A Finiteness Result for Complex Hadamard Matrices in Maximal Abelian Self-Adjoint Subalgebras of $\mathrm{M_n}(\mathbb{C})$

Shuler Hopkins
Sewanee: The University of the South (sghopkin@sewanee.edu)
and
Remus Nicoară
University of Tennessee Knoxville (rnicoara@utk.edu)

Abstract

Let $\mathcal{A} = U\mathrm{D_n}(\mathbb{C})U^*$ be a Maximal Abelian Self-Adjoint Subalgebra (MASA) of $\mathrm{M_n}(\mathbb{C})$, where $\mathrm{D_n}(\mathbb{C})$ denotes the diagonal matrices and $U \in \mathrm{M_n}(\mathbb{C})$ is a unitary matrix. Assume that U is *full superregular*, i.e. all the minors of U are nonzero. We show that $\mathcal{A}$ contains at most finitely many complex Hadamard matrices, up to equivalence given by multiplication by complex units. In particular, since almost every unitary is full superregular (with respect to the Haar distribution), it follows that almost every MASA of $\mathrm{M_n}(\mathbb{C})$ contains only finitely many complex non-equivalent Hadamard matrices.

1 Introduction

A complex Hadamard matrix is a matrix $H \in \mathrm{M_n}(\mathbb{C})$ having all entries of absolute value 1 and all rows mutually orthogonal (with respect to the complex inner product). Equivalently, $\frac{1}{\sqrt{n}}H$ is a unitary matrix with all entries of the same absolute value. For example the Discrete Fourier Transform $F_n = (\omega^{k\cdot l})_{0\leq k,l\leq n-1}$, with $\omega = e^{2\pi \mathrm{i}/n}$, is a complex Hadamard matrix.

In recent years complex Hadamard matrices have found significant applications in various topics of mathematics and physics, including Quantum Information Theory (see [16], [1], [13], [12]), Operator Algebras (see [7],[6],[9],[10],[8]), Cyclic Roots of Unity (see [5]), and Fuglede's Conjecture in Harmonic Analysis (see [14]). A general classification of complex Hadamard matrices is not available. A catalogue of most known complex Hadamard matrices can be found in [13]. The complete classification is only known for $n \leq 5$ (see [4]) and for self-adjoint matrices of order 6 (see [2]).

In this paper we prove finiteness results for complex Hadamard matrices with certain symmetries. More precisely, we look at complex Hadamard matrices belonging to a fixed Maximal Abelian Self-Adjoint Subalgebra (MASA) of $\mathrm{M_n}(\mathbb{C})$. Denote by $\mathrm{D_n}(\mathbb{C})$ the algebra of $n\times n$ diagonal matrices with complex entries. Then any MASA $\mathcal{A}$ of $\mathrm{M_n}(\mathbb{C})$ is of the form $\mathcal{A} = U\mathrm{D_n}(\mathbb{C})U^*$, where $U \in \mathrm{M_n}(\mathbb{C})$ is a unitary matrix. The main result of this paper is the following:

Theorem 1.1. Let $U \in \mathrm{M_n}(\mathbb{C})$ be a unitary matrix that is *full superregular* (i.e., all minors of U are nonzero). Then the algebra $\mathcal{A} = U\mathrm{D_n}(\mathbb{C})U^*$ contains at most finitely many complex Hadamard matrices, up to equivalence given by multiplication by complex units.

To prove this result, we first embed the *real* algebraic variety of complex Hadamard matrices that belong to $\mathcal{A} = U\mathrm{D_n}(\mathbb{C})U^*$ in a *complex* algebraic variety of $\mathbb{C}^N$, with $N = 2n$. Since any compact complex algebraic variety of $\mathbb{C}^N$ is finite, it is sufficient to show that our complex variety is compact. The difficulty lies in proving that it cannot be unbounded. We achieve this by employing a 'derivative at infinity' argument, which leads to new relations that contradict the superregularity of U. The contradiction is obtained by first proving a more general version of *Tao's uncertainty principle* for cyclic groups of prime order from [15] (see also Haagerup's equivalent formulation of this principle from [5]).

