [6].

Lemma 8. *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 a smaller positive argument. 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 $F^* = (\frac{\omega^{(i-1)(j-1)}}{n^{1/2}})$ is the conjugate of the Fourier matrix. Moreover, F is unitary.*

The next lemma is [16, Theorem 3], which also appeared as [5, Theorem 3.1]. It was already used in [9].

Lemma 9. *Let A be a circulant matrix of order $n > 0$ with entries in $\{0, 1\}$. Let m be an even positive integer. Assume that $A^m \in \mathbb{Z}I + \mathbb{Z}J$. Then $A \in \{0, P, J, J - P\}$, where P is a permutation matrix of order n.*

Using Lemma 6 and Lemma 9 Craigen and Kharaghani [5, Lemma 4] proved:

Lemma 10. *Let H be a circulant Hadamard matrix of order $n > 0$ such that for some positive number m*

$$H^m = n^{\frac{m}{2}} I.$$

Then $n \leq 4$.

We can also write the case $n > 1$ of Lemma 10 as

Lemma 11. *Let H be a circulant Hadamard matrix of order $n > 1$, and let $K := H/\sqrt{n}$. Assume that for some positive number m the orthogonal matrix K has multiplicative order m. Then $n = 4$.*

3. Proof of Theorem 1

Proof. Assume the existence of a circulant Hadamard matrix H that satisfies the hypothesis. By Brualdi's result in the introduction (see [4]) we can take H to be nonsymmetrical. This implies that

$$\text{some eigenvalue of } H \text{ is non-real.} \tag{15}$$

In our special case $n = 4p^{2a}q^{2b}$ with odd prime numbers, say, $p < q$. Write the Euclidean division (long division) of the representer polynomial $R(x)$ of H by the cyclotomic polynomial $\Phi_n(x)$ as

$$R(x) = Q(x)\Phi_n(x) + S(x), \tag{16}$$

with, say, $S(x) = s_d x^d + s_{d-1} x^{d-1} + \cdots + s_1 x + s_0$ so that $d = \deg(S(x))$. Let $\omega \in \mathbb{C}$ be an n-th primitive root of 1. Since by (16) one has $R(\omega) = S(\omega)$, (15) implies that we have $d > 0$. From Lemma 7 one has $R(\omega)R(\overline{\omega}) = 1$, thus

$$S(\omega)S^*(\omega) = n\omega^d, \tag{17}$$

where $S^*(x)$ is the reciprocal polynomial of $S(x)$. From Condition 1 and (17) we get easily $s_0 = s_1 = \cdots = s_{d-1} = 0$ and $s_d^2 = n$. Therefore $S(\omega) = s_d\omega^d$. Now, from Lemma 5 we get

$$p^a q^b = |s_d/2| \leq (p + q - 1)(pq)! \exp(pq) + 1, \tag{18}$$

But, (18) contradicts to hypothesis. This finishes the proof of the theorem. □

4. Proof of Theorem 2

Proof. Assume the existence of a circulant Hadamard matrix H that satisfies the hypothesis. In particular, by Brualdi's result above (see again [4]) we can assume that H has some non-real eigenvalue. In our special case $n = 4p^2q^2$ with odd prime numbers, say, $p < q$. Using the same notation as in Section 3, from Condition 1 and (17) we get as before $s_j = 0$ for $j = 0, \ldots, d-1$ and $s_d^2 = 4p^2q^2$ so that, up to switching q and $-q$, from (17) we obtain

$$S(\omega) = 2qp\omega^d, \text{ and } S^*(\omega) = 2qp.$$

From (16) this implies

$$R(\omega) = 2qp\omega^d. \tag{19}$$

From (19) and Lemma 7 it follows that v^d, where v is any n-th primitive root of 1, are eigenvalues of the orthogonal matrix $M := H/2qp$. Any other eigenvalue λ of M has the form $\lambda = R(\omega^t)/2qp$ with $1 \leq t \leq n$. If λ is real, then it equals 1 or -1 so that it has order at most equal to 2; if λ is non-real, then by the hypothesis $\lambda = R(\omega^k)/2qp$ for some k coprime with n. This means that $\lambda = v^d$ for the n-th primitive root of 1, $v = \omega^k$. Therefore each eigenvalue of M has finite order. In other words, the diagonalizable matrix M (see Lemma 8) has finite multiplicative order. By Lemma 11 this implies the contradiction $n = 4$. This proves the theorem. □

5. Proof of Theorem 3

Proof. Assume the existence of a circulant Hadamard matrix H that satisfies the hypothesis. In particular,

$$n > 4. \tag{20}$$

We can take H of the form $H = \mathrm{circ}(1, h_2, \ldots, h_n)$ with $h_j \in \{-1, 1\}$. Let $B = A^* = A$. Then

$$\mathrm{Tr}(AB) = \mathrm{Tr}(AA^*) = \sum_{i,j} a_{ij}^2.$$

In each row of the circulant matrix A of order n there are, say, t zeros, and thus $n - t$, 1's or -1's. Since $a_{ij} \neq 0$ implies $a_{ij}^2 = 1$, we get

$$\mathrm{Tr}(AB) = n(n - t). \tag{21}$$

But $AB = AA^* = A^2 = \frac{1}{4}(H^2 + H^{*2} + 2HH^*)$. Since H is Hadamard, then we obtain $AB = \frac{1}{4}(H^2 + H^{*2} + 2nI)$, where I is the identity matrix of order n. Taking traces on both sides of the latter equality we get $\mathrm{Tr}(AB) = \frac{1}{4}(2\mathrm{Tr}(H^2) + 2n^2)$ so that using hypothesis (a) we obtain

$$\mathrm{Tr}(AB) = \frac{n^2}{2}. \tag{22}$$

From (21) and (22) it follows that

$$t = \frac{n}{2}. \tag{23}$$

By Lemma 7 the eigenvalues μ of H are of the form $\mu = \sqrt{n}\exp(i\theta)$. It follows then by (b) that the eigenvalues $\lambda = \sqrt{n}\cos(\theta)$ of A have arguments θ in between $-\pi/2$ and $\pi/2$.

