Bull. Austral. Math. Soc. 05B20
Vol. 44 (1991) [109–115]

EQUIVALENCE CLASSES OF INVERSE ORTHOGONAL AND UNIT HADAMARD MATRICES

R. Craigen

In 1867, Sylvester considered $n \times n$ matrices, (a_{ij}), with nonzero complex-valued entries, which satisfy $(a_{ij})\left(a_{ij}{}^{-1}\right) = nI$. Such a matrix he called ***inverse orthogonal***. If an inverse orthogonal matrix has all entries on the unit circle, it is a ***unit Hadamard matrix***, and we have orthogonality in the usual sense. Any two inverse orthogonal (respectively, unit Hadamard) matrices are ***equivalent*** if one can be transformed into the other by a series of operations involving permutation of the rows and columns and multiplication of all the entries in any given row or column by a complex number (respectively a number on the unit circle). He stated without proof that there is exactly one equivalence class of inverse orthogonal matrices (and hence also of unit Hadamard matrices) in prime orders and that in general the number of equivalence classes is equal to the number of distinct factorisations of the order. In 1893 Hadamard showed this assertion to be false in the case of unit Hadamard matrices of non-prime order. We give the correct number of equivalence classes for each non-prime order, and orders $\leqslant 3$, giving a complete, irredundant set of class representatives in each order $\leqslant 4$ for both types of matrices.

1. Introduction

Recall that the determinant of a matrix with entries from the unit disc in $\mathbb{C}$ achieves the Hadamard bound if and only if the rows are pairwise orthogonal and all entries have absolute value 1 [4].

Definition: A complex valued $n \times n$ matrix A with entries on the unit circle whose rows are pairwise orthogonal is a *unit Hadamard matrix of order n*.

A warning to the reader: A unit Hadamard matrix is not the same as what Butson and others have called a *generalised Hadamard matrix* (in spite of this being perhaps the most natural generalisation—Hadamard matrices, we recall, arose at first as a restriction of the notion of what we have termed unit Hadamard matrices). Butson [**1**] refers only to those matrices whose entries are nth roots of unity; others [**3, 6**] use the term *generalised Hadamard matrix* to refer to matrices with entries taken from a group, satisfying certain combinatorial constraints.

Received 17 August 90
Thanks to Cantian Lin, who suggested the term *unit Hadamard matrix*.

https://doi.org/10.1017/S0004972700029506 Published online by Cambridge University Press

DEFINITION: A *monomial matrix* is a unitary matrix with precisely one nonzero entry in each row and column. Two unit Hadamard matrices A and B are *equivalent* provided there are monomial matrices M and N such that $A = MBN$.

Clearly the nonzero entries of a monomial matrix lie on the unit circle, and such matrices form a group. Thus we have defined an equivalence relation on the set of unit Hadamard matrices. Sylvester studied these equivalence classes in 1867, pointing out that there is at least one class in each order n, given by the *Vandermonde*, V_n, of the nth roots of unity [7]. Using the Kronecker product he constructed distinct unit Hadamard matrices in each order, one for each factorisation of the order. For example in order 4, he constructed the matrices

$$V_2 \otimes V_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \tag{1}$$

$$V_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \tag{2}$$

He seemed sure that this procedure would give inequivalent matrices representing all equivalence classes in each order. [His precise words were, " ... the problem ... admits of a general and complete solution ... what I have scarcely a doubt is true (but which I have not yet attempted to demonstrate), that such a matrix [the Vandermonde in prime orders] ... contains the complete solution ... I now proceed to state [the rule for arbitrary orders] ... there will be as many distinct types of solutions [equivalence classes] as there are distinct modes of breaking up n into factors."] (Actually his statement was slightly more general than this, as we shall see in Section 4.) In 1893 Hadamard [4] demonstrated this to be false in the case of non-prime orders. We shall give a slight variant of his method in Sections 2 and 3 and consider the analogous problem for the more general case of *inverse orthogonal matrices* (the problem originally considered by Sylvester) in Section 4.

