New duality operator for complex circulant matrices and a conjecture of Ryser

Luis H. Gallardo

Mathematics
University of Brest
Brest, France

Luis.Gallardo@univ-brest.fr

Submitted: May 6, 2015; Accepted: Mar 10, 2016; Published: Mar 18, 2016
Mathematics Subject Classifications: 11A07, 15A24, 15B34

Abstract

We associate to any given circulant complex matrix C another one $E(C)$ such that $E(E(C)) = C^*$ the transpose conjugate of C. All circulant Hadamard matrices of order 4 satisfy a condition C_4 on their eigenvalues, namely, the absolute value of the sum of all eigenvalues is bounded above by 4. We prove by a "descent" that uses our operator E that the only circulant Hadamard matrices of order $n \geqslant 4$, that satisfy a condition C_n that generalizes the condition C_4 and that consist of a list of $n/4$ inequalities for the absolute value of some sums of four eigenvalues of H, are the known ones.

Keywords: Fourier matrix; Fourier transform; Circulant Hadamard matrices; Ryser's Conjecture

1 Introduction

A complex matrix H of order n is *complex Hadamard* if $HH^* = nI_n$, where I_n is the identity matrix of order n, and if every entry of H is in the complex unit circle. Here, the $()^*$ means transpose and conjugate. When such H has only real entries, so that H is a $\{-1, 1\}-$matrix, H is called *Hadamard*. An $n \times n$ matrix H is circulant, say $H = \mathrm{circ}(h_1, \ldots, h_n)$, if the i-th row H_i of H is given by $H_i = [h_{1-i+1}, \ldots, h_{n-i+1}]$, the subscripts being taken modulo n, for example $H_2 = [h_n, h_1, h_2, \ldots, h_{n-1}]$. For a circulant matrix $H := \mathrm{circ}(h_1, \ldots, h_n)$, the polynomial

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

is called the *representer* polynomial of H. A long standing-conjecture of Ryser (see [15, pp. 134]) is:

Conjecture 1. Let $n \geqslant 4$. If H is a circulant Hadamard matrix of order n, then $n = 4$.

Details about previous results on the conjecture and a short sample of recent related papers are in [16], [8], [7], [14], [2], [3], [5], [4], [12], [11] and the bibliography therein. Some of the papers above contains also computer computations related to the problem. A good source of numerical data about the problem is available in [13].

For the history of the conjecture up to 2012, see [11]; see also [7] that describes the current state of knowledge up to 1993. It is worth consulting more general classic accounts on Hadamard matrices that include some results about the conjecture, in [1] and in [18]. Of course, the conjecture being at the center of several very interesting mathematical subjects, some "false" proofs were also published (see [8] for a description of older attempts, and see [6], for a description of a recent's one). We prove the conjecture under the following mild condition: H satisfies the condition C_n.

Definition 2. A complex circulant matrix C of order $n = 4k$ and representer polynomial $R_C(x)$ satisfies the condition C_n if and only if for all $i = 1, \ldots, k$ one has

$$|\lambda_i + \lambda_{k+i} + \lambda_{2k+i} + \lambda_{3k+i}| \leqslant 2. \tag{1}$$

where the eigenvalues of $K := C/\sqrt{n}$ are defined by $\lambda_j := R_K(\exp(2\pi ij/n))$.

It is easy to check that all 8 circulant Hadamard matrices of order 4 satisfy the condition C_4, namely that the absolute values of the sum of all its eigenvalues is at most 4. Moreover, if a circulant Hadamard matrix H of order $n = 4h^2$ satisfies the condition C_n then by adding all these $n/4$ inequalities in (1) we get the trivial inequality in which "Tr" means "trace", $2h = |\mathrm{Tr}(H/\sqrt{n})| \leqslant n/2 = 2h^2$. Having said that, we will now proceed to the details. It is sufficient to prove the following theorem that is our main result.

