Reprinted from JOURNAL OF COMBINATORIAL THEORY

Vol. 6, No. 3, April 1969
Printed in Belgium

Automorphism Groups of Hadamard Matrices*

WILLIAM M. KANTOR

University of Wisconsin, Madison, Wisconsin, 53706

Communicated by Marshall Hall

Received December 11, 1967

ABSTRACT

Automorphism groups of Hadamard matrices are related to automorphism groups of designs, and the automorphism groups of the Paley-Hadamard matrices are determined.

According to Hall [3], an automorphism of a Hadamard matrix H of size n is a pair (P, Q) of $n \times n$ monomial matrices such that $PHQ = H$. The automorphisms of H form a group Γ. $1 = (I, I)$ and $\sigma = (-I, -I)$ are in the center of Γ. $\bar{\Gamma} = \Gamma/\langle\sigma\rangle$ acts faithfully as a permutation group on the union of the sets of rows and columns of H.

If $\mathscr{D}$ is a Hadamard design and M a $(-1, 1)$ incidence matrix of $\mathscr{D}$, then $H = M^+$ is the Hadamard matrix obtained from M by adjoining a column c and a row r of 1's.

$\mathscr{D}$ determines a design $\mathscr{D}^+$ as follows. The points of $\mathscr{D}^+$ are the points of $\mathscr{D}$ together with a new point r; the blocks of $\mathscr{D}^+$ are (i) the blocks of $\mathscr{D}$ with r adjoined, and (ii) the complements $\mathscr{C}B$ of the blocks B of $\mathscr{D}$. $(B \cup \{r\}, \mathscr{C}B)$ is called a parallel class of blocks. A $(-1, 1)$ incidence matrix of $\mathscr{D}^+$ may be obtained from the $n \times 2n$ matrix $(M^+, -M^+)$ by removing the columns c and $-c$. This implies the following

THEOREM 1. *The automorphism group of $\mathscr{D}^+$ is isomorphic to $\bar{\Gamma}_c$.*

If M is symmetric, and $\gamma \in \Gamma_c$ moves r, then there is an element $\gamma' \in \Gamma_r$ moving c. Then $\gamma\gamma'$ moves r and c:

THEOREM 2. *If $\mathscr{D}$ admits a polarity, and Γ_c has an element moving r, then Γ has an element moving both r and c.*

* Research supported by NSF Grant GP 7083.

THEOREM 3. *If $\bar{\Gamma}$ is 2-transitive on rows but not faithful on columns, then $\mathscr{D}$ is a projective space.*

PROOF: The subset Σ of elements of Γ fixing all columns is a normal subgroup of Γ, and $\bar{\Sigma} = \Sigma/\langle\sigma\rangle$ acts regularly on rows. It follows from the 2-transitivity of $\bar{\Gamma}$ that $\bar{\Sigma}$ is row-transitive and elementary Abelian. $\bar{\Sigma}$ may be regarded as an automorphism group of $\mathscr{D}^+$ transitive on points and fixing each parallel class. Then the stabilizer of a block in $\bar{\Sigma}$ has index $\leqslant 2$, so that the blocks correspond to the cosets of subgroups of index 2, and $\mathscr{D}^+$ is an affine space.

If $\gamma \in \Gamma$ fixes all rows of H and $\delta \in \Gamma$ fixes all columns of H, then $\gamma^{-1}\delta^{-1}\gamma\delta$ fixes all rows and columns and thus $=1$ or σ. This implies the following:

THEOREM 4. *If $\mathscr{D} = PG(d, 2)$ then $\bar{\Gamma}$ is a semidirect product of $PSL(d, 2)$ with an elementary Abelian group of order 2^{2d}.*