There has been considerable work on the problem of enumerating the equivalence classes of Hadamard matrices [8, Chapter 9]. Unit Hadamard matrices whose entries are all real are just Hadamard matrices, and equivalence classes of Hadamard matrices are the same, whether our definition or the usual one (involving only *real* monomial matrices) is used. Sylvester's claim is contradicted even in this setting, for there are *sixty* Hadamard equivalence classes in order 24 (Kimura, [5]), while there are only *seven* distinct factorisations of 24. Moreover, we see that among those constructed

https://doi.org/10.1017/S0004972700029506 Published online by Cambridge University Press

by Sylvester, the only matrices equivalent to real matrices would be those formed by applying the Kronecker product repeatedly to V_2, and so the order would necessarily be a power of 2. Hence, a Hadamard matrix existing in any other order is a counterexample. Butson [1] pointed out that Sylvester was even incorrect in claiming that the matrices corresponding to two different factorisations of the order are inequivalent, for if $(i,j) = 1$, $V_i \otimes V_j$ is equivalent to V_{ij}. This is easy to see if we consider the fact that the matrices constructed by Sylvester are precisely the character tables of abelian groups, each Kronecker product reflecting a decomposition of the group into direct factors. The rest follows from the primary decomposition theorem for abelian groups.

2. Enumerating the classes in orders $\leqslant 4$

There is clearly only one class of unit Hadamard matrices of order 1. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a unit Hadamard matrix of order 2. Any unit Hadamard matrix may be *normalised* so that the first row and column consist of all 1's by multiplying by appropriate diagonal monomial matrices. So without loss of generality, we may take $a = b = c = 1$, and this clearly forces $d = -1$. Thus there is only one class in order 2.

Now let $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & a & b \\ 1 & c & d \end{pmatrix}$ be a normalised unit Hadamard matrix of order 3. The condition of orthogonality between the first row and column and the others gives us the relations $b = c = -1 - a$ and $d = a$. Thus orthogonality between rows 2 and 3 yields $1 + a(-1-\overline{a}) + (-1-a)\overline{a} = 0$. Thus $1 + a + a^2 = 0$, and so a is a cube root of unity. It follows that there is exactly one class in order 3, represented by V_3.

We shall now demonstrate that the set of such classes in order 4 has the same cardinality as the continuum. Let $\lambda \in \mathbb{C}$, $|\lambda| = 1$. Then

$$A(\lambda) := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & \lambda & -\lambda \\ 1 & -1 & -\lambda & \lambda \end{pmatrix} \tag{3}$$

is a unit Hadamard matrix (equivalent to that considered by Hadamard [4]). We claim that $A(\lambda)$ is equivalent to $A(\lambda')$ if and only if $\lambda' = \pm\lambda$ or $\pm\overline{\lambda}$:

On the one hand, when we transpose the last two rows, we see that $A(\lambda)$ is equivalent to $A(-\lambda)$, and by multiplying the third row by $\overline{\lambda}$ and the last row by $-\overline{\lambda}$, transposing the first and second columns with the third and fourth, we see that it is equivalent to $A(\overline{\lambda})$. It follows that $A(\pm\lambda)$, $A(\pm\overline{\lambda})$ are all equivalent.

On the other hand, if $A(\lambda)$ is equivalent to $A(\lambda')$, we can multiply $A(\lambda)$ on the left and right by appropriate monomial matrices and so obtain a matrix whose entries

https://doi.org/10.1017/S0004972700029506 Published online by Cambridge University Press

are $\pm 1, \pm\lambda'$, and which has one row and one column whose entries are all equal to 1. If we ignore the sign of the entries of the resulting matrices for the moment we have essentially three cases, corresponding to attempts to "normalise" $A(\lambda)$ in this way with respect to a row and column, neither of which intersects the lower right block, as in (4); one of which intersects this block, as in (5); or both of which intersects this block, as in (6):

$$(4) \qquad A(\lambda) \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & \lambda' & \lambda' \\ 1 & 1 & \lambda' & \lambda' \end{pmatrix};$$

$$(5) \qquad A(\lambda) \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ \lambda' & \lambda' & 1 & 1 \\ \lambda' & \lambda' & 1 & 1 \end{pmatrix};$$

$$(6) \qquad A(\lambda) \longrightarrow \begin{pmatrix} \lambda' & \lambda' & 1 & 1 \\ \lambda' & \lambda' & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Clearly, after replacing the missing signs and performing appropriate permutations on the rows and columns, in (4) and (6) we have $\lambda' = \pm\lambda$, and in (5), $\lambda' = \pm\overline{\lambda}$. This shows that we have an uncountably infinite number of inequivalent matrices $A(\lambda)$.

