On the Least Number of Cell Orbits of a Hadamard Matrix of Order n

WARWICK DE LAUNEY AND RICHARD STAFFORD

ABSTRACT. The automorphism group of any Hadamard matrix of order n acts on the set of cell co-ordinates $\{(i,j) \mid i,j = 1,2,\ldots,n\}$. Let $f(n)$ denote the least number of cell orbits amongst all the Hadamard matrices of order n. This paper describes Hadamard matrices with a small number of cellwise orbits, and in particular proves some results about the function f. We show that, except possibly for $t = 23$, $f(4t) \leq 2$ for $t = 1,2,\ldots,25$.

1. Introduction

The automorphism group of any Hadamard matrix of order n acts on several sets. It acts on the set of row indexes $\{i = 1,2,\ldots,n\}$, the set of column indexes $\{i = 1,2,\ldots,n\}$, and the set of cell co-ordinates $\{(i,j) \mid i,j = 1,2,\ldots,n\}$. Each such action divides its domain into orbits. Let $f(n)$ denote the least number of cell orbits amongst all the Hadamard matrices of order n. This paper shows that, at least initially, f grows very slowly. Indeed, the first order n for which $f(n)$ could be greater than 2 is $n = 92$.

In this paragraph, we explain why we think the behavior of $f(n)$ is important. First, notice that the cellwise-action of the automorphism group of a Hadamard matrix implies constraints on the contents of the matrix. Suppose $\phi \in \mathrm{Aut}\,(H)$ moves entry x_{ij} to entry x_{st}. Then $x_{ij} = x_{st}$ or $x_{ij} = -x_{st}$, depending on whether ϕ negated x_{ij}. Therefore, if one knows the automorphism group of a Hadamard matrix and how it acts, then the number of trials needed to find all such Hadamard matrices is at most 2^m where m is the number of cell orbits. In this paper, we show how certain important classes of Hadamard matrices with classical automorphism groups have a small number of cell orbits. Thus $f(n)$ is small for many orders n. It is natural to ask whether there are other orders of n for which

$f(n)$ is small, and, if so, what are the corresponding group actions. If $f(n)$ grows slowly, say logarithmically with n, and there is some simply-described class of automorphism groups for Hadamard matrices with a small number of cell-orbits, then we could at the very least easily construct even large Hadamard matrices by guessing one ± 1 value for each of a small number of cell-orbits.

In this paper, we begin the investigation of f, by computing the number of cell orbits for three important classes of Hadamard matrices. We will show that the Sylvester matrices have one cell orbit, and, excepting the matrices of orders 4,8, and 12, the two families of Paley Hadamard matrices have just two cell orbits. We also show that $f(mn) \leq f(n)f(m)$. Thus one can show that $f(n) \leq 2$ for many orders n.

2. Examples of Hadamard Matrices with Small Number of Orbits

We begin with the smallest possible example of cellwise action.

2.1. Sylvester Hadamard Matrices.

Example 2.1. *Let*

$$K_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Consider the following identities wherein

- *we have used the numbers* $1, 2, 3$ *and* 4 *to keep track of the cells, and*
- *assigned signs to coincide with those in* K_1.

We have

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 1 & -2 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & -3 \end{bmatrix}$$

Thus there are automorphisms of K_1 *which permute the cells as follows:*

- *interchange cells* 1 *and* 3 *and interchange cells* 2 *and* 4, *and*
- *interchange cells* 1 *and* 2 *and interchange cells* 3 *and* 4.

Thus $\mathrm{Aut}\,(K_1)$ *acts transitively on the cells of* K_1.

Now the Sylvester Hadamard matrix K_m of order 2^m is the Kronecker product of m copies of K_1. The following lemma will allow us to determine the number of cell orbits of K_m.

Lemma 2.2. *Suppose the matrices A and B have a and b cell orbits respectively. Then $A \otimes B$ has at most ab cell orbits.*

