The 2-Transitive Complex Hadamard Matrices

G. Eric Moorhouse
Dept. of Mathematics, University of Wyoming, Laramie WY, U.S.A.

Abstract. We determine all possibilities for a complex Hadamard matrix H admitting an automorphism group which permutes 2-transitively the rows of H. Our proof of this result relies on the classification theorem for finite 2-transitive permutation groups, and thereby also on the classification of finite simple groups.

Keywords. complex Hadamard matrix, 2-transitive, distance regular graph, cover of complete bipartite graph

1. Introduction

Let H be a *complex Hadamard matrix of order v,* i.e. a $v \times v$ matrix whose entries are complex roots of unity, satisfying $HH^* = vI$, where $*$ denotes conjugate-transpose. Butson's original definition in [3] considered as entries only p-th roots of unity for some prime p, while others [42], [32], [8] have considered $\pm 1, \pm i$ as entries. These are generalisations of the *(ordinary) Hadamard matrices* (having entries ± 1); other generalisations with group entries are described in Section 2.

1.1 Example. *The complex Hadamard matrix*

$$H_6 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega^2 & \omega^2 & \omega \\ 1 & \omega & 1 & \omega & \omega^2 & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega & \omega^2 & \omega^2 & \omega & 1 \end{bmatrix}, \qquad \omega = e^{2\pi i/3}$$

of order 6 corresponds (as in Section 2) to the distance transitive triple cover of the complete bipartite graph $K_{6,6}$ which appears in [2, Thm. 13.2.2].

An *automorphism* of H is a pair $(M_1\,, M_2)$ of monomial matrices such that $M_1 H M_2^* = H$. Here, a *monomial matrix* is a $v \times v$ matrix having a single nonzero entry in each row and column, these nonzero entries being complex roots of unity. Let G be a group of automorphisms of H, and let Z be the set of all elements of G of the form $(\alpha I, \alpha I)$. Thus G is a central extension of the cyclic group Z. Now $\overline{G} := G/Z$ permutes the set of all rows

and columns of H faithfully (although $\overline{G}$ permutes the rows of H not necessarily faithfully, and the columns not necessarily faithfully).

If H is a complex Hadamard matrix and D_1, D_2 are monomial matrices of the same order v, then $\widetilde{H} := D_1 H D_2^*$ is a complex Hadamard matrix of order v which is *(monomially) equivalent* to H, and every group G of automorphisms of H yields a group $(D_1, D_2)G(D_1^*, D_2^*) \cong G$ of automorphisms of $\widetilde{H}$, whose permutation group induced on the rows and columns of $\widetilde{H}$ is equivalent to the permutation group induced by G on the rows and columns of H.

1.2 Theorem. *If $\overline{G}$ permutes 2-transitively the rows of H, then H is monomially equivalent to one of the following six types:*

- *(Syl_v) H is of generalised Sylvester type, i.e. $v = p^n$ is a prime power and H is a character table of an elementary abelian group of order p^n. In this case $\overline{G} \leq p^{2n}GL(n,p)$. When $p = 2$, H is a Sylvester Hadamard matrix.*
- *(Pal_v) H is of Paley type, with $v = q + 1$ for some prime power q. If $q \equiv 3 \mod 4$ then $H = I + C$ is an ordinary "skew-type" Hadamard matrix, where C is a skew-symmetric conference matrix [34, p.173]; otherwise $q \equiv 1 \mod 4$ and $H = I + iC$ where C is a symmetric conference matrix. Either $\overline{G} \trianglerighteq PSL(2,q)$ acting in its usual representation of degree $q+1$, or $v = 12$ and $\overline{G}$ is the Mathieu group M_{12}.*
- *(H_6) $v = 6$, H is given by Example 1.1, and $\overline{G} \trianglerighteq A_6$.*
- *(H_{28}) $v = 28$, $\overline{G} \trianglerighteq P\Sigma L(2,8) = PSL(2,8)$:3 and the entries of H are complex seventh roots of 1; see Example 2.3.*
- *(IL_{36}) $v = 36$, $\overline{G} \cong Sp(6,2)$, which yields a unique example due to Ito and Leon [22]. Here $H = I + C$ where C is a $(0, \pm 1)$-adjacency matrix of a 2-transitive two-graph (see [40]).*
- *($Sp_{v,t,\alpha}$) $v = q^{2d} \geq 16$ where q is a power of 2, and H arises from Construction 5.7 (see Example 1.3 when $v = 16$). Here $\overline{G}$ has a normal elementary abelian subgroup $\overline{N}$ of order $v = q^{2d}$ and $\overline{G}/\overline{N}$ is a known transitive subgroup of $Sp(2d,q)$. The construction depends on a parameter $t \in \mathbb{F}_q - \mathbb{F}_2$ and on an arbitrary choice of complex root of unity α.*

These examples have all been studied elsewhere, with the possible exceptions of (H_{28}) and ($Sp_{v,t,\alpha}$). Note that types (Syl_v) = (Pal_v) for $v \in \{4, 8\}$; also type ($Sp_{v,t,\pm 1}$) coincides with (Syl_v) where $v = 4^d \geq 16$ (see Construction 5.7). The smallest example of the type ($Sp_{v,t,\alpha}$) is the following.

1.3 Example. *($Sp_{16,t,\alpha}$) is given by*

$$H_{16,\alpha} = \begin{bmatrix} J & A & B & C \\ A & J & C & B \\ B & C & J & A \\ C & B & A & J \end{bmatrix}$$

where J, A, B and C are given by

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -\alpha & \alpha & -1 \\ -\alpha & 1 & -1 & \alpha \\ \alpha & -1 & 1 & -\alpha \\ -1 & \alpha & -\alpha & 1 \end{bmatrix}, \begin{bmatrix} 1 & \alpha & -1 & -\alpha \\ \alpha & 1 & -\alpha & -1 \\ -1 & -\alpha & 1 & \alpha \\ -\alpha & -1 & \alpha & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 & -\alpha & \alpha \\ -1 & 1 & \alpha & -\alpha \\ -\alpha & \alpha & 1 & -1 \\ \alpha & -\alpha & -1 & 1 \end{bmatrix}$$

respectively. Here $\alpha \in \mathbb{C}$ is an arbitrary root of unity. An automorphism group $\cong 2^5{:}A_5$ having $Z = \{\pm(I, I)\}$ permutes 2-transitively the rows of $H_{16,\alpha}$, as well as the columns (but not equivalently). In this case t is superfluous since the two choices of $t \in \mathbb{F}_4 - \mathbb{F}_2$ give equivalent H's.

To prove Theorem 1.2, we first reduce to the case $\overline{G}$ permutes both the rows and columns of H faithfully (see Theorem 3.8 which generalises a result of Kantor [26]). Then $\overline{G}$ is a 2-transitive permutation group, so $\overline{G}$ is either *almost simple* ($\overline{G}_0 \leq \overline{G} \leq Aut(\overline{G}_0)$ for some nonabelian simple group $\overline{G}_0$), or of *affine type* ($\overline{G} = \overline{NL}$ where $\overline{N}$ is a regular normal elementary abelian subgroup of order p^n, and $\overline{L} \leq Aut(\overline{N}) \cong GL(n, p)$ is transitive on the nonidentity elements of $\overline{N}$). We then make use of the complete list of the 2-transitive groups, available in [28] as a result of the classification of finite simple groups.

Theorem 1.2 extends some earlier work ([20], [26]; see also [21]) although our proofs are independent. In particular the cases of Theorem 1.2 for which $\overline{G}$ is almost simple and H is an ordinary Hadamard matrix, are due to Ito [20]. His proof used the list of almost simple 2-transitive groups known in 1979, and by [28] we now know that this list is complete.

In Section 2 we describe the relationships of complex Hadamard matrices to other matrices with entries in a finite group, and thereby the implications of Theorem 1.2 for distance-regular graphs. Except for the cases (Pal_{q+1}) with $q \equiv 1 \mod 4$, and ($Sp_{v,t,\alpha}$), the matrices of Theorem 1.2 give rise to distance regular covers of complete bipartite graphs. In Section 3 we enumerate the several ways in which complex Hadamard matrices arise from 2-transitive permutation groups via monomial representations satisfying rather mild conditions. It is this ease with which 2-transitive complex Hadamard matrices arise from 2-transitive permutation groups that shows why the proof of Theorem 1.2 evidently requires the classification of finite 2-transitive permutation groups. The proof of Theorem 1.2 is given in Section 4 (in case $\overline{G}$ is almost simple) and in Section 5 (in case $\overline{G}$ is of affine type). Some material needed for the proofs in Section 5 is included in two appendices

which review basic concepts of 1-cohomology: Section 6 for linear groups acting on their natural modules, and Section 7 for $Sp(2d, q)$ and $G_2(q)'$ in even characteristic. In contrast with the situation with classifying 2-transitive symmetric designs [29], we have found no way to avoid explicit computations with 1-cocycles, for reasons mentioned in Section 7.

2. Generalised Hadamard Matrices and Covering Graphs

We refer to [9], [25], [4] for generalised Hadamard matrices and [2], [14] for graph terminology.

Let $\mathcal{G}$ be a finite group, and let $\gamma = \sum_{g\in\mathcal{G}} g \in \mathbb{Z}\mathcal{G}$ where $\mathbb{Z}\mathcal{G}$ is the integral group ring of $\mathcal{G}$. A *generalised Hadamard matrix over* $\mathcal{G}$ is a $v \times v$ matrix $H = \left[h_{ij}\right]$ with entries $h_{ij} \in \mathcal{G}$ such that $HH^* \equiv vI \mod \gamma$, where $H^* = \left[h_{ji}^{-1}\right]$ and the product HH^* is computed in the ring of $v \times v$ matrices over $\mathbb{Z}\mathcal{G}$. The condition $HH^* \equiv vI \mod \gamma$ is equivalent to the requirement that for all $i \neq j$, the expression $h_{ik}h_{jk}^{-1}$ represents each element of $\mathcal{G}$ equally often for $k = 1, 2, \ldots, v$; it follows that $|\mathcal{G}|$ divides v. If $\phi : \mathcal{G} \to \phi(\mathcal{G})$ is a group homomorphism and $H = \left[h_{ij}\right]$ is a generalised Hadamard matrix over $\mathcal{G}$, then $\phi(H) = \left[\phi(h_{ij})\right]$ is a generalised Hadamard matrix over $\phi(\mathcal{G})$, called a *homomorphic image of* H.

Every generalised Hadamard matrix over a cyclic group $\mathcal{G}$ of order n naturally yields a complex Hadamard matrix whose entries are n-th roots of unity, but not conversely. For example, for every finite abelian group A, the ordinary character table of A is a complex Hadamard matrix; but this is not a generalised Hadamard matrix over a finite group unless A is elementary abelian. However, if p is prime, then every complex Hadamard matrix with p-th roots of unity as entries is equivalent to a generalised Hadamard matrix over a cyclic group of order p.

It is natural to ask for an extension of Theorem 1.2 which classifies the generalised Hadamard matrices H over an arbitrary finite group $\mathcal{G}$, such that $Aut(H)$ permutes 2-transitively the rows of H, but this is apparently infeasible at present due to the large number of known examples in the case $\mathcal{G}$ is elementary abelian. For example, the multiplication table of any finite nearfield F yields a generalised Hadamard matrix H over a (multiplicative) elementary abelian group $\mathcal{G}$ isomorphic to the additive group of F, for which $Aut(H)$ has a subgroup isomorphic to the affine group of F permuting 2-transitively the rows of H. Consequently every homomorphic image $\phi(H)$ is also 2-transitive. Although the finite nearfields have been classified, the matrices arising as $\phi(H)$ for some F and ϕ have not.

Given a finite graph Γ and any vertex x of Γ, let $\Gamma(x) = \{x\} \cup \{\text{neighbours of } x \text{ in } \Gamma\}$. If $\overline{\Gamma}$ is another finite graph, then a *covering map* is a surjective map $\psi : \Gamma \to \overline{\Gamma}$

of the respective vertex sets such that for every vertex x of Γ, ψ restricts to a bijection $\Gamma(x) \to \overline{\Gamma}(\psi(x))$. The *fibres* of such a map are the sets $\psi^{-1}(y)$ for each vertex y of $\overline{\Gamma}$. If $\overline{\Gamma}$ is connected, these fibres have the same cardinality. Note that the fibres of ψ are cocliques in Γ, and the set of edges between any two fibres $\psi^{-1}(y), \psi^{-1}(y')$ (where $y \neq y'$ are vertices of $\overline{\Gamma}$), is either a matching or empty, according as y, y' are or are not adjacent in $\overline{\Gamma}$. The *fibre group* (called by some others the covering group) of the cover is the set of automorphisms of Γ which preserve each fibre. We call the fibre group *transitive* if it transitively permutes the vertices in each fibre.

Now suppose Γ is distance-regular of diameter d. We say Γ is *antipodal* if for every vertex $x \in \Gamma$, any two vertices at distance d from x are at distance d from each other. Such a graph Γ naturally covers a distance-regular graph $\overline{\Gamma}$ of diameter $\lfloor d/2 \rfloor$, and the fibres of the covering map are the equivalence classes of the antipodality relation on Γ (see [14, p.203]).

2.1 Proposition ([13, Prop.5.9])**.** *Let Γ be an antipodal distance-regular graph. Then Γ is bipartite of diameter 4 if and only if Γ is a cover of a complete bipartite graph.*

Such graphs arise from generalised Hadamard matrices (and in particular from complex Hadamard matrices over p-th roots of unity whenever p is prime) as follows. Let $H = \left[h_{ij}\right]$ be a generalised Hadamard matrix of order v over $\mathcal{G}$, and let $\Gamma = \Gamma_H$ be the graph with vertices $\{P_{i,x}\,,\, Q_{i,x} : 1 \leq i \leq v,\ x \in \mathcal{G}\}$ and edges $\{P_{i,x}\,,\, Q_{j,xh_{ij}}\}$. The map $P_{i,x} \mapsto P_i$, $Q_{j,y} \mapsto Q_j$ gives a *covering map* $\psi : \Gamma \to K_{v,v}$, where $K_{v,v}$ is the complete bipartite graph with vertices $\{P_i, Q_i : 1 \leq i \leq v\}$ and edges $\{P_i, Q_j\}$ for all i, j. The group $\mathcal{G}$ regularly permutes the vertices in each fibre via $P_{i,x} \mapsto P_{i,gx}\,,\, Q_{j,y} \mapsto Q_{j,gy}$ for $g \in \mathcal{G}$. This construction is reversible, which leads to part (a) of the following; conclusion (b) is essentially [23, Lemma 2.2(1)].

