Math. Z. 109, 246 – 252 (1969)

Automorphism Groups of Designs*

William M. Kantor

1. Introduction

From a geometric point of view, the most interesting designs (see § 2 for definitions) are generally those admitting fairly large automorphism groups. The methods of finite permutation groups may be applied to such designs, and vice versa, as in [5, 6, 8, 11, 13 and 14]. We shall prove several general results which are useful in the study of automorphism groups of designs, and then use some of these to characterize some designs admitting large automorphism groups. Further applications are found in [11].

A Hadamard design is a symmetric design with $k=(v-1)/2$ (see [3] or [17] for the connection with Hadamard determinants). The best known examples of such designs – other than the Desarguesian projective spaces over $GF(2)$ – are the Paley designs ([15]; cf. [18] and [11]). The points of a Paley design are the elements of $F=GF(v)$, where $v>3$ is a prime power $\equiv 3 \pmod 4$, while the blocks are the translates under F^+ of the set Q of non-zero squares of F. This design admits an automorphism group of odd order $\{x \to x^\sigma t+a \mid t\in Q, a\in F, \sigma\in \mathrm{Aut}(F)\}$ which is transitive on incident point-block pairs; this group is not always the full automorphism group (cf. [11]).

Theorem 1.1. *Paley designs are the only Hadamard designs admitting automorphism groups which are transitive on incident point-block pairs but which are not* 2*-transitive on points.*

A larger class of designs will also be considered, all related to F. Our characterizations of some of these designs generalize many of the results of Lüneburg [13], whose approach is different.

Many of the results of this paper are quoted in Dembowski [3]. The author is indebted to Dr. Dembowski for his many helpful comments and suggestions.

2. Definitions

It is occasionally useful to consider incidence structures in which distinct blocks may be incident with precisely the same sets of points (or dually). It will be clear from context whether or not blocks can be identified with their sets of points (or dually). A tactical configuration is a finite incidence structure consisting of v points and b blocks in which each point is on $r<b$ blocks and each block is on $k<v$ points. Here $b\,k=v\,r$. A design is a tactical configuration in which every two distinct points are on λ blocks. Then $\lambda(v-1)=r(k-1)$.

* Research supported by the National Aeronautics and Space Administration.

Moreover, Fisher's inequality states that $b \geqq v$ [17, p. 99]. Those designs for which $b = v \geqq k+2$ are called symmetric designs. For such designs $r = k$ and every two distinct blocks are on precisely λ points. A Hadamard design is a symmetric design for which $v-1=2k$.

If x is a point of a design $\mathscr{D}$ then $\mathscr{D}_x$ is the tactical configuration whose points are the points $\neq x$ and whose blocks are the blocks on x, with induced incidence. $\mathscr{D}_x$ has parameters $v_x = v-1$, $b_x = r$, $k_x = k-1$ and $r_x = \lambda$. The complementary design of a symmetric design is the symmetric design $\mathscr{D}'$ whose points and blocks are those of $\mathscr{D}$ and for which incidence is equivalent to non-incidence in $\mathscr{D}$. Here the parameters are $v' = v$, $k' = v-k$ and $\lambda' = v - 2k + \lambda$.

Many of the relevant definitions concerning permutation groups are found in Wielandt [19]. The rank of a transitive permutation group is the number of orbits of the stabilizer of a point. A permutation group is called (sharply) 2-homogeneous if it is (sharply) transitive on the set of unordered pairs of points.

It will be necessary to distinguish between the action of automorphism groups on points and on blocks. Thus, we shall speak of point-orbits, block-rank, and so on. A flag of an incidence structure is an incident point-block pair, and it is then clear what is meant by a (sharply) flag-transitive automorphism group.

If v is a prime power and $F = GF(v)$, then $S(v)$ is the group of all semilinear mappings $x \to x^\sigma t + a$ on F, where $t \neq 0$ and a are in F and $\sigma \in \mathrm{Aut}(F)$. $L(v)$ is the normal subgroup of $S(v)$ consisting of those mappings for which $\sigma = 1$.