Theorem 3. *Let h be an odd positive integer. If there exists a circulant Hadamard matrix H of order $n = 4h^2$ that satisfies the condition C_n then there exists also a circulant Hadamard matrix K of order h^2.*

However, it is better to be a bit more precise.

Corollary 4. *Let $n \geqslant 4$. If H is a circulant Hadamard matrix of order n that satisfies the condition C_n, then $n = 4$.*

In section 2 are collected all the necessary tools. Theorem 9 that describes a kind of "duality operator" may have an interest in itself. The most important of all these tools is Lemma 16 in which we manage the main reduction step for the proof of the theorem. The proof of Theorem 3 appear in section 4. The proof of Corollary 4 appears in section 5.

Thinking to the reader, we added section 3 just after the tools in section 2. Indeed, we believe that even an "informal" account of the main new ideas and general strategy of the proof, merits a special section. Thus, we hope that by just reading this section, and before entering the technical details, the reader, may have (working on an analogy) a rough idea of what is going here.

2 Some tools

The following classical result of Turyn [17] is useful.

Lemma 5. *The order n of a circulant Hadamard matrix H such that $n > 4$, must be of the form $n = 4h^2$, with h an odd integer with at least two distinct prime divisors.*

We recall the definition of the Fourier matrix and of the Fourier transform (see [9, pp. 31–35]):

Definition 6. Let n be a positive integer. Let $w = \exp(2i\pi/n)$.

(a) The Fourier matrix F of order n is defined (note the star in the left-hand member), by
$$\sqrt{n}F^* = V([1, w, w^2, \ldots, w^{n-1}]) = (w^{(i-1)(j-1)}).$$

(b) For a matrix A with m rows and n columns and (i, j) entry equal to $a_{i,j}$, we denote, as usual, by A^T the "transpose" of A i.e., the matrix with n rows and m columns which (i, j) entry is $a_{j,i}$.

(c) Let $P(x) := c_1 + c_2x + \cdots + c_nx^{n-1}$ be a complex polynomial of degree $< n$. The Fourier transform of the vector $c \in \mathbb{C}^n$ defined by $c := [c_1, \ldots, c_n]^T$, is the vector $d := [d_1, \ldots, d_n]^T \in \mathbb{C}^n$ defined by
$$\sqrt{n} \cdot [\overline{c_1}, \ldots, \overline{c_n}] \cdot F = [\overline{d_1}, \ldots, \overline{d_n}],$$
where the $\overline{(\cdot)}$ denotes complex conjugation.

We need two other results, both are simple consequences of the definitions for which we may check [9]. A kind of "double dual" property for complex circulant matrices appears in the next theorem.

Lemma 7. *Let $A = \operatorname{circ}(a_1, \ldots, a_n)$ with representer polynomial $R_A(x) \in \mathbb{C}[x]$. Let $w := \exp(2i\pi/n)$. Set $B := \operatorname{circ}(\lambda_1, \ldots, \lambda_n)$ where $\lambda_j := R_A(w^{j-1})$, $j = 1, \ldots, n$, are the eigenvalues of A in some order. Let $R_B(x) \in \mathbb{C}[x]$ be the representer polynomial of B. Set $b_j := R_B(w^{i-1})$ for all $j = 1, \ldots, n$ be the eigenvalues of B in some order. Then for all $j = 1, \ldots, n$*
$$b_j = n \cdot a_{n-j+2}$$
where the subscripts are considered modulo n. Moreover, if all a_i from $i = 1, \ldots, n$ are real, then $B = B^*$.

