Under a mild condition, Ryser's Conjecture holds for every $n := 4h^2$ with $h > 1$ odd and non square-free

Luis H. Gallardo[*]

Univ Brest, UMR CNRS 6 205, Laboratoire de Mathématiques de Bretagne Atlantique, 6, Av. Le Gorgeu, C.S. 93 837, Cedex 3, F-29 238 Brest, France

Received April 4, 2020; accepted November 7, 2020

Abstract. We prove, under a mild condition, that there is no circulant Hadamard matrix H with $n > 4$ rows when $\sqrt{n/4}$ is not square-free. The proof introduces a new method to attack Ryser's Conjecture, that is a long-standing difficult conjecture.

AMS subject classifications: 11R18, 15B34, 11A25, 11A05

Key words: circulant matrices, Hadamard matrices, sums of roots of unity, complex unit circle, cyclotomic fields

1. Introduction

A matrix of order n is a square matrix with n rows. A *circulant* matrix $A := \operatorname{circ}(a_1, \ldots, a_n)$ 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 of its predecessor by one position. For example, the second row of A is $[a_n, a_1, \ldots, a_{n-1}]$. A useful circulant matrix of order n is the matrix J with all its entries equal to 1, i.e., $J := circ(1, \ldots, 1)$. 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 $H_1 := \operatorname{circ}(1), H_2 := -H_1, H_3 := \operatorname{circ}(1, -1, -1, -1), H_4 := -H_3, H_5 := \operatorname{circ}(-1, 1, -1, -1), H_6 := -H_5, H_7 := \operatorname{circ}(-1, -1, 1, -1), H_8 := -H_7, H_9 := \operatorname{circ}(-1, -1, -1, 1), H_{10} := -H_9$.

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

Despite several deep computations (see [14]), no one has been able, to discover any other circulant Hadamard matrix. In 1963 (see [4, p. 97], [19]), Ryser proposed the conjecture of the non-existence of these matrices when $n > 4$. Ryser's conjecture has since attracted much attention [5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 18, 21].

Bernhard Schmidt and collaborators [11, 12, 13] obtained the most important and deep results on the Conjecture, by developing new algebraic tools related to cyclotomic fields and group rings. Let n be the order of a possible circulant Hadamard matrix. Schmidt's results helped Logan and Mossinghoff [14] to obtain the nice result that up to order $4 \cdot 10^{30}$ there are only 4489 undecided values of n.

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

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 [21] 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.

The aim of the present paper is to prove the Conjecture for all n's for which $\sqrt{n/4}$ is divisible by a prime power p^a with $a > 1$, under a mild condition on the eigenvalues of K. Our proof is based on specializing some classical results about sums of roots of unity by Conway and Jones (see [3]).

More precisely, our main result is

Theorem 1. *Let $H = \mathrm{circ}(h_1, \dots, h_n)$ be a circulant Hadamard matrix of order $n \geq 4$. Then $n = 4$ provided $h := \sqrt{n/4}$ is not square-free and provided that some non-real eigenvalue of $K := H/\sqrt{n}$ is an algebraic integer.*

The second condition (on an eigenvalue of K) is important in order to be able to use the Conway and Jones's result. The condition is mild since it concerns just one eigenvalue of K, while it is known [2] that if *all* eigenvalues of K are algebraic integers, then H is actually symmetric and Brualdi's result above applies to prove that $n = 4$. Unfortunately, we do not know how this condition depends on n or on the prime divisors of n, thus our result cannot help to obtain new specific values of n for which the conjecture holds. In particular, we were not able to improve, even for one specific value of n, the results of Schmidt and collaborators mentioned above.

The necessary tools for the proof of the theorem are given in Section 2. The proof of Theorem 1 is presented in Section 3. For the n-th root of unity γ, by $o(\gamma)$ we denote its multiplicative order, i.e. the minimal positive integer m such that $\gamma^m = 1$. For a matrix M with complex entries, by M^* we denote the transpose conjugate matrix of M and $\mathrm{diag}(d_1, \dots, d_n)$ denotes a diagonal matrix of order n.

