J. Austral. Math. Soc. 21 (1976) (Series A), 247–256.

GROUP PROPERTIES OF HADAMARD MATRICES

MARSHALL HALL, JR.

(Received 26 March 1975)

Communicated by W. D. Wallis

1. Introduction

An Hadamard matrix H is a square matrix of order n all of whose entries are ± 1 such that

$$HH^T = nI.$$

There are matrices of order 1 and 2

$$H_1 = [1], \qquad H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

and for all other Hadamard matrices the order n is a multiple of 4, $n = 4m$. It is a reasonable conjecture that Hadamard matrices exist for every order which is a multiple of 4 and the lowest order in doubt is 268.

With every Hadamard matrix H_{4m} a symmetric design D exists with

$$(1.1) \qquad v = 4m - 1, \qquad k = 2m - 1, \qquad \lambda = m - 1.$$

Such a design is given by normalizing H by changes of sign in rows and columns to make the first row and column consist entirely of $+1$'s. The positions of the $+1$'s in the rest of the matrix H give such a design D. Such designs D are called Hadamard designs and can conversely be used to construct an Hadamard matrix.

If H_{4m} is a normalized Hadamard matrix of order $4m$ then let us take H_{4m} and $-H_{4m}$ and delete the first row of each. There remain $8m - 2$ rows each containing exactly $2m$ $(+1)$'s. The positions of these $+1$'s give a design D^+ of $8m - 2$ blocks of size $2m$ with the property that every triple occurs $m - 1$ times. For each block, its complement is a block and every other block intersects it in m points. D^+ is a 3-design in which every triple of points occurs together $m - 1$ times.

This research was supported in part by a National Science Foundation Grant.

https://doi.org/10.1017/S1446788700017845 Published online by Cambridge University Press

A further class of symmetric designs D^* with

$$v = 4t^2, \qquad k = 2t^2 - t, \qquad \lambda = t^2 - t, \tag{1.2}$$

taken as the positions of $+1$'s in the rows of a $v \times v$ matrix gives a non-normalized Hadamard matrix.

Groups can be used in the construction of designs D, D^+, or D^* to yield a Hadamard matrix. Conversely if H is an Hadamard matrix, monomial ± 1 permutation matrices P, Q with

$$P^{-1}HQ = H \tag{1.3}$$

yield an automorphism of H. These groups and their inter-relations are discussed here.

2. Hadamard designs and Hadamard matrices

If $H = H_{4m}$ is an Hadamard matrix of order $4m$, then

$$H_{4m}H_{4m}^T = 4mI_{4m} \tag{2.1}$$

where every entry of H is ± 1. This property of being an Hadamard matrix is clearly preserved by the following operations on H:

i) permuting rows of H
ii) permuting columns of H
iii) changing the sign of a row of H
iv) changing the sign of a column of H.

If one Hadamard matrix H^* can be obtained from another H by a succession of these operations, this is clearly an equivalence relation between H^* and H. We will have

$$H^* = P^{-1}HQ \tag{2.2}$$

where P and Q are monomial permutations, the monomial factors being ± 1, where P describes the changes on the rows and Q the changes on the columns. If $H^* = H$ then in

$$H = P^{-1}HQ \tag{2.3}$$

we say that $\alpha = (P, Q)$ is an automorphism of H. These automorphisms form a group $G = A(H)$ in the obvious way since if $\alpha_1 = (P_1, Q_1)$ and $\alpha_2 = (P_2, Q_2)$ are automorphisms of H then also $\alpha_1\alpha_2 = (P_1P_2, Q_1Q_2)$ is an automorphism. The center of the automorphism group $A(H)$ includes the identity $1 = (I, I)$ and $\sigma = (-I, -I)$. So (2.3) gives $H^{-1}PH - Q$. The group $A(H)$ is clearly determined by either the row group of P's or the column group of Q's. We may always change the signs of the columns of H so that the first row consists entirely

https://doi.org/10.1017/S1446788700017845 Published online by Cambridge University Press

of $+1$'s and then change the signs of the rows so that first column consists entirely of $+1$'s. We say $H = H_{4m}$ is normalized and write.

$$(2.4) \qquad H_{4m} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & & & \\ \cdot & & & \\ \cdot & & U & \\ \cdot & & & \\ 1 & & & \end{bmatrix}$$

