TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 146, December 1969

2-TRANSITIVE SYMMETRIC DESIGNS([1])

BY
WILLIAM M. KANTOR

1. **Introduction.** The study of a finite 2-transitive group Γ from a geometric point of view involves intransitive subgroups Δ displacing all points. For, at least two block designs may be associated with such a pair Γ, Δ. These are constructed by choosing an orbit B of Δ, and letting points be the points permuted by Γ and blocks be the distinct sets B^γ, $\gamma \in \Gamma$. In the particular case in which the degree v of Γ is $|\Gamma:\Delta|$, this construction produces two designs, both of which are symmetric designs. That is, there are v points and blocks, $k=|B|$ points on each block, k blocks on each point, and, if $\lambda=k(k-1)/(v-1)$, every two distinct points are on λ blocks and every two distinct blocks are on λ points. Moreover, Γ acts as a 2-transitive automorphism group of these symmetric designs, and Δ is the stabilizer of a block. Conversely, if a symmetric design admits an automorphism group Γ 2-transitive on points, then Γ has such a subgroup Δ of index v, namely, the stabilizer of a block. We are thus led to the problem of determining all symmetric designs admitting 2-transitive automorphism groups. The design of points and hyperplanes of a finite projective space has this property. The unique Hadamard design $\mathscr{H}_{11}$ with $v=11$, $k=5$ and $\lambda=2$ admits a 2-transitive automorphism group isomorphic to $PSL(2, 11)$ ([31]; see §2). We will place restrictions on symmetric designs and their automorphism groups in order to obtain characterizations of projective spaces and $\mathscr{H}_{11}$ among symmetric designs. However, we will not attempt to classify the groups themselves, as this is an entirely different type of problem [32].

Throughout this section, and most of this paper, we will assume that $k|(v-1)$. This condition is satisfied by both projective spaces and $\mathscr{H}_{11}$. Let Γ, Δ and B be as before, suppose that $|\Gamma:\Delta|=v$ and $k|(v-1)$, and let $\mathscr{D}$ be the corresponding symmetric design. Δ has two orbits, B and its complement $\mathscr{C}B$. Γ has a simple normal 2-transitive subgroup Γ^* such that $\Gamma^* \cap \Delta$ is still transitive on both B and $\mathscr{C}B$; this generalizes a result of Wagner [32] concerning 2-transitive collineation groups of finite projective spaces. If Δ is not faithful on B then $\mathscr{D}$ is a finite projective space and Γ contains the little projective group; this is a special case of a result of Ito [17]. If Δ is faithful and 2-transitive on B, then it has a simple normal subgroup which is 2-transitive on B and transitive on $\mathscr{C}B$. These results, proved in §5, depend heavily on the fact that Δ is primitive on $\mathscr{C}B$.

Received by the editors October 30, 1967 and, in revised form, May 15, 1969.

([1]) Research supported by the National Aeronautics and Space Administration.

In Theorem 7.2 we consider the case where Δ has a cyclic subgroup sharply transitive on B. In §8 this theorem is used to determine the full automorphism groups of Paley designs [28] and to prove the following result on permutation groups of prime degree. If v is prime, the order of the normalizer of a Sylow v-subgroup is at least vk, and $k^{1/2}+1>(v-1)/k$, then $\Gamma \approx PSL(3, 2)$ or $PSL(2, 11)$. The difficult part of the proof of these results involves showing that Δ is primitive on B.

Other characterizations use additional numerical or transitivity conditions. If p is prime and $d \geqq 2$ then $PG(d, p)$ is the only 2-transitive symmetric design with the same parameters as $PG(d, p)$ (Corollary 12.2). If Δ is 2-transitive on B, then $\mathscr{D}$ is of known type provided that either (i) $\mathscr{D}$ has the same parameters as a projective space, or (ii) $\mathscr{D}$ is a Hadamard design (Theorems 11.1 and 11.5). Set $n=k-\lambda = k(v-k)/(v-1)$ and $s=(v-1)/k$. If Δ is 2-transitive on both B and $\mathscr{C}B$, then $\mathscr{D}$ is of known type if either (i) $(n, 2s-1)=1$, or (ii) n is a prime power and $\lambda \neq 2$ (Theorems 11.2 and 11.3). These results are proved by means of Diophantine conditions obtained from the action of the stabilizer of two points. In Theorem 9.3, different methods are used to show that, if n is prime, then $\Gamma \approx PSL(3, n)$, $PGL(3, n)$ or $PSL(2, 11)$.

We also consider the larger class of symmetric designs consisting of those symmetric designs admitting an automorphism group fixing a block and transitive on the remaining blocks. Such groups have been considered in projective planes by Wagner [33]. It will be convenient to make the following standing assumption. *The only symmetric designs to be considered are those for which* $\lambda > 1$. Although many of our results can be stated so as to hold for projective planes, they are not of interest in this case in view of the results of Ostrom and Wagner [27] and [33].

2. **Definitions.** The definitions of (symmetric) designs and their parameters v, b, k, r and λ can be found in [7], [11], [20] or [30]. Incidence will generally be identified with set-theoretic inclusion. If p and q are distinct points of a design, the intersection of all the blocks on p and q is called the line joining p and q; there is a unique line containing any two given distinct points. If B is a block, $\mathscr{C}B$ denotes the set of points not on B.

In a design, $v-1>k$ and distinct blocks are not on precisely the same sets of points. It will occasionally be necessary to allow the possibility that at least one of these requirements does not hold. It will be clear from context when this is occurring. Similar considerations will also apply to incidence structures other than designs.

The parameters of a symmetric design satisfy the relation

$$\lambda(v-1) = k(k-1). \tag{2.1}$$

$n=k-\lambda$ is the order of the design. Set $s=(v-1, k-1)$. (2.1) implies the following

LEMMA 2.1. *The following statements are equivalent for a symmetric design.* (i) $k|(v-1)$; (ii) $v-1=sk$; (iii) $v-k=sn$; (iv) $(k, \lambda)=1$; (v) $v=(s^2n-1)/(s-1)$,

$k=(sn-1)/(s-1)$ *and* $\lambda=(n-1)/(s-1)$; *and* (vi) $v=s^2\lambda+s+1$ *and* $k=s\lambda+1$. *In particular, if all these conditions hold then* $(v, k)=1$ *and* $n>\lambda$.

The stabilizer in Γ of the objects $0, 0', \ldots$ is denoted by $\Gamma_{00'\ldots}$. Thus, for example, Γ_S is the global stabilizer of the set S, and Γ_{xy} is the stabilizer of the points x and y (and never denotes the stabilizer of the line joining x and y). If Σ is a subgroup of Γ then $N_\Gamma(\Sigma)$ is the normalizer of Σ in Γ.

A permutation group is said to be k-homogeneous if it is transitive on the set of k-element subsets of the set of permuted points. The rank of a transitive permutation group is the number of orbits of the stabilizer of a point.

By convention, isomorphic groups and designs will be identified. Also, a projective space will be identified with the design of its points and hyperplanes.