Proof. Set $r := \sqrt{n}$. By definition of the Fourier transform (see Definition 6) we have
$$r[\overline{\lambda_1}, \ldots, \overline{\lambda_n}] \cdot F = [\overline{b_1}, \ldots, \overline{b_n}], \quad r[\overline{a_1}, \ldots, \overline{a_n}] \cdot F = [\overline{\lambda_1}, \ldots, \overline{\lambda_n}]$$
where F is the Fourier matrix (see again Definition 6). This implies that
$$[\overline{b_1}, \ldots, \overline{b_n}] = n \cdot [\overline{a_1}, \ldots, \overline{a_n}] \cdot F^2 = n \cdot [\overline{a_1}, \overline{a_n}, \overline{a_{n-1}}, \ldots, \overline{a_2}], \tag{2}$$
since the symmetric matrix $F^2 = \Gamma = (g_{i,j})$ has $g_{1,1} = 1$, $g_{i,j} = 1$ when $i + j = n + 2$ and zeros everywhere else. The result follows by conjugation of both sides of (2). Assume that all a_i's are real. Then it follows that the b_i's are also real. This proves that $B = B^*$. □

Lemma 8. *Let $H := \mathrm{circ}(h_1, \ldots, h_n)$ be a circulant matrix of order $n > 1$, with real entries h_j. Let $w := \exp(2i\pi/n)$. Let $R_H(x)$ be its representer polynomial. Let $\rho := \mathrm{circ}(\lambda_1, \ldots, \lambda_n)$ where $\lambda_j := R_H(w^{j-1})$, for all $j = 1, \ldots, n$. For $i = 1, \ldots, n$, let R_i be the i-th row of ρ. Then for all $j = 1, \ldots, n$ we have*

$$\frac{\langle R_1, R_j\rangle}{n} = m_1^2 + m_2^2 v^{j-1} + \cdots + m_n^2 v^{(j-1)(n-1)}$$

where $v := \overline{w}$, the conjugate of w, $\langle \cdot, \cdot \rangle$ is the hermitian product $\langle x, y\rangle := x_1\bar{y_1} + \cdots + x_n\bar{y_n}$, and $m_j := h_{n-j+2}$ where the subscripts are considered modulo n.

Proof. By Lemma 7, $\rho = n \cdot F^* \mathrm{diag}(h_1, h_n, h_{n-1}, \ldots, h_2)F$, where F is the Fourier matrix. But, $\rho = \rho^*$ so that $\beta := \rho\rho* = \rho^2 = n^2 \cdot F^* \mathrm{diag}(h_1^2, h_n^2, h_{n-1}^2, \ldots, h_2^2)F$. We have also by direct multiplication $\beta = \mathrm{circ}(\langle R_1, R_1\rangle, \ldots, \langle R_1, R_n\rangle)$. Let us define some vectors of length n. For $j \in \{1, 2, \ldots, n\}$ let $e_j := [0, \ldots, 1, 0, \ldots, 0]$ with the 1 being at position j. We compute then

$$\langle R_1, R_j\rangle / \, n = \frac{1}{n} \cdot (e_1 \cdot \beta \cdot e_j) = e_1 \cdot (\sqrt{n}F^*) \cdot \mathrm{diag}(h_1^2, h_n^2, h_{n-1}^2, \ldots, h_2^2) \cdot (\sqrt{n}F) \cdot e_j. \quad (3)$$

Observe that by definition of F we have $e_1 \cdot \sqrt{n}F^* = [1, 1, \ldots, 1]$ so that (3) becomes $\langle R_1, R_j\rangle / \, n = [h_1^2, h_n^2, \ldots, h_2^2] \cdot F/\sqrt{n} \cdot e_j$. But,

$$\sqrt{n}F \cdot e_j = [1, \overline{w}^{j-1}, \overline{w}^{2(j-1)}, \ldots, \overline{w}^{(n-1)(j-1)}]^T.$$

The result follows from this. □

We resume both lemmas in the theorem.