Proof. The element $(\sigma, \tau) \in \mathrm{Aut}\,(A) \times \mathrm{Aut}\,(B)$ acts on the cells (a, b) in $A \otimes B$ so that $(\sigma, \tau)(a, b) = (\sigma(a), \tau(b))$. (Here a and b are themselves ordered pairs.) Therefore the cell orbits of the action of $\mathrm{Aut}\,(A) \times \mathrm{Aut}\,(B)$ each are direct products of a cell orbit of $\mathrm{Aut}\,(A)$ on A and a cell orbit of $\mathrm{Aut}\,(B)$ on B. Since $\mathrm{Aut}\,(A \otimes B)$ contains $\mathrm{Aut}\,(A) \times \mathrm{Aut}\,(B)$, each cell orbit of $\mathrm{Aut}\,(A \otimes B)$ is a union of cell orbits of $\mathrm{Aut}\,(A) \times \mathrm{Aut}\,(B)$. Moreover, each cell orbit of $\mathrm{Aut}\,(A) \times \mathrm{Aut}\,(B)$ lies in at most one cell orbit of $\mathrm{Aut}\,(A \otimes B)$; so $A \otimes B$ has at most ab cell orbits. $\square$

Theorem 2.3. *The Sylvester Hadamard matrices have just one cell orbit.*

Proof. Every Sylvester Hadamard matrix is the Kronecker product of order 2 Sylvester Hadamard matrices. Now apply Lemma 2.2. $\square$

Theorem 2.4. *If there is an Hadamard matrix of order n, then, for all nonnegative integers t, we have $f(2^t n) \le f(n)$.*

Proof. Let H be an Hadamard matrix of order n with $f(n)$ cell orbits. Then the Kronecker product of H with the Sylvester Hadamard matrix of order 2^t has at most $f(n)$ cell orbits. $\square$

In general we have

Theorem 2.5. *If there are Hadamard matrices of orders m and n, then $f(mn) \le f(m)f(n)$.*

2.2. **Paley Hadamard Matrices.** In this section, we show that the Paley Hadamard matrices have two cell orbits except in small orders where they have just one orbit. First we define the matrices and identify key features of their automorphism groups. Then we prove our result. The full automorphism groups of the Paley matrices are discussed in detail in [1] and [2].

Gilman [3] and Paley [5] gave a construction for a conference matrix C of order $q + 1$, which is symmetric if $q \equiv 1 \pmod 4$ and antisymmetric if $q \equiv 3 \pmod 4$. In both cases, we may define C

as follows. Let V denote the 2-dimensional vector space over $\mathrm{GF}(q)$ with basis $\{b_1, b_2\}$. Let $S = \{b_1 + \lambda b_2 \mid \lambda \in \mathrm{GF}(q)\} \cup \{b_2\}$. So S is a complete set of distinct representatives for the 1-dimensional subspaces of V. Now fix a field multiplication on V by identifying V with $\mathrm{GF}(q^2)$ so that the field addition coincides with the vector space addition. Let det denote any alternating bilinear form on V, and let χ denote the quadratic character on $\mathrm{GF}(q^2)$. Then the matrix

$$C = [\, \chi \det(x, y)\,]_{x,y \in S}$$

is a Paley conference matrix of order $q+1$. Without loss of generality we may take

$$\det(x, y) = x_1 y_2 - x_2 y_1 = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix},$$

where $x = x_1 b_1 + x_2 b_2$ and $y = y_1 b_1 + y_2 b_2$.

The entire automorphism group for C is generated by two kinds of elements. Firstly, there are the automorphisms which correspond to elements of $\mathrm{GL}(2, q)$. For all $A \in \mathrm{GL}(2, q)$ we have

$$\det(Ax, Ay) = \det(A) \det(x, y),$$

and

$$\chi(\det((Ax, \det(A)Ay))) = \chi((\det(A))^2 \det(x, y)) = \chi \det(x, y).$$

Therefore A induces an automorphism ϕ_A on C where

$$(x, y) \overset{\phi_A}{\longmapsto} (Ax, \det(A)Ay). \tag{1}$$

Next let p be the prime dividing q, and define σ on V so that $\sigma(x_1 b_1 + x_2 b_2) = x_1^p b_1 + x_2^p b_2$. Then the mapping

$$(x, y) \overset{\phi_\sigma}{\longmapsto} (\sigma(x), \sigma(y))$$

is an automorphism of C. These automorphisms generate $\mathrm{Aut}\,(C)$. So $\mathrm{Aut}\,(C)$ is a homomorphic image of $\mathrm{G\Gamma L}(2, q)$, the group of semilinear permutations on V over $\mathrm{GF}(q)$.