A Hadamard design is a symmetric design for which $v-1=2k$. There is a unique Hadamard design $\mathscr{H}_{11}$ with $v=11$, $k=5$ and $\lambda=2$, and the full automorphism group Γ of $\mathscr{H}_{11}$ is isomorphic to $PSL(2, 11)$ (Todd [31]). Γ is 2-transitive on both the points and blocks of $\mathscr{H}_{11}$. If B and B' are distinct blocks of $\mathscr{H}_{11}$ and q is a point not on B, then the following statements hold and should be regarded as models for many of our results.

(2.2i) Γ_B acts faithfully on B as $PSL(2, k-1)$ in its usual representation. In particular, Γ_B is sharply 3-transitive on B.

(2.2ii) Γ_B acts faithfully on $\mathscr{C}B$ as $PSL(2, 5)$ in its usual representation.

(2.2iii) Γ_B acts faithfully on the blocks $\neq B$ as A_5 in a primitive rank 3 representation of degree 10 (cf. [34, p. 94]).

(2.2iv) Γ_{qB} acts on B as a Frobenius group of order $k\lambda$.

(2.2v) $\Gamma_{BB'}$ acts faithfully on $B-B\cap B'$ as a Frobenius group of order $n\lambda$.

(2.2vi) $\Gamma_{BB'}$ acts unfaithfully on $B\cap B'$ as a sharply 2-transitive group.

3. **Known results.** For future reference we state some known results which will be needed several times.

PROPOSITION 3.1 (DEMBOWSKI [4]; HUGHES [14]; PARKER [29]). *An automorphism group of a symmetric design has equally many point- and block-orbits.*

The method used by Dembowski [4] in order to prove Proposition 3.1 will frequently be employed in our proofs.

LEMMA 3.2. *Every line L of a design has at most* $(b-\lambda)/(r-\lambda)$ *points.*

Proof [8]. There are $b-\lambda-|L|(r-\lambda)$ blocks not meeting L.

PROPOSITION 3.3 (DEMBOWSKI AND WAGNER [8]; CF. [7] AND [19]). *The following statements are equivalent for a symmetric design* $\mathscr{D}$.

(i) $\mathscr{D}$ *is a projective space.*

(ii) *All lines have* $(v-\lambda)/(k-\lambda)$ *points.*

(iii) $\mathscr{D}$ *admits an automorphism group such that the stabilizer of each line is transitive on the points not on the line.*

LEMMA 3.4. *If* $\mathfrak{p}$ *and* $\mathfrak{p}'$ *are orbits of a finite permutation group* Γ, *and if* $x \in \mathfrak{p}$, *then the lengths of all the orbits of* Γ_x *on* $\mathfrak{p}'$ *are divisible by* $|\mathfrak{p}'|/(|\mathfrak{p}|, |\mathfrak{p}'|)$.

LEMMA 3.5 (LIVINGSTONE AND WAGNER [22]). *Let* Γ *be a group t-transitive on a set S. If p is a prime, and* Σ *is maximal among the p-subgroups of* Γ *fixing more than t points of S, then* $N_\Gamma(\Sigma)$ *is k-transitive on the set of fixed points of* Σ.

We will generally use the well-known special case of this lemma in which Σ is a Sylow subgroup of the stabilizer of t points and Σ fixes more than t points [34, p. 20].

4. **Preliminary results.** Proposition 3.1 readily implies that an automorphism group of a symmetric design is 2-transitive on points if and only if it is 2-transitive on blocks (Dembowski [4]). Thus, we may unambiguously use the terms 2-transitive automorphism group (of a symmetric design) and 2-transitive symmetric design.

LEMMA 4.1. *From a 2-transitive group* Γ *of degree v having an intransitive subgroup* Δ *of index v displacing all points a symmetric design* $\mathscr{D}$ *may be constructed on which* Γ *acts as an automorphism group. The points of* $\mathscr{D}$ *are the points permuted by* Γ, *and the blocks are the images under* Γ *of one of the orbits of* Δ. *Conversely, every 2-transitive automorphism group of a symmetric design has such an intransitive subgroup.*

Proof. The construction yields a design with at most $|\Gamma:\Delta| = v$ blocks, and thus a symmetric design. The converse follows from the preceding remarks.

We list some simple, useful facts.

LEMMA 4.2. *Let* Δ *be an automorphism group of a symmetric design* $\mathscr{D}$ *with* $(v, k) = 1$ *such that* Δ *fixes a block B and is transitive on the remaining blocks.*

(i) Δ *is transitive on B and* $\mathscr{C}B$.

(ii) *If* $p \in B$ *and* $q \notin B$, *then* Δ_p *is transitive on* $\mathscr{C}B$ *and* Δ_q *is transitive on B.*

(iii) *If* $k|(v-1)$ *and* $q \notin B$, *then* Δ_q *is transitive on the blocks on q.*

(iv) *With the notation and hypothesis of* (iii), *all orbits of* Δ_q *in* $\mathscr{C}B-\{q\}$ *have lengths divisible by k. In particular, if* $\mathscr{D}$ *is a Hadamard design then* Δ *is 2-transitive on* $\mathscr{C}B$.

(v) Δ *is 2-transitive on B if and only if, for* $p \in B$, Δ_p *is transitive on the blocks* $\neq B$ *on p and on the blocks not on p.*

(vi) *If* $k|(v-1)$, Δ *is 2-transitive on B, and p and p' are distinct points of B, then all orbits of* $\Delta_{pp'}$ *in* $\mathscr{C}B$ *have lengths divisible by n.*

(vii) *With the hypotheses of* (vi), *if* $p \in B$ *and* $q \notin B$ *then all orbits of* Δ_{pq} *on* $B-\{p\}$ *have lengths divisible by* λ.

(viii) *With the notation and hypotheses of* (vi), $\Delta_{pp'}$ *is transitive on the blocks on p' but not on p.*

(ix) *With the hypotheses of* (vi), *if* $p \in B$, $p \in C \neq B$ *and* $p \notin C'$, *then* Δ_{pC} *is transitive on* $B-B \cap C$ *and* $\Delta_{pC'}$ *is transitive on* $B \cap C'$.

Proof. (i) and (ii) follow from Proposition 3.1 and Lemma 3.5.

(iii) By (i), Δ has orbits of lengths $v-k$ on $\mathscr{C}B$ and $v-1$ on the blocks $\neq B$. Lemmas 3.4 and 2.1 then imply that the lengths of the orbits of Δ_q of blocks $\neq B$ are divisible by $(v-1)/(v-k, v-1)=k$.

(iv) Consider the tactical configuration $\mathscr{T}$ consisting of the blocks on q and the points of $\mathscr{C}B-\{q\}$, with induced incidence. Since Δ_q is block-transitive on $\mathscr{T}$ by (iii), the desired lengths are divisible by $(v-k-1)/(v-k-1, k-\lambda-1)=k$ by [20, Proposition 4.5] and Lemma 2.1.

(v) This follows from (ii) by applying Proposition 3.1 to Δ_p.

(vi) Δ_p has orbits of lengths $v-k$ on B and $k-1$ on $B-\{p\}$. The result then follows from Lemmas 3.4 and 2.1.

(vii) By (vi), all orbits of Δ on ordered triples (p, p', q) with $p, p' \in B$, $p \neq p'$ and $q \notin B$, have lengths divisible by $k(k-1)n$. By (ii), all orbits of Δ_{pq} on $B-\{p\}$ have lengths divisible by $k(k-1)n/k(v-k)=\lambda$.