Theorem 9. *Let n be a positive integer. Let $C := \mathrm{circ}(c_1, \ldots, c_n)$ where $c_i \in \mathbb{C}$ for all $i = 1, \ldots, n$. Put $E(C) := \frac{\mathrm{circ}(\lambda_1, \ldots, \lambda_n)}{\sqrt{n}}$, where the λ_i's are the eigenvalues of C in the order given by the Fourier transform $\sqrt{n}\,[\overline{c_1}, \ldots, \overline{c_n}] \cdot F = [\overline{\lambda_1}, \ldots, \overline{\lambda_n}]$. Write $E(E(C)) := \frac{\mathrm{circ}(b_1, \ldots, b_n)}{\sqrt{n}}$, where the b_i's are the eigenvalues of $E(C)$ in the order given by the Fourier transform $\sqrt{n}\,[\overline{d_1}, \ldots, \overline{d_n}] \cdot F = [\overline{b_1}, \ldots, \overline{b_n}]$, where $d_i := \frac{\lambda_i}{\sqrt{n}}$ for all $i \in \{1, \ldots, n\}$. In other words, $E(C) = \mathrm{circ}(d_1, \ldots, d_n)$. Then*

(a) $E(E(C)) = C^*$.

(b) If, moreover $c_j \in \{-1, 1\}$ for all $j = 1, \ldots, n$, then $C = C^*$ and $E(C) \cdot E(C)^* = nI_n$.

Proof. Part (a) follows from Lemma 7. First result in Part (b) follows from Lemma 7. The second result in part (b) follows from Lemma 8 by taking $H = C$, so that $\rho := \sqrt{n} \cdot E(C)$, since $m_j^2 = c_{n-j+2}^2 = 1$. More precisely, with these choices Lemma 8 gives $\langle R_1, R_1\rangle = n(1 + \cdots + 1) = n^2$ and $\langle R_1, R_j\rangle = 1 + w^{j-1} + w^{(j-1)2} + \cdots + w^{(j-1)(n-1)} = 0$, that is, we get $E(C) \cdot E(C)^* = nI_n$ as claimed. □

The following simple lemma in Davis's book is useful also.

Lemma 10. *Let* $\Lambda := \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. *Then* $\Gamma := F^*\Lambda F$ *is a circulant matrix of order* n.

Proof. See [9, Theorem 3.2.3]. □

The following result is well known and it is easy to check.

Lemma 11. *All eigenvalues of any Hadamard matrix of order* n *have the absolute value* $\sqrt{n}$.

The following class of matrices, *a priori*, an extension of the notion of Hadamard complex matrices, is important for the proof.

Definition 12. Let n be a positive integer. Let $C = (c_{ij})$ be a complex matrix of order n. Then we say that C is a *lower*-Hadamard matrix if $C \cdot C^* = nI_n$ and for each pair of indices $i, j \in \{1, \ldots, n\}$ one has $|c_{ij}| \leqslant 1$.

It is practical to recall here the definition.

Definition 13. Let n be a positive integer. For any column vector $v \in \mathbb{C}^n$, say $v = [v_1, \ldots, v_n]^T$, we define its 2-norm $||v||$ by

$$||v||^2 = v_1\overline{v_1} + \cdots + v_n\overline{v_n}.$$

The proposition below shows that we are *not* extending the class of complex Hadamard matrices. It is good news for us.

Proposition 14. *Let* n *be a positive integer. Then, a matrix* C *of order* n, *is a lower-Hadamard matrix if and only if* C *is a complex Hadamard matrix.*

Proof. One direction is trivial. Assume then that C is a lower-Hadamard matrix. Taking determinants in both sides of $C \cdot C^* = nI_n$ we get $|\det(C)| = n^{n/2}$. But, by Hadamard's inequality we have

$$n^{n/2} = |\det(C)| \leqslant \prod_{i=1}^{n} ||\mathrm{col}_i(C)||, \tag{4}$$

where $\mathrm{col}_i(C)$ is the i-th column of C. Therefore, by hypothesis, and by definition 13

$$||\mathrm{col}_i(C)||^2 = \sum_{k=1}^{n} c_{ki}\overline{c_{ki}} = \sum_{k=1}^{n} |c_{ki}|^2 \leqslant \sum_{k=1}^{n} 1 = n.$$

