A FINITENESS RESULT FOR CIRCULANT CORE COMPLEX HADAMARD MATRICES

REMUS NICOARA AND CHASE WORLEY
UNIVERSITY OF TENNESSEE, KNOXVILLE

Abstract. We show that for every prime number p there exist finitely many circulant core complex Hadamard matrices of size $p+1$. The proof uses a 'derivative at infinity' argument to reduce the problem to Tao's uncertainty principle for cyclic groups of prime order (see [Tao]).

1. Introduction

A complex Hadamard matrix is a matrix $H \in M_n(\mathbb{C})$ having all entries of absolute value 1 and all rows mutually orthogonal. Equivalently, $\frac{1}{\sqrt{n}}H$ is a unitary matrix with all entries of the same absolute value. For example, the *Fourier matrix* $F_n = (\omega^{ij})_{1\leqslant i,j\leqslant n}$, $\omega = e^{2\pi \mathrm{i}/n}$, is a Hadamard matrix.

In the recent years, complex Hadamard matrices have found applications in various topics of mathematics and physics, such as quantum information theory, error correcting codes, cyclic n-roots, spectral sets and Fuglede's conjecture. A general classification of real or complex Hadamard matrices is not available. A catalogue of most known complex Hadamard matrices can be found in [TaZy]. The complete classification is known for $n \leqslant 5$ ([Ha1]) and for self-adjoint matrices of order 6 ([BeN]).

Hadamard matrices arise in operator algebras as construction data for hyperfinite subfactors. A unitary matrix U is of the form $\frac{1}{\sqrt{n}}H$, H Hadamard matrix, if and only if the algebra of $n \times n$ diagonal matrices $\mathcal{D}_n$ is orthogonal onto $U\mathcal{D}_nU^*$, with respect to the inner product given by the trace on $M_n(\mathbb{C})$. Equivalently, the square of inclusions:

$$\mathfrak{C}(H) = \begin{pmatrix} \mathcal{D}_n & \subset & M_n(\mathbb{C}) \\ \cup & & \cup \\ \mathbb{C} & \subset & U\mathcal{D}_nU^* \end{pmatrix}, \tau$$

is a *commuting square*, in the sense of [Po1],[Po2], [JS]. Here τ denotes the trace on $M_n(\mathbb{C})$, normalized such that $\tau(1) = 1$. The standard invariant of the subfactor constructed from this commuting square is not at all well understood, except for some very basic examples of complex Hadamard matrices.

In this paper we look at one of the more elegant classes of complex Hadamard matrices, called circulant core matrices. These are Hadamard matrices of the form:

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & x_0 & x_1 & \cdots & x_{n-2} \\ 1 & x_{n-2} & x_0 & \cdots & x_{n-3} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 1 & x_1 & x_2 & \cdots & x_0 \end{bmatrix}$$

That is to say, a circulant core matrix A is a matrix of the form $A = \begin{bmatrix} 1 & 1 \\ 1 & A' \end{bmatrix}$, where A' is a circulant matrix. The addition of 1's on the first row and column is motivated by the normal form of a Hadamard matrix.

In this paper we prove that for every prime p there exist finitely many circulant core Hadamard matrices of size $p+1$. Examples of such matrices are known for instance when $p = 3 \mod 4$ (see [Pa]). We first turn the problem into one involving a complex algebraic variety, rather than working within the real algebraic variety of complex Hadamard matrices. Since any compact algebraic variety in $\mathbb{C}^n$ is finite, it is sufficient to show that our variety is compact. We prove it is bounded by employing a 'derivative at infinity' argument, which allows us to obtain new relations that lead to a contradiction. The contradiction is obtained by using Tao's uncertainty principle for cyclic groups of prime order, which relies on a theorem of Chebotarev (see [Tao], [Ha2]).