We note that almost every unitary matrix (with respect to the Haar distribution) has all minors nonzero, hence it is full superregular and it satisfies the hypothesis of our theorem.

For a large class of concrete examples, consider real orthogonal Cauchy-like matrices. These matrices were completely classified in [3], in connection to Information Theory. The terminology *full superregular* comes from Information Theory, as full superregular matrices can be used to generate maximal distance separable block codes. Cauchy matrices are known to be full superregular.

Another interesting example of a unitary full superregular matrix is the Discrete Fourier Transform F_n for n prime. Indeed, it is a classical result of Chebotarëv that all the minors of this matrix are nonzero (see [15] for an elementary proof). In this case, it is easy to see that the algebra $\mathcal{A} = F_n\mathrm{D_n}(\mathbb{C})F_n^*$ is the algebra of circulant matrices:

$$\mathcal{A} = \left\{ \begin{pmatrix} x_0 & x_1 & x_2 & \dots & x_{p-1} \\ x_{p-1} & x_0 & x_1 & \dots & x_{p-2} \\ x_{p-2} & x_{p-1} & x_0 & \dots & x_{p-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1 & x_2 & x_3 & \dots & x_0 \end{pmatrix} : x_0, x_1, \dots x_{p-1} \in \mathbb{C} \right\}.$$

Thus, as a consequence of our result we also obtain that there exist only finitely many circulant complex Hadamard matrices of prime dimension (up to multiplication by complex units). This is a theorem of Haagerup from [5], and it is the result that inspired this paper.

2 Proof of the main result

In this section we prove Theorem 1.1. Let $U \in \mathrm{M_n}(\mathbb{C})$ be a unitary full superregular matrix. We want to show that the algebra $\mathcal{A} = U\mathrm{D_n}(\mathbb{C})U^*$ contains at most finitely many complex Hadamard matrices, up to multiplication by complex units.

For convenience, we note that $\mathrm{D_n}(\mathbb{C}) = \sqrt{\mathrm{n}}\mathrm{D_n}(\mathbb{C})$ so we can write $\mathcal{A} = \sqrt{n}U\mathrm{D_n}(\mathbb{C})U^*$. Thus we want to prove that there exist only finitely many complex Hadamard matrices of the form $\sqrt{n}UDU^*$ (up to complex units multiplication), with D a diagonal matrix.

For any $x = (x_0, \dots, x_{n-1}) \in \mathbb{C}^n$ denote by D_x the diagonal matrix with entry x_k on position (k, k) for all $k \in \mathbb{Z}_n$, and denote by $\hat{x}_{i,j}$ the $(i, j)^{\text{th}}$ entry of the matrix $\sqrt{n}UD_xU^*$.

Note that if $\sqrt{n}UD_xU^*$ is a Hadamard matrix then in particular UD_xU^* is unitary, so $|x_k| = 1$ for all $k \in \mathbb{Z}_n$. By replacing the matrix $\sqrt{n}UD_xU^*$ by the matrix $\overline{x_0}\sqrt{n}UD_xU^* = \sqrt{n}U(\overline{x_0}D_x)U^*$, or equivalently by replacing D_x by $\overline{x_0}D_x$, it suffices to work with diagonal matrices D_x with $x_0 = 1$ (up to equivalence via complex units multiplication).

The next proposition is crucial to the proof, as it allows us to work with a *complex* algebraic manifold instead of the *real* algebraic manifold of complex Hadamard matrices in $\mathcal{A}$.