2.2 Proposition. *(a) A generalised Hadamard matrix H of order v over $\mathcal{G}$ is equivalent to an antipodal distance-regular cover Γ of $K_{v,v}$ with a transitive fibre group isomorphic to $\mathcal{G}$.*

(b) Let H and Γ be as in (a). If Γ is distance-transitive, then H admits a group of automorphisms permuting its rows 2-transitively.

The converse of (b) fails; indeed, Γ need not even be vertex-transitive given that H has an automorphism group 2-transitive on rows. We have included (b) to compare our result with the recent description of all distance-transitive covers of complete bipartite graphs by Ivanov et al. [23]. Every cover in their list has a transitive elementary abelian fibre group. Note that [23] does not completely list all antipodal distance-transitive covers

of $K_{v,v}$; their case (5) leads to many possible examples which apparently defy complete classification.

Now Theorem 1.2 yields a classification of all distance-regular covers Γ of complete bipartite graphs having a cyclic transitive fibre group, such that $Aut(\Gamma)$ is 2-transitive on one of the two sets of v fibres. Of these, the only ones which are distance-transitive are those arising from (Syl_{p^n}) (Pal_{12}) and (H_6) (cf. [23], [2, p.228]). In fact the cover corresponding to (H_{28}), which we proceed to construct, is not even vertex-transitive!

2.3 Example. Here we construct a 7-fold cover Γ of $K_{28,28}$ with a transitive fibre group, which yields the matrix (H_{28}) of order 28 having seventh roots of unity as entries, cited in Theorem 1.2. Let $F = \mathbb{F}_8$, and let $tr : F \to \{0,1\}$ be the trace map $a \mapsto a + a^2 + a^4$. The graph Γ has $196 + 189 + 7 = 392$ vertices

$$\begin{aligned} &P_{(abc)}\,, && a,b,c \in F, \quad b \neq 0, \qquad tr(ac/b^2) = 1;\\ &Q^{(i)}_{(xyz)}\,, && x,y,z \in F \text{ not all zero}, \quad y^2 = xz, \quad i \in \mathbb{Z}/3\mathbb{Z};\\ &R_{(0y0)}\,, && 0 \neq y \in F \end{aligned}$$

and edges

$$\begin{aligned} &\left\{P_{(abc)}\,,\, Q^{(i)}_{(xyz)}\right\} && \text{for } ax^{2^i} + by^{2^i} + cz^{2^i} = 1;\\ &\left\{P_{(abc)}\,,\, R_{(0y0)}\right\} && \text{for } by = 1. \end{aligned}$$

The automorphisms

$$P_{(abc)} \mapsto P_{\lambda^{-1}(abc)}\,, \quad Q^{(i)}_{(xyz)} \mapsto Q^{(i)}_{\lambda(xyz)}\,, \quad R_{(0y0)} \mapsto R_{\lambda(0y0)}$$

for $0 \neq \lambda \in F$ form a transitive fibre group of order 7. The 28 fibres of type "P" correspond bijectively to the 28 lines $ax + by + cz = 0$ in $PG_3(F)$ which do not meet the conic $y^2 = xz$. The semilinear transformations $A \in \Gamma L(3,F)$ preserving the conic $y^2 = xz$ form a group $\cong \Gamma L(2,8) = (7 \times PSL(2,8))\!:\!3$ acting on Γ via

$$P_{(abc)} \mapsto P_{(abc)A^{-1}}\,, \quad Q^{(i)}_{(xyz)} \mapsto Q^{(i)}_{(xyz)A}\,, \quad R_{(0y0)} \mapsto R_{(0y0)A}\,.$$

Moreover, there is an automorphism

$$P_{(abc)} \mapsto P_{(a^2b^2c^2)}\,, \quad Q^{(i)}_{(xyz)} \mapsto Q^{(i+1)}_{(xyz)}\,, \quad R_{(0y0)} \mapsto R_{(0y0)}$$

of order 3 in the centre of $Aut(\Gamma)$. Using the computer software `NAUTY` [35], we verify that these automorphisms generate the *full* automorphism group $Aut(\Gamma) \cong 3 \times \Gamma L(2,8) = 3 \times (7 \times PSL(2,8))\!:\!3$ with three orbits on vertices: types "P", "Q" and "R" of size 28·7, 27·7 and 7 respectively.

3. Monomial Representations

Every group G of automorphisms of a complex Hadamard matrix H acts naturally by way of a pair of monomial representations which facilitate the study of G and H, as we describe. We use some basic results in the character theory of finite groups, as found in [19], and we present some specialised results on monomial representations, most of which can be found in [17]. Except at one point in Construction 3.6, none of the results in this section require the classification of finite 2-transitive permutation groups.

Recall that a monomial matrix is a square matrix with exactly one nonzero entry in each row and column, such that these nonzero entries are complex roots of unity. Let $\pi : G \to GL(v, \mathbb{C})$ be a linear representation of a finite group G. Then π is a *monomial representation* if for all $g \in G$, $\pi(g)$ is a monomial matrix. For any two representations $\pi, \pi' : G \to GL(v, \mathbb{C})$, let $\mathfrak{C}(\pi, \pi')$ be the vector space of all complex $v \times v$ matrices A such that $\pi(g)A = A\pi'(g)$ for all $g \in G$. We also abbreviate $\mathfrak{C}(\pi) := \mathfrak{C}(\pi, \pi)$. Now $\dim \mathfrak{C}(\pi, \pi') = [\chi, \chi']$ where χ, χ' are the characters afforded by π, π' respectively, and $[\ ,\ ]$ is the usual inner product on the space of $\mathbb{C}$-valued class functions of G. Abusing notation, we write $[\pi, \pi'] := [\chi, \chi'] = \dim \mathfrak{C}(\pi, \pi')$.

We say π and π' are *(linearly) equivalent* (resp. *monomially equivalent*) if $\mathfrak{C}(\pi, \pi')$ contains an invertible matrix (resp. a monomial matrix). If $\pi : G \to GL(v, \mathbb{C})$ is a monomial representation, the *permutation representation associated to* π is the permutation representation of G of degree v induced by π on the set of coordinate axes $\{\langle e_1 \rangle, \ldots, \langle e_v \rangle\}$ where $e_1, \ldots, e_v$ is the standard basis of column vectors of $\mathbb{C}^v$. We say that a monomial representation is *transitive, 2-transitive,* etc. if the associated permutation representation has the property named.

Let L be a subgroup of G, with derived subgroup L', and let $\lambda \in Hom(L, \mathbb{C}^\times) \cong L/L'$, the group of all representations (characters) of L of degree 1. Let $g_1{=}1, g_2, \ldots, g_v \in G$ be a set of right coset representatives of L in G, where $v = [G : L]$. The *induced representation* $\lambda^G : G \to GL(v, \mathbb{C})$ is defined (cf. [19, p.62]) by

$$\lambda^G(g) = \left[\lambda^\circ(g_i g g_j^{-1}) \ : \ 1 \le i, j \le v\right] \quad \text{where } \lambda^\circ(x) = \begin{cases} \lambda(x), & x \in L; \\ 0, & x \in G - L. \end{cases}$$

Then λ^G is a transitive monomial representation of G, which is determined to within monomial equivalence by G, L and λ (see [19, p.66]). Conversely, every transitive monomial representation of G of degree v is monomially equivalent to λ^G for some $\lambda \in Hom(L, \mathbb{C}^\times)$ where $L \le G$ is a subgroup of index v.

3.1 Definition. *Let L be a subgroup of a group G. We denote by $SC_G(L)$ the set of all $\lambda \in Hom(L, \mathbb{C}^\times)$ for which the following (clearly) equivalent conditions are satisfied, where $K = \ker(\lambda) \trianglelefteq L$:*

(i) $\lambda(g^{-1}hg) = \lambda(h)$ *whenever* $g \in G$ *and* $h, g^{-1}hg \in L$.

(ii) For $g \in G$ *and* $h \in L$, $g^{-1}h^{-1}gh \in L$ *implies* $g^{-1}h^{-1}gh \in K$.

We remark that condition (ii) implies that K is strongly closed in L in the sense of [39, p.583], whence our acronym SC.

3.2 Lemma. *If $\lambda, \mu \in SC_G(L)$ are distinct, then λ^G and μ^G are inequivalent.*

Proof. For $h \in L$, $Tr\,\lambda^G(h) = \sum_{i=1}^{v} \lambda^\circ(g_i h g_i^{-1}) = \lambda(h) Tr\,1_L^G(h)$ where $Tr\,1_L^G(h) \geq 1$ since h fixes at least one coset $Lh = L$. We may therefore uniquely recover the values of $\lambda \in Hom(L, \mathbb{C}^\times)$ from those of $Tr\,\lambda^G(h)$ and the result follows. □

3.3 Lemma. *Let G have a 2-transitive permutation representation of degree v with point stabiliser L, and let $\lambda \in Hom(L, \mathbb{C}^\times)$.*

(i) If $\lambda \in SC_G(L)$ then λ^G has two distinct irreducible constituents, each of multiplicity one, with degrees $v_1 \leq v_2$ where $v_1 + v_2 = v$. Also $\mathfrak{C}(\lambda^G) = \langle I, C \rangle_{\mathbb{C}}$ where $C^* = C$, and the entries of C are zeroes on the diagonal and roots of unity elsewhere. Moreover $C^2 = (v-1)I + \alpha C$ where $\alpha^2 = (v-1)(v_2 - v_1)^2 / v_1 v_2$.

(ii) If $\lambda \notin SC_G(L)$ then λ^G is irreducible, i.e. $\mathfrak{C}(\lambda^G) = \langle I \rangle_{\mathbb{C}}$.

Proof. Let $A = \left[a_{ij}\right] \in \mathfrak{C}(\lambda^G)$. Given $g \in G$ and $1 \leq i, j \leq v$, there are uniquely determined i' and j' such that $Lg_i g = Lg_{i'}$ and $Lg_j g = Lg_{j'}$. Comparing (i, j')-entries on both sides of $\lambda^G(g)A = A\lambda^G(g)$ gives

$$\lambda(g_i g g_{i'}^{-1}) a_{i'j'} = \lambda(g_j g g_{j'}^{-1}) a_{ij}\,. \tag{3.3a}$$

In particular $a_{i'i'} = a_{ii}$, so all diagonal entries of A are equal. The 2-transitivity of G on right cosets of L implies that each off-diagonal entry, say a_{12}, uniquely determines the others via (3.3a). It is straightforward to show that (3.3a) has a solution with $a_{12} \neq 0$ if and only if $\lambda \in SC_G(L)$.

Case (i): $\lambda \in SC_G(L)$. Then (3.3a) has a solution $A = \left[a_{ij}\right]$ with zero diagonal, $a_{12} = 1$, and for all $i' \neq j'$, $a_{i'j'}$ is a root of unity. Thus $\mathfrak{C}(\lambda^G) = \langle I, A \rangle_{\mathbb{C}}$ has dimension $[\lambda^G, \lambda^G] = 2$, so λ^G has two irreducible constituents, each appearing with multiplicity one ([19, Cor.5.17]). Now $\lambda^G(g) A \lambda^G(g)^* = A$ implies $\lambda^G(g) A^* \lambda^G(g)^* = A^*$ for all $g \in G$, so $A^* = \zeta A$ where ζ is a root of unity. Set $C = \beta A$ where $\beta^2 = \zeta$, so that $C^* = C$. Since $\mathfrak{C}(\lambda^G)$ is an algebra of dimension 2 over $\mathbb{C}$, $C^2 = CC^* = (v-1)I + \alpha C$ for some

$\alpha \in \mathbb{C}$. Indeed $\mathfrak{C}(\lambda^G) = \langle E_1, E_2\rangle_{\mathbb{C}}$ where $E_iE_j = \delta_{ij}E_i$, $E_1 + E_2 = I$ and $Tr(E_i) = v_i$. Write $C = a_1E_1 + a_2E_2$. The relations $v_1 + v_2 = v$, $Tr(C) = a_1v_1 + a_2v_2 = 0$ and $Tr(C^2E_i) = a_i^2v_i = (v - 1 + \alpha a_i)v_i$ yield $\alpha^2 = (v-1)(v_2 - v_1)^2/v_1v_2$.

Case (ii): $\lambda \notin SC_G(L)$. Every solution of (3.3a) has off-diagonal entries zero. Then $\mathfrak{C}(\lambda^G) = \langle I\rangle_{\mathbb{C}}$ has dimension $[\lambda^G, \lambda^G] = 1$, so λ^G is irreducible. □

We proceed to describe several sufficient conditions under which 2-transitive permutation groups naturally give rise to complex Hadamard matrices. Then in Theorem 3.7 we show that there are no constructions other than these. Moreover, each of the cases described below actually occurs for some G and H, as we shall see in Sections 4 and 5.