2. Diagonalizing Circulant Core Matrices

Let n be a fixed positive integer. Denote by $\mathcal{Q}$ the set of all circulant core matrices

$$X = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & x_0 & x_1 & \cdots & x_{n-2} \\ 1 & x_{n-2} & x_0 & \cdots & x_{n-3} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 1 & x_1 & x_2 & \cdots & x_0 \end{bmatrix}$$

defined by the vector $(x_0, \cdots, x_{n-2}) \in \mathbb{C}^{n-1}$, and such that $1 + x_0 + x_1 + ... + x_{n-2} = 0$.

Note that the set of circulant core Hadamard matrices is a subset of $\mathcal{Q}$, since the condition $1 + x_0 + x_1 + ... + x_{n-2} = 0$ is equivalent to the orthogonality of the first two rows of X for a matrix $X \in \mathcal{Q}$.

We prove that $\mathcal{Q}$ is closed to taking adjoints, and its elements commute. This motivates finding a unitary matrix which simultaneously diagonalizes the matrices in $\mathcal{Q}$.

We first show that if $X \in \mathcal{Q}$, then $X^* \in \mathcal{Q}$. Indeed, this follows from the fact that the set of circulant matrices of size $n-1$ is $*$-closed (it is in fact an abelian $*$-algebra), and $\sum_{k=0}^{n-2} \overline{x}_k = \overline{\sum_{k=0}^{n-2} x_k} = -1$.

We now show that the elements of $\mathcal{Q}$ commute. Let $X, Y \in \mathcal{Q}$ with circulant cores X' and Y' respectively. Since X' and Y' are circulant matrices, we have $X'Y' = Y'X'$. If $i \neq 0 \neq j$, then we have

$$\begin{aligned} (XY)_{ij} &= \sum_{k=0}^{n-1} x_{ik} y_{kj} \\ &= 1 + \sum_{k=1}^{n-1} x_{k-i} y_{j-k} \\ &= 1 + (X'Y')_{ij} \\ &= 1 + (Y'X')_{ij} \\ &= (YX)_{ij} \end{aligned}$$

If $i = 0, j \neq 0$, then

$$(XY)_{0j} = \sum_{k=0}^{n-1} x_{0k} y_{kj} = \sum_{k=0}^{n-1} y_{kj} = 1 + \sum_{k=1}^{n-1} y_{j-k} = 0$$
$$(YX)_{0j} = \sum_{k=0}^{n-1} y_{0k} x_{kj} = \sum_{k=0}^{n-1} x_{kj} = 1 + \sum_{k=1}^{n-1} x_{j-k} = 0$$

A similar calculation can be shown when $i \neq 0, j = 0$. Also note that

$$(XY)_{00} = \sum_{k=0}^{n-1} x_{0k} y_{k0} = \sum_{k=0}^{n-1} 1 = n = \sum_{k=0}^{n-1} 1 = \sum_{k=0}^{n-1} y_{0k} x_{k0} = (YX)_{00}.$$

Therefore, we have $XY = YX$ for any $X, Y \in \mathcal{Q}$.

Consider now the matrix

$$w = \begin{bmatrix} 1-\sqrt{n} & 1+\sqrt{n} & 0 & \cdots & 0 \\ 1 & & & & \\ \vdots & & F_{n-1} & & \\ 1 & & & & \end{bmatrix} = \begin{bmatrix} 1-\sqrt{n} & 1+\sqrt{n} & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & \lambda_1 & \lambda_2 & \cdots & \lambda_{n-2} \\ 1 & 1 & (\lambda_1)^2 & (\lambda_2)^2 & \cdots & (\lambda_{n-2})^2 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & 1 & (\lambda_1)^{n-1} & (\lambda_2)^{n-1} & \cdots & (\lambda_{n-1})^{n-2} \\ 1 & 1 & (\lambda_1)^{n-2} & (\lambda_2)^{n-2} & \cdots & (\lambda_{n-2})^{n-2} \end{bmatrix}$$

where F_{n-1} is the Fourier matrix of order $n-1$ and $\lambda_j = e^{i2\pi j/(n-1)}$ $(1 \leqslant j \leqslant n-2)$.

