Applied Mathematics E-Notes, 12(2012), 182-188 © ISSN 1607-2510
Available free at mirror sites of http://www.math.nthu.edu.tw/∼amen/

On A Special Case Of A Conjecture Of Ryser About Hadamard Circulant Matrices*

Luis Gallardo†

Received 2 June 2012

Abstract

There is no Hadamard circulant matrices H of order $n > 4$ with (a) first column $[x_1, \ldots, x_n]^*$ where $x_1(x_i + x_{\frac{n}{2}+i}) > -2$ for all $i = 1, \ldots, n/2$ and (b) such that $A + B$ is symmetric, where A, B are matrices of order $n/2$ such that the first $n/2$ lines of H have the form $[A, B]$.

1 Introduction

We discovered recently Ryser's conjecture as Problem 3 in [10, page 97]. Let $n > 0$ be a positive integer. Let π_n be the matrix in the standard basis of the *left-shift* operator that transforms a vector $(x_1, x_2, \ldots, x_n)^*$ (where * means "conjugate-transpose") to the vector $(x_2, \ldots, x_n, x_1)^*$.

Analogously let define ψ_n be the matrix in the standard basis of the *right-shift* operator that transforms a vector $(x_1, x_2, \ldots, x_n)^*$ to the vector $(x_n, x_1, \ldots, x_{n-1})^*$.

A *circulant* matrix C of order n is a matrix that is a polynomial in π_n, i.e., $C = P(\pi_n)$ where $P \in \mathbb{Z}[t]$ is a polynomial in one variable t with rational integral coefficients. More precisely, $P(t) = c_1 + c_2 t + \ldots + c_n t^{n-1}$ where $[c_1, c_2, \ldots, c_n]$ is the first row of C. P is called the *representer* polynomial of C. We also write

$$C = circ(c_1, c_2, \ldots, c_n)$$

and therefore, we have

$$C = P(\pi_n).$$

Analogously, a *left-circulant* matrix S of order n is a matrix that is a polynomial in ψ_n.

For example, all circulant matrices of order 4 are polynomials with integer coefficients in the matrix $\pi_4 = circ(0, 1, 0, 0)$, namely

$$\pi_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

*Mathematics Subject Classifications: 15B34, 11B30.

†Department of Mathematics, University Of Brest, 6, Av. Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France

A *Hadamard* matrix $H = (h_{i,j})$ of order n is a matrix with integer coefficients that satisfies the following two conditions:

(a) For all $1 \leq i, j \leq n$ one has $h_{i,j} \in \{-1, 1\}$.

(b) One has $H^*H = nI_n$ where I_n is the identity matrix of order n.

An example of a Hadamard circulant matrix is: $H = circ(-1, -, 1, -1, 1)$, namely

$$H = \begin{bmatrix} -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \end{bmatrix}$$

Indeed, the complete list of all known Hadamard circulant matrices consists of $\pm H$ and $\pm$ the other shifts of H by π_4, plus $\pm I_1$ where $I_1 = [1]$ is the trivial identity matrix of order 1. More precisely, all known Hadamard circulant matrices belong to the following list of ten matrices:

$$\{H, -H, \pi_4 H, -\pi_4 H, \pi_4^2 H, -\pi_4^2 H, \pi_4^3 H, -\pi_4^3 H, I_1, -I_1\}.$$

Ryser's conjecture (see [13, page 134]) is the inexistence of matrices of order $n > 4$ that are circulant and Hadamard matrices simultaneously. There are many published papers in this area (see e.g., [13], [6], [16] [17], [12], [2], [14], [7], [15], [14], [3], [9] and the bibliography therein).

The existence or nonexistence of circulant Hadamard matrices is important since the problem is at the intersection of several branches of mathematics. First of all we have a classical linear algebra problem (as in the special case considered in the present paper). But the problem is also related to the classical orthogonal group, since H circulant Hadamard of order n is equivalent to $H/\sqrt{n}$ belongs to the orthogonal group $O(n, \mathbb{Q})$, where $\mathbb{Q}$ is the field of rational numbers. Moreover, there is also a complex analysis aspect on the problem since H being circulant, it is diagonalized over the complex numbers by the unitary Fourier matrix F defined by $F^* = (\frac{1}{\sqrt{n}} w^{(i-1)(j-1)})$ where $w = e^{\frac{2\pi i}{n}}$ is an n-th complex root of unity. Second, there is a number theory aspect on the problem, since the n-th classical cyclotomic polynomial $\phi_n(t)$ over $\mathbb{Q}$ is a divisor of the representer polynomial of H, so the condition on H implies conditions on $\phi_n(t)$. Third, the problem has a combinatorial aspect also since the columns of H whose entries are in $\{-1, 1\}$ should be two by two orthogonal. Furthermore, the conjecture is a long-standing one since remains unresolved since 1963. A recent short survey of what is known about Ryser's conjecture appear (among other results) in [3].