For the definition and properties of Dickson nearfields, see Zassenhaus [20].

3. 2-Homogeneous Groups

The following result provides a description of 2-homogeneous groups which are not 2-transitive.

Proposition 3.1. *If Γ is a transitive permutation group on a finite set S, where $v = |S| > 3$, then the following statements are equivalent.*

i) *Γ has rank 3 and all orbits of Γ_x, $x \in S$, have odd lengths.*

ii) *Γ is 2-homogeneous but not 2-transitive on S.*

iii) *v is a prime power $\equiv 3 \pmod 4$, and Γ is similar to a 2-homogeneous subgroup of $S(v)$.*

If Γ is represented as in iii), *then Γ contains the set Σ of all translations $x \to x + a$, $a \in F = GF(v)$, as a normal subgroup. $\Gamma \cap L(v)$ is a normal Frobenius subgroup of Γ with kernel Σ. If Q is the group of non-zero squares of F, then the orbits of Γ_0 are $\{0\}$, Q and $-Q$.*

Proof. i)$\Rightarrow$ii). Let k and l be the lengths of the orbits $\neq \{x\}$ of Γ_x. Suppose that Γ has even order. By Higman [5, Lemmas 5 and 7], there are integers λ and μ such that $\mu\, l = k(k-\lambda-1)$ and $d = (\lambda-\mu)^2 + 4(k-\mu)$ is a square. Then $k \equiv l \equiv 1 \pmod 2$ implies that $\mu \equiv \lambda \pmod 2$, $d \equiv 0 \pmod 4$ and $2k + (\lambda-\mu)(k+l) \equiv 2 \pmod 4$. This contradicts the fact that $2\sqrt{d}$ divides $2k + (\lambda-\mu)(k+l)$ (Higman [5, Lemma 7]).

Thus Γ has odd order and $k=l=(v-1)/2$ by Higman [5, Corollary 1]. If x and y are distinct points of S then $|\Gamma:\Gamma_{\{x,y\}}|=|\Gamma:\Gamma_{xy}|=v(v-1)/2$. It follows that Γ is transitive on the unordered pairs of points of S.

ii)$\Rightarrow$iii). Γ is clearly primitive, and is solvable by the Feit-Thompson Theorem [4]. Thus there is a transitive elementary abelian normal subgroup Σ of Γ. If Σ is identified with S then $\sigma\to\sigma^{-1}$, $\sigma\in S$, is a permutation not in Γ which centralizes Γ_1 and together with Γ thus generates a solvable 2-transitive group $\hat{\Gamma}$ on S containing Γ as a subgroup of index 2. Huppert's classification of such groups [9] completes the proof (cf. [12, p. 402]).

Suppose that Γ is represented as in iii). As above, Σ is a normal subgroup of Γ. It is easy to see that the orbits of Γ_0 are $\{0\}$, Q and $-Q$, so that i) holds. $\Gamma_0/\Gamma_0\cap L(v)$ is isomorphic to a group of automorphisms of F. If $v=p^e$, where p is prime, it follows that $(p^e-1)/2\leqq|\Gamma_0|\leqq e\,|\Gamma_0\cap L(v)|$. Thus, $\Gamma_0\cap L(v)\neq 1$.

Corollary 3.2. *If Γ is a sharply 2-homogeneous permutation group of degree v then Γ is similar to the group of mappings $x\to x\circ t+a$ on a Dickson nearfield K, where $a\in K$ and t is in the group of non-zero squares of K. In particular, Γ is contained as a subgroup of index 2 in a sharply 2-transitive group $\hat{\Gamma}$.*

This follows from the preceding Proposition together with Zassenhaus' results on nearfields [20].

4. Orbits and Imprimitivity Classes

It is often very useful to have information concerning transitivity or primitivity properties of automorphism groups of designs. Dembowski [2], Hughes [7], and Parker [16] have shown that the numbers of point- and block-orbits of an automorphism group of a symmetric design are equal. The following result is a straightforward generalization of this.