The definition of w is inspired by the fact that the Fourier matrix F_{n-1} diagonalizes the circulant matrices of size $n-1$. We will check that w^*aw is a diagonal matrix, for any $a \in \mathcal{Q}$. Note however that w is not a unitary matrix. We will use the polar decomposition of w, $w = u|w|$ (where $|w| = \sqrt{w^*w}$) to create a unitary $u = w|w|^{-1}$ that also diagonalizes $\mathcal{Q}$.

We first show that $|w|$ is a diagonal matrix with non-zero entries, so $|w|^{-1}$ is well defined.

Let us list the entries w_{jk} of the matrix w:

$$w_{00} = 1-\sqrt{n}$$

$$w_{01} = 1+\sqrt{n}$$

$$w_{0k} = 0 \text{ for } 2 \leqslant k \leqslant n-1$$

$$w_{j0} = 1 \text{ for } 1 \leqslant j \leqslant n-1$$

$$w_{jk} = e^{i2\pi(j-1)(k-1)/(n-1)} \text{ for } 1 \leqslant j,k \leqslant n-1$$

It follows that

$$
\begin{aligned}
(w^*w)_{00} &= (1-\sqrt{n})^2 + (n-1) = 2(n-\sqrt{n}) \\
(w^*w)_{10} &= (w^*w)_{01} = (1+\sqrt{n})(1-\sqrt{n}) + (n-1) = 0 \\
(w^*w)_{k0} &= (w^*w)_{0k} = 0 + \sum_{k=1}^{n-1} e^{i2\pi k/(n-1)} = 0 \text{ for } 2 \leqslant k \leqslant n-1 \\
(w^*w)_{11} &= (1+\sqrt{n})^2 + (n-1) = 2(n+\sqrt{n}) \\
(w^*w)_{kk} &= 0 * 0 + \sum_{k=0}^{n-2} e^{i2\pi k/(n-1)} e^{-i2\pi k/(n-1)} = n-1 \text{ for } 2 \leqslant k \leqslant n-1 \\
(w^*w)_{21} &= (w^*w)_{12} = \sum_{j=0}^{n-1} (w^*)_{2j} w_{j1} = 0(1+\sqrt{n}) + \sum_{j=1}^{n-1} e^{-i2\pi(k-1)/(n-1)} \cdot 1 = 0 \\
(w^*w)_{2k} &= (w^*w)_{k2} = \sum_{j=0}^{n-1} \overline{w}_{j2} w_{jk} = \sum_{j=1}^{n-1} \overline{w}_{j2} w_{jk} = \sum_{j=1}^{n-1} e^{-i2\pi(j-1)/(n-1)} \cdot e^{i2\pi(k-1)(j-1)/(n-1)} \\
&= \sum_{j=1}^{n-1} e^{i2\pi(j-1)(k-2)/(n-1)} = (n-1)\delta_{2k} \text{ for } 2 \leqslant k \leqslant n-1 \\
(w^*w)_{jk} &= \sum_{m=0}^{n-1} \overline{w}_{mj} w_{mk} = \sum_{m=1}^{n-1} \overline{w}_{mj} w_{mk} = \sum_{m=1}^{n-1} e^{i2\pi(m-1)(k-j)/(n-1)} \\
&= (n-1)\delta_{jk} \text{ for } 2 \leqslant j,k \leqslant n-1
\end{aligned}
$$

Hence, we have that

$$
w^*w = \begin{bmatrix}
2(n-\sqrt{n}) & 0 & 0 & 0 & \cdots & 0 \\
0 & 2(n+\sqrt{n}) & 0 & 0 & \cdots & 0 \\
0 & 0 & n-1 & 0 & \cdots & 0 \\
0 & 0 & 0 & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & n-1 & 0 \\
0 & 0 & 0 & \cdots & 0 & n-1
\end{bmatrix}
$$