3.4 Construction. *Let G have a 2-transitive permutation representation of degree v with point stabiliser L, and let R be another subgroup of G of index v such that $LR = G$ (in particular L and R are not conjugate in G). Suppose λ^G and ρ^G are irreducible and equivalent for some $\lambda \in Hom(L, \mathbb{C}^\times)$ and $\rho \in Hom(R, \mathbb{C}^\times)$. Then $\mathfrak{C}(\lambda^G, \rho^G) = \langle H\rangle_{\mathbb{C}}$ for some complex Hadamard matrix H.*

Proof. The construction of ρ^G required a set of representatives for the right cosets of R in G, say k_1=1, $k_2, \ldots, k_v$. By hypothesis, $\mathfrak{C}(\lambda^G, \rho^G) = \langle A\rangle_{\mathbb{C}}$ where $A = \big[a_{ij}\big]$ is invertible. For all $i, i', j, j' \in \{1, 2, \ldots, v\}$ there exists $g \in G$ such that $Lg_ig = Lg_{i'}$ and $Rk_jg = Rk_{j'}$. (Indeed, by hypothesis we may write $g_ik_j^{-1} = \ell r$ and $g_{i'}k_{j'}^{-1} = \ell' r'$ for some $\ell, \ell' \in L$ and $r, r' \in R$, then set $g = g_i^{-1}\ell r' k_{j'}$.) Comparing (i, j')-entries on both sides of $\lambda^G(g)A = A\rho^G(g)$ yields

$$\lambda(g_igg_{i'}^{-1})a_{i'j'} = \rho(k_jgk_{j'}^{-1})a_{ij}\,, \quad \text{where } g_igg_{i'}^{-1} \in L,\ k_jgk_{j'}^{-1} \in R. \tag{3.4a}$$

We may suppose that some entry of A is 1; then by (3.4a), all entries of A are roots of unity. Moreover,

$$\lambda^G(g)AA^*\lambda^G(g)^* = A\rho^G(g)\rho^G(g)^*A^* = AA^*$$

for all $g \in G$ implies that $AA^* \in \mathfrak{C}(\lambda^G) = \langle I\rangle_{\mathbb{C}}$, so $AA^* = vI$ as required. □

3.5 Construction. *Let G have a 2-transitive permutation representation of degree v with point stabiliser L, and let $\lambda \in SC_G(L)$ so that $\mathfrak{C}(\lambda^G) = \langle I, C\rangle_{\mathbb{C}}$, $C^* = C$, $C^2 = (v-1)I + \alpha C$ and $\alpha^2 = (v-1)(v_2 - v_1)^2/v_1v_2$ in the notation of Lemma 3.3. Then there exists a complex Hadamard matrix $H \in \mathfrak{C}(\lambda^G)$ iff $\alpha^2 \in \{0, 1, 2, 3, 4\}$, in which case H is a*

multiple of $I-\beta C$ or $I-\overline{\beta}C$ where β is a root of unity satisfying $\beta+\overline{\beta}=\alpha$. In particular for $v \geq 5$, λ is nonprincipal; for $v \leq 4$, H is of type (Syl_v).

Proof. Any complex Hadamard matrix in $\mathfrak{C}(\lambda^G)$ must be a multiple of $H = I - \beta C$ for some root of unity β, where $HH^* = (I-\beta C)(I-\overline{\beta}C) = vI + (\alpha - \beta - \overline{\beta})C$ implies that $\beta + \overline{\beta} = \alpha$. These conditions imply that $\alpha^2 \in \mathbb{Q}$ is an algebraic integer ≤ 4, so $\alpha^2 \in \{0,1,2,3,4\}$. The converse is immediate.

If $\lambda = 1_L$ then $C = \pm(J-I)$ where J is the all-1 matrix. Now when $v \geq 5$, $|\alpha| = v-2 > 2$, contradicting $\alpha = \beta + \overline{\beta}$.

It is easy to verify that every complex Hadamard matrix of order $v \leq 3$ is of type (Syl_v). Finally if $v = 4$ it is easy to check that every 4×4 matrix C with zero diagonal, roots of unity off the diagonal, such that $C^* = C$ and $C^2 = 3I + \alpha C$, is monomially equivalent to

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & \gamma & \overline{\gamma} \\ 1 & \overline{\gamma} & 0 & \gamma \\ 1 & \gamma & \overline{\gamma} & 0 \end{bmatrix}$$

where $\gamma^4 = 1$, and that every complex Hadamard matrix in $\langle I, C\rangle_{\mathbb{C}}$ is then of type (Syl_4). □

3.6 Construction. *Let G have two inequivalent 2-transitive permutation representations 1_L^G and 1_R^G of degree v with the same character. Then $\mathfrak{C}(1_L^G, 1_R^G) = \langle J, D\rangle_{\mathbb{C}}$ where J is the all-1 matrix and D is the incidence matrix of a symmetric 2-(v,k,ℓ) design admitting a group $\cong G$ of automorphisms permuting points and blocks 2-transitively via the representations 1_L^G and 1_R^G. Then $\mathfrak{C}(1_L^G, 1_R^G)$ contains a complex Hadamard matrix H iff $v = 3$ or $4(k-\ell)$, and in the latter case H is a multiple of $2D - J$. Every H arising in this way is of type (Syl_v).*

Proof. The fact that $\mathfrak{C}(1_L^G, 1_R^G) = \langle J, D\rangle_{\mathbb{C}}$ where D is the incidence matrix of a symmetric 2-(v,k,ℓ) design is well known; see e.g. [11], [29]. Any linear combination of J and D whose entries are roots of unity, must be a multiple of $H = D + \alpha(J - D)$ where α is some root of unity. Since $DD^\top = (k-\ell)I + \ell J$ and $DJ = JD = kJ$, we obtain $HH^* = vI + [v - (1-\alpha)(1-\overline{\alpha})(k-\ell)](J-I)$. For H to be a complex Hadamard matrix, we must assume that $v = (1-\alpha)(1-\overline{\alpha})(k-\ell)$. Since the rational number $v/(k-\ell)$ equals an algebraic integer $(1-\alpha)(1-\overline{\alpha}) \leq 4$, we have $v/(k-\ell) \in \{1,2,3,4\}$. Using the necessary condition $\ell(v-1) = k(k-1)$ for a symmetric design, we obtain either $v = 3$ and H is of type (Syl_3), or $v = 4(k-\ell)$ with $\alpha = -1$ and $H = 2D - J$.

Now Kantor [29] has classified the 2-transitive symmetric 2-designs, using the classification of finite 2-transitive permutation groups. From his list, we see that the only

designs with $v = 4(k-\ell)$ are the symplectic 2-$(2^{2m}, 2^{2m-1} \pm 2^{m-1}, 2^{2m-2} \pm 2^{m-1})$ designs. It is obvious from the construction of these designs in [27, Sec.3] that H is a Sylvester Hadamard matrix in this case. □

Let G be a set of automorphisms of a complex Hadamard matrix H of order v, as in Section 1. Elements of G are of the form $g = (\Pi_1(g), \Pi_2(g))$ where the maps $g \mapsto \Pi_i(g)$ are faithful monomial representations of G. Since $H \in \mathfrak{C}(\Pi_1, \Pi_2)$, these two representations of G are linearly equivalent. If $\widetilde{H} = D_1 H D_2^*$ where D_1, D_2 are fixed monomial matrices, then $\widetilde{H} \in \mathfrak{C}(\widetilde{\Pi}_1, \widetilde{\Pi}_2)$ where $\widetilde{\Pi}_i(g) = D_i \Pi_i(g) D_i^*$. Let L be the stabiliser of row 1 in G, i.e. $L = \{g \in G :$ the $(1,1)$-entry of $\Pi_1(g)$ is nonzero$\}$. By the previous remarks, we may suppose that $\Pi_1 = \lambda^G$ for some $\lambda \in Hom(L, \mathbb{C}^\times)$, after replacing H (and Π_1) by a monomially equivalent matrix (and representation) if necessary. We may further assume either that Π_2 is of a preferred form (ρ^G or $\rho_1^G \oplus \rho_2^G$) *or* that H has first row $(1, 1, \ldots, 1)$, whichever is more convenient for our purposes at the time.

3.7 Theorem. *Let G be a group of automorphisms of a complex Hadamard matrix H of order $v \geq 3$, and define the monomial representations $\Pi_1, \Pi_2 : G \to GL(v, \mathbb{C})$ as above. If Π_1 is 2-transitive, then one of the following conclusions (i)–(iii) must hold, after replacing H by a monomially equivalent matrix if necessary.*

(i) H arises from G by one of the Constructions 3.4–6.

(ii) $\Pi_1 = \lambda^G$ is reducible, where $\lambda \in SC_G(L)$. G has two orbits on columns of H, viz. $\Pi_2 = \rho_1^G \oplus \rho_2^G$ where $\rho_i \in Hom(R_i, \mathbb{C}^\times)$, ρ_i^G is irreducible and $[G : R_1] + [G : R_2] = v$. Any two complex Hadamard matrices in $\mathfrak{C}(\lambda^G, \rho_1^G \oplus \rho_2^G)$ are equivalent.

(iii) G has two inequivalent permutation actions of degree v, with stabilisers L and R. $\Pi_1 = \lambda^G$ and $\Pi_2 = \rho^G$ are reducible and equivalent, where $\lambda \in SC_G(L)$ and $\rho \in SC_G(R)$ are nonprincipal.

Proof. By assumption, $\mathfrak{C}(\Pi_1, \Pi_2)$ contains an invertible matrix H, so Π_1 and Π_2 are linearly equivalent.

Case I: $\lambda \notin SC_G(L)$. Here $\Pi_1 = \lambda^G$ and Π_2 are both irreducible. Then Π_2 permutes the columns of H transitively, so $\Pi_2 = \rho^G$ for some $\rho \in Hom(R, \mathbb{C}^\times)$ for some subgroup $R < G$ of index v.

If R is conjugate to L in G, then L fixes some column of H and we may suppose that $R = L$. For all $h \in L$, comparing $(1,1)$-entries on both sides of $\lambda^G(h)H = H\rho^G(h)$ yields $\lambda(h)h_{11} = \rho(h)h_{11}$. Since $h_{11} \neq 0$, we obtain $\rho = \lambda$. But then $H \in \mathfrak{C}(\lambda^G) = \langle I \rangle_{\mathbb{C}}$, which is impossible for $v > 1$.

Hence R is not conjugate to L in G. We must show that $LR = G$, so that G and H satisfy the hypotheses of Construction 3.4. Let $k_1{=}1, k_2, \ldots, k_v$ be a set of right coset representatives for R in G. Now $\mathfrak{C}(\lambda^G, \rho^G)$ is the set of all $v \times v$ matrices $A = \big[a_{ij}\big]$ satisfying (3.4a) for all $g \in G$, where $Lg_i g = Lg_{i'}$ and $Rk_j g = Rk_{j'}$. By hypothesis, (3.4a) holds for $H = \big[h_{ij}\big]$ in place of $A = \big[a_{ij}\big]$. It clearly follows that (3.4a) holds for the matrix $A = \big[a_{ij}\big]$ defined by

$$a_{ij} = \begin{cases} h_{ij}, & \text{if } g_i k_j^{-1} \in LR; \\ 0, & \text{otherwise.} \end{cases}$$

Indeed, $Lg_{i'}k_{j'}^{-1}R = Lg_i g g^{-1} k_j^{-1} R = Lg_i k_j^{-1} R$, so $a_{i'j'} = h_{i'j'}$ iff $a_{ij} = h_{ij}$. Since $\dim \mathfrak{C}(\lambda^G, \rho^G) = 1$, $A = H$ and so every $g_i k_j^{-1}$ lies in LR. This implies that $LR = G$ as required.

Case II: $\lambda \in SC_G(L)$. Here λ^G has two irreducible constituents, and G has at most two orbits on the columns of H.

If in fact G has two orbits on the columns of H, then we may suppose that $\Pi_2 = \rho_1^G \oplus \rho_2^G$ where $\rho_i \in Hom(R_i, \mathbb{C}^\times)$ and R_1, R_2 are subgroups whose indices v_1, v_2 satisfy $v_1 + v_2 = v$. It is clear that $\mathfrak{C}(\lambda^G, \rho_1^G \oplus \rho_2^G) = \langle A_1, A_2 \rangle_{\mathbb{C}}$ where A_1 (resp. A_2) agrees with H in the first v_1 columns (resp. the last v_2 columns) and is zero elsewhere, with $A_1 + A_2 = H$. Clearly every complex Hadamard matrix in $\langle A_1, A_2 \rangle_{\mathbb{C}}$ is equivalent to H, so (ii) holds. Hence we may suppose that G permutes the columns of H transitively, and $\Pi_2 = \rho^G$ where $\rho \in Hom(R, \mathbb{C}^\times)$, $[G : R] = v$.

If R is conjugate to L in G, then as before we may assume $R = L$. Now $[\rho^G, \rho^G] = [\lambda^G, \lambda^G] = 2$ implies that $\rho \in SC_G(L)$ and by Lemma 3.2, $\rho = \lambda$ so H arises from Construction 3.5. Hence we may assume R is not conjugate to L in G. If λ is nonprincipal, then by Frobenius reciprocity $[\rho, 1_R] = [\rho^G, 1_G] = [\lambda^G, 1_G] = [\lambda, 1_L] = 0$ so ρ is nonprincipal, and case (iii) holds. Otherwise $\lambda = 1_L$ and $\rho = 1_R$, so $[1_R^G, 1_R^G] = [1_L^G, 1_L^G] = 2$ and G permutes 2-transitively the right cosets of R, so H arises from Construction 3.6. □

The following generalises a result of Kantor [26, Thm.3], and will be required in Sections 4 and 5. Recall that Z is the set of all elements of G of the form $(\alpha I, \alpha I)$.

3.8 Theorem. *If G/Z is not faithful on the columns of H, or on the rows of H, then H is of generalised Sylvester type.*

Proof. Let K_1 (resp. K_2) be the kernel of the permutation representation of G on the rows (resp. columns) of H. Thus $K_i \lhd G$ is the set of all $g \in G$ such that $\Pi_i(g)$ is diagonal. It is easy to see that K_1/Z (resp. K_2/Z) permutes the columns (resp. rows) of H semiregularly. For example, if $k \in K_1$ fixes column j of H, then comparing entries on both sides of

$\Pi_1(k)H = H\Pi_2(k)$, we see that $\Pi_1(k) = \alpha I$ and so $\Pi_2(k) = \alpha I$ also. In particular, $|K_i/Z|$ divides v. Also G induces permutation groups G/K_1 and G/K_2 on the rows and columns of H, respectively.