In U each row (or column) contains $2m-1$ $(+1)$'s and $2m$ (-1)'s. U determines a symmetric block design D with

$$(2.5) \qquad v = 4m-1, \qquad k = 2m-1, \qquad \lambda = m-1$$

where the rows (alternately columns) of D correspond to points and the columns (alternately rows) correspond to blocks and a point P_i of D is on a block B_j of D if the entry u_{ji} is $+1$. A symmetric design D with parameters $v = 4m-1$, $k = 2m-1$, $\lambda = m-1$ is called an Hadamard design and any such design can be used to construct a $(-1, 1)$ incidence matrix U which, when bordered by a column of $+1$'s and a row of $+1$'s as in (2.4) gives a normalized Hadamard matrix $H = H_{4m}$. An automorphism β of D is of course a permutation of the points of D and another of the blocks of D which preserves incidence in D. Thus any automorphism of an Hadamard design D is immediately equivalent to an automorphism of the corresponding normalized Hadamard matrix H fixing the first row r and first column c.

There is a design D^+ intermediate between D and H. The points of D^+ are the points of D and a new point r. The blocks of D^+ are (i) the blocks of D with r adjoined and (ii) the complements $C(B)$ of blocks B of D. A $(-1, 1)$ incidence matrix of D^+ may be obtained from the

$$4m \times 8m \text{ matrix } \begin{pmatrix} H_{4m} \\ -H_{4m} \end{pmatrix}$$

by deleting the first row r of H_{4m} and $-r$ of $-H_{4m}$. From this we have the following theorem.

THEOREM 2.1. *The automorphism group of D^+ is isomorphic to $G_r/\langle\sigma\rangle$.*

A further class of symmetric designs D^* leads to Hadamard matrices of square order. For these designs D^* we have

$$(2.6) \qquad v = 4t^2, \qquad k = 2t^2 - t, \qquad \lambda = t^2 - t.$$

If we take rows as points and blocks as columns and put $a_{ij} = +1$ if the ith point

https://doi.org/10.1017/S1446788700017845 Published online by Cambridge University Press

is on the jth block and $a_{ij} = -1$ otherwise, then the matrix $A = [a_{ij}]$ will be an Hadamard matrix of order $4t^2$.

3. A representation of the symmetric group associated with an Hadamard matrix

Let $H = H_{4n}$ be a normalized Hadamard matrix of order $4n$. The first row of H consists entirely of $+1$'s and every other row has $2n$ $(+1)$'s and $2n$ (-1)'s. Let r be the first row of H and let s be a further row and let $1,.2,\cdots, 4n$ be partitioned into subsets Y and Z so that $h_{st} = 1$ if $t \in Y$ while $h_{st} = -1$ if $t \in Z$. Each of Y and Z containing $2n$ subscripts. Associated with the row s we define a matrix $W(s) = [w_{ij}]$, $i, j = 1,\cdots,4n$ where

$$\begin{array}{llll} w_{ii} = 1, & i \in Y & & \\ w_{ii} = (n-1)/n, & i \in Z & & \\ w_{ij} = 0 \text{ if} & i \neq j & \text{and } i \text{ or } j \in Y & \\ w_{ij} = -1/n \text{ if} & i \neq j & \text{and } i \in Z,\ j \in Z. & \end{array} \tag{3.1}$$

In the special case in which $Y = \{1, 2, \cdots, 2n\}$, $Z = \{2n+1, \cdots, 4n\}$, W has the form

$$W = \left[\begin{array}{c|c} I_{2n} & 0 \\ \hline 0 & U \end{array}\right], \qquad U = \frac{1}{n}\begin{bmatrix} n-1, & -1,\cdots, & -1 \\ -1, & n-1,\cdots, & -1 \\ \cdot & & \\ \cdot & & \\ \cdot & & \\ -1, & -1,\cdots, & n-1 \end{bmatrix} \tag{3.2}$$

$$U = I_{2n} - \frac{1}{n} J_{2n},$$

where as usual J_m is the $m \times m$ matrix all of whose entries are 1's.

We now find that

$$\begin{gathered} (\overset{Y}{1,\cdots,1},\ \overset{Z}{1,\cdots,1})W(s) = (\overset{Y}{1,\cdots,1},\ \overset{Z}{-1,\cdots,-1}) \\ (\overset{Y}{1,\cdots,1},\ \overset{Z}{-1,\cdots,-1})W(s) = (\overset{Y}{1,\cdots,1},\ \overset{Z}{1,\cdots,1}). \end{gathered} \tag{3.3}$$

A further row of H has half its Z entries $+1$ and half its Z entries -1. We now find

Y

(3.4) $h = (1, \cdots, 1, \ -1, \cdots, -1, \ 1, \cdots, 1, \ -1, \cdots, -1), \qquad hW(s) = (h).$

The net result of this is that

$$HW(s) = H^* \tag{3.5}$$

where H^* is obtained from H by interchanging the first row r and the row s, and leaving all further rows fixed. Similarly if we take the matrix W,

$$W = I_{4n} - \frac{1}{2n} J_{4n}, \tag{3.6}$$

then

$$HW = H', \tag{3.7}$$

where the first row of H' is the negative of the first row of H and all other rows if H' are the same as those of H. All the W's are orthogonal matrices and are involutions.