It follows that $|w|^{-1}$ is a well defined diagonal matrix, which also implies $u_{jk} = w_{jk}|w|^{-1}_{kk}$. Thus

$$
u = \begin{bmatrix}
\frac{1-\sqrt{n}}{\sqrt{2(n-\sqrt{n})}} & \frac{1+\sqrt{n}}{\sqrt{2(n+\sqrt{n})}} & 0 & \cdots & 0 \\
\frac{1}{\sqrt{2(n-\sqrt{n})}} & \frac{1}{\sqrt{2(n+\sqrt{n})}} & \frac{1}{\sqrt{n-1}} & \cdots & \frac{1}{\sqrt{n-1}} \\
\frac{1}{\sqrt{2(n-\sqrt{n})}} & \frac{1}{\sqrt{2(n+\sqrt{n})}} & \frac{\lambda_1}{\sqrt{n-1}} & \cdots & \frac{\lambda_{n-2}}{\sqrt{n-1}} \\
\vdots & \vdots & \vdots & \cdots & \vdots \\
\frac{1}{\sqrt{2(n-\sqrt{n})}} & \frac{1}{\sqrt{2(n+\sqrt{n})}} & \frac{\lambda_1^{n-2}}{\sqrt{n-1}} & \cdots & \frac{\lambda_{n-2}^{n-2}}{\sqrt{n-1}}
\end{bmatrix}
$$

where $\lambda_j = e^{i2\pi j/(n-1)}$.

For the following computations, denote $\hat{x}_j$ to be the j^{th} entry of the Fourier Transform of the vector $x = (x_0, x_1, \cdots, x_{n-2})$: $\hat{x}_j = \sum_{k=0}^{n-2} e^{i2\pi kj/(n-1)} x_k$.

We now show that $d = u^* a u$ is a diagonal matrix, for all $a \in \mathcal{Q}$. The entries of the matrix d are $d_{jk} := (u^* a u)_{jk} = (w^* a w)|w|_{jj}^{-1}|w|_{kk}^{-1}$.

From $(w^* a w)_{jk} = \sum_{m=0}^{n-1} \sum_{r=0}^{n-1} \overline{w}_{mj} a_{mr} w_{rk}$, it follows that

$$\begin{aligned}
(w^* a w)_{00} &= \sum_{m=0}^{n-1} \left[\overline{w}_{m0} a_{m0} w_{00} + \sum_{r=1}^{n-1} \overline{w}_{m0} a_{mr} w_{r0} \right] \\
&= \sum_{m=0}^{n-1} \left[\overline{w}_{m0} \left((1-\sqrt{n}) + \sum_{r=1}^{n-1} a_{mr} \right) \right] \\
&= (1-\sqrt{n}) \left((1-\sqrt{n}) + \sum_{r=1}^{n-1} a_{0r} \right) + \sum_{m=1}^{n-1} \left[\overline{w}_{m0} \left((1-\sqrt{n}) + \sum_{r=1}^{n-1} a_{mr} \right) \right] \\
&= (1-\sqrt{n})((1-\sqrt{n}) + (n-1)) + \sum_{m=1}^{n-1} (1-\sqrt{n}) + \sum_{m=1}^{n-1} \sum_{r=1}^{n-1} a_{mr} \\
&= (1-\sqrt{n})((1-\sqrt{n}) + (n-1)) + \sum_{m=1}^{n-1} (1-\sqrt{n}) + \sum_{m=1}^{n-1} \sum_{r=1}^{n-1} x_{(r-m) \mod (n-1)} \\
&= (1-\sqrt{n})((1-\sqrt{n}) + (n-1)) + (1-\sqrt{n})(n-1) + (n-1) \sum_{k=0}^{n-2} x_k \\
&= (1-\sqrt{n})((1-\sqrt{n}) + (n-1)) + (1-\sqrt{n})(n-1) + (n-1)(-1) \\
&= -2n(1-\sqrt{n})
\end{aligned}$$