Proposition 2.1. If $\sqrt{n}UD_xU^*$ is a Hadamard matrix with $x_0 = 1$, and if we let $y = (y_0, y_1, ..., y_{n-1})$ with $y_k = \overline{x_k}$, then (x, y) is a solution to the set of equations

$$x_0 = y_0 = 1,\ x_k y_k = 1,\ \hat{x}_{k,0}\hat{y}_{0,k} = 1 \text{ for all } k \in \mathbb{Z}_n.$$

Proof. By design, $x_0 = y_0 = 1$. Since $\sqrt{n}UD_xU^*$ is Hadamard, in particular UD_xU^* is unitary, which implies D_x is unitary, which implies $|x_k| = 1$ for all k. Thus for all $k \in \mathbb{Z}_n$

$$x_k y_k = x_k \overline{x_k} = x_k \frac{1}{x_k} = 1.$$

Now, since $\sqrt{n}UD_xU^*$ is Hadamard each entry has modulus 1, and thus $|\hat{x}_{k,0}| = 1$ for all $k \in \mathbb{Z}_n$. Note also that, since $(UD_xU^*)^* = UD_{\overline{x}}U^* = UD_yU^*$, we have $\hat{y}_{0,k} = \overline{\hat{x}_{k,0}}$. Hence for all $k \in \mathbb{Z}_n$ we have:

$$\hat{x}_{k,0}\hat{y}_{0,k} = \hat{x}_{k,0}\overline{\hat{x}_{k,0}} = 1.$$

□

We now introduce some notations that will be used in the next proposition. For $K, L \subset \mathbb{Z}_n$, denote by $(U)_{K\times L}$ the submatrix of U obtained by keeping the elements at the intersection of the rows of U indexed by K with the columns of U indexed by L. Also, for $x \in \mathbb{C}^n$ define its support, $supp(x)$, to be the set of all $k \in \mathbb{Z}_n$ such that $x_k \neq 0$.

The following statement is in the vein of Tao's uncertainty principle from [15].

Proposition 2.2. Suppose U is an $n \times n$ unitary matrix which is full superregular (i.e., $\det(U)_{K\times L} \neq 0$ for any subsets $K, L \subset \mathbb{Z}_n$ with $|K| = |L| \geq 1$). For every nonzero $x \in \mathbb{C}^n$ and for every $t \in \mathbb{Z}_n$ we have:

$$|supp(x)| + |supp(\hat{x}_t)| \geq n + 1$$

where $\hat{x}_t = (\hat{x}_{k,t})_{0\leq k\leq n-1} \in \mathbb{C}^n$ is the t^{th} column of $\sqrt{n}UD_xU^*$.

Proof. Suppose by contradiction that for some nonzero $x \in \mathbb{C}^n$ and some $t \in \mathbb{Z}_n$ we have:

$$|supp(x)| + |supp(\hat{x}_t)| \leq n.$$

Set $L = supp(x)$, then $|L| \geq 1$ (since $x \neq 0$) and

$$|\mathbb{Z}_n \setminus supp(\hat{x}_t)| = n - |supp(\hat{x}_t)| \geq |supp(x)| = |L|.$$

So we may choose $K \subset \mathbb{Z}_n \setminus supp(\hat{x}_t)$ such that $|K| = |L|$. Since $K \subset \mathbb{Z}_n \setminus supp(\hat{x}_t)$, we have for all $k \in K$

$$0 = \hat{x}_{k,t} = \sqrt{n} \sum_{i \in \mathbb{Z}_n} u_{k,i} x_i u^*_{i,t} = \sqrt{n} \sum_{i \in L} u_{k,i} x_i u^*_{i,t}.$$

Let $T \subset \mathbb{Z}_n$ such that $t \in T$ and $|T| = |L| = |K|$. Note that the (k,t) entry of $\sqrt{n} U D_x U^*$ is

$$(\sqrt{n}(U)_{K \times L}(D_x)_{L \times L}(U^*)_{L \times T})_{k,t} = \sqrt{n} \sum_{i \in L} u_{k,i} x_i u^*_{i,t}.$$

As this holds for all $k \in K$, the t^{th} column of $\sqrt{n}(U)_{K \times L}(D_x)_{L \times L}(U^*)_{L \times T}$ consists only of zeros. This implies

$$0 = \det\left(\sqrt{n}(U)_{K \times L}(D_x)_{L \times L}(U^*)_{L \times T}\right) = \sqrt{n} \det(U)_{K \times L} \cdot \det(D_x)_{L \times L} \cdot \det(U^*)_{L \times T}.$$