Thus,

$$||\mathrm{col}_i(C)|| \leqslant \sqrt{n} = n^{1/2}. \tag{5}$$

It follows then from (4) that we *cannot* have strict inequality $<$ in (5) for any given column of C. I.e., we cannot have for *some* $i \in \{1, \ldots, n\}$

$$||\mathrm{col}_i(C)|| < n^{1/2}. \tag{6}$$

In other words it is impossible to have simultaneously (4) and (6), for if both were true then we obtain from (4) the contradiction $n^{n/2} < (n^{1/2})^n$. Therefore, we have now, for any given $k \in \{1, \ldots, n\}$

$$S_k := |c_{1k}|^2 + \cdots + |c_{nk}|^2 = n. \tag{7}$$

But by hypothesis, $|c_{ik}| \leqslant 1$, so, if for some i we have $|c_{ik}| < 1$ then we get (from (7)) the contradiction $n = S_k < n$. Thus, we must have $|c_{ik}| = 1$ for all k and for all i such that $\{i, k\} \subseteq \{1, \ldots, n\}$. This finishes the proof. □

It will be clear in the proof of the main theorem, and in the proof of the crucial Lemma 16, why Proposition 14 is good news for us.

We use the obvious decomposition below of a circulant matrix of even order n in four blocks of order $n/2$, (see [12] for a related result based on the same decomposition), in order to build a smaller size matrix C attached to H.

Lemma 15. *Let n be a positive even integer. Let $H = \mathrm{circ}(h_1, \ldots, h_n)$ be a circulant matrix of order n. Then there exist matrices A, B, K of order $\frac{n}{2}$ such that*

(a)

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

(b) $K := A + B$ is circulant.

The lemma below is our main result. The theorem would follow quickly from it.

Lemma 16. *Let h be an odd positive integer. Assume that H is a circulant Hadamard matrix of order n, where $n = 4h^2$, that satisfies the condition C_n. Then, there exists a circulant lower-Hadamard matrix C of order $n/4$ such that $C = C^*$.*

Proof. Let $R = E(H)$ following Theorem 9 applied to H. By part (b) of the same Theorem 9, one has $R = R^*$ and $RR^* = nI_n$. Set $S = \frac{A+B}{2}$ where A and B are defined by Lemma 15 applied to the matrix R. Thus, S is circulant. Write $S = \mathrm{circ}(s_1, \ldots, s_n)$. Since R is, trivially, lower-Hadamard, we claim that S satisfies $SS^* = (n/4)I_{n/2}$. Moreover, we claim that S is hermitian. In order to prove the claim observe that $|a_i| \leqslant 1$ and $|b_i| \leqslant 1$. It follows that we have also $|s_i| = \left|\frac{a_i+b_i}{2}\right| \leqslant \frac{1+1}{2} = 1$, where a_i is the i-th entry in row 1 of A, and b_i is the i-th entry in row 1 of B. This proves the necessary conditions on the entries of S; and it is the core of the proof. We now check the equation $SS^* = (n/4)I_{n/2}$. From $RR^* = nI_n$, one gets by block multiplication $AA^* + BB^* = nI_{n/2}$ and $AB^* + BA^* = 0$. Thus,

$$AA^* + AB^* + BA^* + BB^* = AA^* + BB^* = nI_{n/2}. \tag{8}$$

It follows from (8), and the definition of S, that S satisfies the equation. It remains to prove that S is hermitian. From the definition of A and B one has $A = A^*$ and $B = B^*$ since $R = R^*$. It follows that $S^* = S$. We have then established the claim. In order to complete the proof we apply now, by using our condition C_n, an analogue construction to