Hence, we have that

$$d_{00} = \frac{-2n(1-\sqrt{n})}{2(n-\sqrt{n})} = -\sqrt{n}.$$

We also have

$$\begin{aligned}
(w^* a w)_{11} &= \sum_{m=0}^{n-1} \left[\overline{w}_{m1} a_{m0} w_{01} + \sum_{r=1}^{n-1} \overline{w}_{m1} a_{mr} w_{r1} \right] \\
&= \sum_{m=0}^{n-1} \left[\overline{w}_{m1} \left((1+\sqrt{n}) + \sum_{r=1}^{n-1} a_{mr} \right) \right] \\
&= \overline{w}_{01}((1+\sqrt{n}) + \sum_{r=1}^{n-1} a_{0r}) + \sum_{m=1}^{n-1} \sum_{r=1}^{n-1} \overline{w}_{m1}(1+\sqrt{n}) + \sum_{m=1}^{n-1} \sum_{r=1}^{n-1} \overline{w}_{m1} a_{mr} \\
&= (1+\sqrt{n})((1+\sqrt{n}) + (n-1)) + (1+\sqrt{n})(n-1) + \sum_{m=1}^{n-1} \sum_{r=1}^{n-1} \overline{w}_{m1} a_{mr} \\
&= (1+\sqrt{n})((1+\sqrt{n}) + (n-1)) + (1+\sqrt{n})(n-1) - (n-1) \\
&= 2n(1+\sqrt{n})
\end{aligned}$$

which yields $d_{11} = \frac{2n(1+\sqrt{n})}{2(n+\sqrt{n})} = \sqrt{n}$.

Next we have

$$\begin{aligned}(w^*aw)_{01} &= \sum_{m=0}^{n-1}\left[\overline{w}_{m0}a_{m0}w_{01} + \sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}\right] \\ &= \overline{w}_{00}a_{00}w_{01} + \sum_{r=1}^{n-1}\overline{w}_{00}a_{0r} + \sum_{m=1}^{n-1}\overline{w}_{m0}a_{m0}w_{01} + \sum_{m=1}^{n-1}\sum_{m=1}^{n-1}\overline{w}_{m0}a_{mr} \\ &= (1-\sqrt{n})(1)(1+\sqrt{n}) + (1-\sqrt{n})(n-1) + (1+\sqrt{n})(n-1) + (-1)(n-1) \\ &= 0\end{aligned}$$

which gives $d_{01} = d_{10} = 0$.

Now let $2 \leqslant j \leqslant n-1$. It follows that

$$\begin{aligned}(w^*aw)_{0j} &= \sum_{m=0}^{n-1}\left[\overline{w}_{m0}a_{m0}w_{0j} + \sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{rj}\right] = \sum_{m=0}^{n-1}\left[\sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{rj}\right] \\ &= \sum_{r=1}^{n-1}\overline{w}_{00}a_{0r}w_{rj} + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{rj} \\ &= (1-\sqrt{n})\sum_{m=1}^{n-1}e^{i2\pi(r-1)(j-1)/(n-1)} + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{rj} \\ &= \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{rj} = \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}e^{i2\pi(r-1)(j-1)/(n-1)}x_{(r-m) \mod (n-1)} \\ &= \sum_{r=1}^{n-1}\left[e^{i2\pi(r-1)(j-1)/(n-1)}\sum_{m=1}^{n-1}x_{(r-m) \mod (n-1)}\right] = -\sum_{r=1}^{n-1}e^{i2\pi(r-1)(j-1)/(n-1)} = 0\end{aligned}$$

hence $d_{0j} = d_{j0} = 0$ for $2 \leqslant j \leqslant n-1$.