But this is a contradiction since $\det(U)_{K \times L} \neq 0$, $\det(U^*)_{L \times T} \neq 0$, and $\det(D_x)_{L \times L} = \prod_{l \in L} x_l \neq 0$ since $L = supp(x)$. $\square$

Proposition 2.3. Suppose U is an $n \times n$ unitary matrix which is full superregular. For every nonzero $x \in \mathbb{C}^n$ and for every $s \in \mathbb{Z}_n$ we have:

$$|supp(x)| + |supp(\hat{x}^s)| \geq n + 1$$

where $\hat{x}^s = \{\hat{x}_{s,l}\}_{l \in \mathbb{Z}_n}$ is the s^{th} row of $\sqrt{n} U D_x U^*$.

Proof. This follows from the the previous proposition applied to $\overline{x}$, by using that $|supp(x)| = |supp(\overline{x})|$ and $|supp(\hat{x}^s)| = |supp(\hat{\overline{x}}_s)|$. The last equality follows by noticing that the s^{th} row of $\sqrt{n} U D_x U^*$ is the conjugate of the s^{th} column of $\sqrt{n} U D_{\overline{x}} U^*$, hence their supports have the same cardinality. $\square$

We are now ready to prove Theorem 1.1. Note that, by using Proposition 2.1, the following statement will imply Theorem 1.1.

Theorem 2.1. If U is a full superregular unitary matrix, then there are only finitely many complex solutions to the following set of equations

$$x_0 = y_0 = 1, \qquad x_k y_k = 1, \qquad \hat{x}_{k,0} \hat{y}_{0,k} = 1 \qquad \text{for all } k \in \mathbb{Z}_n.$$

Proof. Suppose, by contradiction, that there are infinitely many $z = (x, y) \in \mathbb{C}^n \times \mathbb{C}^n$ that satisfy the system of equations. Since this system yields a complex algebraic variety, and compact complex algebraic varieties in $\mathbb{C}^N$ are finite (see for instance Theorem 14.3.i in [11]; here $N = 2n$), it follows that the set of solutions to the system is not compact. This set is clearly closed, thus is must be unbounded. Let $(z^{(m)})_{m \geq 1} = ((x^{(m)}, y^{(m)}))_{m \geq 1}$ be a sequence such that

$$\lim_{m \to \infty} \|z^{(m)}\|_2 = \infty.$$

Here we use the notation $\|z^{(m)}\|_2$ for the complex Euclidian norm of the element $z^{(m)} \in \mathbb{C}^{2n}$. Next note that

$$\|x^{(m)}\|_2^2 \|y^{(m)}\|_2^2 = \left(1 + \sum_{i=1}^{n-1} |x_i|^2\right)\left(1 + \sum_{i=1}^{n-1} |y_i|^2\right) \geq \|z^{(m)}\|_2^2 - 1$$

which implies $\|x^{(m)}\|_2\|y^{(m)}\|_2 \to \infty$. Now we set

$$r^{(m)} = \frac{x^{(m)}}{\|x^{(m)}\|_2}, \qquad s^{(m)} = \frac{y^{(m)}}{\|y^{(m)}\|_2}.$$

Since $\|s^{(m)}\|_2 = \|r^{(m)}\|_2 = 1$ for all m, the sequence $(r^{(m)}, s^{(m)})_{m\geq 1}$ is bounded, hence it has a convergent subsequence. By replacing the original sequence by its convergent subsequence, we may assume that the following limits exist:

$$r = \lim_{m\to\infty} r^{(m)}, \qquad s = \lim_{m\to\infty} s^{(m)}.$$

It follows that for all $k \in \mathbb{Z}_n$ we have

$$r_k s_k = \lim_{m\to\infty} r_k^{(m)} s_k^{(m)} = \lim_{m\to\infty} \frac{x_k^{(m)} y_k^{(m)}}{\|x^{(m)}\|_2\|y_k^{(m)}\|_2} = \lim_{m\to\infty} \frac{1}{\|x^{(m)}\|_2\|y^{(m)}\|_2} = 0$$