If $X \in \langle W, \{W(s)\}\rangle = S$, then

$$HX = PH \tag{3.8}$$

where P is a monomial permutation, and conversely if P is any monomial permutation there is an $X \in S$ satisfying (3.8). If it should happen that $X = Q$ is in monomial form, then immediately

$$P^{-1}HQ = H \tag{3.9}$$

and (P, Q) is an automorphism of H. Conversely, if (3.9) is an automorphism of H, let (3.8) determine X from P. But then $HX = HQ$ and so $X = Q$ is in monomial form.

THEOREM 3.1. *With $W(s)$ determined by* (3.1) *and W determined by* (3.6), *the group $S = \langle W, \{W(s)\}\rangle$ is isomorphic to the full group of* ± 1 *monomial permutations on* $4n$ *points, and the subgroup K of S which is in monomial form consists precisely of the column representation of automorphisms of H.*

From $P^{-1}HQ = H$ we have

$$Q = H^{-1}PH = \frac{1}{4n} H^T PH = \left(\frac{H}{\sqrt{4n}}\right)^{-1} P \left(\frac{H}{\sqrt{4n}}\right) \tag{3.10}$$

with H of order $4n$, so that $H/\sqrt{4n}$ will be an orthogonal matrix. From this it follows that Q will be an orthogonal matrix of denominator d dividing $4n$, meaning that dQ has integral entries. If $4n = dh$ with $(d, h) = 1$ it follows that those Q's with denominator dividing d will correspond to P's which are a proper subgroup of the full monomial subgroup.

The author (1975) has found one very interesting case of a group of such semi-automorphisms. The H_{24} coming from the Paley construction based on the quadratic residues modulo 23, has semi-automorphisms of denominator dividing 3 which are the split extension of an elementary Abelian group of order 2^{12} by the Mathieu group M_{24}. This is of particular interest because M_{24} cannot be in the group of ordinary automorphisms of any H_{24}.

4. Group constructions of Hadamard matrices

Many of the known types of difference sets yield Hadamard designs D. These are discussed in my book *Combinatorial Theory*, Hall (1962) and in greater detail by Baumert (1971).

The main types are:

S: Singer difference sets for $PG(m,2)$, $v = 2^{m+1}-1$, $k = 2^m - 1$, $\lambda = 2^{m-1}-1$.

Q: Quadratic residues in $GF(q)$, $q = p^r \equiv 3 \pmod 4$, $v = q = 4t-1$, $k = 2t-1$, $\lambda = t-1$.

H_6: Let p be a prime of the form $p = 4x^2 + 27$ and let r be a primitive root of p such that $\mathrm{Ind}_r(3) \equiv 1 \pmod 6$ where $\mathrm{Ind}_r(b)$ is the index of b with respect to r. Then there are residues b such that $\mathrm{Ind}_r(b) \equiv 0,1,3 \pmod 6$ for a difference set with $v = p = 4t-1$, $k = 2t-1$, $\lambda = t-1$.

T: Twin primes $v = pq$, p and q primes, $q = p+2$. There is a difference set modulo pq including the $(p-1)\ (q-1)/2$ residues b for which

$$\left(\frac{b}{p}\right) = \left(\frac{b}{q}\right) \neq 0$$

and also the residues $0, q, 2q, \cdots, (p-1)q$. Here $v = pq = 4t-1$, $k = 2t-1$, $\lambda = t-1$.

GMW: Type of Gordon, Mills, Welch with the same parameters as Singer sets: $v = 2^{m+1}-1$, $k = 2^m - 1$, $\lambda = 2^{m-1}-1$. There are also some other special cases known when $v = 127$, $k = 63$, $\lambda = 31$.