2. Tools

The following is well known. See, e.g., [10, p. 1193], [16, p. 234], [21, pp. 329-330].

Lemma 1. *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 entries and $2h^2 \mp h$ negative entries. Finally, 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 $v \in \{1, w, w^2, \dots, w^{n-1}\}$, satisfy*

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

In more detail (see [4]), one has

Lemma 3. *Let $C = circ(c_1, \dots, c_n)$ be a circulant matrix of order $n > 0$ with* representer *polynomial $P(t) = c_1 + c_2 t + \dots + c_n t^{n-1}$. Let w be the primitive complex*

n-th root of unity with a smaller positive argument. Then C is diagonalizable and $C = F^*\Delta F$, where $\Delta = \mathrm{diag}(P(1), P(w), \ldots, P(w^{n-1})$ is a diagonal matrix containing the eigenvalues of C and $F^* = (\frac{w^{(i-1)(j-1)}}{n^{1/2}})$ is the transpose conjugate of the Fourier matrix. Moreover, F is unitary.

The following lemma follows from Lemma 2, but it is more useful. We give a short proof below.

Lemma 4. *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. Let $M := (H + J)/2$ and let $S(x)$ be its representer polynomial. Then $2S(x) = R(x) + 1 + x + \cdots x^{n-1}$ and all non-real eigenvalues $S(v)$ of M, where $v \in \{1, w, w^2, \ldots, w^{n-1}\}$, satisfy*

$$|S(v)| = \sqrt{n/4}.$$

Proof. The first statement is trivial. In order to prove the second, observe that by Lemma 1 one has $n = 4h^2$ for some odd positive integer h. Observe that $HH^* = 4h^2I$, $HJ = JH^* = 2hJ$ and $J^2 = nJ$. Thus

$$MM^* = HH^*/4 + (HJ + JH^*)/4 + J^2/4 = h^2I + (h + h^2)J. \tag{1}$$

Diagonalizing both sides of (1), it follows from Lemma 3 that

$$\mu \cdot \overline{\mu} = h^2, \tag{2}$$

where μ is a non-real eigenvalue of M, i.e., $\mu = S(v)$ for some $v \in \{1, w, w^2, \ldots, w^{n-1}\}$, since the diagonal matrix (with the notations of Lemma 3),

$$\Delta := FMF^* = \mathrm{diag}(S(1), S(w), \ldots, S(w^{n-1}) = \mathrm{diag}(2h^2+h, R(w)/2, \ldots, R(w^{n-1})/2), \tag{3}$$

and $|R(w^j)| = 2h$. Equation (3) holds since $FJF^* = \mathrm{diag}(n, 0, \ldots, 0)$. □

We also need the classical result of Kronecker (see e.g., [17, pp. 97-98]) and its special case of cyclotomic extensions (see e.g., [17, Theorem 8.1.10 a)]).

Lemma 5. (a) *The only algebraic integers whose all conjugates lie on the unit circle are the roots of unity.*

(b) *Let $n > 0$ be an even positive integer. Let $L := \mathbb{Q}(w)$, where w is a primitive n-th root of 1, be a cyclotomic extension of the rational numbers. The only algebraic integers in L whose all conjugates lie on the unit circle belong to $\{1, w, \ldots, w^{n-1}\}$.*

The next lemma (see [20, Lemma 8.6]) is frequently used in the theory of group representations. Here, it is useful to finish the proof of Theorem 1.

Lemma 6. *Let $c_1, \ldots, c_\ell$ be ℓ complex numbers of absolute value 1. If*

$$|c_1 + \cdots + c_\ell| = \ell, \text{ then } c_1 = \cdots = c_\ell.$$

We require a special version of [3, Theorem 1]. In order to state it, we need the following definition and lemma.

