Trades in complex Hadamard matrices*

PADRAIG Ó CATHÁIN †
IAN M. WANLESS ‡
School of Mathematical Sciences
Monash University, VIC 3800, Australia

No Institute Given

Abstract. A *trade* in a complex Hadamard matrix is a set of entries which can be changed to obtain a different complex Hadamard matrix. We show that in a real Hadamard matrix of order n all trades contain at least n entries. We call a trade *rectangular* if it consists of a submatrix that can be multiplied by some scalar $c \neq 1$ to obtain another complex Hadamard matrix. We give a characterisation of rectangular trades in complex Hadamard matrices of order n and show that they all contain at least n entries. We conjecture that all trades in complex Hadamard matrices contain at least n entries.
2010 Mathematics Subject classification: 05B05, 42C15, 94A08
A *complex Hadamard matrix* of order n is an $n \times n$ complex matrix with unimodular entries which satisfies the matrix equation

$$HH^{\dagger} = nI_n,$$

where $H^{\dagger}$ is the conjugate transpose of H. If the entries are real (hence ± 1) the matrix is Hadamard. The notion of a trade is well known in the study of t-designs and Latin squares [1]. For a complex Hadamard matrix we define a *trade* to be a set of entries which can be altered to obtain a different complex Hadamard matrix of the same order. In other words, a set T of entries in a complex Hadamard matrix H is a trade if there exists another complex Hadamard matrix H' such that H and H' disagree on every entry in T but agree otherwise. If H is a real Hadamard matrix, we would insist that H' is also real.

Example 1. The 8 shaded entries in the Paley Hadamard matrix below form a trade.

$$\begin{pmatrix}
+ & + & + & + & + & + & + & + \\
+ & - & - & - & + & - & + & + \\
+ & + & - & - & - & + & - & + \\
+ & + & + & - & - & - & + & - \\
+ & - & + & + & - & - & - & + \\
+ & + & - & + & + & - & - & - \\
+ & - & + & - & + & + & - & - \\
+ & - & - & + & - & + & + & -
\end{pmatrix}$$

*This work was inspired by the discussion after Will Orrick's talk at the ADTHM'14 workshop, and most of the work was undertaken at the workshop. The authors are grateful to the workshop organisers and to BIRS. Research supported by ARC grants FT110100065 and DP120103067.
†*E-mail: p.ocathain@gmail.com*
‡*E-mail: ian.wanless@monash.edu*

If each of the shaded entries is replaced by its negative, the result is another Hadamard matrix.

We use the word *switch* to describe the process of replacing a trade by a new set of entries (which must themselves form a trade). In keeping with the precedent from design theory, our trades are simply a set of entries that can be switched. Information about what they can be switched to does not form part of the trade (although it may be helpful in order to see that something is a trade). For real Hadamard matrices there can only be one way to switch a given trade, since only two symbols are allowed in the matrices and switching must change every entry in a trade. However, for complex Hadamard matrices there can be more than one way to switch a given trade.

Example 2. Let u be a nontrivial third root of unity. The following matrix is a 7×7 complex Hadamard matrix. The shaded entries again form a trade; they can be multiplied by an arbitrary complex number c of modulus 1 to obtain another complex Hadamard matrix. This matrix is due originally to Petrescu [5], and is available in the online database [2].

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -u & u & -u^2 & -1 & -1 & -u \\ 1 & u & -u & -1 & -u^2 & -1 & -u \\ 1 & -u^2 & -1 & u & -u & -u & -1 \\ 1 & -1 & -u^2 & -u & u & -u & -1 \\ 1 & -1 & -1 & -u & -u & u & -u^2 \\ 1 & -u & -u & -1 & -1 & -u^2 & u \end{pmatrix}$$