(viii) Δ_p has orbits of lengths $v-k$ on the blocks not on p and $k-1$ on $B-\{p\}$. By Lemmas 3.4 and 2.1, the lengths of the orbits of $\Delta_{pp'}$ of blocks not on p are divisible by n. (viii) then follows from the fact that there are n blocks on p' not on p.

(ix) For, by (viii), Δ is transitive on the ordered triples (p, p', C) with $p, p' \in B$, $p \in C$ and $p' \notin C$.

Lemma 4.3. *Let B be a block of a symmetric design such that every line contained in B has h points. Then $(h-1)|(k-1, \lambda-1)$.*

Proof. If p is a point of B and B' is a block $\neq B$ on p, then there are $(k-1)/(h-1)$ lines on p contained in B, $(\lambda-1)/(h-1)$ of which are also contained in B'.

Lemma 4.4. *Let $\mathscr{D}$ be a design whose lines all have the same number $h>2$ of points. If $\mathscr{D}$ admits an automorphism group Δ fixing a block B and 2-transitive on $\mathscr{C}B$, then $\mathscr{D}$ is a projective space.*

Proof. Each line $\nsubseteq B$ contains at least two points of $\mathscr{C}B$. Since some such line meets B, all such lines meet B and the result follows from [19]. (We require this result in the special case where $\mathscr{D}$ is assumed to be a 2-transitive symmetric design, in which case Proposition 3.3 could have been used.)

Lemma 4.5. *Let Γ be an automorphism group of a design $\mathscr{D}$ which is 2-transitive on points and transitive on blocks and such that, for each block B, Γ_B is 2-transitive on both B and $\mathscr{C}B$. Then, for each point p, Γ_p has rank $\rho \leqq 5$ on the points $\neq p$. Moreover, $\rho=3$ if $\mathscr{D}$ is symmetric and $\rho>3$ only if $v=2k$.*

Proof. Suppose first that $v>2k$. If $p \in B$ then Γ_{pB} is transitive on $\mathscr{C}B$ (Burnside [2, p. 204, Ex. 10]). Thus, if $p \neq q$ then Γ_{pq} has four block-orbits, namely, the blocks on p but not q, those on q but not p, those on both p and q, and those on neither p nor q. Then $\rho \leqq 3$ by [20, Theorem 4.1]. By Proposition 3.1, $\rho=3$ if $\mathscr{D}$ is symmetric. If $v<2k$ then $\mathscr{D}$ may be replaced by its complementary design.

Suppose that $v=2k$. If Γ_{pB} is transitive on $\mathscr{C}B$ we may proceed as before. If Γ_{pB} is intransitive on $\mathscr{C}B$ then, by Lemma 4.1, it has precisely two orbits on $\mathscr{C}B$. Thus, Γ has precisely two orbits of triples (p, B, q) with $p \in B$ and $q \notin B$, so that Γ_{pq} has six block-orbits in this case. As before we conclude that $\rho \leqq 5$. (That $\rho=3$ for symmetric designs has been obtained independently by H. Wielandt.)

5. **Primitivity and simplicity.** Given a 2-transitive automorphism group Γ of a symmetric design $\mathscr{D}$, it is useful to know whether or not the stabilizer Γ_B of a block B is 2-transitive on B or on $\mathscr{C}B$. Many of our results involve either proving or assuming the 2-transitivity of Γ_B on B or $\mathscr{C}B$. According to Lemma 4.2 (iv), if $\mathscr{D}$ is a Hadamard design then Γ_B is 2-transitive on $\mathscr{C}B$. The following simple result, which will not be needed later, is the corresponding result for projective spaces.

PROPOSITION 5.1. *If Γ is a 2-transitive collineation group of a finite projective space and H is a hyperplane, then Γ_H is 2-transitive on $\mathscr{C}H$.*

Proof. By [27] we may assume that the space has dimension >2. Let p and q be distinct points of a line L. If Γ_{pq} has t orbits of points not on L, by Wagner [32, Lemma 3] Γ_{pq} has $t+3$ point-orbits and t orbits of planes $\supset L$. By Proposition 3.1, Γ_{pq} has t orbits of hyperplanes $\supset L$, and thus 3 orbits of hyperplanes $\not\supset L$. These must be the hyperplanes on p but not q, those on q but not p, and those on neither p nor q. This implies the result.

THEOREM 5.2. *If Δ is an automorphism group of a symmetric design $\mathscr{D}$ with $k|(v-1)$ fixing a block B and transitive on the remaining blocks, then Δ is primitive on $\mathscr{C}B$.*

Proof. By Lemma 4.2iii, Δ is transitive on the incident point-block pairs of the design $\mathscr{D}_B$ of points not on B and blocks $\neq B$. Here $r_B=k$ and $\lambda_B=\lambda$ are relatively prime by Lemma 2.1. The result then follows from [20, Theorem 4.8].

We note that [20, Theorem 4.7] may be used to replace the condition $k|(v-1)$ by weaker conditions.

COROLLARY 5.3. *If Γ is a 2-transitive automorphism group of a symmetric design $\mathscr{D}$ with $k|(v-1)$, and if some nontrivial element of Γ fixes a block pointwise, then $\mathscr{D}$ is a projective space and Γ contains the little projective group.*

Proof. By Theorem 5.2, the pointwise stabilizer of a block B is transitive on $\mathscr{C}B$. The result then follows from [19, Theorem 3], which in the present case is merely a simple application of Proposition 3.3.

It is also clear that an automorphism group of a symmetric design is faithful on the complements of blocks provided that $n>\lambda$. Ito [17] has proven Corollary 5.3 independently and without any restrictions on parameters. The preceding proof is somewhat simpler than his, and we are only concerned with the case $k|(v-1)$. Ito's result implies that, if Γ is a 2-transitive automorphism group of a symmetric design with $(v, k)=1$ (and $\lambda>1$), and if B is a block, then Γ_B is nonsolvable. For otherwise, Γ_B has an elementary abelian normal subgroup Σ. Since either $(|\Sigma|, k)=1$ or $(|\Sigma|, v-k)=1$, Σ fixes a point of B or $\mathscr{C}B$, and thus fixes B or $\mathscr{C}B$ pointwise by Lemma 4.2i. By Ito's theorem, Γ_B is nonsolvable, a contradiction. Thus, Γ_B is nonsolvable.

If Δ is the stabilizer of a block in a 2-transitive automorphism group of a symmetric design, then Δ is transitive on the pairs (p, C) with $p \in B-B \cap C$ (Lemma 4.2ii). Although [20, Theorem 4.8] can then be applied to the design of points of B and intersections of B with the complements of the blocks $\neq B$, the results are not satisfactory: Δ is primitive on B if $k|(v-1)$ and n is square-free. Somewhat more can be proved concerning the transitivity of normal subgroups of Δ on B; see the proof of Lemma 7.3.