$$\hat{r}_{k,0}\hat{s}_{0,k} = \lim_{m\to\infty} \hat{r}_{k,0}^{(m)} \hat{s}_{0,k}^{(m)} = \lim_{m\to\infty} \frac{\hat{x}_{k,0}^{(m)} \hat{y}_{0,k}^{(m)}}{\|x^{(m)}\|_2\|y^{(m)}\|_2} = \lim_{m\to\infty} \frac{1}{\|x^{(m)}\|_2\|y^{(m)}\|_2} = 0.$$

This implies that

$$\begin{aligned} &supp(r) \cap supp(s) = \emptyset \ \text{ hence } |supp(r)| + |supp(s)| \leq n \\ &supp(\hat{r}_0) \cap supp(\hat{s}^0) = \emptyset \ \text{ hence } |supp(\hat{r}_0)| + |supp(\hat{s}^0)| \leq n. \end{aligned}$$

Combining this with Proposition 2.2 and Proposition 2.3, we obtain

$$2n + 2 \leq |supp(r)| + |supp(s)| + |supp(\hat{r}_0)| + |supp(\hat{s}^0)| \leq 2n.$$

This contradiction ends the proof. □

Thus Theorem 1.1 follows, by combining Proposition 2.1 with Theorem 2.1.

References

[1] Barros e Sá, N., and Bengtsson, I. Families of complex Hadamard matrices. *Linear Algebra Appl. 438*, 7 (2013), 2929–2957.

[2] Beauchamp, K., and Nicoara, R. Orthogonal maximal abelian $*$-subalgebras of the 6×6 matrices. *Linear Algebra Appl. 428*, 8-9 (2008), 1833–1853.

[3] Fasino, D. Orthogonal cauchy-like matrices. *Numerical Algorithms 92* (2023), 619–637.

[4] Haagerup, U. Orthogonal maximal abelian $*$-subalgebras of the $n \times n$ matrices and cyclic n-roots. In *Operator algebras and quantum field theory (Rome, 1996)*. Int. Press, Cambridge, MA, 1997, pp. 296–322.

[5] Haagerup, U. Cyclic p-roots of prime lengths p and related complex hadamard matrices. *arXiv:0803.2629v1 [math.AC]* (2008).

[6] Jones, V., and Sunder, V. Introduction to subfactors. *London Math. Soc. Lect. Notes 234* (1994).

[7] Jones, V. F. R. Planar algebras. *New Zealand Journal of Mathematics 52* (2021), 1–107.

[8] Nicoară, R. Subfactors and Hadamard matrices. *J. Operator Theory 64*, 2 (2010), 453–468.

[9] Popa, S. Orthogonal pairs of $*$-subalgebras in finite von Neumann algebras. *J. Operator Theory 9*, 2 (1983), 253–268.

[10] Popa, S. Classification of subfactors: the reduction to commuting squares. *Invent. Math. 101*, 1 (1990), 19–43.

[11] Rudin, W. Function theory in the unit ball of ^{n}. *Grundlehren der mathematischen Wissenschaften 241* (1980).

[12] Szöllősi, F. Complex hadamard matrices of order 6: a four-parameter family. *J. London Math. Soc. 85*, 3 (2012), 616–632.

[13] Tadej, W., and Życzkowski, K. A concise guide to complex Hadamard matrices. *Open Syst. Inf. Dyn. 13*, 2 (2006), 133–177.

[14] Tao, T. Fuglede's conjecture is false in 5 and higher dimensions. *Math. Res. Lett. 11*, 2-3 (2004), 251–258.

[15] Tao, T. An uncertainty principle for cyclic groups of prime order. *Math. Res. Lett. 12*, 1 (2005), 121–127.

[16] Werner, R. F. All teleportation and dense coding schemes. *J. Phys. A*, 34 (2001), 7081–7094.