the matrix S, instead that applying it to the matrix R. In other words we do the following. Observe that $n/2 = 2h^2$ is an even positive integer. Define then the matrices K and L both of order $n/4$ by applying Lemma 15 to the circulant matrix S. I.e., one has

$$S = \begin{bmatrix} K & L \\ L & K \end{bmatrix}.$$

More precisely, the first rows $Row_K(1)$, $Row_L(1)$ of K and L are respectively: $Row_K(1) = [s_1, \ldots, s_{n/4}]$ and $Row_L(1) = [s_{n/4+1}, \ldots, s_{n/2}]$. We define now our target matrix C by

$$C := K + L. \tag{9}$$

By Lemma 15 C is a circulant matrix of order $n/4$. Write $C = \mathrm{circ}(c_1, \ldots, c_{n/4})$.

Put $R = E(H) = \mathrm{circ}(d_1, \ldots, d_n)$. Since H satisfies the condition C_n one has

$$|c_i| = \left|s_i + s_{n/4+i}\right| = |(d_i + d_{i+h^2} + d_{i+2h^2} + d_{i+3h^2})/2| \leqslant \frac{2}{2} = 1$$

for all $i = 1, \ldots, n/4$.

We claim that C is a circulant lower-Hadamard matrix of order $n/4$. The only thing that remains to be proved is the equality: $CC^* = (n/4)I_{n/4}$. As before we have the following. From $SS^* = (n/4)I_{n/2}$, one gets by block multiplication $KK^*+LL^* = (n/4)I_{n/4}$ and $KL^* + LK^* = 0$. Thus, by (9)

$$CC^* = KK^* + KL^* + LK^* + LL^* = KK^* + LL^* = (n/4)I_{n/4},$$

that proves the equality. It remains to prove that C is hermitian. From the definition of K and L one has $K = K^*$ and $L = L^*$ since $S = S^*$. It follows that $C^* = C$. We have then established that C is a circulant lower-Hadamard matrix of order $n/4$, and that C is hermitian. This proves the lemma. □

Now, we describe the eigenvalues of our matrix C defined above.

Lemma 17. *The eigenvalues of the matrix C defined in Lemma 16 are elements of the set $Eig(C) := \{\sqrt{n}/2, -\sqrt{n}/2\}$.*

Proof. Since C is hermitian by Lemma 16 the result follows from Lemma 11. □

3 Informal account of the new idea for the proof

The idea is to try to build a circulant Hadamard matrix, say T_2, of smaller size than a given circulant Hadamard matrix H of order n, that satisfies the condition C_n. Of course, this appears at first view like an impossible task. However, the fact that H is formed of four blocks of size $n/2$ since H is circulant, suggest a first try. Assume that

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

Then it is easy to see, using that $HH^* = I_n$ and block multiplication, that $T_1 := (A + B)/2$, of size $n/2$ is circulant, has its entries in $\{-1, 0, 1\}$ and satisfies $T_1T_1^* = (n/4)I_{n/2}$. Repeating the procedure we got (we cannot now divide by 2), say, $T_2 := C + D$, of size $n/4$ is circulant with entries in $\{-2, -1, 0, 1, 2\}$ and satisfies $T_2T_2^* = (n/4)I_{n/4}$. Besides the problem with the entries not equal to -1 or to 1 these circulant matrices, may exist !. For example, for $n = 36$ (for which of course it is known that there are no circulant Hadamard matrix), we got, by example $T_2 := \mathrm{circ}(0, 1, -1, 0, 1, -1, 0, 1, 2)$ that satisfies $T_2T_2^* = 9I_9$. An interesting comment of the referee is that an orthogonal matrix with few entries often appear in "frames" in some lattices such as Leech lattice.