P: Let $q \equiv 1 \pmod 4$ with $q = p^r$ a prime power. We construct a $q \times q$ matrix $K = [k_{ij}]$ where $k_{ij} = \chi(a_i - a_j)$ the quadratic character over $GF(q)$ and where $a_0 = 0$, $a_1 = 1$, $a_2, \cdots, a_{q-1}$ are the elements of $GF(q)$. Let S be the $q+1 \times q+1$ matrix obtain by bordering K:

https://doi.org/10.1017/S1446788700017845 Published online by Cambridge University Press

$$S = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \cdot & & & \\ \cdot & & K & \\ \cdot & & & \\ \cdot & & & \\ 1 & & & \end{bmatrix} \qquad \text{Here } S = S^T, \quad S^2 = qI.$$

Then a construction of Paley gives an Hadamard matrix

$$H_{2q+2} = \left[\begin{array}{c|c} I+S & -I+S \\ \hline -I+S & -I-S \end{array}\right] \tag{4.1}$$

The writer showed that for the Hadamard matrices of type Q that Aut(H) always contains $P\Sigma L_2(q)$, the special linear fractional group together with the field automorphisms of $GF(q)$.

Pless (1972) has shown that for H given by (4.1) the automorphism group contains $P\Gamma L_2(q)$, the general linear fractional group extended by the field automorphisms.

All Hadamard matrices of order 12 are equivalent and Hall (1962) has shown that the automorphism group of H_{12} modulo its center of order 2 is isomorphic to the quintuply transitive Mathıeu group M_{12}. H_{12} can be taken as type Q with $q = 11$ or type P with $q = 5$. It has been shown by Kantor (1969) that for all other cases for type Q the linear fractional group is the full group of automorphisms and in unpublished results that is also true for type P.

5. Rank 3 groups and strongly regular graphs

A graph $\mathcal{S}$ on v points is regular if each point is joined to the same number k of other points. It is strongly regular if the number of points joined to two points P and Q depends only on whether or not P and Q are joined to each other, the points being λ points if P and Q are joined and μ points if P and Q are not joined. If it should happen that $\lambda = \mu$, this immediately yields a design with parameters

$$v, k, \lambda, \tag{5.1}$$

the v blocks each consisting of points joined to a particular point. If $\mu = \lambda + 2$ taking the i^{th} block to consist of the i^{th} point and the k joined to it gives a design with parameters

$$v, \quad k^* = k + 1, \qquad \lambda^* = \lambda + 2 = \mu. \tag{5.2}$$

https://doi.org/10.1017/S1446788700017845 Published online by Cambridge University Press

In particular, a primitive transitive group G of even order on v points in which the stabilizer of a point (a) has exactly 3 orbits

$$(a),\quad \Delta(a),\quad \Gamma(a), \tag{5.3}$$

where $|\Delta(a)| = k$, $|\Gamma(a)| = l$, will yield a strongly regular graph joining point a to the points at the orbit $\Delta(a)$. There are a number of cases of such groups which lead to designs D or D^* and so to Hadamard matrices whose group of automorphisms includes G as a subgroup.

Higman (1964) has shown that the parameters of a strongly regular graph satisfy

$$\begin{aligned} &1 + k + l = v \\ &\mu l = k(k - \lambda - 1) \\ &d = (\lambda - \mu) + 4(k - \mu) \text{ is a square} \\ &\begin{Bmatrix} f_2 \\ f_3 \end{Bmatrix} = \frac{2k + (\lambda - \mu)(k + l) \pm \sqrt{d}(k + l)}{\pm 2d} \end{aligned} \tag{5.4}$$

where f_2 and f_3 are the multiplicities of the eigenvalues of the incidence matrix A of the graph apart from the eigenvalue k with multiplicity 1.

An interesting special case is the following. The simple group $U_4(2) \cong Sp_4(3)$ of order 25920 has a rank 3 representation on 36 points with orbit lengths 1, 15, 20 and $\lambda = \mu = 6$. This gives a design D^* 36, 15, 6 for an H_{36}. The corresponding Hadamard design D with parameters 35, 17, 8 has the symmetric group S_8 in its representation on complementary 4's, say 1234 | 5678 as its automorphism group and the full group of automorphisms of H is the larger group $Sp_6(2)$ of order 1,451,520.

A further interesting case is derivable from the group M_{12}. It contains two classes of subgroups isomorphic to $PSL_2(11)$, one on 11 points, the other on 12 points. The representations of M_{12} on cosets of $PSL_2(11)$ is of 144 points being imprimitive in the first case and primitive in the second. In both cases the representation is of rank 5 with a stabilizer having orbits of lengths 1, 66, 11, 11, 55, and in both cases the 66 orbits give an H_{144} with a D^* design 144, 66, 30. In the imprimitive case the 55 orbit and either 11 orbit also give such a design.