We prove in the present paper (see Theorem 1) a simple special case of the full conjecture, not noticed in the literature, by using a nice result of Ma [11, Theorem 3]. Craigen and Kharaghani [5], had already used this result to reprove (among other results) a 1965's result of Brualdi [4], namely that the only Hadamard circulant symmetric matrices H of order n occur when $n \in \{1, 4\}$. Observe that H circulant and symmetric is equivalent to H circulant and $HM_n = M_n H$, where M_n is the *mirror* matrix of order n defined in section 2. This matrix is also called *counteridentity* in [10, p. 28]. See also section 2 for definitions of the matrices $I_{n/2}, J_{n/2}$ used in (1) below.

We prove also in section 3 (see Corollary 1) that we cannot improve the result by considering a more general commutation condition. Namely, one has for suitable rational numbers $u, v \in \mathbb{Q}$ with $(u, v) \neq (1, 0)$:

$$(A + B)M_{n/2} = M_{n/2}(A + B)(uI_{n/2} + vJ_{n/2}) \tag{1}$$

(see also Lemma 6), instead of the simple commutation property: $(A + B)M_{n/2} = M_{n/2}(A + B)$ that we used in the proof of Theorem 1. Indeed (see Lemma 6 and Corollary 3), (1) implies that $n = 4$ or $(u, v) = (1, 0)$ so that the result is optimal for these kind of modifications.

2 Some Tools

Let $n > 0$ be a positive integer. We denote by I_n the identity matrix of order n. The following two square matrices of order n play a significant role: $J_n = (J_{r,s})$ where $J_{r,s} = 1$ for all r, s and $M_n = (M_{i,j})$ the *mirror* matrix defined by $M_{i,j} = 1$ if $i + j = n + 1$ and $M_{i,j} = 0$ otherwise. Let r be a real number. We say that a matrix A of order n with real entries is *r-regular* if $AJ_n = J_nA = rJ_n$. Observe that for a r-regular matrix A, r is the common sum of all the entries in a given line or column of A. If all entries of a matrix M are in $\{0, 1\}$ we say that M is a $\{0, 1\}$ matrix.

The following is well known but useful.

LEMMA 1. Let H be a Hadamard matrix of order $n > 4$. Then $4 \mid n$.

LEMMA 2. Let H be a Hadamard and circulant matrix of order $n > 0$. Set $M = M_n$. Then the matrix HM is Hadamard, symmetric, and left-circulant.

PROOF. One has $(HM)(HM)^* = HMM^*H^* = HH^* = H^*H = nI$; the other conditions are also easily checked.

LEMMA 3. Let H be a circulant and Hadamard matrix of order $n > 0$. Then n is a perfect square. So $n = 4h^2$ for some nonzero integer $h \neq 0$.

PROOF. The matrix $H = circ(c_1, \ldots, c_n)$ is r-regular, with $r = c_1 + \cdots + c_n$ since H is circulant. Since we have also $H^*J_n = rJ_n$ we obtain $nJ_n = HH^*J_n = r^2J_n$. The result follows.

LEMMA 4. Let H be a circulant Hadamard matrix of order $n = r^2 > 0$ and with first column $C_1 = [x_1, \ldots, x_n]^*$. Set

$$\delta_i = x_1(x_i + x_{\frac{n}{2}+i})$$

for each $i = 1, \ldots, n/2$. Then

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

where A, B are matrices of order $n/2$.

(b) $K = A + B$ is circulant and r-regular.

(c) If for all $i = 1, \ldots, n/2$ one has

$$\delta_i > -2,$$

then all entries of $C = \frac{K}{2}$ are in $\{0, x_1\}$.

PROOF. Since H is circulant we have (a). It is well known that H is r-regular. By definition of K, K is circulant with first column

$$[x_1 + x_{\frac{n}{2}+1}, \ldots, x_i + x_{\frac{n}{2}+i}, \ldots, x_{\frac{n}{2}} + x_n]^*$$

and the sum of the entries on any line or column of K equals r, the sum of all elements in C_1. This proves (b). Since $x_j \in \{-1, 1\}$ for all $j = 1, \ldots, n$, one has

$$\delta_j \in \{-2, 0, 2\}$$

so that (c) implies the result.