We need then to "fix" the problem with the entries in such a manner that we do *not* have trivial solutions as above. This can be done by considering a slightly more general form of a circulant Hadamard matrix. Namely, considering instead a matrix H with complex entries that satisfies $HH^* = nI_n$ and has its entries in the complex unit disk. First of all we prove (see Proposition 14) that these matrices are exactly the same as the matrices with the same constraint but having its entries exactly in the boundary of the disk. This uses the classical Hadamard's inequality. Then with the help of the Fourier transform we obtain a kind of "duality operator" E (see Theorem 9). After that (see Lemma 16) we build an analogue of the construction above, beginning now with $E(H)$ instead that with H, that works in the more general context, and then (see proof on next section) we are able to show that we can really do the "fix", i.e., we are able to build a kind of "descent". This "descent" is possible by the condition C_n on the eigenvalues of H, (see (2)) above.

We are now ready to show our main result.

4 Proof of Theorem 3

Let $n = 4h^2$. Let H be a circulant Hadamard matrix of order n. From Lemma 16 there exists a circulant, lower-Hadamard matrix C of order $n/4$ such that C is hermitian. Write $C = \mathrm{circ}(c_1, \ldots, c_{h^2})$. We define (see Lemma 10) a circulant matrix T by $T = h \cdot F^* \mathrm{diag}(c_1, \ldots, c_{h^2})F$ where F is the Fourier matrix defined in Definition 6, and $\mathrm{diag}(c_1, \ldots, c_{h^2})$ is a diagonal matrix of order h^2 with diagonal entries c_i for $i = 1 \ldots, h^2$. Let $T := \mathrm{circ}(t_1, \ldots, t_{h^2})$. Observe that the eigenvalues of T are $hc_1, \ldots, hc_{h^2}$. More precisely, see Theorem 9, one has $E(T) = C$. Define now the circulant matrix $D = \mathrm{circ}(d_1, \ldots, d_{h^2})$ of order $n/4$ by

$$D := E(E(T)). \tag{10}$$

By Lemma 17 we see that the eigenvalues of C are in $\{h, -h\}$. This together with the definition of D (see Theorem 9) implies that one has for all $i = 1, \ldots, h^2$ $d_i \in \{-1, 1\}$. More precisely: from (4) and the definition of $E(C)$ (see Theorem 9) we have $D = E(E(T)) = E(C) = \frac{\mathrm{circ}(\delta_1, \ldots, \delta_{h^2})}{h}$ where the δ_i's, for $i = 1, \ldots, h^2$ satisfy $\delta_i \in \{h, -h\}$, by Lemma 17. Now, we come back to T. Since C is a circulant lower-Hadamard matrix of order h^2, by Proposition 14 we have that, indeed, C is a circulant complex Hadamard

matrix. This means, in particular, that all the entries of the first row of C, namely all the c_i from $i = 1, \ldots, h^2$ satisfy

$$|c_i| = 1 \tag{11}$$

(and *not* just merely that $|c_i| \leqslant 1$). Here we touch, really the point of the proof.

Since C is a circulant complex Hadamard matrix of order h^2, we have also $CC^* = h^2 I_{h^2}$. We will show now that (11) has important consequences:

We claim that $TT^* = h^2 I_{h^2}$. Proof of the claim using (11):

$$\begin{aligned} TT^* &= h^2 \cdot F^* \mathrm{diag}(c_1, \ldots, c_{h^2}) F F^* \mathrm{diag}(\overline{c_1}, \ldots, \overline{c_{h^2}}) F \\ &= h^2 \cdot F^* \mathrm{diag}(|c_1|^2, \ldots, |c_{h^2}|^2) F = h^2 \cdot F^* \mathrm{diag}(1, \ldots, 1) F \\ &= h^2 \cdot F^* I_{h^2} F = h^2 \cdot F^* F = h^2 \cdot I_{h^2}. \end{aligned}$$

It remains just the following claim about the entries in the first row of the circulant matrix T: We claim that for all $i = 1, \ldots, h^2$ one has $t_i \in \{-1, 1\}$. Proof of the claim: By Theorem 9 part (a) one has $E(E(T)) = T^*$. But, by (10), this means

$$T^* = D. \tag{12}$$

But, each entry of the matrix D is in $\{1, -1\}$. So by (12), each entry of the matrix T^* is in $\{-1, 1\}$. Therefore, each entry of the matrix T is also in $\{-1, 1\}$. This proves the claim. We have then

(a) The matrix T is a circulant matrix of order h^2. All its entries belong to the set $\{1, -1\}$, and

(b) the circulant matrix T of order h^2 satisfies $TT^* = h^2 I_{h^2}$.