The *size* of a trade is the number of entries in it. We say that a trade is *rectangular* if the entries in the trade form a submatrix that can be switched by multiplying all entries in the trade by some complex number $c \neq 1$ of unit modulus. In a complex Hadamard matrix each row and column is a rectangular trade. Thus there are always $1 \times n$ and $n \times 1$ rectangular trades. Similarly, in any real Hadamard matrix we may exchange any pair of rows to obtain another Hadamard matrix. The rows that we exchange necessarily differ in exactly half the columns, so this reveals a $2 \times \frac{n}{2}$ rectangular trade (and similarly there are always $\frac{n}{2} \times 2$ rectangular trades in real Hadamard matrices). Less trivial trades were used by Orrick [4] to generate many non-equivalent Hadamard matrices of orders 32 and 36. The smaller of Orrick's two types of trades was a $4 \times \frac{n}{4}$ rectangular trade that he called a "closed quadruple". Closed quadruples are often but not always present in Hadamard matrices. The trades just discussed all have size equal to the order n of the host matrix. The trade in Example 1 is a non-rectangular example with the same property.

Trades in real Hadamard matrices and related codes and designs have been studied occasionally in the literature, either to produce invariants to aid with classification or to produce many inequivalent Hadamard matrices. See [4] and the references cited there. In the complex case, trades are related to parameterising complex Hadamard matrices, some computational and theoretical results are surveyed in [6].

Throughout this note we will assume that $H = [h_{ij}]$ is a complex Hadamard matrix of order n. We will use r_i to denote the i-th row of H. If B is a set of columns then

$r_{i,B}$ denotes the row vector which is equal to r_i on the coordinates B and zero elsewhere. We use $\overline{B}$ for the complement of the set B.
We now characterise rectangular trades. We will use $\langle \cdot, \cdot \rangle$ for the standard Hermitian inner product under which rows of a complex Hadamard matrix are orthogonal.

Lemma 1. *Suppose that a trade T in a complex Hadamard matrix H can be switched by multiplying the entries in T by a complex number $c \neq 1$ of unit modulus.*

1. *Let B be the set of columns in which row r_i of H contains elements of T. If r_j is a row of H that contains no elements of T then $r_{i,B}$ is orthogonal to $r_{j,B}$.*
2. *T forms a rectangular trade on rows A and columns B if and only if $r_{i,B}$ is orthogonal to $r_{j,B}$ for every $r_i \in A$ and $r_j \notin A$.*

Proof. First, since the rows of H are orthogonal, we have that

$$0 = \langle r_i, r_j \rangle = \langle r_{i,B}, r_{j,B} \rangle + \langle r_{i,\overline{B}}, r_{j,\overline{B}} \rangle$$

Now, multiplying the entries in the set of columns B by c, we have that

$$0 = \langle cr_{i,B}, r_{j,B} \rangle + \langle r_{i,\overline{B}}, r_{j,\overline{B}} \rangle = c\langle r_{i,B}, r_{j,B} \rangle + \langle r_{i,\overline{B}}, r_{j,\overline{B}} \rangle$$

Subtracting, we find that $(c-1)\langle r_{i,B}, r_{j,B} \rangle = 0$. Given that $c \neq 1$ the first claim of the Lemma follows.
We have just shown the necessity of the condition in the second claim. To check sufficiency we just have to verify that any two rows r_i, r_j in A will be orthogonal after multiplication by c. This follows from

$$\langle cr_{i,B}, cr_{j,B} \rangle + \langle r_{i,\overline{B}}, r_{j,\overline{B}} \rangle = |c|\langle r_{i,B}, r_{j,B} \rangle + \langle r_{i,\overline{B}}, r_{j,\overline{B}} \rangle = \langle r_{i,B}, r_{j,B} \rangle + \langle r_{i,\overline{B}}, r_{j,\overline{B}} \rangle = 0.$$

It is of interest to consider the size of a smallest possible trade. For (real) Hadamard matrices of order n we show that arbitrary trades have size at least n, with equality obviously achievable in a variety of ways. Then we show that in the general case rectangular trades have size at least n. The question for arbitrary trades in complex Hadamard matrices remains open.