Theorem 4.1. *An automorphism group Γ of a design has at least as many block-orbits as point-orbits.*

Proof. For not necessarily symmetric designs, equation (11) of Dembowski [2] becomes $\det(AB)=r\,k(r-\lambda)^{t-1}$, where Γ has t point-orbits and t' block-orbits and A and B are $t\times t'$ resp. $t'\times t$ matrices. As in the proof of Fisher's inequality in [17], $t'\geqq\operatorname{rank}(A)\geqq\operatorname{rank}(AB)=t$.

Corollary 4.2. *An automorphism group of a design is 2-transitive on points provided that, for each point x, the stabilizer of x is transitive on the blocks on x and on the blocks not on x.*

Lemma 4.3. *If Γ is a point- and block-transitive automorphism group of a tactical configuration, and x and X are a point and a block, then Γ_X has as many point-orbits as Γ_x has block-orbits.*

Proof. Both quantities are the number of orbits of Γ on the pairs (x, X).

Theorem 4.4. *If Γ is a point- and block-transitive automorphism group of a design, then the block-rank of Γ is at least as large as the point-rank of Γ.*

Proof. By Theorem 4.1 and Lemma 4.3,

$$\begin{aligned} \textit{block-rank of } \Gamma &= \textit{number of block-orbits of } \Gamma_X \\ &\geqq \textit{number of point-orbits of } \Gamma_X \\ &= \textit{number of block-orbits of } \Gamma_x \\ &\geqq \textit{number of point-orbits of } \Gamma_x \\ &= \textit{point-rank of } \Gamma. \end{aligned}$$

Theorem 4.4 generalizes a result of Dembowski [2, Satz 4]. Both Theorems 4.1 and 4.4 have been obtained independently by Block [1]. The above proof of Theorem 4.4 is more elementary than his proof.

Proposition 4.5. *Let Γ be an automorphism group of a tactical configuration such that each block-orbit of Γ has length divisible by b/e, where e is an integer. Then each point-orbit of Γ has length divisible by $v/(v, e\,k)$. In particular, there are at most $(v, e\,k)$ point-orbits.*

Proof. If $\mathfrak{p}$ is a point-orbit and $\mathfrak{b}$ a block-orbit, let $(\mathfrak{p}, \mathfrak{b})$ be the number of points of $\mathfrak{p}$ on each block in $\mathfrak{b}$. Then $r = \sum_{\mathfrak{b}} (\mathfrak{p}, \mathfrak{b})\,|\mathfrak{b}|/|\mathfrak{p}|$, so that b/e divides $r\,|\mathfrak{p}|$. It follows that $e\,r\,|\mathfrak{p}|/b = e\,k\,|\mathfrak{p}|/v$ is an integer. (The case $e = 1 = (v, k)$ of Proposition 4.5 is due to Lüneburg [14, Lemma 1].)

Corollary 4.6. *If Γ is a flag-transitive automorphism group of a design, then* i) *if $(v-1, k-1) = 1$ then Γ is 2-transitive on points; and* ii) *if $(v-1, k-1) = 2$ then Γ is either 2-transitive on points or has rank 3 on points and, for each point x, the point-orbits $\neq \{x\}$ of Γ_x have length $(v-1)/2$.*

Proof. Apply Proposition 4.5 to the tactical configuration $\mathscr{D}_x$ (see Section 2).

The following two results generalize Higman and McLaughlin [6, Proposition 3]. Applications are found in [11].