(i) Suppose that $\overline{K}_2 := K_2/Z$ is nontrivial. Now G induces a permutation group $\overline{G} = G/Z$ on the rows of H, with a regular normal subgroup $\overline{K}_2 := K_2/Z$. Therefore $\overline{G}$ is of affine type and $\overline{K}_2$ is elementary abelian of order $v = p^n$ for some prime p. Since K_2 fixes each column of H, the restriction of Π_2 to K_2 is of the form

$$\Pi_2(g) = diag\big[\phi_1(g), \phi_2(g), \ldots, \phi_v(g)\big], \qquad \phi_i \in Hom(K_2, \mathbb{C}^\times).$$

We may assume that the first row of H is $(1, 1, \ldots, 1)$, and that g_1=1, g_2, ..., g_v (the right coset representatives for L) were chosen as elements of K_2. As usual, $\Pi_1(g_i)$ is a permutation matrix with $(1, i)$-entry equal to 1. Comparing $(1, j)$-entries on both sides of $\Pi_1(g_i)H = H\Pi_2(g_i)$ yields $H = \big[\phi_j(g_i) : 1 \le i, j \le v\big]$. Since H is nonsingular, the homomorphisms ϕ_j are distinct. Now for all $g \in Z$, the value of $\phi_j(g)$ is independent of j, so $\{\phi_j/\phi_1 : 1 \le j \le v\}$ are distinct linear characters of $\overline{K}_2$. But $|Hom(\overline{K}_2, \mathbb{C}^\times)| = p^n = v$, so the set $\{\phi_j/\phi_1\}$ comprises *all* linear characters of $\overline{K}_2$. Now H is equivalent to $\big[\phi_1(g_i)^{-1}\phi_j(g_i) : 1 \le i, j \le v\big]$, the character table of $\overline{K}_2$.

(ii) Now suppose $\overline{K}_1 := K_1/Z$ is nontrivial. Then for all $k \in K_1$,

$$\Pi_1(k) = diag\big[\psi_1(k), \psi_2(k), \ldots, \psi_v(k)\big]$$

where $\psi_i \in Hom(K_1, \mathbb{C}^\times)$ is defined by $\psi_i(k) = \lambda(g_i k g_i^{-1})$. By assumption K_1 properly contains Z, so there exist i, j such that $\psi_i \ne \psi_j$. For all $i' \ne j'$, we will show that $\psi_{i'} \ne \psi_{j'}$. Since G permutes 2-transitively the rows of H, there exists $g \in G$ such that $Lg_i g = Lg_{i'}$ and $Lg_j g = Lg_{j'}$. It easily follows that $\psi_{i'}(k) = \psi_i(gkg^{-1})$ and $\psi_{j'}(k) = \psi_j(gkg^{-1})$ for all $k \in K_1$, and $\psi_i \ne \psi_j$ implies $\psi_{i'} \ne \psi_{j'}$.

Since all the ψ_s's agree on Z, the maps $\{\psi_s/\psi_1 : 1 \le s \le v\}$ are distinct linear characters of $\overline{K}_1$, so $|\overline{K}_1| \ge v$. But $|\overline{K}_1|$ divides v, so $|\overline{K}_1| = v$ and $Hom(\overline{K}_1, \mathbb{C}^\times) = \{\psi_s/\psi_1 : 1 \le s \le v\}$. Moreover, the argument above with $i = i' = 1$ and $g \in L$ shows that L permutes the nonidentity elements of $Hom(\overline{K}_1, \mathbb{C}^\times)$ transitively. It follows that $\overline{K}_1 \cong Hom(\overline{K}_1, \mathbb{C}^\times)$ is elementary abelian of order $v = p^n$.

Let k_1=1, k_2, ..., k_v be a set of right coset representatives for Z in K_1, so that $G = \bigcup_{s=1}^{v} Rk_s$ where R is the stabiliser of the first column of H. We have that $\Pi_2(g) = \big[\rho^\circ(k_i g k_i^{-1}) : 1 \le i, j \le v\big]$ for some $\rho \in Hom(R, \mathbb{C}^\times)$. Comparing (i, j)-entries on both sides of $\Pi_1(k_j)H = H\Pi_2(k_j)$ yields $H = \big[h_{i1}\psi_i(k_j)^{-1} : 1 \le i, j \le v\big]$, which is equivalent to the character table of $\overline{K}_1$. □

Henceforth we denote $\overline{G} = G/Z$ and $\overline{L} = L/Z$. Since λ is faithful on Z, the following is clear and will be useful later.

3.9 Lemma. *$L' \cap Z = 1$. In particular if $\overline{L}' = \overline{L}$ then $L = Z \times L'$.* □

4. The 'Almost Simple' Case

Throughout Section 4 we assume the following, in addition to the notation of Sections 1 and 3.

4.1 Assumption. *G is a group of automorphisms of a complex Hadamard matrix H of order $v \geq 5$, and $\overline{G} = G/Z$ is almost simple, permuting 2-transitively the rows of H. Also $\overline{G}$ permutes both the rows and columns of H faithfully (otherwise Theorem 3.8 would apply). Moreover no proper subgroup of G is 2-transitive on the rows of H.*

By [28], we list the possibilities for $\overline{G}$ and v, indicating also which groups have two inequivalent permutation representations of the same degree. Using [16], we indicate also $M(\overline{G})$, the Schur multiplier of $\overline{G}$, whenever $M(\overline{G}) \neq 1$.

4.2 List (cf. Kantor [28])**.** *$\overline{G}$ is among the following.*

(1) A_v, $v = 5$ *or* $v \geq 7$. $M(A_7) = Z_6$ *and* $M(A_v) = Z_2$ *otherwise.*

(2) $PSL(n,q)$, $n \geq 2$, $v = (q^n-1)/(q-1)$, $(n,q) \neq (2,2),(2,3),(2,4),(4,2)$. *Two representations if* $n > 2$. $M(PSL(2,9)) = Z_6$, $M(PSL(3,2)) = Z_2$, $M(PSL(3,4)) = Z_3 \times Z_4^2$, *and* $M(PSL(n,q)) = Z_{(q-1,n)}$ *otherwise.*

(3) $PSU(3,q)$, $v = q^3+1$, $q \geq 3$. $M(PSU(3,q)) = Z_{(q+1,3)}$.

(4) $Sz(q)$, $v = q^2+1$, $q = 2^{2e+1} \geq 8$. $M(Sz(8)) = Z_2 \times Z_2$.

(5) ${}^2G_2(q)$, $v = q^3+1$, $q = 3^{2e+1} \geq 3$.

(6) $Sp(2n,2)$, $n \geq 3$, $v = 2^{2n-1} \pm 2^{n-1}$. $M(Sp(6,2)) = Z_2$.

(7) $PSL(2,11)$, $v = 11$. *Two representations.* $M(PSL(2,11)) = Z_2$.

(8) A_7, $v = 15$. *Two representations.* $M(A_7) = Z_6$.

(9) M_{11}, $v = 12$.

(10) M_v, $v = 22, 23$. $M(M_{22}) = Z_{12}$.

(11) HS, $v = 176$. *Two representations.* $M(HS) = Z_2$.

(12) Co_3, $v = 276$.

Note that several 2-transitive groups have been omitted by the assumption that G is minimal, and to avoid some duplicates. With only one exception, $\overline{G}$ is nonabelian simple, so by minimality of G, we have $G' = G$, and Z is a quotient of $M(\overline{G})$ (see [31, p.19]). In the exceptional case $\overline{G} \cong {}^2G_2(3) \cong P\Sigma L(2,8)$, $v = 28$ we have $\overline{G} = \langle \overline{G}', \overline{\sigma} \rangle$ where $\overline{G}' \cong PSL(2,8)$, $M(\overline{G}') = 1$, $\overline{\sigma}^3 = 1$; we may suppose $G = \langle G', \sigma \rangle$ where $G' \cong PSL(2,8)$, $Z = \langle \sigma^3 \rangle$ and σ has order $3^e \geq 3$.

4.3 Lemma. *Under Assumption 4.1, Construction 3.4 cannot occur.*

Proof. Construction 3.4 requires $[\overline{G} : \overline{L}] = [\overline{G} : \overline{R}] = v$ where $\overline{L}, \overline{R}$ are not conjugate in $\overline{G}$. In each relevant case from List 4.2, we check that the representation of $\overline{G}$ on the cosets of $\overline{R}$ is also 2-transitive, but $1_{\overline{L}}^{\overline{G}}$ and $1_{\overline{R}}^{\overline{G}}$ are linearly equivalent, i.e. $[1_{\overline{L}}^{\overline{G}}, 1_{\overline{R}}^{\overline{G}}] = 2$ and so $\overline{LR} \neq \overline{G}$ and $LR \neq G$, contrary to Construction 3.4. Indeed if $\overline{G} = PSL(n,q)$ and $v = (q^n - 1)/(q-1)$ then $\mathfrak{C}(1_{\overline{L}}^{\overline{G}}, 1_{\overline{R}}^{\overline{G}})$ contains an incidence matrix of a symmetric design. In the other cases $\overline{G} = PSL(2,11)$ ($v = 11$), A_7 ($v = 15$), and HS, we obtain $[1_{\overline{L}}^{\overline{G}}, 1_{\overline{R}}^{\overline{G}}] = 2$ by [5]. □

4.4 Lemma. *Under Assumption 4.1, Case (ii) of Theorem 3.7 ($\overline{G}$ intransitive on columns of H) can arise only in cases (Syl_8) = (Pal_8), (H_6), (H_{28}).*

Proof. By assumption, $\overline{G}$ has subgroups $\overline{R}_1, \overline{R}_2$ whose indices v_1, v_2 satisfy $v_1 + v_2 = v$, $1 \leq v_1 \leq v_2 \leq v - 1$. By [6], [38, Thm.9], [33, Thm.C], [5], the only possibilities are

(i) $\overline{G} \cong PSL(2,q)$, $v_1 = 1$, $v_2 = q \in \{5, 7, 11\}$;
(ii) $\overline{G} \cong {}^2G_2(3) \cong P\Sigma L(2,8)$, $v_1 = 1$, $v_2 = 27$; or
(iii) $\overline{G} \cong M_{11}$, $v_1 = 1$, $v_2 = 11$.

In cases (i) and (iii), we have $G' = G$ so $\rho_1 = 1_G$, $Z = 1$ (since ρ_1 is faithful on Z) and $[\lambda, 1_L] = [\lambda^G, 1_G] = 1$ so $\lambda = 1_L$.

Case $G = PSL(2,5) = R_1$, $R_2 = A_4$: ρ_2 and $\overline{\rho_2}$ are the two nonprincipal linear characters of A_4, with values in $\{1, \omega, \overline{\omega}\}$ where $\omega = e^{2\pi i/3}$. Then H or its conjugate $\overline{H}$ must be of type (H_6), since (H_6) admits such a group of automorphisms, and by Theorem 3.7(ii) the action of G determines H to within monomial equivalence. Moreover, (H_6) and $\overline{(H_6)}$ are equivalent, by a straightforward exercise, so H is of type (H_6).

Case $G = PSL(2,7) = R_1$, $R_2 = S_4$: Now ρ_2 is the unique nonprincipal linear character of S_4, with values ± 1. We argue as in the previous case, that H is of type (Syl_8)=(Pal_8).

Case $G = PSL(2,11) = R_1$, $R_2 = A_5$: This case cannot occur since A_5 has no nonprincipal linear character.

Case $\overline{G} = P\Sigma L(2,8)$, $G = \langle G', \sigma \rangle$, $G' \cong PSL(2,8)$, $Z = \langle \sigma^3 \rangle$, $|\sigma| = 3^e \geq 3$: Now $L = (L \cap G')\langle \sigma \rangle$ where $L \cap G'$ is dihedral of order 18. Since G' is perfect, $\rho_1|_{G'} = 1_{G'}$ and as before we obtain $\lambda|_{L \cap G'} = 1_{L \cap G'}$. Since $G = G'L$, $\lambda^G|_{G'} = (\lambda|_{L \cap G'})^{G'} = 1_{L \cap G'}^{G'}$, which by [5] has 4 distinct irreducible constituents with degrees 1,9,9,9. Also $R_2 = Z \times (R_2 \cap G')$ where $R_2 \cap G'$ is a Frobenius group 2^3:7, so G' has four orbits on columns and $M_2|_{G'} = 1_{G'} \oplus \eta_1^{G'} \oplus \eta_2^{G'} \oplus \eta_3^{G'}$ where $\eta_i \in Hom(R_2 \cap G', \mathbb{C}^\times)$ are distinct nonprincipal characters with values in $\langle e^{2\pi i/7} \rangle$. On the other hand, a matrix H_{28} arising from Example 2.3 admits

the group $PSL(2,8)$ acting in this way. It follows that $\mathfrak{C}(1_{L\cap G'}^{G'},\ 1_{G'} \oplus \eta_1^{G'} \oplus \eta_2^{G'} \oplus \eta_3^{G'}) = \langle A_1, A_2, A_3, A_4\rangle_{\mathbb{C}}$ where $A_1 + A_2 + A_3 + A_4 = H_{28}$ and A_1 (resp. A_2, A_3, A_4) agrees with H_{28} in column 1 (resp. columns 2–10, 11–19, 20–28) and has zeroes elsewhere. Clearly any two complex Hadamard matrices in $\langle A_1, A_2, A_3, A_4\rangle_{\mathbb{C}}$ are equivalent.

Case $G = M_{11} = R_1$, $R_2 = PSL(2,11)$: This case cannot occur since $PSL(2,11)$ has no nonprincipal linear character. □

4.5 Lemma. *Under Assumption 4.1, Construction 3.5 yields (Pal_v) and (IL_{36}) only.*

Proof. Since $\lambda \in SC_G(L) - \{1_L\}$ in Construction 3.5, both of the following conditions hold:

(4.5a) the *character condition* $v = v_1 + v_2$ where v_1, v_2 are the degrees of two inequivalent nonprincipal irreducible representations of G, both of which are faithful on Z; and

(4.5b) the *feasibility condition* $\alpha^2 = (v-1)(v_2 - v_1)^2/v_1v_2 \le 4$.

We check which groups G (with $\overline{G}$ in List 4.2) satisfy these two primary constraints.

Case $\overline{G} = A_v$, $v = 5$ or $v \ge 7$: If $G = A_v$, $v \ge 7$ then $L = L' = A_{v-1}$ so $SC_G(L) = \{1_L\}$. If $G = 2A_v$ (the unique nonsplit double cover of A_v) then $L = 2A_{v-1}$ remains nonsplit over Z (see e.g. the construction of $2A_v$ in [31, §2.12]) so $L' = L$. If G is one of A_5, $3A_7$ or $6A_7$ then by [5], G has no representation Π_2 of degree v such that $[\Pi_2, \Pi_2] = 2$ and $[\Pi_2, 1_G] = 0$.