Definition 1. *Let α, β be n-th roots of unity in $\mathbb{C}$, we say that α and β are equivalent, and write $\alpha \sim \beta$, if $o(\frac{\alpha}{\beta})$ is square-free, where $o(t)$ is the multiplicative order of the n-th root of unity t.*

In the following lemma we give a detailed proof of a particular case of two assertions of Conway and Jones [3], the first (that appears just before the statement of their Theorem 1) is about the above definition, and the second (it is at the beginning of the proof of the same theorem) is about a characterization of the equivalence, crucial for the proof of the theorem. Although these are simple facts, and part (b) of Lemma 7 is not directly used in our proof, they are important as a background in our special case.

Lemma 7. *Let $h > 1$ be an odd number, let $n := 4h^2$, let $a := \operatorname{rad}(n)$ be the greatest square-free divisor of n, let $w = \exp(2\pi i/n)$ and let $\Omega := w^a$. Then*

(a) *The relation $\sim$ defined in Definition 1 is an equivalence relation.*

(b) *The $\mathbb{Q}$-linear map $\sigma : \mathbb{Q}(w) \to \mathbb{Q}(w)$ defined by $\sigma(1) = 1$ and $\sigma(w) := w\Omega$ is an automorphism of $\mathbb{Q}(w)$ that has the following property: Given two integers k, ℓ there exists an integer c such that*

$$\sigma(w^k) = \Omega^c w^k,\ \sigma(w^\ell) = \Omega^c w^\ell \tag{4}$$

is equivalent to

$$w^k \sim w^\ell.$$

Proof. In order to prove (a), observe that for an n-th root of unity α, $\alpha \sim \alpha$ holds since it is equivalent to: $1 = o(1)$ is square-free. If for two n-th roots of unity α, β one has $\alpha \sim \beta$, then $(\alpha/\beta)^k = 1$ for some divisor k of a. Thus $(\beta/\alpha)^k = 1$, so that $\beta \sim \alpha$. If α, β, γ are n-th roots of unity such that $\alpha \sim \beta$ and $\beta \sim \gamma$, then we can assume, without loss of generality, that

$$o(\alpha/\beta) = P_1 P_2 \tag{5}$$

and that

$$o(\beta/\gamma) = P_1 P_3, \tag{6}$$

where P_1, P_2, P_3 are divisors of a with $\gcd(P_1, P_2) = 1 = \gcd(P_1, P_3)$ and $\gcd(P_2, P_3) = 1$. Compute now (using (5) and (6))

$$(\alpha/\gamma)^{P_1P_2P_3} = (\alpha/\beta \cdot \beta/\gamma)^{P_1P_2P_3} = ((\alpha/\beta)^{P_1P_2})^{P_3} \cdot ((\beta/\gamma)^{P_1P_3})^{P_2} = 1 \cdot 1 = 1. \tag{7}$$

It follows from (7) that $\alpha \sim \gamma$, thereby proving part (a) of the lemma. We now prove part (b). Since $\sigma(w) = w^{a+1}$ and $\gcd(a+1, n) = 1$, one sees that σ is an automorphism of $\mathbb{Q}(w)$. This implies that for any integer d one has

$$\sigma(w^d) = w^d \Omega^d. \tag{8}$$

Assume now the existence of an integer c such that (4) holds. It follows then from (8) that $\Omega^k = \Omega^\ell = \Omega^c$. Thus $k = \ell + t_0 n/(a+1)$ for some integer t_0. But, $\gcd(a+1, n) = 1$ so that $t_0 = t(a+1)$ for an integer t. In other words, one has $k - \ell = tn$ so that $w^{k-\ell} = 1$. This proves that $w^k \sim w^\ell$. Assume now that $w^k \sim w^\ell$. Thus

$$w^{(k-\ell)a} = 1. \tag{9}$$

Define $b := n/a$. Since w has order $n = ab$, one gets from (9) that $ab \mid (k-\ell)a$. In other words, we have

$$b \mid k - \ell. \tag{10}$$

But $o(\Omega) = b$, so that $\Omega^{k-\ell} = 1$. This proves that (4) holds for $c := k$. This proves part (b) and finishes the proof of the lemma. □

The following special case of the result of Conway and Jones [3, Theorem 1] that follows from Lemma 7 is crucial.