Theorem 4.7. *Let Γ be a point-transitive automorphism group of a design $\mathscr{D}$ such that, for each point x, the length of each orbit of Γ_x of blocks on x is divisible by r/e, where e is an integer. Then Γ is point-primitive provided that either* i) *$r > e\,\lambda(e\,k - e - 2)$, or* ii) *$\lambda > (r/e, \lambda)(e^2(r/e, \lambda) - 1)$.*

Theorem 4.8. *A flag-transitive automorphism group Γ of a design $\mathscr{D}$ is point-primitive provided that either* i) *$r > \lambda(k-3)$,* ii) *$\lambda > (r, \lambda)((r, \lambda) - 1)$,* iii) *$(r, \lambda) = 1$,* iv) *$(r, \lambda) = 2$ and either $\lambda \neq 2$ or $r \neq 2(k-3)$,* v) *$(r - \lambda, k) = 1$, or* vi) *$(v, k) = 1$, $r = k + \lambda$ and k is square-free.*

Proof of Theorems 4.7 *and* 4.8. If Γ is imprimitive there are $n > 1$ imprimitivity classes, each having $c > 1$ points, which are permuted transitively by Γ ([19, p. 12]). Here $v = n\,c$. Let $0, t_1, \ldots, t_h$ be the distinct values taken by $|X \cap \mathfrak{C}|$ as X ranges over all blocks and $\mathfrak{C}$ over all classes. If $\mathfrak{C}$ is a class and $x \in \mathfrak{C}$, there are $(r/e)\,w_j$ blocks on x meeting $\mathfrak{C}$ in t_j points, where w_j is an integer ($j = 1, \ldots, h$). If $t - 1 = \sum_j w_j(t_j - 1)$, then

$$\lambda(c-1) = \sum_j (r/e)\,w_j(t_j - 1) = (r/e)(t-1). \qquad (1)$$

Together with $\lambda(v-1)=r(k-1)$ and $v=n\,c$ this implies that $t>1$ and

$$\lambda(n-1)=(r/e)\{e(k-1)-n(t-1)\}=(r/e)\{(n-e)-(n\,t-e\,k)\}. \tag{2}$$

Since $n>1$, $e(k-1)\geqq n(t-1)+1\geqq(n-1)+2\geqq r/e\,\lambda+2$, and Theorem 4.7 i) cannot hold. By (2), $s=\{(n-e)-(n\,t-e\,k)\}(r/e,\lambda)/\lambda$ is a positive integer, so that $r\geqq k$ (Fisher's inequality), (1) and (2) imply that

$$\begin{aligned}(r/e,\lambda)&=r\,s/e(n-1)\geqq\{n\,t-(n\,t-e\,k)\}\,s/e^2(n-1)\\&>n\,t\,s/e^2(n-1)-(n-e)\,s/e^2(n-1)\\&>t\,s/e^2-s/e^2\geqq(t-1)/e^2.\end{aligned} \tag{3}$$

By (1), $\lambda|(r/e,\lambda)(t-1)$ so that Theorem 4.7 ii) cannot hold. This proves Theorem 4.7.

From now on assume that the additional hypothesis of Theorem 4.8 holds: $e=1$. i) and ii) follow from Theorem 4.7. iii) is a special case of ii) due to Dembowski. If $(r,\lambda)=2$ then (3) implies that iv) cannot hold.

Thus far we have been following the argument of Higman and McLaughlin fairly closely. We gain additional information by observing that a second design $\mathscr{D}_1$ may be constructed by taking the imprimitivity classes as points and the blocks of $\mathscr{D}$ as blocks, incidence being "class meets block". The parameters of $\mathscr{D}_1$ are $v_1=n$, $b_1=b$, $k_1=k/t$ and $\lambda_1=\lambda\,c^2/t^2$. The value of λ_1 may be checked by fixing distinct classes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ and counting in two ways the triples (x_1,x_2,X) with $x_i\in\mathfrak{C}_i$ and x_i on X $(i=1,2)$. Thus

$$t|(\lambda\,v,k)=(\lambda-r+r\,k,k)=(r-\lambda,k)$$

and v) cannot hold. Also, if $r=k+\lambda$ then

$$t^2|(\lambda\,v^2,k^2)=(b\,k^2-v\,k,k^2)=(v,k)\,k$$

and vi) cannot hold, proving Theorem 4.8.