Case $\overline{G} = PSL(n,q)$, $(n,q) \ne (2,2), (2,3), (2,4), (2,9), (3,4)$; $v = (q^n-1)/(q-1)$: We may also suppose $(n,q) \ne (3,2), (4,2)$ since the character condition (4.5a) is not satisfied by G in these cases, by [5]. By [31, p.246] we have $G \cong SL(n,q)/Z_0$ for some $Z_0 \le Z(SL(n,q))$ and $Z = Z(SL(n,q))/Z_0$. We have $L = \widehat{L}/Z_0$ where

$$\widehat{L} = \left\{ \begin{bmatrix} A & u \\ 0 & \delta \end{bmatrix} : A \in GL(n-1,q),\ u \in F^{n-1},\ \delta = (\det A)^{-1} \right\}, \qquad F = \mathbb{F}_q\,.$$

Now $[L : L']$ is cyclic of order $(q-1)/m$ where $m = |Z_0|$, and every linear character of L is of the form $\lambda(g) = \delta^{ms}$ for some integer s dividing $(q-1)/m$, where $g = \left[\begin{smallmatrix} A & u \\ 0 & \delta \end{smallmatrix}\right] \bmod Z_0$. If $n > 2$, let $h = diag(1, \ldots, 1, \varepsilon^{-1}, \varepsilon) \in L$ where $\langle\varepsilon\rangle \in F^\times$, and choose $g \in G$ such that $g^{-1}hg = diag(\varepsilon^{-1}, \varepsilon, 1, \ldots, 1)$. Then $\lambda \in SC_G(L)$ implies $\varepsilon^{ms} = \lambda(h) = \lambda(g^{-1}hg) = 1$, so $ms = q-1$ and $\lambda = 1_L$, a contradiction.

Otherwise $n = 2$. Let $h = \left[\begin{smallmatrix} \varepsilon^{-1} & 0 \\ 0 & \varepsilon \end{smallmatrix}\right] \in L$, $w = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$; then $\varepsilon^{ms} = \lambda(h) = \lambda(w^{-1}hw) = \varepsilon^{-ms}$. Since $\lambda \neq 1_L$, q is odd and $ms = (q-1)/2$, we obtain $m \leq 2$ and $\lambda(g) = \chi(\delta)$ where

$$\chi : F \to \mathbb{C}, \qquad \chi(a) = \begin{cases} 1, & \text{if } a \text{ is a nonzero square in } F; \\ -1, & \text{if } a \text{ is a nonsquare in } F; \text{ or} \\ 0, & \text{if } a = 0. \end{cases}$$

Let $\{(x_i, y_i) : 1 \leq i \leq q\} = \{(a, 1) : a \in F\}$ with $(x_1, y_1) = (0, 1)$ and $(x_{q+1}, y_{q+1}) = (1, 0)$. As right coset representatives for L in G, we may use

$$g_i = \begin{bmatrix} 1 & 0 \\ x_i & 1 \end{bmatrix} \bmod Z_0\,, \quad 1 \leq i \leq q; \qquad g_{q+1} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \bmod Z_0\,.$$

Then $\mathfrak{C}(\lambda^G) = \langle I, C_0 \rangle_{\mathbb{C}}$ where C_0 is the Paley conference matrix

$$C_0 = \left[\chi(x_i y_j - x_j y_i) \,:\, 1 \leq i, j \leq q+1\right]$$

satisfying $C_0 C_0^\top = qI$.

If $q \equiv 1 \mod 4$ then $\lambda(-I) = \chi(-1) = 1$ so $-I \in Z_0$ and $G = PSL(2, q)$. By Construction 3.5, H is equivalent to $I \pm iC_0$. By a straightforward exercise, $I + iC_0$ and $I - iC_0$ are monomially equivalent.

If $q \equiv 3 \mod 4$ then $ms = (q-1)/2 \equiv 1 \mod 2$ implies $m = 1$ and $G = SL(2, q)$. We have Construction 3.5 with $C = iC_0$, and H is a multiple of $I + C_0$ or $I - C_0$. Again we check that $I + C_0$ and $I - C_0$ are equivalent.

Case $\overline{G} = PSU(3, q)$, $v = q^3 + 1$, $q \geq 3$: We have $G \cong SU(3, q)/Z_0$ where $|Z_0| = 1$ or 3. The only possibilities for $\{v_1, v_2\}$ satisfying the character condition are $\{1, q^3\}$ or $\{q^2-q+1,\, q(q^2-q+1)\}$. This follows from the character degrees listed in [10, p.30,31], with the observation that $SU(3, 3)$ has only one irreducible character of degree 14; cf. [5, p.14]. The feasibility condition (4.5b) yields $\alpha^2 = (v-1)(v_2-v_1)^2/v_1v_2 = (q^3-1)^2$ or $q^2(q-1)^2$, so $\alpha^2 > 4$, a contradiction.

Case $\overline{G} = Sz(q)$, $v = q^2 + 1$, $q = 2^{2e+1} \geq 8$: If G is a nonsplit double cover of $Sz(8)$ with $|Z| = 2$, by [5, p.28] G fails the character condition. Otherwise $G = Sz(q)$ and L is the normaliser of a Sylow 2-subgroup of G. By [38, p.141], $1_L \neq \lambda \in Hom(L, \mathbb{C}^\times)$ implies λ^G is irreducible, a contradiction.

Case $\overline{G} = {}^2G_2(q)$, $v = q^3 + 1$, $q = 3^{2e+1} \geq 3$: Since $M(\overline{G}) = 1$, $G = {}^2G_2(q)$. The only possibilities for $\{v_1, v_2\}$ satisfying the character condition are $\{1, q^3\}$ or $\{q^2-q+1,\, q(q^2-q+1)\}$. This follows from [5, p.6] for $q = 3$, or [43, p.87] for $q \geq 27$. By (4.5b) we have $\alpha^2 = (q^3-1)^2$ or $q^2(q-1)^2$, so $\alpha^2 > 4$, a contradiction.

Case $\overline{G} = Sp(2n,2)$, $v = 2^{2n-1} \pm 2^{n-1}$, $n \geq 3$*:* If G is a nonsplit double cover of $Sp(6,2)$, $|Z| = 2$, $v \in \{28, 36\}$ then by [5, p.47] G fails the character condition. Otherwise $G = Sp(2n,2)$, $L = GO^{\pm}(2n,2)$, $L' = \Omega^{\pm}(2n,2)$ and $|L/L'| = 2$ (see [27], [41, Ch.11]). Each choice of subgroup L has a unique nonprincipal linear character λ. Moreover $\mathfrak{C}(\lambda^G) = \langle I, C\rangle_{\mathbb{C}}$ where C has zero diagonal, entries ± 1 elsewhere, and $C^{\top} = C$, $C^2 = (v-1)I + \alpha C$, $\alpha = 2^{n-1} \mp 2$ ([37, Thm.9.7]). Since $|\alpha| \leq 2$, we obtain $n = 3$, $\alpha = 2$, $v = 36$ and $H = I - C$ is of type (IL_{36}) as constructed in [22].

Cases (7)–(12) from List 4.2: Either $G = \overline{G}$ or G is a nonsplit m-fold cover of $\overline{G}$ for some m dividing $|M(\overline{G})|$. By [5] only two of the remaining possibilities for G satisfy the character condition: either $G = HS$, $v_1 = 22$, $v_2 = 154$; or $G = Co_3$, $v_1 = 23$, $v_2 = 253$. Then $|\alpha| = 30$ or 50 respectively, contrary to (4.5b). □

4.6 Lemma. *Under Assumption 4.1, case (iii) of Theorem 3.7 cannot occur.*

Proof. Once again, $\lambda \in SC_G(L) - \{1_L\}$ forces the character condition (4.5a). Among the groups from List 4.2 having a subgroup R of index v not conjugate to L, only one group is found to satisfy this character condition: $G = HS$, $v = 176$. Then $L \cong R \cong PSU(3,5)$:2 and λ, ρ are the unique nonprincipal linear characters of L, R resp., with both λ^G and ρ^G having constituent degrees 22 and 154. However, $[\lambda^G, \rho^G] = 1$ by [12, p.348], since their characters of degree 154 differ for certain elements $g \in HS$ of order 8. □

This completes the proof of Theorem 1.2 in the case $\overline{G}$ is almost simple.

5. The 'Affine' Case

In this section we complete the proof of Theorem 1.2 in the remaining cases, where $\overline{G}$ is of affine type. A review of the relevant definitions used here pertaining to the 1-cohomology of linear groups may be found by looking ahead to Section 6, and Section 7 where some of the more technical results which we require are found. Here we shall *not* assume that G has no proper subgroup permuting 2-transitively the rows of H. Instead, we shall (as explained in the next paragraph) reduce to the case that L splits over Z, at the cost of enlarging Z (and thereby L and G) if necessary, without changing $\overline{L}$ or $\overline{G}$.

As before, $\Pi_1 = \lambda^G$ where $\lambda \in Hom(L, \mathbb{C}^{\times})$. Let $\mathcal{U} = \{\lambda(g) : g \in L\} \subset \mathbb{C}^{\times}$, a group of roots of unity, and define $Z_{\mathcal{U}} = \{(\alpha I, \alpha I) : \alpha \in \mathcal{U}\}$. By definition, $Z \leq Z_{\mathcal{U}}$. The products $GZ_{\mathcal{U}}$ and $LZ_{\mathcal{U}}$ are defined in $GL(n,\mathbb{C}) \times GL(n,\mathbb{C})$, and the maps $\Pi_1, \Pi_2 : GZ_{\mathcal{U}} \to GL(n,\mathbb{C})$ denote, as before, the projections $\Pi_i : (M_1, M_2) \mapsto M_i$. Clearly, Π_1 and Π_2 are monomial representations of $GZ_{\mathcal{U}}$, and $\Pi_1(g)H = H\Pi_2(g)$ for all $g \in GZ_{\mathcal{U}}$. There is a unique

extension of λ to $LZ_{\mathcal{U}}$ determined by $\lambda(\alpha I, \alpha I) = \alpha$, so that $\Pi_1 = \lambda^{GZ_{\mathcal{U}}}$. Moreover since $\lambda(Z_{\mathcal{U}}) = \mathcal{U}$, we have $LZ_{\mathcal{U}} = Z_{\mathcal{U}} \times K$ where K is the kernel of $\lambda : LZ_{\mathcal{U}} \to \mathcal{U}$. To summarise, in the remaining cases we may assume the following with no loss of generality.

5.1 Assumption. *G is a group of automorphisms of a complex Hadamard matrix H of order $v \geq 3$ where $\overline{G} = G/Z$ is of affine type, permuting the rows of H faithfully and 2-transitively, and the columns of H faithfully. Thus $\overline{G} = \overline{NL}$ where $\overline{N} = N/Z$ is elementary abelian of order $v = p^n$ permuting the rows of H regularly, and $\overline{L} = L/Z$ is identified with a subgroup of $GL(n,p)$ transitive on $\overline{N}^\times := \overline{N} - \{1\}$. Moreover, $\Pi_1 = \lambda^G$ where $\lambda \in Hom(L, \mathbb{C}^\times)$ and $L = Z \times K$ where $K = \ker(\lambda) \cong \overline{L}$. In particular $G = N \rtimes K$.*

We may assume, when it is convenient to do so, that G has no proper subgroup satisfying Assumption 5.1. In particular, it will often be convenient to assume that $K \cong \overline{L}$ is a minimal transitive subgroup of $GL(n,p)$.

5.2 List (cf. Kantor [28])**.** *One of the following holds (after replacing K by a transitive subgroup if necessary):*

(1) $K \leq \Gamma L(1,v)$, $p \not| \, |K|$.
(2) $K = SL(d,q)$, $v = q^d = p^n$, $(d,q) \neq (2,2)$.
(3) $K = Sp(2d,q)$, $v = q^{2d} = p^{2m}$; $(d,q) \neq (1,2), (2,2)$.
(4) $K = G_2(q)'$, $v = q^6 = 2^n$. *For $q > 2$, $G_2(q)$ is perfect, but $G_2(2) \cong PSU(3,3) : 2$.*
(5) $K \trianglerighteq SL(2,3)$ *or* $SL(2,5)$; $K \leq GL(2,p)$, $v = p^2$, $p \in \{5, 7, 11, 19, 23, 29, 59\}$ *and* $p \not| \, |K|$.
(6) $K \cong 2^{1+4}_{-}{:}5 \leq Sp(4,3)$, $v = 3^4$.
(7) $K \cong SL(2,13) \leq Sp(6,3)$, $v = 3^6$.

In particular we have excluded $SL(2,2)$ for $v = 4$ since this contains $GL(1,4)$ of order 3. We have excluded $Sp(4,2) \cong S_6$ and $Sp(4,2)' \cong A_6$ for $v = 16$, since both contain $Sp(2,4) \cong A_5$.

5.3 Lemma. *Assume that H is not of type (Syl_v). Then we may suppose (after replacing G by a subgroup G_0 if necessary, where Assumption 5.1 is satisfied with G_0 in place of G) that $|Z| = p = 2$ and that N is elementary abelian of order 2^{n+1}. Moreover, $H^1(K, V^*) \neq 0$ where $V = F^n \cong \overline{N}$ as FK-modules, $V^* = Hom(V, F)$ and $F = \mathbb{F}_2$. Also $K' = K$ and λ is the unique nonprincipal linear character of $L = Z \times K$.*

Proof. We have $Z = Z_a \times Z_{p^r}$ where $|Z_a| = a$, $|Z_{p^r}| = p^r$ and $p \not| \, a$. By the Schur-Zassenhaus Theorem, $N = Z_a \times \widetilde{N}$ for some subgroup $\widetilde{N} \leq N$ and so $G = Z_a \times (\widetilde{N} \rtimes K)$. Now Assumption 5.1 holds for $\widetilde{N} \rtimes K$ in place of G, so we may suppose that $Z_a = 1$, $|Z| = p^r$ and $|N| = p^{r+n}$. Since $K \cong \overline{L} \leq GL(n,p)$ is transitive on $\overline{N}^\times$, by a theorem of

P. Hall [15, p.198], N is either abelian or extraspecial. Closer consideration of the structure of p-groups and use of the transitivity of K on $\overline{N}^\times$ shows that one of the following holds:

(a) $v = 4$, N is quaternion of order 8, $|Z| = 2$, $K \leq GL(2,2)$.