Lemma 8. *Any vanishing sum S of n-th roots of unity also vanishes when restricted to any equivalent class of the relation $\sim$ defined in Definition 1, i.e., the partial sum of just those terms of S from the given equivalence class vanishes.*

Given a positive integer n by $\mathrm{rad}(n)$ we denote the product of all distinct prime divisors of n.

Lemma 9. *Let $h > 1$ be an odd positive integer. Let $n := 4h^2$. Then the following two statements are equivalent.*

(i)

$$\mathrm{rad}(n) > \sqrt{n/4} + 1, \tag{11}$$

(ii) *h is square-free*

Proof. First of all, observe that (11) is equivalent to

$$h + 1 < 2 \cdot \mathrm{rad}(h). \tag{12}$$

Assume (ii). Then $\mathrm{rad}(h) = h$. Thus (12) holds since (12) is equivalent to $h > 1$. Thus (i) holds. Assume now (i) so that (12) holds. Since $\mathrm{rad}(h)$ divides h, we can write $h = \alpha \cdot \mathrm{rad}(h)$ for some positive odd integer α. We claim that $\alpha = 1$. Assume, on the contrary, that $\alpha > 1$. Then

$$h + 1 = \alpha \cdot \mathrm{rad}(h) + 1 \geq 3 \cdot \mathrm{rad}(h) + 1 > 2 \cdot \mathrm{rad}(h). \tag{13}$$

We see that (13) contradicts (12) . This proves the claim, so that (ii) holds. □

3. Proof of Theorem 1

Proof. Assume that $n > 4$. Put $w := \exp(2\pi i/n)$. Observe that H is regular since H is circulant. In particular, Lemma 1 implies that $n = 4h^2$ for some positive odd integer $h > 1$. Write $H = \mathrm{circ}(h_1, \ldots, h_n)$ and let $R(x)$ be the representer polynomial of H. Put $M := (H+J)/2$ and let $S(x)$ be the representer polynomial of M. Observe that H and $2M$ have the same non-real eigenvalues, since 0 with multiplicity $n-1$ is eigenvalue of J. Thus by hypothesis and by Lemma 4 there exists a non-real eigenvalue α of M/h that belongs to $\mathbb{Z}[w]$, the ring of integers of the cyclotomic field $\mathbb{Q}(w)$, and to the complex unit circle. By Lemma 5 this means that α is a power of w.

Therefore, by Lemma 4 one has that $S(\alpha) = h\alpha$ is an eigenvalue of M, where α is a power of w. In other words, we have for some $c \in \{1, \ldots, n-1\}$, some subset W of $\{1, \ldots, n\}$ and some permutation $\tau : \{1, \ldots, n\} \to \{1, \ldots, n\}$

$$hw^c = \sum_{j \in W} h_{\tau(j)} \omega^{\tau(j)-1}. \tag{14}$$

Dividing both sides of (14) by $-w^c = w^{n/2+c}$ we get for some t with $1 \leq t \leq n$ and some integral exponents $0 \leq e_1 < \cdots < e_t \leq n-1$

$$-h = w^{e_1} + \cdots + w^{e_t} \tag{15}$$

since $h_{\tau(j)}$ belong to $\{-1, 1\}$ and we can replace any negative coefficient by a positive one using again $-1 = w^{n/2}$.

There are four cases:

(a) One has that $e_1 = 0$, and for some j one has $e_j = n/2$. It follows that $w^{e_1} + w^{e_j} = 0$. Thus in (15) $-h$ is a sum of $t-2$ powers of w with no exponent equal to 0 or to $n/2$

(b) One has that $e_1 = 0$, and for no j one has $e_j = n/2$. Thus we get from (15) that $-h-1$ is a sum of $t-1$ powers of w with no exponent equal to 0 or to $n/2$.

(c) One has that $e_1 \neq 0$, and for some j one has $e_j = n/2$. Thus we get from (15) that $-h+1$ is a sum of $t-1$ powers of w with no exponent equal to 0 or to $n/2$.

(d) One has that $e_1 \neq 0$, and for no j one has $e_j = n/2$. In other words, already in (15) one has that $-h$ is a sum of t powers of w with no exponent equal to 0 or to $n/2$.