For $q \equiv 3 \pmod 4$, Paley's Type I Hadamard matrix H_1 is defined to be $I + C$. We may write this matrix as

$$[\, h(x, y)\,]_{x,y \in S},$$

where

$$h(x, y) = \begin{cases} \chi(x/y) & \text{if } x/y \in \mathrm{GF}(q), \\ \chi(\det(x, y)) & \text{if } x/y \notin \mathrm{GF}(q). \end{cases}$$

Notice that if $A \in \mathrm{GL}(2,q)$ satisfies $\chi\det(A) = 1$ then ϕ_A is in $\mathrm{Aut}\,(H_1)$. However, if $\chi\det(A) = -1$, then A does not induce an automorphism on H_1, since when $x/y \in \mathrm{GF}(q)$, we have

$$\chi(Ax/\det(A)Ay) = -\chi(x/y).$$

Let $\mathrm{GS}(2,q)$ denote the set of elements A of $\mathrm{GL}(2,q)$ such that $\chi\det(A) = 1$, and let $\mathrm{G\Gamma S}(2,q)$ denote the subgroup of $\mathrm{G\Gamma L}(2,q)$ obtained by adjoining σ to $\mathrm{GS}(2,q)$. Then except for $q = 3,7$ and 11, the elements ϕ_g where $g \in \mathrm{G\Gamma S}(2,q)$ generate $\mathrm{Aut}\,(H_1)$. Notice that for all $g \in \mathrm{G\Gamma S}(2,q)$, the automorphism ϕ_g moves diagonal cells to diagonal cells.

For $q \equiv 1 \mod 4$, Paley's Type II Hadamard matrix H_2 is defined to be the matrix

$$H_2 = \begin{bmatrix} I+C & -I+C \\ -I+C & -I-C \end{bmatrix}.$$

This matrix divides naturally into four quadrants of order $q+1$. Within each quadrant one has diagonal entries and off-diagonal entries. We will be interested in how $\mathrm{Aut}\,(H_2)$ acts on these eight pieces.

We describe $\mathrm{Aut}\,(H_2)$. Firstly, H_2 has a special automorphism ξ. Let

$$U = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$$

Then $H_2 = UH_2U^\top$, so $\xi = (U,U)$ is an automorphism H_2. ξ has order 4, and its square $(-I,-I)$ generates the center of $\mathrm{Aut}\,(H_2)$. It interchanges the upper right quadrant with the lower left quadrant, and interchanges the upper left quadrant with the lower right.

Next one obtains a (non-faithful) action of $\mathrm{G\Gamma L}(2,q)$ on H_2. Notice that if one allows ϕ_g (where $g \in \mathrm{G\Gamma S}(2,q)$) to act on each quadrant of H_2, then one obtains an automorphism π_g of H_2. Moreover, if $A \in \mathrm{GL}(2,q)$ has nonsquare determinant, then the analogous action of A produces the matrix

$$H_2^A = \begin{bmatrix} -I+C & I+C \\ I+C & I-C \end{bmatrix}. \tag{2}$$

But if we put

$$P = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix}.$$

then

$$H_2 = PH_2^A Q^\top \qquad \text{and} \qquad H_2 = QH_2^A P^\top \tag{3}$$

So the combined operation α_A on H_2 of ϕ_A on the quadrants followed by premultiplying by P and postmultiplying by Q is an automorphism of H_2. Notice that α_A interchanges each cell in the bottom half of H_2 with its corresponding cell in the top half of H_2. Similarly, using the second identity in (3), one obtains another automorphism β_A which interchanges each cell in the left half of H_2 with its corresponding cell in the right half of H_2. The elements π_g (where $g \in \mathrm{G\Gamma S}(2,q)$), α_A, β_A (where $A \in \mathrm{GL}(2,q) \setminus \mathrm{GS}(2,q)$) and ξ generate Aut (H_2).

Theorem 2.6. *The Paley Type I and Type II Hadamard matrices have two cell orbits except when the order is 4,8 or 12. In those cases, there is just one cell orbit.*

Proof. We consider the Type I matrices first. Let K be the group of automorphisms ϕ_A of H_1 where $A \in \mathrm{GS}(2,q)$. Then K

- fixes the diagonal,
- moves the rows and columns of H_1 in lock step (i.e. identically), and
- acts doubly transitively on the rows and columns.

The first two assertions are immediate from (1). To see the third assertion holds, note that the matrix

$$A_{\mu,\lambda} = \begin{bmatrix} 1 & \mu - \lambda \\ 0 & 1 \end{bmatrix}$$

in $\mathrm{GS}(2,q)$ fixes the row labeled $(0,1)$ and moves the row labelled $(1,\lambda)$ to the row labelled $(1,\mu)$. Moreover, the matrix

$$A_\lambda = \begin{bmatrix} 0 & -1 \\ 1 & \lambda \end{bmatrix}$$

moves the row labeled $(0,1)$ to the row labeled $(1,\lambda)$. So K acts transitively on the rows and the stabilizer of row $(0,1)$ acts transitively on the rest of the rows. Therefore K acts doubly transitively on the rows.