5. Proof of Theorem 1.1

It is easy to see that a group of the type described in Proposition 3.1 is flag-transitive on the corresponding Paley design. Conversely, suppose that Γ is a flag-transitive automorphism group of a Hadamard design $\mathscr{D}$, but is not 2-transitive on points. By Corollary 4.6 and Proposition 3.1, v is a prime power and we may assume that $\Gamma<S(v)$. By Proposition 3.1, $\Phi=\Gamma\cap L(v)$ acts on points and blocks as a Frobenius group with kernel Σ. Let X be a block. Since $\Phi_X\cap\Sigma=1$ and the commutator subgroup of Φ is contained in Σ, Φ_X fixes some point, say 0. Then Γ_X fixes 0, or $\Gamma_X=\Gamma_0$. By Proposition 3.1, $\mathscr{D}$ is isomorphic to a Paley design, proving Theorem 1.1. A similar proof yields the

Corollary 5.1. *Paley designs and their complementary designs are the only symmetric designs admitting automorphism groups which are 2-homogeneous but not 2-transitive on points.*

6. Sharply Flag-Transitive Designs

Let K be a Dickson nearfield with v elements, $3<v\equiv 3 \pmod 4$, in which multiplication is denoted by $\circ$. The group of all linear mappings on K of the form $x\to x\circ t+a$, where $a\in K$ and t is in the group $Q(K)$ of squares of K, is a sharply 2-homogeneous group Γ. Let G be a non-trivial subgroup of $Q(K)$. We construct a design $\mathscr{D}(K,G)$ as follows: points are the elements of K and blocks are the distinct sets G^{γ}, $\gamma\in\Gamma$, with incidence the same as inclusion. Since Γ is 2-homogeneous, the incidence structure defined in this manner is a design. $\mathscr{D}(K,Q(K))$ is a Paley design. Γ_G is the group of mappings $x\to x\circ g$, $g\in G$. It follows that $\mathscr{D}(K,G)$ has parameters $b=v(v-1)/2k$, $k=|G|$, $r=(v-1)/2$ and $\lambda=(k-1)/2$. Proposition 3.1 implies the following

Proposition 6.1. *The sharply 2-homogeneous group defined by a Dickson nearfield K with $|K|\equiv 3 \pmod 4$ is a sharply flag-transitive automorphism group of $\mathscr{D}(K,G)$ for any $G\leqq Q(K)$. If K is a field, then the group of all mappings $x\to x^{\sigma}t+a$, where $a\in K$, $t\in Q(K)$ and $\sigma\in\operatorname{Aut}(K)$, is a maximal automorphism group of $\mathscr{D}(K,G)$ of odd order.*

Proposition 6.2. *Let Γ be a sharply flag-transitive, sharply 2-homogeneous automorphism group of a design $\mathscr{D}$ with $(v,k)=1$. Then $\mathscr{D}$ is isomorphic to $\mathscr{D}(K,G)$ for some Dickson nearfield K with v elements and some $G\leqq Q(K)$.*

Proof. We may assume that Γ is represented as in Corollary 3.2. Let B be a block. Since $(v,k)=1$, Γ_B has trivial intersection with the Frobenius kernel of Γ and thus fixes some point x. The 2-transitive automorphism group $\hat{\Gamma}$ of Corollary 3.2 may be used to pass to an isomorphic design for which $x\in B$ and $x=0$. Then the sharp transitivity of Γ_{0B} on B implies that B is a subgroup of $Q(K)$.

Theorem 6.3. *Let $\mathscr{D}$ be a design admitting a sharply flag-transitive automorphism group and such that $v=2r+1\equiv 3 \pmod 4$ and $(v,k)=1=(r,\lambda)$. Then $\mathscr{D}$ is isomorphic to $\mathscr{D}(K,G)$ for some Dickson nearfield K and some $G\leqq Q(K)$.*

Proof. Since $r=(v-1)/2$ and $\lambda=(k-1)/2$, Corollary 4.6 and Propositions 3.1 and 6.2 imply the result.