THEOREM 5.4. *Let Δ be an automorphism group of a symmetric design $\mathscr{D}$ with $k|(v-1)$ which fixes a block B and is faithful on B. If Δ is 2-transitive on B and transitive on $\mathscr{C}B$, then Δ has a simple normal subgroup which is 2-transitive on B and transitive on $\mathscr{C}B$.*

Proof. Let Π be a minimal normal subgroup of Δ. Since Δ is primitive on both B and $\mathscr{C}B$ by Theorem 5.2, and Δ is faithful on these sets, Π is transitive on B and $\mathscr{C}B$ and Lemma 4.2 applies to Π. Π is nonabelian since $k\neq v-k$. It then follows from a result of Burnside [2, p. 202] that Π is simple.

We will assume that Π is not 2-transitive on B and obtain a contradiction from a detailed examination of the orbits of Π_p for $p \in B$.

Π_p has the following orbits: (i) $\{p\}$; (ii) $\mathscr{C}B$; (iii) $(k-1)/t$ point-orbits on $B-\{p\}$, each of length t; (iv) $\{B\}$; (v) $(k-1)/u$ orbits of blocks $\neq B$ on p, each of length u; and (vi) $(v-k)/w$ orbits of blocks not on p, each of length w. Here the constancy of the lengths of the orbits of types (v) and (vi) follows from $\Pi_p \trianglelefteq \Delta_p$ and Lemma 4.2v. $\mathfrak{p}$, $\mathfrak{B}^*$ and $\mathfrak{B}$ will denote orbits of types (iii), (v) and (vi), respectively. Proposition 3.1 implies that

(5.1) $$snw^{-1}-1 = (v-k)w^{-1}-1 = (k-1)(t^{-1}-u^{-1}).$$

(5.2) If $B' \neq B$ then all orbits of $\Pi_{B'}$ on $B \cap B'$ and $B-B \cap B'$ have lengths u/s and w/s, respectively.

For, consider an orbit of Π of incident (nonincident) pairs (p, B') with $p \in B$. Π is transitive on B, and each orbit of Π_p of blocks B' has length u (resp. w). Π is transitive on the blocks B', and, since $\Delta_{B'}$ is transitive on both $B \cap B'$ and $B-B \cap B'$ by Lemma 4.2v, all orbits of $\Pi_{B'}$ on $B \cap B'$ (resp. $B-B \cap B'$) have the same length u_0 (resp. w_0). The length of an orbit of Π of pairs (p', B) is thus $ku=(v-1)u_0$ (resp. $kw=(v-1)w_0$), and (5.2) follows from the fact that $v-1=sk$.

We note that

(5.3) $$u > t.$$

For, (5.1) implies that $u \geqq t$ and $u=t$ only if $w=sn$. Since $(u/s, w/s)|(\lambda, n)=1$, (5.2) and Lemma 3.4 then imply that $\Pi_{p'B'}$ is transitive on $B-B \cap B'$ whenever

$p' \in B \cap B'$. If p', x and y are distinct points of B they are noncollinear in the complementary design of $\mathscr{D}$ by Lemma 3.2. There is then a block B' on p' but on neither x nor y. Since we have shown that $\Pi_{p'B'}$ has an element moving x to y, Π is 2-transitive on B. This contradiction proves (5.3).

If $\mathfrak{B}$ is an orbit of Π_p of blocks not on p, let $\langle \mathscr{C}\mathfrak{B} \rangle$ be the set of points $\neq p$ of B lying in the complement of each block in $\mathfrak{B}$; although different $\mathfrak{B}$'s may yield the same set $\langle \mathscr{C}\mathfrak{B} \rangle$, we will regard $\langle \mathscr{C}\mathfrak{B} \rangle$ as depending upon $\mathfrak{B}$. This definition implies that

(5.4) $$\text{If } B_1 \in \mathfrak{B} \text{ then } |B_1 \cap [(B - \langle \mathscr{C}\mathfrak{B} \rangle) - \{p\}]| = \lambda.$$

As Δ_p is transitive on the $\mathfrak{B}$'s, $w' = |\langle \mathscr{C}\mathfrak{B} \rangle|$ is independent of the choice of $\mathfrak{B}$. Note that w' may be 0. Since $p' \in \langle \mathscr{C}\mathfrak{B} \rangle$ and $p' \in \mathfrak{p}$ imply that $\mathfrak{p} \subseteq \langle \mathscr{C}\mathfrak{B} \rangle$, $\langle \mathscr{C}\mathfrak{B} \rangle$ contains w'/t orbits $\mathfrak{p}$. Since Δ_p is transitive on the $(k-1)/t$ $\mathfrak{p}$'s and the $(v-k)/w$ $\mathfrak{B}$'s, it follows that

(5.5) Each $\mathfrak{p}$ is contained in $(w't^{-1}) \cdot (v-k)w^{-1}/(k-1)t^{-1} = w'n/w\lambda$ sets $\langle \mathscr{C}\mathfrak{B} \rangle$.

Fix $p' \in B - \{p\}$. $\Delta_{pp'}$ is transitive on the blocks on p' but not on p (Lemma 4.2viii), and hence also on those orbits $\mathfrak{B}$ having a block on p'. (5.5) and the definition of $\langle \mathscr{C}\mathfrak{B} \rangle$ imply that there are $(v-k)w^{-1} - w'n(w\lambda)^{-1}$ such orbits $\mathfrak{B}$. The number of blocks of such a $\mathfrak{B}$ which are on p' is independent of $\mathfrak{B}$, by the transitivity of $\Delta_{pp'}$. Since each of the n blocks on p' but not on p belongs to exactly one such $\mathfrak{B}$, it follows that

(5.6) Every point $\neq p$ of $B - \langle \mathscr{C}\mathfrak{B} \rangle$ is on $n/\{snw^{-1} - w'n(w\lambda)^{-1}\} = \lambda w/(s\lambda - w')$ blocks of $\mathfrak{B}$.

Let $p' \in \mathfrak{p}$. Lemma 4.2viii implies that $\Delta_{p\mathfrak{p}}$ is transitive on those orbits $\mathfrak{B}$ such that $\mathfrak{p} \nsubseteq \langle \mathscr{C}\mathfrak{B} \rangle$. (5.6), $|\mathfrak{p}| = t$ and $|\mathfrak{B}| = w$ then imply that

(5.7) If $\mathfrak{p} \nsubseteq \langle \mathscr{C}\mathfrak{B} \rangle$, then the number of points of $\mathfrak{p}$ on each block of $\mathfrak{B}$ is $t \cdot \{\lambda w(s\lambda - w')^{-1}\}/w = \lambda t/(s\lambda - w')$.

