On the Nonexistence of Hermitian Circulant Complex Hadamard Matrices

R. Craigen*and H. Kharaghani†
craigen@alpha.uleth.ca, kharaghani@hg.uleth.ca
Department of Mathematics and Computer Science
University of Lethbridge
T1K 3M4

Abstract

We prove that there is no circulant Hermitian complex Hadamard matrix of order $n > 4$.

1 Introduction

The following conjecture is related in [6].

Conjecture 1 *There is no circulant Hadamard matrix of order $n > 4$.*

Of course, these exist in orders 1 (trivially) and 4, an example of the latter having first row (-111). Now the matrices in these cases are not only circulant, but also symmetric. One may guess that, if circulant Hadamard matrices exist in order n, then symmetric circulant Hadamard matrices are bound to exist also. However, some time ago, Brualdi and Newman [1] eliminated the latter possibility by giving results having the following immediate consequence.

Theorem 1 *There is no symmetric circulant Hadamard matrix of order $n > 4$.*

McKay and S. Wang [5] proved the same result more recently in a different fashion.

We say that a matrix A is *r-regular* if $AJ = JA = rJ$. It is easy to show that if $AA^t = \lambda I$, then this is equivalent to $AJ = rJ$. The following result is well-known.

Lemma 2 *If H is a complex circulant Hadamard matrix of order n, then n is a sum of two squares and H is $\pm\sqrt{n}$-regular. Moreover, if H is real then n is a square.*

*Supported by an NSERC Postdoctoral Fellowship
†Supported by an NSERC grant

Proof: Circulant matrices are regular. Suppose H is r-regular. Then $HJ = H^tJ = rJ$ and $HH^tJ = r^2J = nJ$, so $r = \pm\sqrt{n}$. Clearly, r is a Gaussian (respectively rational) integer. The result follows. □

There are more sophisticated existence and non-existence results relative to this question. For example, Turyn has shown that there exist symmetric (not necessarily Hermitian) complex Hadamard matrices of orders 2^t, $0 \le t \le 4$, and that these are the only admissible values of t (even without the condition of symmetry), and that there are no complex circulant Hadamard matrices of order $2q$, where q is an odd prime power [8]. He has also shown that the only admissible orders for circulant Hadamard matrices are $4n^2$, where n is odd, and eliminated a number of these cases, such as n a prime power, as well [7]. Jedwab and Lloyd [3] have shown that, with six possible exceptions, there is no circulant Hadamard matrix of order less than 10^8.

2 Some new cases

We will require the following result of Ma [4].

Theorem 3 *If A is a circulant $(0,1)$-matrix satisfying $A^m = dI + \lambda J$, then $A = 0$, P, J or $J - P$, where P is a permutation matrix.*

Lemma 4 *Let H be a circulant Hadamard matrix of order n, such that, for some $m > 0$, $H^m = n^{\frac{m}{2}}I$. Then $n \le 4$.*

Proof: We let $A = \frac{1}{2}(H + J)$. By lemma 2, H is regular, and so, then, is any integral power of H. It follows that $A^m = n^{\frac{m}{2}}I + \lambda J$, where λ is an integer. From Ma's result, $H = 2A - J = \pm J$ or $\pm(2P - J)$. So H is $\pm n$-or-$\pm(n-2)$-regular, and it follows that $n = 1$ or 4. □

The following result reproves and generalizes the result of Brualdi and Newman.

Theorem 5 *A circulant Hadamard matrix H of order $n > 4$ cannot satisfy $PH = H^t$, where P is any permutation matrix.*

Proof: Multiplying both sides by H on the right and P^t on the left, we obtain that $H^2 = nP^t$. Since P is a permutation matrix, it has finite multiplicative order, and so H satisfies the condition of theorem 4, with m equal to twice the multiplicative order of P. □

Matrices M satisfying $PM = M^t$ are interesting to study for their own sake (see [2]), and they often arise in the study of Hadamard matrices. Of course we may replace P in the corollary by any matrix of finite multiplicative order.

Theorem 6 *There is no circulant Hadamard matrix H of order $n > 4$ such that H^k is symmetric, for any $k > 0$.*

Proof: In this case, H satisfies the condition of theorem 4, with $m = 2k$. □

Now we generalize the theorem of Brualdi and Newman in another direction. A complex matrix A is called *skew-Hermitian* if $A^* = -A$, where $*$ represents the Hermitian adjoint.

Theorem 7 *There is no Hermitian (or skew-Hermitian) circulant complex Hadamard matrix of order* $n > 4$.

Proof: Suppose a Hermitian circulant complex Hadamard matrix, $A + Bi$, exists. Then A and B are circulant, $A = A^t$ and $B = -B^t$. So $(A + Bi)(A + Bi)^* = A^2 + 2ABi - B^2 = nI$. It follows that $AB = 0$ and $A^2 - B^2 = nI$. Therefore, $H = A + B$ is a circulant Hadamard matrix, and H^2 is symmetric. The result follows from corollary 6. The skew-Hermitian case follows from the observation that $A + Bi$ is Hermitian if and only if $B - Ai$ is skew-Hermitian. □

Remark. In contrast to the real case, there are skew-Hermitian complex circulant Hadamard matrices of orders 1 and 4.

References

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

[2] R. Craigen, *Matrices equivalent to their transpose by permutations.* preprint., 1992.

[3] J. Jedwab and S. Lloyd, *On the nonexistence of Barker sequences.* to appear.

[4] S. L. Ma, *On rational circulants satisfying* $A^m = dI + \lambda J$, Lin. Alg. Appl., 62 (1984), pp. 155–161.

[5] J. H. McKay and S. S. Wang, *On a theorem of Brualdi and Newman*, Lin. Alg. Appl., 92 (1987), pp. 39–43.

[6] H. J. Ryser, *Combinatorial Mathematics*, no. 14 in The Carus Mathematical Monographs, MAA/John Wiley and Sons, 1963.

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

[8] ——, *Complex Hadamard matrices*, in Combinatorial Structures and their Applications, New York, 1970, pp. 435–437.

(Received 4/11/92)