(b) $N = Z \times N_0$ where Z is cyclic of order p^r and N_0 is elementary abelian of order $v = p^n$.

(c) $N = p^{1+2d}$, an extraspecial group of exponent p, p odd, $Z(N) = Z$, $|Z| = p$, $K \leq Sp(2d,p)$.

In case (a), we may suppose $K = GL(2,2)'$ of order 3, and $G = SL(2,3)$. If case (ii) of Theorem 3.7 occurs then $v_1 = 1$, $v_2 = 3$; since $Z \subset G'$ we obtain $\rho_1|_Z = 1_Z$, contradicting the fact that ρ_1 is faithful on Z. Hence H arises from Construction 3.5 and H is of type $(Pal_4) = (Syl_4)$.

Next suppose (b) holds. Then K normalises $\Omega_1(N)$, the (elementary abelian) subgroup generated by elements of N of order p, and Assumption 5.1 holds for $\Omega_1(N) \rtimes K$ in place of G. After replacing G by $\Omega_1(N) \rtimes K$ if necessary, we may suppose that $|Z| \leq p$.

If in fact $Z = 1$ then N is elementary abelian of order $v = p^n$ and $\lambda = 1_L$. In this case $[\lambda^G, 1_G] = 1$ so Construction 3.4 does not apply. Also since $\lambda = 1_L$, we may rule out Construction 3.5 and case (iii) of Theorem 3.7. Otherwise case (ii) of Theorem 3.7 holds. Since $[\lambda^G, 1_G] = 1$, we have $\rho_1^G = 1_G$ and $R_1 = G$. Now $[G : R_2] = p^n - 1$ is not divisible by p, so N permutes the columns of H trivially, and H is of type (Syl_v) by Theorem 3.8.

Otherwise $|Z| = p$. If $H^1(K, V^*) = 0$ then $N = Z \times N_0$ where N_0 is K-invariant (see Section 6.1), so Assumption 5.1 holds with N_0K in place of G, and H is of type (Syl_v) by the previous paragraph. Therefore we may suppose $H^1(K, V^*) \neq 0$. In particular if $K \leq Sp(V)$, then $V^* \cong V$ as EK-modules (see Section 6.1), and $H^1(K, V) = 0$.

Cases (1), (5), (6) of List 5.2 are now excluded by the fact that $H^1(K, V) \neq 0$ (see Section 6.3). In case (7) of List 5.2, we have $K \cong SL(2,13) < Sp(6,3)$. Now $K = \langle g, h \rangle$ for elements $g, h \in K$ of order 14, where $\langle g \rangle \cap \langle h \rangle = Z(Sp(6,3))$, so $H^1(K, V^*) = H^1(K, V) = 0$ by [30, p.9(β)], a contradiction. So one of the cases (2)–(4) of List 5.2 must hold, and since $H^1(K, V^*) \neq 0$, we have $p = 2$; see [24], [29]. Also $K' = K$. If $\lambda = 1_L$ and H is not of type (Syl_v) then case (ii) of Theorem 3.7 holds and $\lambda^G = 1_L^G$ has constituent degrees $v_1 = 1$, $v_2 = v - 1$. Since ρ_1 is faithful on Z, we have $Z \cap G' = 1$, a contradiction. Hence λ is the unique nonprincipal linear character of $L = Z \times K$.

By the condition $H^1(K, V^*) \neq 0$, we have either $K = Sp(2d, q)$, $v = q^{2d}$ (q even) or $K = SL(3,2)$, $v = 2^3$ (see [24] and recall that $SL(2,q) = Sp(2,q)$). Suppose $K = SL(3,2)$ and $v = 2^3$, so N is elementary abelian of order 2^4. If Construction 3.4 holds then by (3.4a), the entries of H may be taken as ± 1 (note that λ, ρ take values ± 1 only) and H is

the unique ordinary Hadamard matrix of order 8 (type $(Syl_8) = (Pal_8)$). Case (ii) of Theorem 3.7 cannot occur since $\overline{G}$ has no nontrivial permutation representation of degree < 8. Otherwise (Construction 3.5 or case (iii) of Theorem 3.7) λ^G has constituents ρ_1, ρ_2 with degrees $v_1 \le v_2$ where $v_1 + v_2 = 8$ and so $1 \le v_1 \le 4$. By Clifford's Theorem, $\rho_1|_N$ is a sum of isomorphic 1-dimensional FN-modules. Since K has no transitive permutation representation of degree 2, 3 or 4 by [5, p.3], $\rho_1|_K$ has a trivial 1-dimensional FK-submodule U, say. Since U is also N-invariant, it is an FG-module, necessarily trivial since $G' = G$. Thus $[\lambda^G, 1_G] \ge 1$ implies $\lambda = 1_L$ by Frobenius reciprocity, a contradiction.

Thus $K = Sp(2d, q)$, $v = q^{2d}$ where q is even, and the conclusion holds in case (b).

Finally, suppose case (c) holds. There is only one conjugacy class of complements of $\overline{N}$ in $\overline{G}$, since $H^1(K, \overline{N}) = 0$ by [24]. This rules out Construction 3.4 and case (iii) of Theorem 3.7. If case (ii) of Theorem 3.7 holds, then we have a subgroup $R_1 \le G$ of index $v_1 \le p^{2d} - 1$. Also $Z \subseteq R_1$ but $Z \not\subseteq R_1'$ since ρ_1 is faithful on Z. Therefore $N \cap R_1$ is an abelian subgroup of N, which implies that $|N \cap R_1| = p^{1+k}$ where $k \le d$. In fact, $1 \le k \le d$ since $[N : N \cap R_1] \le [G : R_1] < p^{2d}$. Now $\overline{G}$ acts transitively on the $p^{2d} - 1$ nonidentity elements of $\overline{N}$, with $\overline{R_1 N}$ preserving the $p^k - 1$ nonidentity elements of $\overline{N \cap R_1}$, so that $[G : R_1 N] = [\overline{G} : \overline{R_1 N}] \ge (p^{2d} - 1)/(p^k - 1) \ge p^d + 1$. Thus $[G : R_1] = [G : R_1 N][N : N \cap R_1] = p^{2d-k}[G : R_1 N] \ge p^d(p^d + 1) > v$, a contradiction. Therefore Construction 3.5 holds. Now $L = Z \times K$ where $Z = \langle z \rangle$ is of order p, and $\lambda(z) = \zeta \in \mathbb{C}$ is a primitive pth root of 1. We may identify G with a subgroup of $Sp(2d + 2, p)$ as follows; cf. [41, Ex.8.5]. Let $F = \mathbb{F}_p$, $V = F^{2d+2}$ with a nondegenerate bilinear form β. Fix vectors $u_0, u_1 \in V$ such that $\beta(u_0, u_1) = 1$. Then $G = N \rtimes K$ is the stabiliser of u_0 in $Sp(2d + 2, p)$. The subgroup N is generated by the transvections $V \to V$, $w \mapsto w + t\beta(w, x)x$ for $t \in F$, $x \in u_0^\perp$, and Z is generated by the transvection $z : w \mapsto w + \beta(w, u_0)u_0$. The complement $K = Sp(2d, p)$ fixes every vector in $\langle u_0, u_1 \rangle$ and acts faithfully on $\langle u_0, u_1 \rangle^\perp$. A set of right coset representatives for Z in N (also for L in G) is

$$\{g_x : x \in \langle u_0, u_1 \rangle^\perp\}, \qquad g_x : w \mapsto w + \beta(w, x)u_0 + \beta(w, u_0)x\,.$$

It is straightforward to check that the matrix $H_1 := \left[\zeta^{-\beta(x,y)} : x, y \in \langle u_0, u_1 \rangle^\perp\right]$ is a character table for the additive group of $\langle u_0, u_1 \rangle^\perp$ of order p^{2d}, and that $H_1 \in \mathfrak{C}(\Pi_1)$ where

$$\Pi_1(g) = \left[\lambda^\circ(g_x g g_y^{-1}) : x, y \in \langle u_0, u_1 \rangle^\perp\right]$$

where as before, $\lambda^\circ : G \to \mathbb{C}$ is the extension of λ having value 0 on $G - L$. Hence $\mathfrak{C}(\Pi_1) = \langle I, C \rangle_{\mathbb{C}}$ where $C = H_1 - I = C^*$ and $C^2 = (p^{2d} - 1)I - 2C$. By Construction 3.5, any complex Hadamard matrix $H \in \mathfrak{C}(\Pi_1)$ is equivalent to H_1, and therefore is of type

(Syl_v). □

For the remainder of the proof, we may assume that the conclusions of Lemma 5.3 hold. Thus K is a transitive subgroup of $Sp(V) = Sp(2d, q)$, $v = q^{2d}$, q even; here $V = E^{2d}$, $E = \mathbb{F}_q$ and $Sp(V)$ is the set of all $k \in GL(V)$ preserving a nondegenerate alternating bilinear form β. Let $tr : E \to F = \mathbb{F}_2$ be the trace map. (As before, $Tr(A)$ is the trace of a square complex matrix A.) Let $Q : V \to E$ be any quadratic form satisfying $Q(x + y) - Q(x) - Q(y) = \beta(x, y)$.

Now $\overline{G}$ is isomorphic to a semidirect product $V \rtimes K$ in which multiplication is defined by

$$(u, k)(w, \ell) = (u^\ell + w, k\ell)$$

(see Section 6). We may identify

$$N = \{(a, x) : a \in F = \mathbb{F}_2\,,\ x \in V\}, \quad (a, x)(b, y) = (a + b, x + y), \qquad Z = \langle (1, 0)\rangle$$

and $G = N \rtimes K$ where the action of K on N is given by

$$(a, x)^k = k^{-1}(a, x)k = (a + tr\,\beta(\varepsilon(k), x^k), x^k)$$

for some $\varepsilon \in Der(K, V)$; see Section 6. Since G does not split over Z, we have $\varepsilon \notin Inn(K, V)$ and to within a group isomorphism, we may suppose that

$$(a, x)^k = (a + tr\,\beta(\eta(k), x^k), x^k) = (a + tr(Q(x) + Q(x^k)), x^k)$$

for all $a \in F$, $x \in V$, $k \in K$, with $\eta(k)$ as defined in Section 7.

Recall that λ is the linear character of $L = Z \times K$ with $\lambda((1, 0)) = -1$, $\lambda|_K = 1$. As right coset representatives for Z in N (also for L in G) we use $g_x = (0, x)$ for $x \in V$. From $\Pi_1(g) = \left[\lambda^\circ(g_x g g_y^{-1}) : x, y \in V\right]$ we obtain

$$(5.4) \qquad \Pi_1(g_u) = \left[\delta_{x+u,y} : x, y \in V\right], \quad \Pi_1(k) = \left[(-1)^{tr(Q(x)+Q(y))}\delta_{x^k,y} \,:\, x, y \in V\right].$$

5.5 Lemma. *$\lambda \in SC_G(L)$ and λ^G has irreducible constituent degrees $v_1 = 2^{2m-1} - 2^{m-1}$ and $v_2 = 2^{2m-1} + 2^{m-1}$. We have $\mathfrak{C}(\Pi_1) = \langle I, C\rangle_{\mathbb{C}}$ where C is real symmetric. If H arises from Construction 3.5 then H is of type (Syl_v). H cannot arise from Construction 3.4.*

Proof. It is straightforward to verify that $\mathfrak{C}(\Pi_1)$ contains $H := \left[(-1)^{tr\,Q(x+y)} : x, y \in V\right]$. Moreover, H is a complex Hadamard matrix of type (Syl_v), since $H = D\widetilde{H}D$ where $D = diag((-1)^{tr\,Q(x)} : x \in V)$ and $\widetilde{H} = \left[(-1)^{tr\,\beta(x,y)} : x, y \in V\right]$ is a character table of

$(V,+)$. Therefore $\mathfrak{C}(\Pi_1) = \langle I, C\rangle_{\mathbb{C}}$ where $C = H - I$, $C^* = C$, $C^2 = (v-1)I - 2C$. The relation $\alpha^2 = (-2)^2 = (v-1)(v_2 - v_1)^2/v_1v_2$ may be solved uniquely for v_1 and v_2 (see Lemma 3.3), yielding the values claimed. □

5.6 Lemma. *If case (ii) of Theorem 3.7 holds then H is of type (Syl_v).*

Proof. In case (ii) of Theorem 3.7, we have $[G : R_1] = 2^{2m-1} - 2^{m-1}$ and $[G : R_2] = 2^{2m-1} + 2^{m-1}$ by Lemma 5.5, and so $R_1 \cong O^+(2d, q)$ and $R_2 \cong O^-(2d, q)$, the stabilisers of quadratic forms Q_1 and Q_2 resp.; see [6]. Choose a column of H, and let $\overline{N}_1$ be its stabiliser in $\overline{N}$. This column is also fixed by R_i^g for some $g \in G$ and $i \in \{1, 2\}$. Since $\overline{N}$ permutes the columns of H intransitively, $\overline{N}_1 \neq 1$. But $\overline{N}_1$ is normalised by R_i^g, which acts irreducibly on $\overline{N}$; therefore $\overline{N}_1 = \overline{N}$. The result follows by Theorem 3.8. □

This leaves only case (iii) of Theorem 3.7, in which the following examples arise.

5.7 Construction. *For each $i \in F = \{0, 1\}$ and $t \in E - F$, define the matrix $A_i = \big[a_i(x + y) : x, y \in V\big]$ where*

$$a_i(x) = \begin{cases} (-1)^{tr[Q(x)/t]}, & \text{if } tr[Q(x)/(t+1)] = i; \\ 0, & \text{otherwise.} \end{cases}$$

Then for every root of unity $\alpha \in \mathbb{C}^\times$, the matrix

$$H_{t,\alpha} := A_0 + \alpha A_1$$

is a complex Hadamard matrix admitting a 2-transitive group as in the conclusion of Lemma 5.3, and $H_{t,\alpha}$ arises from case (iii) of Theorem 3.7. We say $H_{t,\alpha}$ is of type ($Sp_{v,t,\alpha}$). $H_{t,\alpha}$ is of type (Syl_v) iff $\alpha \in \{1, -1\}$. $H_{t+1,\alpha}$ is equivalent to $H_{t,\alpha^{-1}}$.