Theorem 6.4. *Let $\mathscr{D}$ be a design admitting a sharply flag-transitive automorphism group Γ, and such that $v=2r+1\equiv 3 \pmod 4$, $(r,\lambda)=1$ and k is a prime divisor of v. Then $\mathscr{D}$ is isomorphic to the design of points and lines of an affine space over $GF(3)$.*

Proof. Since $|\Gamma|=vr=v(v-1)/2$, Corollary 4.6 and Proposition 3.1 imply that we may assume that Γ is represented in terms of a Dickson nearfield K as in Corollary 3.2. v is a power of k, and $GF(k)$ is in the center of K (Zassenhaus [20]). Thus, we may identify K^{+} with the Frobenius kernel of Γ, and regard K^{+} as a vector space over $GF(k)$. If B is a block containing 0, then $\Gamma_B<K^{+}$. Thus, since B is the orbit of Γ_B containing 0 it may be regarded as a subspace of K^{+} over $GF(k)$. Then B has dimension 1, so that distinct blocks containing 0 meet in 0, and $\lambda=1$. Thus, $k=3$ and $r=(v-1)/(k-1)$, proving the Theorem.

Proposition 6.1 and Theorems 6.3 and 6.4 reduce to results of Lüneburg [13] in the case $k=3$ and $\lambda=1$.

References

1. Block, R. E.: On the orbits of collineation groups. Math. Zeitschr. **96**, 33–49 (1967).
2. Dembowski, P.: Verallgemeinerungen von Transitivitätsklassen endlicher projektiver Ebenen. Math. Zeitschr. **69**, 59–89 (1958).
3. – Finite geometries. Berlin-Heidelberg-New York: Springer 1968.
4. Feit, W., and J. Thompson: Solvability of groups of odd order. Pacific J. Math. **13**, 775–1029 (1963).
5. Higman, D. G.: Finite permutation groups of rank 3. Math. Zeitschr. **86**, 145–156 (1964).
6. –, and J. E. McLaughlin: Geometric *ABA*-groups. Ill. J. Math. **5**, 382–397 (1961).
7. Hughes, D. R.: Collineations and generalized incidence matrices. Trans. AMS **86**, 284–296 (1957).
8. – Extensions of designs and groups: projective, symplectic and certain affine groups. Math. Zeitschr. **89**, 199–205 (1965).
9. Huppert, B.: Zweifach transitive, auflösbare Permutationsgruppen. Math. Zeitschr. **68**, 126–150 (1957).
10. Johnsen, E. C.: Skew-Hadamard abelian group difference sets. J. Algebra **4**, 388–402 (1966).
11. Kantor, W. M.: 2-Transitive symmetric designs (to appear).
12. Livingstone, D., and A. Wagner: Transitivity of finite permutation groups on unordered sets of points. Math. Zeitschr. **90**, 393–403 (1965).
13. Lüneburg, H.: Steinersche Tripelsysteme mit fahnentransitiver Kollineationsgruppe. Math. Ann. **149**, 261–270 (1963).
14. – On Möbius-planes of even order. Math. Zeitschr. **92**, 187–193 (1966).
15. Paley, R. E. A. C.: On orthogonal matrices. J. Math. and Phys. **12**, 311–320 (1933).
16. Parker, E. T.: On collineations of symmetric designs. Proc. AMS **8**, 350–351 (1957).
17. Ryser, H. J.: Combinatorial mathematics. New York: Wiley 1964.
18. Todd, J. A.: A combinatorial problem. J. Math. and Phys. **12**, 321–333 (1933).
19. Wielandt, H.: Finite permutation groups. New York: Academic Press 1964.
20. Zassenhaus, H.: Über endliche Fastkörper. Abh. Math. Sem. Univ. Hamburg **11**, 187–220 (1936).

Dr. William Kantor
University of Illinois
Department of Mathematics
Chicago, Ill. 60680 (USA)

(Received December 12, 1967)