We now show that these are in fact the *only* equivalence classes in order 4. Let A be a 4×4 unit Hadamard matrix, normalised so that the first two rows are $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & a & b & -1-a-b \end{pmatrix}$. Then we must have $|-1-a-b|^2 = (1+a+b)(1+\overline{a}+\overline{b}) = 1$, and so $(a+b)(1+a)(1+b) = 0$. So one of $a+b$ or (without loss of generality) $1+b$ equals zero. In either case, by suitably arranging the columns we can put the first two rows of A into the form

$$(7) \qquad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & -a \end{pmatrix},$$

and so we have

$$(8) \qquad A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & -a \\ 1 & c & d & e \\ 1 & -c & f & g \end{pmatrix}.$$

We may assume that neither a nor c is ± 1, for otherwise, it would follow immediately that A is equivalent to $A(\lambda)$ for some λ. Now since the first and third rows must

https://doi.org/10.1017/S0004972700029506 Published online by Cambridge University Press

be equivalent to (7), one of d and e must equal $-c$ —let us say d, without loss of generality. Then $e = -1$. But since the first and third columns must also be equivalent to (7), we have $c = a$. Applying the condition of orthogonality to the second and third rows, we have $1 - \overline{a} - 1 + a = 0$, and so $a^2 = 1$, which contradicts our assumption about a.

We summarise the results of this section with the following theorem:

Theorem 1. *There is exactly one equivalence class of unit Hadamard matrices in each of the orders* 1, 2 *and* 3, *and an uncountably infinite number of equivalence classes in order* 4. *More precisely,* $\{V_1\}$, $\{V_2\}$, $\{V_3\}$ *and* $\{A(e^{i\theta}), 0 \leqslant \theta \leqslant \pi/2\}$, *are complete sets of representatives of the equivalence classes in these orders.*

3. The number of classes in composite orders

We have verified Sylvester's claim for orders 1, 2, and 3, but shown it to be false for order 4. It follows immediately that the result is false for every order containing a factor of 4, by use of the Kronecker product. However, we now demonstrate that the same holds for *every* composite order.

Lemma 2. *If* $X = (x_{ij})$ *is any* $k \times l$ *matrix with entries from the unit circle in* $\mathbb{C}$, X *is a submatrix of a unit Hadamard matrix of order* kl.

Proof: By analogy with [2]. □

Now if $k, l > 1$ we may take $x_{11} = \lambda$ and $x_{ij} = 1$ when $i > 1$ or $j > 1$. As λ ranges over the unit circle, Lemma 2 gives embeddings of the matrices X so defined into an uncountably infinite number of inequivalent unit Hadamard matrices of order kl, as may be demonstrated analogously with Section 2.

Theorem 3. *If* n *is composite, there are an uncountable number of equivalence classes of unit Hadamard matrices of order* n.

Unfortunately, the construction given in Lemma 2, combined with Vandermondes, cannot produce representatives of all such classes. It is apparent, for example, that no (real) Hadamard matrix of order 12 may be decomposed into a 6×2 array of 2×6 rank one submatrices or into a 3×4 array of 4×3 rank one submatrices, (if X is $k \times l$, the construction borrowed from [2] will produce a matrix in the form of a $k \times l$ array of $l \times k$ rank one submatrices) and nor is it equivalent to V_{12}.

4. Inverse orthogonal matrices and the remaining questions

At no point in his exposition [7] does Sylvester demonstrate, let alone state, a result that appears to be crucial to his whole discussion. He does not deal with orthogonality of complex valued matrices as we would today, but rather introduces the following concept:

https://doi.org/10.1017/S0004972700029506 Published online by Cambridge University Press

DEFINITION: An $n \times n$ matrix $A = (a_{ij})$ with all entries nonzero in the complex plane which satisfies $(a_{ij})(a_{ji}{}^{-1}) = nI$ shall be called *inverse orthogonal.*

Clearly, a matrix is unit Hadamard if and only if it is inverse orthogonal and has all entries on the unit circle, so inverse orthogonal matrices are a generalisation of unit Hadamard matrices. Multiplication of any row or column by a nonzero scalar does not alter the property of inverse orthogonality, and nor does permutation of rows and columns. Thus we may speak of *equivalence classes* of, and *normalised*, inverse orthogonal matrices as we did with unit Hadamard matrices.