The next crucial lemma is [11, Theorem 3], which is also appeared as [5, Theorem 3.1].

LEMMA 5. Let A be a circulant matrix of order $n > 0$ with entries in $\{0, 1\}$. Let m be an even positive integer. Assume that $A^m = dI_n + kJ_n$ for some integers d, k. Then $A \in \{0, P, J_n, J_n - P\}$ where P is a permutation matrix of order n.

The following lemma is useful in order to establish Corollary 1.

LEMMA 6. Set $n = 4h^2$ for an odd integer h. Define r by $n = r^2$ so that r is even and $\frac{r}{2}$ is odd. Let $u, v \in \mathbb{Q}$ be rational numbers. Let $S = (s_{i,j}) \neq J_{\frac{n}{2}}$ be a $\{0, 1\}$ matrix of order $\frac{n}{2}$, $\frac{r}{2}$-regular and such that $T = S(uI + vJ) = (t_{i,j})$, where $I = I_{\frac{n}{2}}, J = J_{\frac{n}{2}}$, is also a $\{0, 1\}$ matrix. Then $(u, v) = (1, 0)$ or $n = 4$.

PROOF. Set $n_2 = \frac{n}{2}$, $r_2 = \frac{r}{2}$. Observe that $SJ = r_2 J$ since S is r_2-regular. Since $T = uS + vr_2 J$, T is t-regular with

$$t = \sum_{j=1}^{n_2} us_{i,j} + vr_2 = r_2(u + vn_2). \tag{2}$$

But $t = r_2$ and $r \neq 0$ so that (2) implies

$$u + vn_2 = 1. \tag{3}$$

Now we exploit the fact that T is a $\{0, 1\}$ matrix. One has $t_{i,j} = us_{i,j} + wr_2$. Case 1: $s_{i,j} = 0$ so that $t_{i,j} = wr_2$. If $v = 0$ then $u = 1$ from (3). If $v \neq 0$ then $t_{i,j} = 1$ so that $v = r_2^{-1}$. We obtain $u = 1 - r$ from (3). But $S \neq 0$ since S is r_2-regular, so there are a pair $(k, l) \neq (i, j)$ with $s_{k,l} \neq 0$ so that $s_{k,l} = 1$ and $t_{k,l} = u + vr_2 = (1 - r) + 1 = 2 - r \in \{0, 1\}$. This implies $r = 2$ so that $n = 4$; or $r = 1$ and $n = 1$. Case 2: $s_{i,j} = 1$ so $t_{i,j} = u + vr_2 \in \{0, 1\}$. If $t_{i,j} = 0$ we get from (3) $2 = v(n - r)$ so that $v = \frac{2}{n-r} \neq 0$. Using again (3) we obtain $u = \frac{r}{r-n}$. But $S \neq J$, so for some $(k, l) \neq (i, j)$, one has $s_{k,l} = 0$, so that $t_{k,l} = wr_2 \in \{0, 1\}$. If $t_{k,l} = 0$ then we get the contradiction $v = 0$, so $t_{k,l} = 1$, i.e., $n = 2r$. It follows that $r(r - 2) = 0$ so that $r = 2$ and $n = 4$. This proves the lemma.

3 The Main Result and its Proof

We deduce our main result:

THEOREM 1. Set $M = M_{\frac{n}{2}}$, $J = J_{\frac{n}{2}}$ and $I = I_{\frac{n}{2}}$. There is no Hadamard circulant matrices $H = \begin{bmatrix} A & B \\ B & A \end{bmatrix}$ of order $n = 4h^2 > 4$ with first column $[x_1, \ldots, x_n]^*$ where $x_1(x_i + x_{\frac{n}{2}+i}) > -2$ for all $i = 1, \ldots, \frac{n}{2}$ and such that

$$(A + B)M = M(A + B) \tag{4}$$

or in equivalent form: such that

$$A + B \quad \text{is symmetric}$$

PROOF. Assume to the contrary the existence of such a matrix H. Observe that $n = 4h^2$ from Lemma 2. We can assume that $x_1 = 1$, since if this is not true we change H by $-H$. By Lemma 2 we have $n = r^2$. Set $M = M_{\frac{n}{2}}$, $J = J_{\frac{n}{2}}$ and $I = I_{\frac{n}{2}}$. One has by Lemma 2 (a)

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

where A, B are matrices of order $\frac{n}{2}$. So

$$K = HM_n = \begin{bmatrix} BM & AM \\ AM & BM \end{bmatrix} \tag{5}$$

is Hadamard symmetric by Lemma 2 so that

$$K^2 = nI. \tag{6}$$

So from (5) and (6) we get

$$(BM)^2 + (AM)^2 = nI, \;\; AMBM + BMAM = 0.$$

It follows that

$$(BM + AM)^2 = nI. \tag{7}$$

Set $C = \frac{(A+B)M}{2}$, $D = \frac{A+B}{2} = CM$. We have then from (7)

$$C^2 = \frac{n}{4}I. \tag{8}$$

So

$$D^2 = CMCM = CMMC = C^2, \tag{9}$$

from (4).