We prove the validity of Construction 5.7 at the same time as we prove the following converse thereof.

5.8 Lemma. *Every complex Hadamard matrix satisfying Assumption 5.1 and the conclusion of Lemma 5.3, and arising from case (iii) of Theorem 3.7, arises from Construction 5.7.*

Proof. Suppose case (iii) of Theorem 3.7 holds. We have $R = \{(a, \varepsilon(k))k : a \in F, k \in K\} < N \rtimes K$ for some $\varepsilon \in Der(K, V)$. We may assume that $\varepsilon(k) = c\eta(k)$ for some $c \in E$, after replacing R by a conjugate thereof if necessary. In order that L and R not be conjugate in G, we require $c \neq 0$. Now R has a nonprincipal linear character ρ, so $R = Z \times R'$ where

$$R' = \{k(b_k, c\eta(k)) : k \in K\}$$

for some $b_k \in F$. The closure of R' under multiplication requires that

$$b_{k\ell} = b_k + b_\ell + tr\,\beta(c\eta(k)^\ell, \eta(\ell))$$

for all $k, \ell \in K$, so by Lemma 7.7 we must have $b_k = tr(c^2\gamma(k))$ for all $k \in K$, where $\gamma(k)$ is defined in Lemma 7.5. From $\Pi_2(g) = \big[\rho^\circ(g_x g g_y^{-1}) : x, y \in V\big]$ we obtain

$$\begin{aligned} &\Pi_2(g_u) = \big[\delta_{x+u,y} : x, y \in V\big], \\ &\Pi_2(k) = \big[(-1)^{b_k + tr(Q(x)+Q(x^k))}\delta_{x^k+c\eta(k),y} \ : \ x, y \in V\big] \end{aligned} \tag{5.9}$$

for all $u \in V$, $k \in K$. We will show that $tr(c) = 0$, using the fact that the representations Π_1 and Π_2 of G are linearly equivalent. Choose an element $k \in K$ as in Lemma 7.6. Then (5.4) yields

$$Tr(\Pi_1(k)) = \big|\{x \in V \ : \ x^k = x\}\big| = |C_V(k)| \geq 1.$$

By Lemma 7.7 we have $b_k = tr(c^2\gamma(k)) = tr(0) = 0$, so by Lemma 7.5 we have $Q(\eta(k)) = 0$. Now from (5.9) we obtain

$$\begin{aligned} Tr(\Pi_2(k)) &= \sum\big\{(-1)^{tr[Q(x)+Q(x^k)]} \ : \ x{\in}V,\ x^k{+}c\eta(k){=}x\big\} \\ &= \sum\big\{(-1)^{tr[Q(x)+Q(x+c\eta(k))]} \ : \ x{\in}V,\ x^k{+}c\eta(k){=}x\big\} \\ &= \sum\big\{(-1)^{tr[c\beta(x,\eta(k))]} \ : \ x{\in}V,\ x^k{+}c\eta(k){=}x\big\} \\ &= (-1)^{tr(c^2)}|C_V(k)| = (-1)^{tr(c)}|C_V(k)| \end{aligned}$$

by choice of k as in Lemma 7.6. Since Π_1 and Π_2 are equivalent representations, this forces $tr(c) = 0$ as claimed, and so by Lemma 7.7 we have $b_k = tr[Q(\eta(k))/t]$ where $t^{-1} + t^{-1/2} = c$. Now it is straightforward to show that $\mathfrak{C}(\Pi_1, \Pi_2)$ contains the matrices defined by

$$H_{t,1} := \big[(-1)^{tr[Q(x+y)/t]} : x, y \in V\big]$$

and

$$H_{t,-1} := \big[(-1)^{tr[Q(x+y)/(t+1)]} : x, y \in V\big].$$

It is not hard to see that $H_{t,1}$ and $H_{t,-1}$ are linearly independent Hadamard matrices of type (Syl_v) and so $\mathfrak{C}(\Pi_1, \Pi_2) = \langle H_{t,1}, H_{t,-1}\rangle_{\mathbb{C}} = \langle A_0, A_1\rangle_{\mathbb{C}}$ where $H_{t,\pm 1} = A_0 \pm A_1$ with A_0, A_1 as in Construction 5.7. Since $A_i \in \mathfrak{C}(\Pi_1, \Pi_2)$, we have $A_i = A_i^* \in \mathfrak{C}(\Pi_2, \Pi_1)$ and so $A_0A_1 \in \mathfrak{C}(\Pi_1) = \langle I, C\rangle_{\mathbb{C}}$ where C is real symmetric by Lemma 5.5. Thus $A_0A_1 = \zeta I + \xi C$ for some $\zeta, \xi \in \mathbb{C}$. Since

$$vI = H_{t,1}^2 = A_0^2 + A_0A_1 + A_1A_0 + A_1^2 = H_{t,-1}^2 = A_0^2 - A_0A_1 - A_1A_0 + A_1^2,$$

we obtain $A_0^2 + A_1^2 = vI,\ A_0A_1 + A_1A_0 = 0$. In particular, $A_0A_1 + (A_0A_1)^* = 0$, which implies $\zeta + \overline{\zeta} = \xi + \overline{\xi} = 0$. Since A_0A_1 has real entries, this forces $\zeta = \xi = 0$ and $A_0A_1 = 0$. It follows that $H_{t,\alpha} = A_0 + \alpha A_1$ is a complex Hadamard matrix for every complex root of unity α. Clearly every complex Hadamard matrix in $\mathfrak{C}(\Pi_1, \Pi_2) = \langle A_0, A_1 \rangle_{\mathbb{C}}$ is of this form.

One checks that the entries h_{xy} of $H_{t,\alpha}$ satisfy $\{h_{xy}h_{x'y}^{-1}h_{x'y'}h_{xy'}^{-1} : x, y, x', y' \in V\} = \{1, -1, \alpha, -\alpha\}$ and so $H_{t,\alpha}$ is not of type (Syl_v) unless $\alpha = \pm 1$. Finally, $H_{t+1,\alpha} = \alpha A_0 + A_1 = \alpha(A_0 + \alpha^{-1}A_1) = \alpha H_{t,\alpha^{-1}}$ is equivalent to $H_{t,\alpha^{-1}}$. □

This completes the proof of Theorem 1.2.

6. Appendix: Cohomology

Throughout this section, V is a finite-dimensional vector space over a field E, and $K \leq GL(V)$. The semidirect product $V \rtimes K$ has multiplication defined by

$$(u, k)(w, \ell) = (u^\ell + w, k\ell).$$

Every subgroup of $V \rtimes K$ complementary to V is of the form $\{(\varepsilon(k), k) : k \in K\}$ where $\varepsilon : K \to V$ is a *derivation,* i.e. $\varepsilon(k\ell) = \varepsilon(k)^\ell + \varepsilon(\ell)$ for all $k, \ell \in K$. Two such complements are conjugate in $V \rtimes K$ iff the corresponding derivations differ by an *inner derivation,* which is a map of the form $k \mapsto u^k - u$ for some fixed $u \in V$. Thus the conjugacy classes of complements of V in $V \rtimes K$ correspond bijectively to elements of the *first cohomology group* $H^1(K, V) = Der(K, V)/Inn(K, V)$, the vector space (over E) of derivations modulo inner derivations.

6.1 Extensions. Let

$$0 \longrightarrow E \longrightarrow \widehat{V} \longrightarrow V \longrightarrow 0$$

be an exact sequence of EK-modules, where $K \leq GL(V)$ acts naturally on V, and E is the trivial EK-module of dimension 1. Then $\widehat{V}$ is given by

$$\{(a, x) : a \in E,\ x \in V\}$$

with the usual vector space structure of $E \oplus V$, and the action of $k \in K$ is given by

$$(a, x) \mapsto (a + \theta_{k^{-1}}(x), x^k)$$

where $\theta_k \in V^* = Hom_E(V, E)$ for all $k \in K$, and the map $\theta : k \to \theta_k$ belongs to $Der(K, V^*)$. Here V^* is an EK-module via $\phi^k(x) = \phi(x^{k^{-1}})$ for all $k \in K$, $\phi \in V^*$, $x \in V$.

Two such derivations θ, θ' yield equivalent extensions of E by V, iff $\theta - \theta' \in Inn(K, V^*)$. In particular, if $H^1(K, V^*) = 0$, then $\widehat{V}$ splits over E, i.e. $\widehat{V} = E \oplus V_0$ where V_0 is an EK-submodule isomorphic to V.

6.2 Duality. In the notation above, if moreover K preserves a nondegenerate bilinear form β on V, then $V^* \cong V$ as EK-modules, so that $H^1(K, V^*) \cong H^1(K, V)$ as E-vector spaces. Moreover $\theta_k(x) = \beta(\varepsilon(k), x^k)$ where $\varepsilon \in Der(K, V)$ is uniquely determined by θ, and the map $\theta \mapsto \varepsilon$ induces $Der(K, V^*) \cong Der(K, V)$.

6.3 Coprime action. If $|K|$ is not divisible by $p = \mathrm{char}(E)$, then $H^1(K, V) = 0$; see [1, (17.10)].

7. Appendix: Minimal Transitive Subgroups of $Sp(2d,q)$, q even

In addition to the assumptions of Setion 6, suppose also that the field $E = \mathbb{F}_q$ has characteristic 2, and that $dim_E(V) = 2d$. Let $Q : V \to E$ be a nondegenerate quadratic form, and let $\beta(x, y) = Q(x+y) - Q(x) - Q(y)$ be the associated nondegenerate alternating bilinear form. We have $O(Q) \leq Sp(V)$, where $O(Q)$ (resp., $Sp(V)$) is the set of all $g \in GL(V)$ which preserve Q (resp., β). Define $\eta : Sp(V) \to V$ by $\beta(\eta(g), x^g)^2 = Q(x^g) + Q(x)$ for all $x \in V$.

7.1 Theorem ([36]). *(i)* $\eta \in Der(Sp(V), V)$.
(ii) $H^1(Sp(V), V)$ *is one-dimensional over* E, *spanned by* η *modulo* $Inn(Sp(V), V)$.
(iii) $\eta(g) = 0$ *iff* $g \in O(Q)$.
(iv) For each transvection of the form $\tau_w : x \mapsto x + \beta(x, w)w$ *where* $w \in V$, *we have* $\eta(\tau_w) = \sqrt{1 + Q(w)}\, w$.
(v) $tr(Q(x^k + \eta(k))) = tr(Q(x))$ *for all* $x \in V$, $k \in Sp(V)$. *In particular,* $tr(Q(\eta(k))) = 0$.

Clearly the definition of $\eta : Sp(V) \to V$ depends on the choice of Q. However, if Q and $\widetilde{Q}$ are two quadratic forms associated to the bilinear form β, then $\widetilde{Q}(x) = Q(x) + \beta(u, x)^2$ for some fixed $u \in V$, and the resulting derivation $\widetilde{\eta}(k) = \eta(k) + u^k - u$ defines the same coset of $Inn(Sp(V), V)$ as does η.

We now take K to be a minimal transitive subgroup of $Sp(V)$. Thus K is either $Sp(2d, q)$ ($(d, q) \neq (1, 2), (2, 2)$) or $G_2(q)' < Sp(6, q)$ (in which case $d = 3$). In particular $K' = K$. The following shows that an explicit 1-cocycle spanning $H^1(G_2(q)', V)$ is given by restricting the 1-cocycle η for $Sp(6, q)$ given above.

7.2 Lemma. *(i)* $\dim H^1(K,V) = 1$, *and every* $\varepsilon \in Der(K,V)$ *is the restriction of some element of* $Der(Sp(V),V)$.

(ii) (cf. [29]) $Aut(V \rtimes K)$ *is 2-transitive on* $H^1(K,V)$.

Proof. $\dim_E H^1(K,V) = 1$ by [24], [29]. Suppose that the derivation $\eta|_K : K \to V$ is inner. By the preceding remarks we may suppose, after replacing $Q(x)$ by $Q(x) + \beta(u,x)^2$ if necessary, that $\eta|_K = 0$. But then by definition of η, $Q(x^k) = Q(x)$ for all $x \in V$ and $k \in K$. This is absurd for $q^{2d} > 2^2$ since K is transitive on $V - \{0\}$. Therefore $\eta|_K$ is not inner and (i) follows.

For $a, b \in E$ and $a \neq 0$, the map $(u,k) \mapsto (au + b\eta(k), k)$ is an automorphism of $V \rtimes K$, inducing the map $\varepsilon \mapsto a\varepsilon + b\eta$ on $Der(K,V)$, and (ii) follows. □

In Section 5 we were forced to consider a *triple* of elements of $H^1(K,V)$: one to specify the choice of extension $1 \to Z \to G \to \overline{G} \to 1$, and two more indicating the permutation actions of $\overline{G}$ on the rows and columns of H. Lemma 7.2(ii) shows that two of these cocycles can be chosen freely, but then to express the third requires explicit use of cocycles. For the purpose of proving Lemma 5.8, we derive an explicit expression for $\eta(g)$. For the remainder of this paper we assume the quadratic form is given by

$$Q(x) = Q(x_1, x_2, \ldots, x_{2d}) = \sum_{i=1}^{d} x_i x_{d+i}.$$

Let $g \in Sp(2d, E)$. Thus

$$g = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

where A, B, C, D are $d \times d$ matrices over E such that $AD^\top + BC^\top = A^\top D + C^\top B = I$ and the matrices $AB^\top$, $CD^\top$, $A^\top C$ and $B^\top D$ are symmetric. We will explicitly determine $\eta(g)$ in terms of A, B, C, D. Our expressions are simplified using the notation

$$\Delta(X) := (x_{11}, x_{22}, \ldots, x_{dd}) \in E^d$$

for every $d \times d$ matrix $X = \big(x_{ij} : 1 \leq i, j \leq d\big)$ over E. The proof of the following is an easy exercise using $char(E) = 2$.