Write $n = a \cdot b$ with $a := \mathrm{rad}(n)$.

Now in each of the cases we apply Lemma 8 to the corresponding vanishing sum restricted to the equivalent class in which each term w^k is equivalent to 1, i.e., we keep only the terms w^k with $w^k \sim 1$. In other words, the terms w^k for which the multiplicative order $o(w^k)$ of $w^k = w^k/1$ is square-free. This gives a reduced vanishing sum of the form

$$0 = \psi(h)w^n + w^{k_1} + \cdots + w^{k_s}, \tag{16}$$

where $s+1 \leq a$, since a is the biggest divisor of n that is square-free, and with b a divisor of the $\gcd(k_1, \ldots, k_s)$. One has $1 < k_1 < \cdots < k_s < n$ and no k_j is equal to $n/2$.

The value of $\psi(h)$ in terms of h depends on the cases and is as follows.

(1) In cases (a) and (d), $\psi(h) = h$. It follows from (16) that we have

$$h = |-h| = |w^{k_1} + \cdots + w^{k_s}| \leq s \leq a - 1 \tag{17}$$

But, $h > 1$ is not square-free, thus Lemma 9 says that $a - 1 \leq h$. It follows then from (17) that $s = h$ so that

$$|w^{k_1} + \cdots + w^{k_s}| = s. \tag{18}$$

It follows then from (18) and by Lemma 6 that all w^{k_j} are equal. This is impossible. This contradiction shows that $n = 4$.

(2) In case (b), one has $\psi(h) = h + 1$. It follows then from (16) that now we have

$$h + 1 = |-h - 1| = |w^{k_1} + \cdots + w^{k_s}| \leq s \leq a - 1. \tag{19}$$

As before, we have $a - 1 \leq h$. Thus, we get that $h + 1 \leq h$ from (19). This contradiction proves that $n = 4$.

(3) In case (c), one has $\psi(h) = h - 1$. It follows then from (16) that now we have

$$h - 1 = |-h + 1| = |w^{k_1} + \cdots + w^{k_s}| \leq s \leq a - 1. \tag{20}$$

Observe that $h-1$ is even, while $a-1$ is odd. Thus the inequality $h-1 \leq a-1$ that comes from (20) is indeed equivalent to the inequality $h - 1 \leq a - 2$, i.e., to $h \leq a - 1$. But, as before, we have that $a - 1 \leq h$. Thus, we get that $h = a - 1$. But this is impossible since $a = 2\,\mathrm{rad}(h)$ and $\mathrm{rad}(h)$ is a divisor of h. This contradiction proves that $n = 4$. This finishes the proof of the theorem.

□

4. Acknowledgements

We thank Reinhardt Euler for the proof of Lemma 9.

References

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

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

[3] J. H. Conway, A. J. Jones, *Trigonometric Diophantine equations (On vanishing sums of roots of unity)*, Acta arithmetica **30**(1976), 229–240.

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

[5] 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.

[6] 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, D. Van Huynh, S. Kirkland, and V. K. Tuan, Eds.), Contemp. Math. **658**, Amer. Math. Soc., Providence, RI, 2016, 9–19.

[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), Paper 1.59, 10 pp.

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

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

[11] K. H. Leung, B. Schmidt, *The field descent method*, Des. Codes Cryptogr. **36**(2005), 171–188.

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

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

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

[15] M. Matolcsi, *A Walsh-Fourier approach to the circulant Hadamard conjecture*, in: *Algebraic design theory and Hadamard matrices*, (C. J. Colbourn, Ed.) Springer Proc. Math. Stat. 133, Springer, Cham, 2015, 201–208.

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

[17] J. Esmonde, R. Murty, *Problems in algebraic number theory*, Springer-Verlag, New York, 1999.

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

[19] H. J. Ryser, *Combinatorial mathematics*, The Mathematical Association of America, John Wiley and Sons Inc., New York, 1963.

[20] J.-P. Serre, *Finite Groups: An Introduction*, International Press, Somerville, MA; Higher Education Press, Beijing, 2016.

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