Theorem 1. *Let H be a Hadamard matrix of order n. Any trade in H has size at least n.*

Proof. Suppose that H' is a Hadamard matrix that differs from H in strictly fewer than n entries. Without loss of generality, we assume that H is normalised, that the first row of H contains the smallest non-zero number, say k, of differences between H and H', and that all differences between H and H' occur in the first r rows. By construction there are at least rk entries in the trade, so $rk < n$. Now consider the submatrix S of H formed by the first k columns and the bottom $n-r$ rows. By Lemma 1, we know that each row of S is orthogonal to the all ones vector. If follows that S contains $(n-r)k/2$ negative entries. But the first column of S consists entirely of ones. So by the pigeon-hole principle, some other column of S must contain at least

$$\frac{(n-r)k}{2(k-1)} > \frac{nk-n}{2(k-1)} = \frac{n}{2}$$

negative entries. This column of H is not orthogonal to the first column, a contradiction.

Now we consider complex Hadamard matrices. The following lemma is the key step in our proof.

Lemma 2. *Let H be a complex Hadamard matrix of order n, and B a set of k columns of H. If α is a non-zero linear combination of the elements of B then α has at least $\lceil \frac{n}{k} \rceil$ non-zero entries.*

Proof. Without loss of generality, we can write H in the form

$$H = \begin{pmatrix} T & U \\ V & W \end{pmatrix}$$

where T contains the columns in B and the rows in which α is non-zero. We will identify a linear dependence among the rows of U, then use this and an expression for the inner product of r_1 and r_2 to derive the required result. We assume that there are t non-zero entries α_i in α and that if $t \geqslant 2$ then they obey $|\alpha_2| \geqslant |\alpha_1| \geqslant |\alpha_i|$ for $3 \leqslant i \leqslant t$. We need to show that $t \geqslant \lceil \frac{n}{k} \rceil$.
For any column c_j not in B, we have that $\langle c_j, \alpha \rangle = 0$ since the columns of H are orthogonal. Thus every column of U is orthogonal to α, and so there exists a linear dependence among the rows of U, explicitly: $h_{1j} = \sum_{i=2}^{t} -\alpha_i \alpha_1^{-1} h_{ij}$, for any $j \notin B$. In particular, this shows that indeed $t \geqslant 2$.
Since H is Hadamard, we know that all of the h_{ij} have absolute value 1, and that rows of H are necessarily orthogonal:

$$\begin{aligned} \langle r_1, r_2 \rangle &= \langle r_{1,B}, r_{2,B} \rangle + \langle r_{1,\overline{B}}, r_{2,\overline{B}} \rangle \\ &= \langle r_{1,B}, r_{2,B} \rangle + \langle \sum_{i=2}^{t} -\alpha_i \alpha_1^{-1} r_{i,\overline{B}}, r_{2,\overline{B}} \rangle \\ &= \langle r_{1,B}, r_{2,B} \rangle + \sum_{i=2}^{t} -\alpha_i \alpha_1^{-1} \langle r_{i,\overline{B}}, r_{2,\overline{B}} \rangle \end{aligned}$$

Since $\langle r_1, r_2 \rangle = 0$ and $\langle r_{i,\overline{B}}, r_{2,\overline{B}} \rangle = -\langle r_{i,B}, r_{2,B} \rangle$, this means that

$$\alpha_2 \alpha_1^{-1} \langle r_{2,\overline{B}}, r_{2,\overline{B}} \rangle = \langle r_{1,B}, r_{2,B} \rangle + \sum_{i=3}^{t} \alpha_i \alpha_1^{-1} \langle r_{i,B}, r_{2,B} \rangle \tag{1}$$

Now, each inner product $\langle r_{i,B}, r_{2,B} \rangle$ is a sum of k complex numbers of modulus one, and $|\alpha_i \alpha_1^{-1}| \leqslant 1$ for $i \geqslant 3$. So the absolute value of the right hand side of (1) is at most $(t-1)k$. In contrast, the absolute value of the left hand side of (1) is $|\alpha_2 \alpha_1^{-1}|(n-k) \geqslant n-k$. It follows that $n-k \leqslant (t-1)k$, and hence $t \geqslant \lceil \frac{n}{k} \rceil$.