Each block $\neq B$ contains n points of $\mathscr{C}B$, so that there are $wn/(v-k) = w/s$ blocks of $\mathfrak{B}$ on each point of $\mathscr{C}B$. Fix $\mathfrak{B}$ and $B_1 \in \mathfrak{B}$ and count in two ways the number of pairs (x, B_2) with $B_1 \neq B_2 \in \mathfrak{B}$ and $x \in B_1 \cap B_2$. By (5.4) and (5.6)

$$0 + 0 + \lambda\{\lambda w(s\lambda - w')^{-1} - 1\} + n(ws^{-1} - 1) = (w-1)\lambda$$

(the four terms on the left correspond to $\{p\}$, $\langle \mathscr{C}\mathfrak{B} \rangle$, $B_1 \cap [(B - \langle \mathscr{C}\mathfrak{B} \rangle) - \{p\}]$ and $\mathscr{C}B$, respectively), which reduces to

(5.8) $$\lambda/(s\lambda - w') = (\lambda - 1 + nsw^{-1})/(k-1).$$

(5.1), (5.7), and (5.8) imply that

(5.9) $$t(\lambda - 1 + nsw^{-1})/(k-1) = ts^{-1} + t(t^{-1} - u^{-1}) \text{ is an integer.}$$

Since $k-1=s\lambda$, (5.6) and (5.8) imply that

$$w(\lambda-1+nsw^{-1})/(k-1) = \{(\lambda-1)ws^{-1}+n\}/\lambda$$

is an integer. By (5.2), ws^{-1} is an integer, so that $n=1+\lambda(s-1)$ implies that

$$-ws^{-1}+1 \equiv 0 \pmod{\lambda}. \tag{5.10}$$

By (5.10) and (5.1),

$$\begin{aligned} 0 &\equiv nsw^{-1}(1-ws^{-1}) = nsw^{-1}-n \\ &\equiv nsw^{-1}-1 = (k-1)(t^{-1}-u^{-1}) \qquad \pmod{\lambda}, \end{aligned}$$

so that

$$s(t^{-1}-u^{-1}) \quad \text{is an integer.} \tag{5.11}$$

By (5.2) and (5.3), su^{-1} and tu^{-1} are $\leqq 1$. Also, either st^{-1} or ts^{-1} is $\leqq 1$. Since both $ts^{-1}-tu^{-1}$ and $st^{-1}-su^{-1}$ are integers by (5.9) and (5.11), it follows that one of them must be 0. $st^{-1}-su^{-1}\neq 0$ by (5.3). Thus,

$$u = s. \tag{5.12}$$

(5.11) then implies that $t\,|\,s=u$, and by (5.3) we have

$$t \leqq s/2. \tag{5.13}$$

If $ws^{-1}=1$, then (5.12) and (5.2) imply that $\Pi_{B'}$ fixes B pointwise; however, Δ is faithful on B and $\Pi_{B'}\neq 1$ by Lemma 4.2i applied to Π. From (5.10) it follows that $ws^{-1}\geqq \lambda+1$, or

$$nsw^{-1} \leqq n/(\lambda+1) = \{1+\lambda(s-1)\}/(\lambda+1) \leqq s-1.$$

Then (5.9) and (5.13) imply that

$$s\lambda = (k-1) \leqq t(\lambda-1+nsw^{-1}) \leqq (s/2)(\lambda-1+s-1),$$

or $2\lambda \leqq \lambda-1+s-1$. In particular,

$$(\lambda-1)/s \quad \text{is not an integer.} \tag{5.14}$$

We now show that (5.12) and (5.14) are incompatible. Fix an orbit $\mathfrak{B}^*$ of Π_p of blocks $\neq B$ on p. Since each block of $\mathfrak{B}^*$ contains n points of $\mathscr{C}B$, each point of $\mathscr{C}B$ is on $un/(v-k)=u/s=1$ block of $\mathfrak{B}^*$. Then distinct blocks of $\mathfrak{B}^*$ have no common point in $\mathscr{C}B$, and thus meet $B-\{p\}$ in the same set $\langle\mathfrak{B}^*\rangle$ of $\lambda-1$ points. Π_p fixes $\langle\mathfrak{B}^*\rangle$, so that $\langle\mathfrak{B}^*\rangle$ is a union of $(\lambda-1)/t$ $\mathfrak{p}$'s. Since Δ_p is transitive on the $(k-1)/t$ orbits $\mathfrak{p}$ and the $(k-1)/u$ orbits $\mathfrak{B}^*$, it follows that each $\mathfrak{p}$ is contained in

$$(k-1)u^{-1}\cdot(\lambda-1)t^{-1}/(k-1)t^{-1} = (\lambda-1)/u = (\lambda-1)/s$$

sets $\langle\mathfrak{B}^*\rangle$. This contradicts (5.14) and proves Theorem 5.4.

LEMMA 5.5. *Let Γ be a 2-transitive automorphism group of a symmetric design $\mathscr{D}$ having a nontrivial regular normal subgroup Σ. Then n is a power of 2 and $v=4n$.*

Proof. Σ is an elementary abelian p-group of order p^d where $d \geqq 2$ (Burnside [2, p. 202]). The points of $\mathscr{D}$ may be regarded as the points of an affine space $\mathscr{A}=AG(d,p)$. Γ is a 2-transitive collineation group of $\mathscr{A}$ and Σ is the translation group of $\mathscr{A}$. Dually, the blocks of $\mathscr{D}$ are the points of an affine space $\mathscr{A}^{\#}$. $\mathscr{A}$ and $\mathscr{A}^{\#}$ are isomorphic but are clearly not identical.

Temporarily regarded $\mathscr{A}$ as embedded in $\mathscr{P}=PG(d,p)$. Γ induces a collineation group of $\mathscr{P}$ which is transitive on the hyperplanes at infinity. According to Lemma 4.2v, applied to the complementary design of $\mathscr{P}$, if x is a point of $\mathscr{A}$ then Γ_x has precisely two orbits of hyperplanes of $\mathscr{A}$. Equivalently, if H is a hyperplane of $\mathscr{A}$ then Γ_H has precisely two point-orbits in $\mathscr{A}$, namely, H and $\mathscr{C}H$ (the complement is taken within $\mathscr{A}$).

Σ_H is a subgroup of Σ of order p^{d-1}. Since Σ_H is a group of translations of $\mathscr{A}^{\#}$, it follows that $\Sigma_H=\Sigma_{H^{\#}}$, where $H^{\#}$ is any one of a unique class of parallel hyperplanes of $\mathscr{A}^{\#}$. We now prove that

$$\Gamma_H \text{ and } \Gamma_{H^{\#}} \text{ are conjugate in } \Gamma. \tag{5.15}$$

Certainly $N_\Gamma(\Sigma_H)=N_\Gamma(\Sigma_{H^{\#}})$, where $\Lambda=N_\Gamma(\Sigma_H)$ is the subgroup of Γ consisting of those collineations fixing the parallel class of H as a whole. Then $\Lambda_H=\Gamma_H$. Λ contains the centralizer of Σ_H in Γ and so contains Σ. Then Λ is transitive on the parallel class of H, so that

$$|\Lambda:\Lambda_H| = |\Lambda:\Lambda_{H^{\#}}| = p. \tag{5.16}$$

Let $\Lambda(H)$ be the set of all elements of Λ fixing all hyperplanes $\|H$. Then $\Lambda/\Lambda(H)$ is a transitive, faithful permutation group on the hyperplanes $\|H$. If $\mathscr{A}$ is once again embedded in the projective space $\mathscr{P}$ and we pass to the dual of $\mathscr{P}$, we see that $\Lambda/\Lambda(H)$ is similar to a group of projectivities on a line of $\mathscr{P}$. More precisely, since Λ fixes the hyperplane at infinity $\Lambda/\Lambda(H)$ may be regarded as a group of linear mappings $x \to ax+b$, $a \neq 0$, on $GF(p)$.