Similarly we have

$$\begin{aligned}(w^*aw)_{1j} &= \sum_{m=0}^{n-1}\left[\overline{w}_{m1}a_{m0}w_{0j} + \sum_{r=1}^{n-1}\overline{w}_{m1}a_{mr}w_{rj}\right] \\ &= \overline{w}_{01}a_{00}w_{0j} + \sum_{r=1}^{n-1}\overline{w}_{01}a_{0r}w_{rj} + \sum_{m=1}^{n-1}\overline{w}_{m1}a_{m0}w_{0j} + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m1}a_{mr}w_{rj} \\ &= (1+\sqrt{n})(1)(0) + \sum_{r=1}^{n-1}(1+\sqrt{n})(1)e^{i2\pi(r-1)(j-1)/(n-1)} + \sum_{m=1}^{n-1}(1)(1)(0) + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}(1)a_{mr}w_{rj} \\ &= \sum_{r=1}^{n-1}\sum_{m=1}^{n-1}a_{mr}w_{rj} = \sum_{r=1}^{n-1}\left[w_{rj}\sum_{m=1}^{n-1}a_{mr}\right] \\ &= (-1)\sum_{r=1}^{n-1}e^{i2\pi(r-1)(j-1)/(n-1)} = 0\end{aligned}$$

which shows that $d_{1j} = d_{j1} = 0$ for $2 \leqslant j \leqslant n-1$.

Note that $a_{mr} = a_{(m+1)(r+1)}$ for $m, r \geqslant 1$. For $2 \leqslant j, k \leqslant n-1$, we have that

$$
\begin{aligned}
(w^* a w)_{jk} &= \sum_{m=0}^{n-1} \left[\overline{mj} a_{m0} w_{0k} + \sum_{r=1}^{n-1} \overline{w}_{mj} a_{mr} w_{rk} \right] \\
&= \sum_{m=0}^{n-1} \left[\sum_{r=1}^{n-1} \overline{w}_{mj} a_{mr} w_{rk} \right] = \sum_{r=1}^{n-1} \overline{w}_{0j} a_{0r} w_{rk} + \sum_{m=1}^{n-1} \sum_{r=1}^{n-1} \overline{w}_{mj} a_{mr} w_{rk} \\
&= \sum_{r=1}^{n-1} (0)(1) w_{rk} + \sum_{m=1}^{n-1} \sum_{r=1}^{n-1} \overline{w}_{mj} a_{mr} w_{rk} = \sum_{m=1}^{n-1} \sum_{r=1}^{n-1} \overline{w}_{mj} a_{mr} w_{rk} \\
&= \sum_{m=0}^{n-2} \sum_{r=0}^{n-2} e^{i2\pi[-m(j-1)+r(k-1)]/(n-1)} x_{(r-m) \mod (n-1)} \\
&= (n-1) \hat{x}_{j-1} \delta_{jk}
\end{aligned}
$$

The last computation proves that $d_{jk} = d_{kj} = \frac{(n-1)\hat{x}_{j-1}}{(n-1)} \delta_{jk} = \hat{x}_{j-1} \delta_{jk}$. Thus, $d = u^* a u$ is indeed a diagonal matrix:

$$
u^* a u = \begin{bmatrix}
-\sqrt{n} & 0 & 0 & 0 & \cdots & 0 \\
0 & \sqrt{n} & 0 & 0 & \cdots & 0 \\
0 & 0 & \hat{x}_1 & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & \hat{x}_{n-3} & 0 \\
0 & 0 & 0 & \cdots & 0 & \hat{x}_{n-2}
\end{bmatrix}
$$

3. The finiteness result

We are now ready to prove the main result of this paper.

Theorem 3.1. *Let p be a prime number. Then there exist at most finitely many circulant core complex Hadamard matrices of size $n = p + 1$.*

Proof. Consider a circulant core Hadamard matrix a:

$$a = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & x_0 & x_1 & \cdots & x_{n-2} \\ 1 & x_{n-2} & x_0 & \cdots & x_{n-3} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 1 & x_1 & x_2 & \cdots & x_0 \end{bmatrix}$$

Since the first two rows of a are orthogonal we know that $a \in \mathcal{Q}$, from which it also follows that $a^* \in \mathcal{Q}$. Let $y_j = \bar{x}_j$, for $0 \leqslant j \leqslant n-2$. Since a is Hadamard, we have $x_j \cdot y_j = 1$.