Therefore we obtain, by the definition of a Hadamard matrix, that T is a circulant Hadamard matrix of odd order h^2. This proves the theorem.

5 Proof of Corollary 4

Put $n = 4h^2$ where h is an odd positive integer. By Theorem 3 we deduce that there exists a circulant Hadamard matrix of odd order h^2. But it is well known that the unique square matrices of odd order k that are circulant and Hadamard, simultaneously, are all of order $k = 1$. More precisely these matrices are the following two square matrices with one, and only one, entry: $I_1 = (1)$ and $I_2 = (-1)$. Therefore, we must have $h = 1$. This proves the corollary.

Acknowledgements

We thank Bahman Saffari for writing his inspiring nice papers on polynomials. In particular, we *warmly* thanks him, for choosing to display the following (non-mathematical) statement: "Whatever is worth doing is worth doing badly" in the Introduction part of the most important of them. We are grateful to the referee for careful reading, for suggestions that improved the presentation of the paper and for an observation that resulted in a much better Lemma 17.

References

[1] S. S. Agaian. Hadamard matrices and their applications. *Lecture Notes in Mathematics*. 1168. Springer-Verlag, Berlin, 1985.

[2] P. Borwein, M. J. Mossinghoff. Wieferich pairs and Barker sequences. *Des. Codes Cryptogr.*. 53(3):149–163, 2009.

[3] P. Borwein, M. J. Mossinghoff. Wieferich pairs and Barker sequences, II. *LMS J. Comput. Math.*. 17(1):24–32, 2014.

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

[5] R. Craigen, G. Faucher, R. Low, and T. Wares, Circulant partial Hadamard matrices. *Lin. Alg. Appl.*. 439:3307-3317, 2013.

[6] R. Craigen, J. Jedwab. "Comment on revised version of "The Hadamard circulant conjecture,"". *arXiv:1111.3437v2 [math.CO]*.

[7] C. Lin, W. D. Wallis. Barker sequences and circulant Hadamard matrices. *J. Combin. Inform. System Sci.*. 18(1–2):19–25, 1993.

[8] C. Lin, W. D. Wallis. On the circulant Hadamard matrix conjecture. *Coding theory, design theory, group theory (Burlington, VT, 1990)*. 213–217, Wiley-Intersci. Publ., Wiley, New York, 1993.

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

[10] S. Eliahou, M. Kervaire. Corrigendum to:"Barker sequences and difference sets", [Enseign. Math. (2) 38, no. 3-4, 345–382, 1992]. *Enseign. Math.*. 40(1–2):109–111, 1994.

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

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

[13] M. J. Mossinghoff, "Wieferich prime pairs, Barker sequences, and circulant Hadamard matrices". 2013, *http://www.cecm.sfu.ca/ mjm/WieferichBarker/*.

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

[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., New York, 1963.

[16] J. Storer, R. Turyn. On binary sequences. *Proc. Am. Math. Soc.*12:394–399, 1961.

[17] R. Turyn, Character sums and difference sets. *Pacific J. Math*, 15:319–346, 1965.

[18] W. D. Wallis, A. P. Street, and J. S. Wallis. Combinatorics: Room squares, sum-free sets, Hadamard matrices. *Lecture Notes in Mathematics*, 292. Springer-Verlag, Berlin-New York, iv+508 pp, 1972.