Sylvester actually claimed that the matrices he obtained form a complete set of normalised representatives of equivalence classes of *inverse orthogonal* matrices. There are two distinct elements to this statement: the first is that a normalised inverse orthogonal matrix is a unit Hadamard matrix; the second is that all unit Hadamard matrices are equivalent to one of the representatives mentioned. I have dealt with the second part up to this point; the first is assumed, but never explicitly mentioned in Sylvester's paper. Surprisingly, the first part fails in much the same way as the second: if λ is any nonzero complex number off the unit circle, $A(\lambda)$ as described in the last section is a normalised inverse orthogonal matrix with non-unit entries. Similarly, the first part fails in every composite order.

The proofs of the following two theorems are practically identical to that of Theorems 1 and 3, bearing in mind that we must substitute reciprocation for complex conjugation wherever it arises:

THEOREM 4. *$\{V_1\}$, $\{V_2\}$, $\{V_3\}$ and $\{A(re^{i\theta}), 0 \leqslant \theta \leqslant \pi/2, r > 0\}$, are complete, irredundant sets of representatives of the equivalence classes of inverse orthogonal matrices in orders $1,2,3$ and 4 respectively.*

THEOREM 5. *If n is composite, there is an uncountable number of equivalence classes of inverse orthogonal matrices of order n which are not representable by unit Hadamard matrices.*

I have been unsuccessful so far in my attempts to confirm either part of Sylvester's claim in prime orders greater than 3 or produce a counterexample. It seems reasonable at this point to name the remaining cases:

CONJECTURE 4.1. *(Sylvester's first conjecture) Any normalised inverse orthogonal matrix of prime order is a unit Hadamard matrix.*

CONJECTURE 4.2. *(Sylvester's second conjecture) Every unit Hadamard matrix of order p, where p is prime, is equivalent to V_p.*

In his notation, Butson [1] showed that for prime p, an $H(p,n)$ can only exist if $p|n$. A further decomposition of Sylvester's second conjecture would be:

(2a) Every unit Hadamard matrix of order p is an $H(n,p)$.

https://doi.org/10.1017/S0004972700029506 Published online by Cambridge University Press

(2b) Every *nontrivial* (as in [1]) $H(n,p)$ is an $H(p,p)$.

(2c) Every $H(p,p)$ is equivalent to V_p.

A proof of (2b) would provide a nice complement for Butson's result. It is easy to verify (2c) for $p = 5, 7$.

There still remains the question as to when in general two of the matrices constructed in Lemma 2 are equivalent, at least when one of m and n is greater than 2. A more difficult problem: give a complete, irredundant set of representatives of the equivalence classes of unit Hadamard matrices in general. Of course, the corresponding questions remain open for inverse orthogonal matrices as well.

References

[1] A. T. Butson, 'Generalized Hadamard matrices', *Proc. Amer. Math. Soc.* **13** (1962), 894–898.

[2] R. Craigen, 'Embedding rectangular matrices in Hadamard matrices' (to appear).

[3] W. de Launey, 'Generalized Hadamard matrices whose rows and columns form a group', in *Combinatorial Mathematics X*: *Lecture Notes in Pure Mathematics* 1036 (Springer-Verlag, Berlin, Heidelberg, New York, 1983).

[4] J. Hadamard, 'Resolution d'une question relative aux determinants', *Bull. Des Sciences Math.* **17** (1893), 240–246.

[5] H. Kimura, 'New Hadamard matrix of order 24', *Graphs Combin.* **5** (1989), 235–242.

[6] J. Seberry, 'A construction for generalized Hadamard matrices', *J. Stat. Plann. Inference* **4** (1980), 365–368.

[7] J. J. Sylvester, 'Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colors, with applications to newton's rule, ornamental tile-work, and the theory of numbers', *Phil. Mag.* **34** (1867), 461–475.

[8] W. D. Wallis, *Combinatorial designs*: *Monographs Textbooks Pure Appl. Math.* 118 (Marcel Dekker, New York, 1988).

Department of Pure Mathematics
University of Waterloo
Waterloo Ontario
Canada N2L 3G1

https://doi.org/10.1017/S0004972700029506 Published online by Cambridge University Press