$\Lambda(H)$ may be described as the set of elements of Λ fixing all cosets of $\Sigma_H=\Sigma_{H^{\#}}$ in Σ. Thus, $\Lambda(H)=\Lambda(H^{\#})$. By (5.16), $\Lambda_H/\Lambda(H)$ and $\Lambda_{H^{\#}}/\Lambda(H)$ are conjugate in $\Lambda/\Lambda(H)$. Since $\Gamma_H=\Lambda_H$ and $\Gamma_{H^{\#}}=\Lambda_{H^{\#}}$, this proves (5.15).

By (5.15) we may assume that $\Gamma_H=\Gamma_{H^{\#}}$. Then Γ_H has two point orbits H and $\mathscr{C}H$ in $\mathscr{D}$, and, dually, two block orbits $H^{\#}$ and $\mathscr{C}^{\#}H^{\#}$ (where $\mathscr{C}^{\#}H^{\#}$ is the complement of $H^{\#}$ within $\mathscr{A}^{\#}$, that is, within the set of blocks of $\mathscr{D}$). Let i be the number of points of H on each block $\in H^{\#}$, and i_c be the number of points of H on each block $\in \mathscr{C}^{\#}H^{\#}$. Then there are $|H^{\#}|i/|H|=i$ blocks of $H^{\#}$ on each point of H and $|\mathscr{C}^{\#}H^{\#}|i_c/|H|=(p-1)i_c$ blocks of $\mathscr{C}^{\#}H^{\#}$ on each point of H. Thus,

$$i+(p-1)i_c = k. \tag{5.17}$$

Fix $x \in H$ and count in two ways the pairs (y, B) with x and y distinct points of $B \cap H$ and B a block of $\mathscr{D}$:

$$(|H|-1)\cdot\lambda = i\cdot(i-1)+(p-1)i_c\cdot(i_c-1),$$

which together with (5.17) implies that

$$(i-i_c)^2 = n. \tag{5.18}$$

We now show that

$$n \mid kp(i-i_c). \tag{5.19}$$

Consider the action of Γ on the ordered pairs (B, H), where B is a block of $\mathscr{D}$ and H is a hyperplane of $\mathscr{A}$. We know that Γ_H has two block-orbits $H^{\#}$ and $\mathscr{C}^{\#}H^{\#}$. Thus, Γ_B has two hyperplane-orbits in $\mathscr{A}$. Moreover, one of these orbits, say $B^{\flat}$, has the following property:

$$B \in H^{\#} \Leftrightarrow H \in B^{\flat}. \tag{5.20}$$

It follows that $p(p^d-1)(p-1)^{-1}|H^{\#}| = v|B^{\flat}|$, so that $|B^{\flat}| = (v-1)/(p-1)$. The number of points of B on a hyperplane $H \in B^{\flat}$ is $|B \cap H|$, which is also $|B \cap H|$ where $B \in H^{\#}$, by (5.20). By the definition of i, each hyperplane in $B^{\flat}$ is on i points of B and hence is on $p^{d-1}-i$ points of $\mathscr{C}B$. It follows that each point of $\mathscr{C}B$ is on

$$\frac{|B^{\flat}|\cdot(p^{d-1}-i)}{|\mathscr{C}B|} = \frac{(v-1)(p^{d-1}-i)}{(p-1)(v-k)} = \frac{k(p^{d-1}-i)}{(p-1)n}$$

hyperplanes of $B^{\flat}$. Thus, mod $n(p-1)$,

$$0 \equiv k(v-pi) = k(v-k)+k^2-kpi = n(v-1)+k^2-kpi$$

(by (2.1)), so that, by (5.17),

$$k^2 \equiv kpi = kp\{k-(p-1)i_c\}$$

or

$$k^2(p-1) \equiv kp(p-1)i_c \pmod{n(p-1)}.$$

It follows that $kpi \equiv k^2 \equiv kpi_c \pmod n$. This proves (5.19).

By (5.18) and (5.19), $n^{1/2} \mid kp$. Everything that has just been proved must hold if $\mathscr{D}$ is replaced by its complementary design. Then also $n^{1/2} \mid (v-k)p$. It follows that $n^{1/2} \mid vp$. Then n is a power of p, and the lemma follows from Mann [24, Theorem 1 and Proposition 1].

The hypotheses of the preceding lemma are satisfied, for example, by the design in (6.4).

THEOREM 5.6. *A 2-transitive automorphism group Γ of a symmetric design with $k \mid (v-1)$ has a simple normal 2-transitive subgroup Π. If, in addition, Γ_B is 2-transitive on the block B, then the same is true of Π_B.*

Proof. Let Π be a minimal normal subgroup of Γ. By Lemma 5.5, $\Pi_B \neq 1$. Then Π_B is transitive on $\mathscr{C}B$. All orbits of Π_B on B have lengths dividing k and hence relatively prime to $v-k$. By Lemma 3.4, Π_{pB} is transitive on $\mathscr{C}B$ for each point p on B. Then Π_p is transitive on $\bigcup \{\mathscr{C}B \mid B \text{ is on } p\}$, so that Π is 2-transitive. Π is simple by [2, p. 202]. Although the last assertion follows from Theorem 5.4, we note that, in the present situation, only the proof of (5.3) is needed because of the dual of Lemma 4.2ii, applied to Π.

The preceding proof depends upon the fact that Π is not regular. For the purpose of Theorem 5.6, instead of Lemma 5.5 we could have used the fact that some block of an abelian difference set design with $(v, k)=1$ is fixed by all (not necessarily numerical) multipliers [11, p. 140].

6. $\lambda=2$. In §§7 and 9 we will reduce the proof of two theorems to the case $\lambda=2$. Special techniques are needed to handle such symmetric designs. The following simple result will be used in §7.

LEMMA 6.1. *$\mathscr{H}_{11}$ is the only symmetric design with $\lambda=2$, $k-1=2^e$, $e\geqq 2$, admitting a 2-transitive automorphism group Γ such that, for each block B, Γ_B acts on B as a subgroup of $P\Gamma L(2, 2^e)$ containing $PSL(2, 2^e)$ as a subgroup of odd index.*

Proof (Wielandt). If $B\neq C$ then a Sylow 2-subgroup Σ of Γ_{BC} has order 2 and fixed 2^{e-1} pairs of points of B. Then Σ fixes $2^{e-1}+1$ blocks, so that by Lemma 3.6,

$$(2^{e-1}+1) \mid |\Gamma| = \{1+k(k-1)/2\}k(k-1)(k-2)t,$$

where $t\mid e$. This implies that $e=2$, as claimed.

The preceding argument can also be used to show that $PSL(2, q)$, represented as a permutation group on the unordered pairs of points in its usual representation, admits no transitive extension if $q>4$ is a power of 2 or a prime power $\equiv 3 \pmod 4$.

A result of Hall [12] suggests that, with a single exception for which $k=9$, it may be possible to weaken the assumption of 2-transitivity in Lemma 6.1.