7.3 Lemma. *(i)* $Tr(X^2) = \Delta(X)\Delta(X)^\top = (Tr\, X)^2$ *for every* $d \times d$ *matrix* X *over* E. *(ii)* $Tr(XY) = \Delta(X)\Delta(Y)^\top$ *whenever* X *and* Y *are symmetric* $d \times d$ *matrices over* E. □

Now

$$\begin{aligned}\beta(x, \eta(g^{-1}))^2 &= \beta(x, \eta(g)^{g^{-1}})^2 = \beta(x^g, \eta(g))^2 = Q(x^g) + Q(x) \\ &= (x_1^2, \ldots, x_d^2)\Delta(AB^\top)^\top + (x_{d+1}^2, \ldots, x_{2d}^2)\Delta(CD^\top)^\top\end{aligned}$$

and so $\eta(g^{-1}) = (\Delta(CD^\top), \Delta(AB^\top))^\sigma$ where σ applies the field automorphism $a \mapsto \sqrt{a}$ to each entry. Since $g^{-1} = \left[\begin{smallmatrix} D & C \\ B & A \end{smallmatrix}\right]^\top$, we conclude the following.

7.4 Lemma. *For* $Q(x) = \sum_{i=1}^d x_i x_{d+i}$ *and* $g = \left[\begin{smallmatrix} A & B \\ D & C \end{smallmatrix}\right] \in Sp(V)$, *we have*

$$\eta(g) = (\Delta(C^\top A), \Delta(D^\top B))^\sigma; \quad \eta(g^{-1}) = (\Delta(CD^\top), \Delta(AB^\top))^\sigma. \qquad \square$$

The fact (Theorem 7.1(v)) that $tr\, Q(\eta(g)) = 0$ anticipates the following.

7.5 Lemma. *For all* $g = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in Sp(V)$, *we have* $Q(\eta(g)) = \gamma(g) + \sqrt{\gamma(g)}$ *where* $\gamma : Sp(2d, E) \to E$ *is defined by*

$$\gamma(g) = Tr(B^\top C) = Tr(BC^\top).$$

Proof. By Lemmas 7.3 and 7.4,

$$\begin{aligned}Q(\eta(g))^2 &= \Delta(C^\top A)\Delta(D^\top B)^\top = Tr(C^\top A D^\top B) = Tr(AD^\top BC^\top) \\ &= Tr\big[(BC^\top + I)BC^\top\big] = Tr\big[(BC^\top)^2\big] + Tr(BC^\top) \\ &= \big[Tr(BC^\top)\big]^2 + Tr(BC^\top) = \gamma(g)^2 + \gamma(g).\end{aligned}$$

□

Denote $C_V(k) = \{x \in V \,:\, x^k = x\}$.

7.6 Lemma. *There exists* $k \in K$ *such that* $\gamma(k) = 0$ *and for all* $c \in E$, *the equation* $x^k + c\eta(k) = x$ *has exactly* $|C_V(k)| \geq 1$ *solutions* $x \in V$, *and each of these solutions satisfies* $\beta(x, \eta(k)) = c$.

Proof. (i) Suppose $K = Sp(2d, q) \leq Sp(V)$. Let $w = (1, 0, 0, \ldots, 0) \in E^{2d}$, and consider the transvection $k = \tau_w \in Sp(V)$ defined by $x \mapsto x + \beta(x, w)w$. Then $\tau_w = \left[\begin{smallmatrix} I & 0 \\ C & I \end{smallmatrix}\right]$ where C has $(1,1)$-entry equal to 1 and all other entries zero. By definition, $\gamma(\tau_w) = Tr(0^\top C) = 0$. By Theorem 7.1(iv) we have $\eta(\tau_w) = w$, and the equation $x^{\tau_w} + cw = x$ is equivalent to $\beta(x, w) = c$; this has q^{2d-1} solutions $x = (x_1, x_2, \ldots, x_{2d})$ where $x_{d+1} = c$.

(ii) Now suppose $K = G_2(q)' < Sp(V)$. We make use of the following elements of $G_2(q)$, as listed in [7] (but beware of misprints): for $t \in E$ we have elements $x_a(t)$, $x_b(t)$, $x_{a+b}(t)$ given by

$$\begin{bmatrix} 1 & t & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & t^2 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & t & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & t & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & t & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & t & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & t^2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & t & 0 & 1 \end{bmatrix}$$

respectively, and $x_{-a-b}(t) = x_{a+b}(t)^\top$. (In order to conform to our choice of bilinear form β, we have expressed these transformations with respect to a different basis than that used in [7]. This amounts to interchanging the fourth and sixth basis vectors.) Let $g = x_a(1)x_{a+b}(1)$, $h = x_b(1)x_{-a-b}(1)$ and

$$k = g^{-1}h^{-1}gh = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \in G_2(q)' = K.$$

We compute $\gamma(k) = 0$ from the definition, and $\eta(k) = (0, 0, 0, 1, 1, 0)$ using Lemma 7.4. We see that the equation $x^k + c\eta(k) = x$ has exactly q solutions $x = (0, c, 0, x_4, c, 0)$ where $x_4 \in E$, and each of these clearly satisfies $\beta(x, \eta(k)) = c$. □

7.7 Lemma. *Given $c \in E$, there is a unique map $K \to F$, $g \mapsto b_g$ such that*

$$b_{gh} = b_g + b_h + tr\,\beta(c\eta(g)^h, \eta(h)) \tag{7.7a}$$

for all $g, h \in K$. This map is given by $b_g = tr(c^2\gamma(g))$. If moreover $tr(c) = 0$, then $b_g = tr[Q(\eta(g))/t]$ where $t \in E$ is a solution of $t^{-1} + t^{-1/2} = c$.

Proof. It is clear that there is at most one map $K \to F$, $g \mapsto b_g$ satisfying (7.7a), for if $g \mapsto b'_g$ is another map satisfying (7.7a), then $g \mapsto b_g - b'_g$ defines a homomorphism from K to the additive group of F, and since $K' = K$ this implies $b'_g = b_g$.

For all g as above and $h = \left[\begin{smallmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{smallmatrix}\right] \in Sp(2d, E)$ also, using Lemma 7.3 and the identity $Tr(XY) = Tr(YX)$ we have

$$\begin{aligned}
\gamma(gh) &= Tr\big[(A\tilde{B} + B\tilde{D})(\tilde{A}^\top C^\top + \tilde{C}^\top D^\top)\big] \\
&= Tr\big[C^\top A\tilde{B}\tilde{A}^\top + D^\top B\tilde{D}\tilde{C}^\top + D^\top A\tilde{B}\tilde{C}^\top + B^\top C\tilde{A}\tilde{D}^\top\big] \\
&= Tr\big[C^\top A\tilde{A}\tilde{B}^\top + D^\top B\tilde{C}\tilde{D}^\top + B^\top C\tilde{B}\tilde{C}^\top + \tilde{B}\tilde{C}^\top + B^\top C\tilde{B}\tilde{C}^\top + B^\top C\big] \\
&= \Delta(C^\top A)\Delta(\tilde{A}\tilde{B}^\top)^\top + \Delta(D^\top B)\Delta(\tilde{C}\tilde{D}^\top)^\top + \gamma(g) + \gamma(h) \\
&= \beta(\eta(g), \eta(h^{-1}))^2 + \gamma(g) + \gamma(h) \\
&= \beta(\eta(g), \eta(h)^{h^{-1}})^2 + \gamma(g) + \gamma(h), \\
c^2\gamma(gh) &= \beta(c\eta(g)^h, \eta(h))^2 + c^2\gamma(g) + c^2\gamma(h).
\end{aligned}$$

Thus $b_g = tr(c^2\gamma(g))$ is the unique solution of (7.7a). Now suppose that $tr(c) = 0$, so that $c = t^{-1} + t^{-1/2}$ for some $t \in E$ (see [18, pp.3,4]). Then using Lemma 7.4,

$$\begin{aligned}
b_g &= tr\big[c^2\gamma(g)\big] = tr\big[t^{-2}\gamma(g) + t^{-1}\gamma(g)\big] = tr\big[t^{-1}\gamma(g)^{1/2} + t^{-1}\gamma(g)\big] \\
&= tr\big[t^{-1}Q(\eta(g))\big].
\end{aligned}$$

(Alternatively, one may verify the latter conclusion indirectly by checking that $tr[Q(\eta(g))/t]$ satisfies (7.7a) if $t^{-1} + t^{-1/2} = c$). □

References

[1] M. Aschbacher, *Finite group theory*, Camb. Univ. Press, Cambridge, 1986.

[2] A.E. Brouwer, A.M. Cohen and A. Neumaier, *Distance-Regular Graphs,* Springer-Verlag, New York, 1989.

[3] A.T. Butson, 'Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences', Canad. J. Math. **15** (1963), 42–48.

[4] C.J. Colbourn and W. de Launey, 'Difference matrices', in: *The CRC Handbook of Combinatorial Designs,* ed. C.J. Colbourn and J.H. Dinitz, CRC Press, Boca Raton, 1996.

[5] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups,* Clarendon Press, Oxford, 1985.

[6] B.N. Cooperstein, 'Minimal degree for a permutation representation of a classical group', *Israel J. Math.* **30** (1978), 213–235.

[7] B. N. Cooperstein, 'Maximal subgroups of $G_2(2^n)$', *J. Algeb.* **70** (1981), 23–36.

[8] R. Craigen, 'Regular conference matrices and complex Hadamard matrices', *Util. Math.* **45** (1994), 65–69.

[9] D.A. Drake, 'Partial λ-geometries and generalized Hadamard matrices over groups', Canad. J. Math. **31** (1979), 617–627.

[10] V. Ennola, 'On the characters of the finite unitary groups', *Ann. Acad. Sci. Fenn. AI* **323** (1963), 1–35.

[11] W. Feit, 'Automorphisms of symmetric balanced incomplete block designs', *Math. Z.* **118** (1970), 40–49.

[12] J.S. Frame, 'Computation of characters of the Higman-Sims group and its automorphism group', *J. Algebra* **20** (1972), 320–349.

[13] A. Gardiner, 'Antipodal covering graphs', *J. Comb. Theory Ser. B* **16** (1974), 255–273.

[14] C.D. Godsil, *Algebraic Combinatorics,* Chapman and Hall, New York, 1993.

[15] D. Gorenstein, *Finite Groups,* Harper and Row, New York, 1968.

[16] R.L. Griess, Jr., 'Schur multipliers of the known finite simple groups. II', Santa Cruz Conf. Finite Groups, *Proc. Sympos. Pure Math.* **37** (1980), 279–282.

[17] D.G. Higman, 'Monomial representations', in: *Finite groups, Sapporo and Kyoto 1974,* ed. N. Iwahori, Japan Soc. Promotion of Science, 1976, pp.55–68.

[18] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields,* Oxford Univ. Press, Oxford, 1979.

[19] I.M. Isaacs, *Character Theory of Finite Groups,* Acad. Press, 1976.

[20] N. Ito, 'Hadamard matrices with "doubly transitive" automorphism groups', *Arch. Math.* **35** (1980), 100–111.

[21] N. Ito and H. Kimura, 'Studies on Hadamard matrices with "2-transitive" automorphism groups', *J. Math. Soc. Japan* **36** (1984), 63–73.

[22] N. Ito and J.S. Leon, 'An Hadamard matrix of order 36', *J. Combin. Theory Ser. A* **34** (1983), 244–247.

[23] A.A. Ivanov, R.A. Liebler, T. Penttila and C.E. Praeger, 'Antipodal distance-transitive covers of complete bipartite graphs', *Europ. J. Combinatorics* **18** (1997), 11-33.

[24] W. Jones and B. Parshall, 'On the 1-cohomology of finite groups of Lie type', in: *Proc. Conf. Finite Groups 1975,* ed. W. R. Scott and F. Gross, Acad. Press, New York, 1976, pp. 313–327.

[25] D. Jungnickel, 'On difference matrices, resolvable transversal designs and generalized Hadamard matrices', *Math. Z.* **167** (1979), 49–60.

[26] W.M. Kantor, 'Automorphism groups of Hadamard matrices', *J. Combin. Theory* **6** (1969), 279–281.

[27] W. M. Kantor, 'Symplectic groups, symmetric designs, and line ovals', *J. Algeb.* **33** (1975), 43–58.

[28] W. M. Kantor, 'Homogeneous designs and geometric lattices', *J. Combin. Theory Ser. A* **38** (1985), 66–74.

[29] W.M. Kantor, 'Classification of 2-transitive symmetric designs', *Graphs Combin.* **1** (1985), 165–166.

[30] W.M. Kantor and R.A. Liebler, 'The rank 3 permutation representations of the finite classical groups', *Trans. Amer. Math. Soc.* **271** (1982), 1–71.

[31] G. Karpilovsky, *The Schur Multiplier,* Clarendon Press, Oxford, 1987.

[32] H. Kharaghani and J. Seberry, 'Regular complex Hadamard matrices', *Congressus Numerantum* **75** (1990), 187–201.

[33] P.B. Kleidman, 'The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups', *J. Algeb.* **117** (1988), 30–71.

[34] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics,* Camb. Univ. Press, Cambridge, 1992.

[35] B.D. McKay, 'nauty user's guide (version 1.5)', Tech. Rpt. TR-CS-90-02, Dept. Comp. Sci., Austral. Nat. Univ., 1990.

[36] H. Pollatsek, 'First cohomology groups of some linear groups over fields of characteristic two', *Ill. J. Math.* **15** (1971), 393–417.

[37] J.J. Seidel, 'A survey of two-graphs', in: *Colloquio Internazionale sulle Teorie Combinatoire,* Accademia Nazionale dei Lincei, Roma, 1976, pp. 481–511. Reprinted in: *Geometry and Combinatorics: Selected Works of J. J. Seidel,* ed. R. A. Mathon and D. G. Corneil, Acad. Press, San Diego, 1991.

[38] M. Suzuki, 'On a class of doubly transitive groups', *Ann. Math.* **75** (1962), 105–145.

[39] M. Suzuki, *Group Theory II,* Springer-Verlag, New York, 1986.

[40] D.E. Taylor, 'Two-graphs and doubly transitive groups', *J. Combin. Theory Ser. A* **61** (1992), 113–122.

[41] D.E. Taylor, *The Geometry of the Classical Groups,* Heldermann Verlag, Berlin, 1992.

[42] R.J. Turyn, 'Complex Hadamard matrices', in: *Combinatorial Structures and their Applications,* ed. R. Guy et al, Gordon and Breach, New York, 1970, pp.435–437.

[43] H.N. Ward, 'On Ree's series of simple groups', *Trans. Amer. Math. Soc.* **121** (1966), 62–89.