Thus, we get

$$D^2 = h^2 I, \tag{10}$$

from $n = 4h^2$.

By the condition and Lemma 2, D is circulant, $\frac{r}{2}$-regular and has all its entries in $\{0, 1\}$. We see from (10) that D^2 is an integral combination of I and J. Thus, we conclude from Lemma 5 that

$$D \in \{0, P, J - P, J\}.$$

where P is a permutation matrix of order $\frac{n}{2}$. Since from (8) $C = DM$ is non singular, we obtain

$$C \in \{PM, (J - P)M\}.$$

Observe that C is $\frac{r}{2}$-regular and that P is 1-regular. So $C = PM$ implies $n = 4$. Since $J - P$ is $(\frac{n}{2} - 1)$-regular, $C = (J - P)M$ implies $\frac{n}{4} = (\frac{n}{2} - 1)^2$. In other words

$$(n - 1)(n - 4) = 0.$$

The result follows.

Following our discussion at the end of the Introduction, our second result follows immediately from Theorem 1:

COROLLARY 1. Set $M = M_{\frac{n}{2}}$, $J = J_{\frac{n}{2}}$ and $I = I_{\frac{n}{2}}$. There is no Hadamard circulant matrices $H = \begin{bmatrix} A & B \\ B & A \end{bmatrix}$ of order $n = 4h^2 > 4$ with first column $[x_1, \ldots, x_n]^*$ where $x_1(x_i + x_{\frac{n}{2}+i}) > -2$ for all $i = 1, \ldots, n/2$ and such that

$$(A + B)M = M(A + B)(uI + vJ)$$

for suitable rational numbers $u, v \in \mathbb{Q}$ such that $(u, v) \neq (1, 0)$.

PROOF. Apply Lemma 6 with $S = M(A+B)$. The result follows then by Theorem 1.

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

References

[1] B. Schmidt, S. L. Ma and K. H. Leung, Nonexistence of abelian difference sets: Lander's conjecture for prime power orders, Trans. Am. Math. Soc., 356(11)(2004), 4343–4358.

[2] B. Schmidt, S. L. Ma and K. H. Leung, New Hadamard matrices of order $4p^2$ obtained from Jacobi sums of order 16, J. Comb. Theory Ser. A, 113(5)(2006), 822–838.

[3] O. Rahavandrainy, L. H. Gallardo and R. Euler, Sufficient conditions for a conjecture of Ryser about Hadamard Circulant matrices, Linear Algebra Appl., 437(12)(2012), 2877–2886.

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

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

[6] R. Turyn and J. Storer, On the binary sequences, Proc. Am. Math. Soc., 12(1961), 394–399.

[7] B. Schmidt and K. H. Leung, The field descent method, Des. Codes Cryptogr., 36(2)(2005), 171–178.

[8] B. Schmidt and K. H. Leung, New restrictions on possible orders of circulant Hadamard matrices, Des. Codes Cryptogr., 64(2012), no. 1–2, 143–151.

[9] M. Kervaire and S. Eliahou, A survey on modular Hadamard matrices, Discrete Math., 302(1-3)(2005), 85–106.

[10] P. J. Davis, Circulant Matrices, 2nd ed., New York, NY: AMS Chelsea Publishing, 1994.

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

[12] M. J. Mossinghoff, Wieferich pairs and Barker sequences, Des. Codes Cryptogr., 53(2009), 149–163.

[13] 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.

[14] B. Schmidt, Cyclotomic integers and finite geometry, J. Am. Math. Soc., 12(4)(1999), 929–952.

[15] B. Schmidt, Towards Ryser's conjecture, European Congress of Mathematics, Vol. I (Barcelona, 2000), Birkhauser, Basel, Progr. Math., 201(2001), 533–541.

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

[17] R. Turyn, Sequences with small correlation, Error Correct. Codes, Proc. Symp. Madison 1968 (1969), 195–228.