LEMMA 6.2. *Let $\mathscr{D}$ be a symmetric design with $\lambda=2\nmid k$ admitting an automorphism group Δ fixing a block B and transitive on the remaining blocks. Then Δ is 3-transitive on B.*

Proof. Since $\lambda=2$, Δ is 2-homogeneous on B. Δ is nonsolvable, as otherwise Δ would have a normal abelian subgroup transitive on both B and $\mathscr{C}B$ (Theorem 5.2), which is impossible. Δ is thus 2-transitive on B [20, Proposition 3.1]. By Lemma 4.2v, if p is on B then Δ_p is 2-homogeneous on $B-\{p\}$. Since $k-1$ is even, Δ_p has even order and thus is 2-transitive on $B-\{p\}$, as claimed.

THEOREM 6.3. *Let $\mathscr{D}$ be a symmetric design with $\lambda=2\nmid k$ admitting an automorphism group Δ fixing a block B and 2-homogeneous on $\mathscr{C}B$. Then one of the following holds:*

(i) *$\mathscr{D}$ is $\mathscr{H}_{11}$;*

(ii) *$k=9$ and Δ acts on B as $PSL(2, 2^3)$ or $P\Gamma L(2, 2^3)$; or*

(iii) *$3\mid k$, v is even and n is a square.*

The proof of Theorem 6.3 will be preceded by several lemmas.

LEMMA 6.4. *Conclusion* (i) *or* (ii) *of Theorem* 6.3 *holds if, in addition,* Δ *is not* 4-*transitive on* B.

Proof. Two points of $\mathscr{C}B$ are on precisely two blocks, each of which meets B in two points. Conversely, two disjoint pairs of distinct points of B determine two blocks $\neq B$ which meet in two points of $\mathscr{C}B$. Since Δ is 2-homogeneous on $\mathscr{C}B$ it follows that Δ is 4-homogeneous on B. Moreover, Δ is transitive on disjoint unordered pairs of distinct points of B, and thus induces A_4 or S_4 on each set of 4 points of B. If Δ is not 4-transitive on B and $k>5$, then by [21] $k=9$ and Δ acts on B as $PSL(2, 2^3)$ or $P\Gamma L(2, 2^3)$.

From now on we will consider the case where Δ is 4-transitive on B. It will frequently be necessary to consider several points at the same time. For this purpose it is convenient to temporarily adopt some new notation. Points will be denoted by positive integers, distinct numbers representing distinct points. 1, 2, 3 and 4 will always denote points of B. The block $\neq B$ on 1 and 2 is B_{12}. The expression $B_{12} \cap B_{34}$ will have its usual meaning; however, $B_{12} \cap B_{13}$ will denote the point $\neq 1$ common to B_{12} and B_{13}.

The complementary design of $PG(2, 2)$ is the only symmetric design with $\lambda=2$ and $k=4$. We will exclude this case.

LEMMA 6.5. *Let* $\mathscr{D}$ *be a symmetric design with* $\lambda=2$ *and* $k>4$ *admitting an automorphism group* Δ *fixing a block* B *and* 4-*transitive on* B.

(i) *If* X *is a block* $\neq B$ *then* Δ_X *is* 2-*transitive on* $X-B\cap X$.

(ii) Δ *is* 2-*transitive on* $\mathscr{C}B$.

(iii) Δ *does not act on* B *as* S_5, A_7 *or* M_{11}.

(iv) *If* Δ_{1234} *fixes more than four points of* B, *then* $k=6$ *and* Δ *is* A_6.

(v) *A Sylow* 2-*subgroup of* Δ_{1234} *fixes* 4, 5, 6, 7 *or* 11 *points of* B.

(vi) *Let* p *be an odd prime and let* Σ *be a Sylow* p-*subgroup of* Δ_{1234}. *Then the set* $\mathscr{D}^*$ *of fixed points and blocks of* Σ *is a symmetric subdesign of* $\mathscr{D}$ *with* $\lambda^*=2$, *and* $N_\Delta(\Sigma)$ *is* 4-*transitive on the set of points of* B *in* $\mathscr{D}^*$.

(vii) B_{12}, B_{13} *and* B_{23} *concur.*

(viii) B_{12}, B_{13} *and* B_{34} *do not concur.*

(ix) *If* $k>6$ *then* $5=B_{12}\cap B_{13}\cap B_{23}$, $6=B_{12}\cap B_{14}\cap B_{24}$, $7=B_{13}\cap B_{14}\cap B_{34}$ *and* $8=B_{23}\cap B_{24}\cap B_{34}$ *are distinct points lying on a block* $B_{9\,10}$, *where* 9 *and* 10 *are in* $B-$ $\{1, 2, 3, 4\}$ (*see Figure* 1).

Proof. (i) Δ_X is transitive on the unordered pairs of points of $B-B\cap X$. Each pair determines a unique block $\neq B$ which meets $X-B\cap X$ in a pair of points. It follows that Δ_X is 2-homogeneous on $X-B\cap X$. Since Δ_X has even order, it is 2-transitive on $X-B\cap X$.

(ii) follows from (i) and the fact that Δ is transitive on the blocks $\neq B$.

(iii) Since $\mathscr{H}_{11}$ does not admit S_5 as an automorphism group fixing a block, Δ is

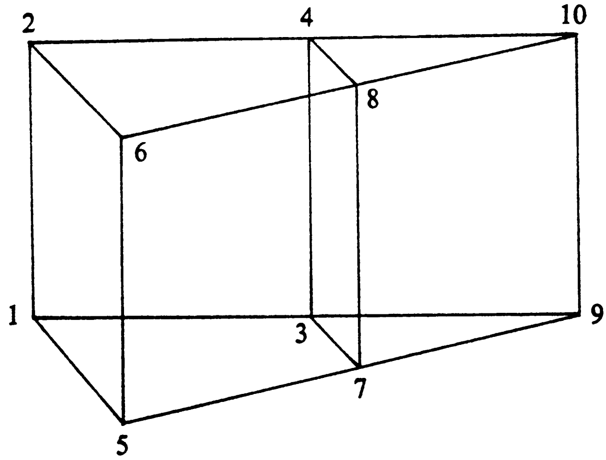

FIGURE 1

not S_5. There is no symmetric design with $\lambda=2$ and $k=7$ (Hussain [15]; this also follows from a result of Chowla and Ryser [7, p. 61], since $1+7(7-1)/2$ is even). If Δ were M_{11} then, by (ii), M_{11} would have a 2-transitive representation of degree $v-k=45$, which is not the case [1].

(iv) According to Nagao [26], Δ is A_6 or one of the groups in (iii).

(v) follows from Lemma 3.5 and a theorem of Hall [10, p. 73].

(vi) Both points of intersection of two blocks of $\mathscr{D}^*$ are in $\mathscr{D}^*$, and dually. $\mathscr{D}^*$ is thus a symmetric design with $\lambda^*=2$ (Majumdar [23]; Dembowski [5, p. 269]). The last assertion follows from Lemma 3.5.

(vii) Otherwise, $5=B_{12}\cap B_{13}$ and $6=B_{12}\cap B_{23}$ are distinct fixed points of Δ_{123} on B_{12}. There is a unique block $X\neq B_{12}$ on 5 and 6. Then Δ_{123} fixes X and neither 1 nor 2 is in X. $B\cap X$ is fixed by Δ_{123} and contains at least one point $\neq 3$. Since Δ is 4-transitive and $k>5$, this is impossible.