Let $q > 3$ be a prime power $\equiv 3 \pmod 4$. The Paley design $\mathscr{P}(q)$ is the Hadamard design defined by the difference set of squares in $GF(q)$. Let $\mathscr{D} = \mathscr{P}(q)$, so that $H = M^+$ is the Paley-Hadamard matrix [6]. Hall [3] has shown that Γ has a subgroup Π containing σ such that $\bar{\Pi} = \Pi/\langle\sigma\rangle$ acts faithfully on both the rows and columns of H as the group of all permutations of $GF(q) \cup \{\infty\}$ of the form $x \to (ax^\theta + b)/(cx^\theta + d)$, $a, b, c, d \in GF(q)$, $ad - bc = 1$, and $\theta \in \operatorname{Aut} GF(q)$; moreover $\Pi_c = \Pi_r$.

THEOREM 5 (Hall [3]). *If $\mathscr{D} = \mathscr{P}(11)$, then $\bar{\Gamma}$ acts on both rows and columns as the Mathieu group M_{12}.*

PROOF: By Hughes [4] and Todd [7], the full automorphism group of $\mathscr{D}^+$ is M_{11}. By Theorem 1, $\bar{\Gamma}_c$ is M_{11}. Since $\bar{\Gamma}_c$ is transitive on the columns $\neq c$, M_{11} is thus represented as a group transitive on these 11 columns. By Theorems 2 and 3, $\bar{\Gamma}$ acts faithfully on columns as a 2-transitive group of degree 12 such that the stabilizer of a column is isomorphic to M_{11}. It is now easy to see that $\bar{\Gamma}$ is M_{12}.

THEOREM 6. *If $\mathscr{D} = \mathscr{P}(q)$, $q > 11$, then $\Gamma = \Pi$.*

Special cases of this result are found in [1].

PROOF: Assume that $\Gamma > \Pi$. $\bar{\Gamma}_{cr}$ acts as an automorphism group of $\mathscr{P}(q)$, and thus $\Gamma_{cr} = \Pi_{cr}$ by [5, Theorem 12.1]. Then $\Gamma_c > \Pi_c = \Pi_{cr}$ implies that Γ_c moves r and thus is 2-transitive on rows. By Theorem 3, $\bar{\Gamma}_c$ acts faithfully on rows as a 2-transitive permutation group such that the stabilizer of a row r acts on the remaining rows as $\bar{\Pi}_{cr}$. It is then not difficult to show that $\bar{\Gamma}_c$ is isomorphic to $\bar{\bar{\Pi}}$ (cf. Zassenhaus [8]; Bender [0]). Since $\bar{\Gamma}_c$ has a faithful transitive representation of degree q on the columns $\neq c$, this readily contradicts a classical result of Galois and Dickson [2, p. 286].

References

0. H. Bender, Endliche zweifach transitive Permutationsgruppen, deren Involutionen keine Fixpunkte haben. *Math. Z.* **104** (1968), 175–204.
1. E. F. Assmus, Jr., H. F. Mattson, Jr., and R. J. Turyn, Research to Develop the Algebraic Theory of Codes, AFCRL-67-0365, 1967.
2. L. E. Dickson, *Linear Groups*, Dover, New York, 1958.
3. M. Hall, Jr., Note on the Mathieu Group M_{12}, *Arch. Math.* **13** (1962), 334–340.
4. D. R. Hughes, On t-Designs and Groups, *Amer. J. Math.* **87** (1965), 761–778.
5. W. M. Kantor, 2-Transitive Symmetric Designs (to appear).
6. R. E. A. C. Paley, On Orthogonal Matrices, *J. Math. and Phys.* **12** (1933), 311–320.
7. J. A. Todd, A Combinatorial Problem, *J. Math. and Phys.* **12** (1933), 321–333.
8. H. Zassenhaus, Kennzeichnung endlicher linearen Gruppen als Permutationsgruppen, *Abh. Math. Sem. Univ. Hamburg* **11** (1936), 17–40.

PRINTED IN BRUGES, BELGIUM, BY THE ST. CATHERINE PRESS, LTD.