In the special case that $t = \frac{n}{k}$, we observe that $n-k = t(k-1)$. This forces $|\langle r_{i,B}, r_{2,B} \rangle| = k$ for $i \neq 2$, which implies that all of the $r_{i,B}$ are collinear, and hence that T is a rank one submatrix of H.

Theorem 2. *If H is a complex Hadamard matrix and T is a rectangular trade with a rows and b columns then $ab \geqslant n$.*

Proof. Without loss of generality, T consists of the upper left $a \times b$ submatrix of H. By hypothesis, $\gamma_1 = \sum_{1 \leqslant i \leqslant a} r_i$ and $\gamma_c = \sum_{1 \leqslant i \leqslant a} (c r_{i,B} + r_{i,\overline{B}})$ are both orthogonal to the space U spanned by the remaining $n-a$ rows of H. Now consider $\gamma_1 - \gamma_c$, which is zero in any column not contained in T. Observe that the orthogonal complement of U is a-dimensional, and that the initial a rows of H span this space: thus $\gamma_1 - \gamma_c$ is in the span of these rows, Lemma 2 applies, and $ab \geqslant n$.

Let H be a Fourier Hadamard matrix of order v, and suppose that $t \mid v$. Then there exist t rows of H containing only t^{th} roots of unity. Their sum vanishes on all but $\frac{v}{t}$ coordinates, so Lemma 2 is best possible.
On the other hand, if H is Fourier of prime order p, the only vanishing sum of p^{th} roots is the complete one. So in this case, a linear combination of at most t rows will contain at most t zero entries.

Open questions

On the basis of Theorem 1 and Theorem 2 we are inclined to think that the answer to the following question is negative:
Question 1: Can there exist trades of size less than n in an $n \times n$ complex Hadamard matrix?

It would also be nice to know how "universal" the rectangular trades we have studied are.
Question 2: Is every trade in a complex Hadamard matrix a linear combination of rectangular trades of the form characterised in Lemma 1?

This work was motivated in part by problems in the construction of compressed sensing matrices [3]. Optimal complex Hadamard matrices for our construction have the property that linear combinations of t rows vanish in at most t components.
Question 3: Describe other families of Hadamard matrices with the property that no linear combination of t rows contains more than t zeros. Or, if such matrices are rare, describe families in which no linear combination of t rows contain more than $f(t)$ zeros for some slowly growing function f.

References

1. E. J. Billington, Combinatorial trades: a survey of recent results, in: W.D. Wallis (Ed.), Designs 2002: Further Computational and Constructive Design Theory, Kluwer, Boston, 2003, pp. 47–67.
2. W. Bruzda, W. Tadej and K. Życzkowski, Catalogue of complex Hadamard matrices, `http://chaos.if.uj.edu.pl/~karol/hadamard/`, retrieved 10/09/2014.
3. D. Bryant and P. Ó Catháin, An asymptotic existence result on compressed sensing matrices. submitted, March 2014.
4. W. P. Orrick, Switching operations for Hadamard matrices, *SIAM J. Discrete Math.* **22** (2008), 31–50.
5. M. Petrescu, Existence of Continuous Families of Complex Hadamard Matrices of Certain Prime Dimensions and Related Results, *PhD thesis, University of California, Los Angeles,* (1997).
6. W. Tadej and K. Życzkowski A Concise Guide to Complex Hadamard Matrices, *Open Systems & Information Dynamics*, **13** (2006), 133–177.