6. Designs D^+ and D^*

The Kronecker product of t copies of the matrix

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

https://doi.org/10.1017/S1446788700017845 Published online by Cambridge University Press

gives an Hadamard matrix of order 2^{2t} where the $+1$'s or -1's form a design D^*. Kantor (to appear) has shown recently that the automorphism group of this design D^* is an elementary 2 group $E(2^{2t})$ extended by $Sp_{2t}(2)$. The full automorphism group of the Hadamard matrix is the product of two elementary 2 groups extended by the automorphism group of $E(2^{2t})$.

Norman (1908) has shown that when $n = 4m$ and m is odd, the design D^+ has a triply transitive automorphism group only for $4m = 12$, and then the group is M_{11}. When H is the Kronecker product of $t\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$'s, then D^+ is the affine geometry over $GF(2)$ and has a triply transitive automorphism group. For m even, it is plausible that these are the only cases for which D^+ has a triply transitive automorphism group.

7. Williamson matrices. Baumert-Hall arrays

Williamson (1944) found Hadamard matrices H_{4m} of the form

$$(7.1) \qquad H_{4m} = \begin{bmatrix} A, & B, & C, & D \\ -B, & A, & -D, & C \\ C, & D, & A, & -B \\ -D, & -C, & B, & A \end{bmatrix}$$

where A, B, C, D were symmetric circulants of order m satisfying

$$(7.2) \qquad A^2 + B^2 + C^2 + D^2 = 4mI_m.$$

This amounts to assuming the existence of the cyclic automorphism group of order m together with its inverting automorphism leaving the matrices A, B, C, D fixed. For these purposes we may replace the cyclic group of order m by any other Abelian group of order m. For $m = 25$ all of these were found by taking, instead of (7.1), the form

$$(7.3) \qquad \begin{bmatrix} A, & -B, & -C, & -D \\ -B, & -A, & -D, & C \\ -C, & D, & -A, & -B \\ -D, & -C, & B, & -A \end{bmatrix}$$

The matrix appears in the D^* form with $v = 100$, $k = 45$, $\lambda = 20$.

Baumert and Hall (1965) found a 12×12 array with $3A$'s, $3B$'s, $3C$'s, $3D$'s in each row and column and in which the rows and columns were formally

https://doi.org/10.1017/S1446788700017845 Published online by Cambridge University Press

orthogonal so that whenever an Hadamard matrix (7.1) of Williamson type of order $4m$ exists, then also an H_{12m} exists.

Wallis (1973) and Turyn, (1972, 1974) working independently, have enormously extended this system of arrays and so greatly expanded the number of known Hadamard matrices. The details are quite complicated, but one interpretation applicable is that of certain orthogonality relations over group rings.

References

L. D. Baumert (1971), *Cyclic difference sets* (Lecture notes in Mathematics No. 182, Springer, Berlin-New York).

L. D. Baumert and Marshall Hall, Jr. (1965), 'A new construction for Hadamard matrices', *Bull. Amer. Math. Soc.* **71**, 169–170.

Marshall Hall, Jr. (1962), 'A note on the Mathieu group M_{12}', *Arch. Math* (*Basel*) **13**, 334–340.

Marshall Hall, Jr. (1967), *Combinatorial theory* (Blaisdell, Walham, Massachusetts, 1967).

Marshall Hall, Jr. (to appear), 'Semi-automorphisms of Hadamard matrices', *Proc. Cambridge Philos. Soc.*

D. G. Higman (1964), 'Finite permutation groups of rank 3', *Math. Z.* **86**, 145–156.

William Kantor (1969), 'Automorphism groups of Hadamard matrices', *J. Combinatorial Theory* **6**, 279–281.

William Kantor (to appear), 'Symplectic groups, symmetric designs and line ovals', *J. Combinatorial Theory.*

Christopher Norman (1968), 'A characterization of the Mathieu group M_{11}', *Math. Z.* **106**, 162–166.

Vera Pless (1972), 'Symmetry codes over $GF(3)$ and new Five-designs', *J. Combinatorial Theory* **12**, 119–142.

R. J. Turyn (1974), 'Hadamard matrices, Baumert-Hall units, four symbol sequences, pulse compression, and surface wave encodings', *J. Combinatorial Theory* **16**, 313–333.

R. J. Turyn (1972), 'An infinite class of Williamson matrices', *J. Combinatorial Theory* **12**, 219–321.

Jennifer Wallis (1973), 'Hadamard matrices of order 28m, 36m, and 44m', *J. Combinatorial Theory* **15**, 323–328.

J. Williamson (1944), 'Hadamard's determinant theorem and the sum of four squares', *Duke Math. J.* **11**, 65–81.

Department of Mathematics
California Institute of Technology
Pasadena, California
U.S.A.

https://doi.org/10.1017/S1446788700017845 Published online by Cambridge University Press