Thus $\cos(\theta) \geq 0$ for each eigenvalue of A. We compute $\mathrm{Tr}(AB)$ now by using the eigenvalues of A. One has $\mathrm{Tr}(AB) = \mathrm{Tr}(AA^*) = \mathrm{Tr}(A^2) = \sum_\lambda \lambda^2 = n\sum_\theta \cos(\theta)^2$. Therefore

$$\sum_\theta \cos(\theta)^2 = \frac{\mathrm{Tr}(AB)}{n}. \tag{24}$$

Since $1 \geq \cos(\theta) \geq 0$, one has $\sum_\theta \cos(\theta)^2 \leq \sum_\theta \cos(\theta) = \frac{\mathrm{Tr}(A)}{\sqrt{n}}$. Thus by (24) and since $A = \mathrm{circ}(1, \ldots)$

$$\frac{\mathrm{Tr}(AB)}{n} \leq \frac{\mathrm{Tr}(A)}{\sqrt{n}} = \sqrt{n}. \tag{25}$$

Directly by (22), or alternatively by ((21) and (23)) from (25) we get

$$\frac{n}{2} \leq \sqrt{n}. \tag{26}$$

Thus, in (26) we obtain

$$n \leq 4.$$

This contradicts (20), thereby finishing the proof of the theorem. □

6. Acknowledgement

We thank Bahman Saffari (Babar) for his nice inspiring papers. We are also grateful to the referee for careful reading, great suggestions, pointing out the important works of Schmidt and Leung in this subject, letting know the bibliography items [13, 20] and more importantly, for his suggestions about the scope of the present paper. We are convinced that the paper is now better thanks to his/her suggestions.

References

[1] S. Agou, *Sur les formules explicites intervenant dans la division euclidienne des polynômes et leurs conséquences*, C. R. Acad. Sci. Paris Ser. A-B **273**(1971), A209–A211.

[2] S. Agou, *Sur les formules explicites intervenant dans la division euclidienne des polynômes à coefficients dans un anneau unitaire et applications diverses*, Publ. Dép. Math. (Lyon) **8**(1971), 107–121.

[3] P. Borwein, M. J. Mossinghoff, *Wieferich pairs and Barker sequences, II*, LMS J. Comput. Math. **17**(2014), 24–32.

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

[5] R. Craigen, H. Kharaghani, *On the nonexistence of Hermitian circulant complex Hadamard matrices*, Australas. J. Combin. **7**(1993), 225–227.

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

[7] 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.

[8] R. EULER, L. H. GALLARDO, O. RAHAVANDRAINY, *Combinatorial properties of circulant Hadamard matrices*, in: *A panorama of mathematics: pure and applied*, (C. M. da Fonseca, A. V. Huynh, S. Kirkland, V. K. Tuan, Eds.), Contemp. Math. **658**, AMS, Providence, Rhode Island, 2016, 9–19.

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

[10] L. H. GALLARDO, *New duality operator for complex circulant matrices and a conjecture of Ryser*, Electron. J. Combin. **23**(2016), Article Number P1.59, 10 pp.

[11] A. HEDAYAT, W. D. WALLIS, *Hadamard matrices and their applications*, Ann. Statist. **6**(1978), 1184–1238.

[12] J. JEDWAB, S. LLOYD, *A note on the nonexistence of Barker sequences*, Des. Codes Cryptogr.**2**(1992), 93–97.

[13] K. H. LEUNG, B. SCHMIDT, *The field descent method*, Des. Codes Cryptogr. **36**(2005), 171–188.

[14] K. H. LEUNG, B. SCHMIDT, *New restrictions on possible orders of circulant Hadamard matrices*, Des. Codes Cryptogr. **64**(2012), 143–151.

[15] K. H. LEUNG, B. SCHMIDT, *The anti-field-descent method*, J. Combin. Theory Ser. A **139**(2016), 87–131.

[16] S. L. MA, *On rational circulants satisfying* $A^m = dI + \lambda J$, Linear Algebra Appl. **62**(1984), 155–161.

[17] 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.

[18] D. B. MEISNER, *On a construction of regular Hadamard matrices*, Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl. **3**(1992), 233–240.

[19] H. J. RYSER, *Combinatorial mathematics*, Carus Mathematical Monographs 14, Mathematical Association of America, New York, 1963.

[20] B. SCHMIDT, K. W. SMITH, *Circulant weighing matrices whose order and weight are products of powers of* 2 *and* 3, J. Combin. Theory Ser. A **120**(2013), 275–287.

[21] R. THANGADURAI, *On the coefficients of cyclotomic polynomials*, in: *Cyclotomic fields and related topics*, (S. D. Adhikari, Ed.), Proceedings of the summer school (Pune, 1999), Bhaskaracharya Pratishthana, Pune, 2000, 311–322.

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