Denote by $\tilde{x}, \tilde{y}$ the vectors in $\mathbb{C}^n$ which are the diagonals of the matrices u^*au, u^*a^*u, where u is the unitary that diagonalizes $\mathcal{Q}$ defined in the previous section. We have

$$\tilde{x} = (-\sqrt{n}, \sqrt{n}, \hat{x}_1, \cdots, \hat{x}_{p-1})$$

and

$$\tilde{y} = (-\sqrt{n}, \sqrt{n}, \hat{y}_{-1}, \cdots, \hat{y}_{-(p-1)}).$$

Note that the indices are considered modulo p.

The fact that the matrix a is Hadamard yields the following system of equations:

$$\sum_{k=0}^{p-1} x_k = \sum_{k=0}^{p-1} y_k = -1 \tag{1}$$

$$x_k y_k = 1 \quad \text{for } k = 0, \cdots, p-1 \tag{2}$$

$$\hat{x}_k \hat{y}_{-k} = n \quad \text{for } k = 1, \cdots, p-1 \tag{3}$$

The second set of equations encodes the fact that the entries of a are of absolute value 1. The first and third sets of equations encode the fact that $a^*a = nI$. Indeed, this follows by conjugating this relation by u^* and using the formulas for the diagonal matrices u^*au, u^*a^*u.

Let W be the complex algebraic variety given by the equations (1), (2), (3). By a classical result, any compact algebraic variety in $\mathbb{C}^n$ is a finite set. Since W is clearly closed, to show W is finite it is sufficient to show that it is bounded. Reasoning by contradiction, assume that there exists a sequence of elements $(x^{(m)}, y^{(m)})$ in W, where $x^{(m)} = (x_0^{(m)}, \cdots, x_{p-1}^{(m)})$ and $y^{(m)} = (y_0^{(m)}, \cdots, y_{p-1}^{(m)})$, such that $\left\|x^{(m)}\right\|_2^2 + \left\|y^{(m)}\right\|_2^2 \to$

∞ as $m \to \infty$. By Cauchy-Schwartz, we have the following inequalities for all m:

$$\begin{aligned}\frac{1}{\sqrt{p}} &\leqslant \left\|x^{(m)}\right\|_2 \\ \frac{1}{\sqrt{p}} &\leqslant \left\|y^{(m)}\right\|_2 \\ p &\leqslant \left\|x^{(m)}\right\|_2 \left\|y^{(m)}\right\|_2\end{aligned}$$

Since $x^{(m)}$ and $y^{(m)}$ are bounded from below by a positive constant and $\left\|x^{(m)}\right\|_2^2 + \left\|y^{(m)}\right\|_2^2 \to \infty$, by eventually passing to a subsequence we may assume that $\left\|x^{(m)}\right\|_2 \left\|y^{(m)}\right\|_2 \to \infty$ as $m \to \infty$.

Define $u^{(m)} = \frac{x^{(m)}}{\left\|x^{(m)}\right\|_2}$, and $v^{(m)} = \frac{y^{(m)}}{\left\|y^{(m)}\right\|_2}$. By using the compactness of the unit ball of $\mathbb{C}^n$, after eventually passing to a subsequence we may assume the following limits exist:

$$u = \lim_{m\to\infty} \frac{x^{(m)}}{\left\|x^{(m)}\right\|_2} \text{ and } v = \lim_{m\to\infty} \frac{y^{(m)}}{\left\|y^{(m)}\right\|_2}.$$

Let $u = (u_0, ..., u_{p-1})$ and $v = (v_0, ..., v_{p-1})$. It follows that for $k = 0, \cdots, p-1$ we have

$$u_k v_k = \lim_{m\to\infty} \frac{x_k^{(m)}}{\left\|x^{(m)}\right\|_2} \frac{y_k^{(m)}}{\left\|y^{(m)}\right\|_2} = \lim_{m\to\infty} \frac{1}{\left\|x^{(m)}\right\|_2 \left\|y^{(m)}\right\|_2} = 0.$$