Now the three assertions imply that the action of K on the cells is permutation isomorphic to the diagonal action of a doubly transitive group on $q+1$ points. Therefore K moves any off-diagonal cell to any other off-diagonal cell. Consequently, H_1 can have at most two orbits: the set of off-diagonal cells and the set of diagonal cells. Now, if $q > 11$, then all the automorphisms of H_1 have the form ϕ_g where $g \in \mathrm{G\Gamma S}(2, q)$. As noted above, ϕ_g moves diagonal cells to diagonal cells. Therefore for $q > 11$, H_1 has two cell orbits. For orders 4 and 8, the Paley matrix is equivalent to a Sylvester matrix. The order 12 Paley matrix has a large automorphism group which does not fix the diagonal [4]. Therefore the Paley matrices of orders $4, 8$ and 12 have just one cell orbit.

Next we consider the Type II matrix. Firstly, the Type II matrix with $q = 5$ is equivalent to the Type I matrix with $q = 11$. So we may suppose that $q > 5$. The group $\mathrm{GS}(2, q)$ acts on the individual quadrants of the Type II matrix. So by the argument for the Type I matrix, there can be at most 8 cell orbits: one diagonal and one off-diagonal for each quadrant. However, the automorphism α moves the cells in the bottom quadrants to the corresponding cells in the quadrants above. This merges the four upper orbits with their corresponding lower orbits. Moreover, the automorphism β moves the cells in the lefthand quadrants to the corresponding cells in the quadrants to the immediate right. Thus the four diagonal orbits become one, and the four off-diagonal orbits become one. In particular, there are just two cell orbits. By inspection, the automorphisms ξ, α_A, β_A (where $A \in \mathrm{G\Gamma L}(2, q) \setminus \mathrm{G\Gamma S}(2, q)$) and ϕ_g (where $g \in \mathrm{G\Gamma S}(2, q)$) all map diagonal cells to diagonal cells. Since these automorphisms generate the entire automorphism group for $q > 5$, one sees that there are exactly two cell orbits. $\square$

It follows that $f(n) \leq 2$ on a rather dense set of integers. It is interesting to note that for the Paley matrices (and trivially for the Sylvester matrices) any assignment of values to cell orbit representatives, and subsequent development via the automorphism group, yields an Hadamard matrix.

3. Concluding Remarks

In this paper, we have exhibited three classes of Hadamard matrices whose automorphism groups divide their cells into one or two orbits. Moreover, we have shown that the minimal number $f(n)$ of cell orbits obtained by an Hadamard matrix is often much less than its order n. Indeed, our results imply the following corollary.

Corollary 3.1. *For $n \equiv 0 \pmod 4$ up to 100, we have $f(n) \leq 2$ except possibly for $n = 92$.*

Proof. Every number $4t$ (where $t = 1, 2, \ldots, 25$) except 92 is of the form $2^s(q+1)$ where either $s \geq 0$ and q is a prime power congruent to 3 modulo 4, or $s > 0$ and q is a prime power congruent to 1 mod 4. $\square$

For many orders, there are several inequivalent Hadamard matrices with just one or two cell orbits. It would be interesting to classify the Hadamard matrices with transitive cellwise action. Theorem 2.5 and Theorem 2.6 imply that there are many Hadamard matrices of large order which have a small number of cell orbits. One would like to know whether $f(n)$ grows slowly, perhaps logarithmically, with n. One would also like to know what automorphism groups arise for Hadamard matrices with a small number of cell orbits.

References

[1] W. de Launey and R. M. Stafford, On cocyclic weighing matrices and the regular group actions of certain Paley matrices, *Discrete Appl. Math.* **102** (2000), no. 1-2, 63–101.

[2] W. de Launey, R. M. Stafford, On the Automorphisms of Paley's Type II Hadamard Matrix, preprint.

[3] R. E. Gilman, On the Hadamard determinant theorem and orthogonal determinants, *Bull. Amer. Math. Soc.* **37** (1931), 30–31.

[4] M. Hall, Note on the Mathieu Group M_{12}, *Arch. Math.* **13** (1962), 334-340.

[5] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933), 311–320.

Warwick de Launey,
Richard Stafford,
Center for Communications Research,
4320 Westerra Court,
San Diego, California 92121-1969,
USA