Similarly, after eventually passing to a subsequence we also have for $k = 1, \cdots, p-1$:

$$\widehat{u}_k \widehat{v}_{-k} = 0.$$

Thus, on the set $\{1, ..., p\}$ we have

$$\operatorname{supp}(u) \cap \operatorname{supp}(v) = \varnothing$$

and

$$\operatorname{supp}(\hat{u}) \cap (-\operatorname{supp}(\hat{v})) = \varnothing$$

It follows that

$$\begin{aligned}|\operatorname{supp}(u)| + |\operatorname{supp}(v)| &\leqslant p \\ |\operatorname{supp}(\hat{u})| + |\operatorname{supp}(\hat{v})| &\leqslant p\end{aligned}$$

so

$$|\operatorname{supp}(u)| + |\operatorname{supp}(v)| + |\operatorname{supp}(\hat{u})| + |\operatorname{supp}(\hat{v})| \leqslant 2p.$$

However, by the Uncertainty Principle in [Tao] applied to the map $u \neq 0$ we have: $|\operatorname{supp}(u)| + |\operatorname{supp}(\hat{u})| \geqslant p + 1$, and similarly for $v \neq 0$: $|\operatorname{supp}(v)| + |\operatorname{supp}(\hat{v})| \geqslant p + 1$.

Hence we obtain

$$\begin{aligned} 2p+2 &\leqslant |\mathrm{supp}(u)| + |\mathrm{supp}(v)| + |\mathrm{supp}(\hat{u})| + |\mathrm{supp}(\hat{v})| \\ &\leqslant 2p \end{aligned}$$

which is a contradiction.

□

References

[BeN] K. Beauchamp and R. Nicoara, Orthogonal maximal abelian $*$-subalgebras of the 6×6 matrices, Journal of Linear Algebra and Applications, **428** (2008), 1833-1853

[Di] P. Dita, *Some results on the parametrization of complex Hadamard matrices*, J. Phys. A, **37** (2004) no. 20, 5355-5374

[Ha1] U. Haagerup, *Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic n-roots*, Operator Algebras and Quantum Field Theory (ed. S.Doplicher et al.), International Press (1997), 296-322

[Ha2] U. Haagerup, *Cyclic p-roots of prime lengths p and related complex Hadamard matrices*, preprint (2008)

[Jo] V. F. R. Jones, *Index for subfactors*, Invent. Math **72** (1983), 1–25

[JS] V. F. R. Jones and V. S. Sunder, *Introduction to subfactors*, London Math. Soc. Lecture Notes Series **234**, Cambridge University Press, 1997

[Ni1] R. Nicoara, A finiteness result for commuting squares of matrix algebras, *J. of Operator Theory* **55** (2006), no. 2, 295-310

[Ni2] R. Nicoara, Subfactors and Hadamard matrices, *J. of Operator Theory* **64** (2010)

[NiWh] R. Nicoara, J. White, *The defect of a group-type commuting square*, Revue Roumaine Math., Issue 2 (2014)

[Pa] R.E.A.C Paley, *Journal of Mathematics and Physics*, Volume 12, pages 311-320 (1993)

[Pe] M. Petrescu, *Existence of continuous families of complex Hadamard matrices of certain prime dimensions and related results*, PhD thesis, Univ. of California Los Angeles, 1997

[Po1] S.Popa, *Classification of subfactors : the reduction to commuting squares*, Invent. Math., **101**(1990),19-43

[Po2] S.Popa, *Othogonal pairs of *-subalgebras in finite von Neumann algebras*, J. Operator Theory **9**, 253-268 (1983)

[TaZy] W. Tadej and K. Zyczkowski, *A concise guide to complex Hadamard matrices* Open Systems & Infor. Dyn. **13**(2006), 133-177

[Tao] Terence Tao, *An uncertainty principle for cyclic groups of prime order* Mathematical Research Letters **12**(2003)