(viii) By (vii), B_{13} and B_{23} are the only blocks on both 3 and $5=B_{12}\cap B_{13}\cap B_{23}$.

(ix) The four points are distinct by (viii). Let X be the block $\neq B_{12}$ on 5 and 6. Since Δ_{1234} fixes B_{12}, 5 and 6, it fixes X. Then Δ_{1234} fixes the point $y\neq 5$ of $B_{13}\cap X$. If $\delta=(1,2)(3,4)\cdots\in\Delta$ then also $\delta=\cdots(5,6)(7,8)\cdots$. Since δ fixes X it follows that $y^\delta\in X$. If $y=7$, then X is on 7 and 8 and the remaining assertions are trivial. If $y=3$ then $y^\delta=4$, so that $X=B_{34}$ and $5=B_{12}\cap B_{23}\cap B_{34}$, contradicting (viii). The only other possibility is that y is a new point. Δ_{1234} then fixes the block $Y\neq B_{13}$ on 3 and y, and hence also the point $z\neq 3$ on $B\cap B_{13}$. z is a new point and is fixed by Δ_{1234}, contradicting (iv).

(vii), (viii) and (ix) are essentially configuration theorems. (vii) is a "tetrahedral" condition, while the remaining two are "cubic" conditions (cf. Figure 1). In order to identify the subdesign generated by four points of B a further property, (6.1), is needed. The proof is, however, slightly more difficult than those of the preceding lemma.

LEMMA 6.6. *There is a unique design $\mathscr{D}_{16}$ satisfying the hypotheses of Lemma 6.5 and which is generated by any four points of B. In this design, $v=16$ and $k=6$.*

Proof. Let $\mathscr{D}$ be a design with $k>6$, satisfying the conditions of Lemma 6.5, and such that any four points of B generate $\mathscr{D}$; that is, $\mathscr{D}$ has no proper subdesign $\mathscr{D}^*$ with $\lambda^*=2$ which contains four points of B. We will use the notation of Lemma 6.5ix.

By Lemma 6.5vi and iv, $\Sigma=\Delta_{1234}$ is a 2-group fixing only four points of B. By Lemma 3.5, $\Delta^*=N_\Delta(\Sigma_9)|_F$ is 4-transitive on the set F of fixed points of Σ_9 on B. Clearly $|F|\geqq 6$. If $f\in F-\{1, 2, 3, 4\}$ then $\Sigma_9\leqq\Sigma_f$ implies, by the maximality of Σ_9 in Σ, that $\Sigma_9=\Sigma_f$. Then $\Delta^*_{1234f}=1$. Δ^* is thus A_6, A_7, M_{11} or M_{12} (cf. [9] and [10, p. 73]). $|f^\Sigma|=|\Sigma:\Sigma_9|=2$ implies that $|F|$ is even, while Σ fixes $\{9, 10\}$. It follows that Δ^* is A_6. We use this to prove that

$$(6.1)\qquad \begin{array}{ll} 5 = B_{49}\cap B_{4\,10}\cap B_{9\,10}, & 6 = B_{39}\cap B_{3\,10}\cap B_{9\,10}, \\ 7 = B_{29}\cap B_{2\,10}\cap B_{9\,10}, & 8 = B_{19}\cap B_{1\,10}\cap B_{9\,10}. \end{array}$$

For, let $\alpha=(1)(2)(3, 9)(4, 10)\cdots\in\Delta$. α interchanges B_{34} and $B_{9\,10}$. Then α fixes $B_{34}\cap B_{9\,10}=\{7, 8\}$ (see Figure 1), that is,

$$7 \text{ or } 8 = 7^\alpha = (B_{13}\cap B_{14}\cap B_{34})^\alpha = B_{19}\cap B_{1\,10}\cap B_{9\,10}.$$

$7^\alpha=7\in B_{13}$ would imply that 1 and 7 are on the three blocks B_{13}, B_{19} and $B_{1\,10}$. Thus, $7^\alpha=8$, proving the final relation in (6.1). In terms of Figure 1 this means that the two blocks containing the opposite vertices of the "cube" 12345678 pass through 9 and 10, respectively. This implies the remaining assertions of (6.1).

Replace the initial points 1, 2, 3, 4 by 9, 10, 3, 4. By Lemma 6.5viii, $11=B_{34}\cap B_{39}\cap B_{49}$ and $12=B_{34}\cap B_{3\,10}\cap B_{4\,10}$ are distinct points. They are new points since $\lambda=2$ implies that 5, 6, 7 and 8 are on no blocks $\neq B_{ij}$, $1\leqq i<j\leqq 4$ or $i=9$, $j=10$. By (6.1) and Lemma 6.5ix, 5, 6, 11 and 12 lie on a block $Y\neq B_{9\,10}$. Since B_{12} and $B_{9\,10}$ are the only blocks containing 5 and 6, it follows that $Y=B_{12}$. At this point we have the following sets of points lying on blocks, where the first two points of each set are on B.

$$(6.2)\qquad \begin{array}{llllll} 1 & 2 & 3 & 4 & 9 & 10 \\ 1 & 2 & 5 & 6 & 11 & 12 \\ 1 & 3 & 5 & 7 & & \\ 1 & 4 & 6 & 7 & & \\ 2 & 3 & 5 & 8 & & \\ 2 & 4 & 6 & 8 & & \\ 3 & 4 & 7 & 8 & 11 & 12 \\ 9 & 10 & 5 & 6 & 7 & 8 \end{array} \qquad \begin{array}{llll} 1 & 9 & 8 & \\ 2 & 9 & 7 & \\ 3 & 9 & 6 & 11 \\ 4 & 9 & 5 & 11 \\ 1 & 10 & 8 & \\ 2 & 10 & 7 & \\ 3 & 10 & 6 & 12 \\ 4 & 10 & 5 & 12 \end{array}$$

We now show that the 16 blocks involved in (6.2) are the blocks of a symmetric subdesign $\mathscr{D}^*$ of $\mathscr{D}$ with $\lambda^*=2$ and $k^*=6$. Set $x=B_{12}\cap B_{19}\cap B_{29}$ and $y=B_{12}$

$\cap B_{1\,10} \cap B_{2\,10}$. If we replace 9, 10, 3, 4 by 9, 10, 1, 2 in the preceding argument, or use the symmetry provided by Δ^*, we find that

$$\{11, 12\} = B_{12} \cap B_{34} = \{x, y\}.$$

$x \neq 11$ as B_{39} and B_{49} are the only blocks on 9 and 11. Thus,

$$12 = B_{12} \cap B_{19} \cap B_{29} \quad \text{and} \quad 11 = B_{12} \cap B_{1\,10} \cap B_{2\,10}. \tag{6.3}$$

$13 = B_{23} \cap B_{29} \cap B_{39}$ and $14 = B_{23} \cap B_{2\,10} \cap B_{3\,10}$ are distinct new points by Lemma 6.4vii and viii and (6.2). Replacing the pairs $\{1, 2\}$ and $\{3, 4\}$ by $\{2, 3\}$ and $\{1, 4\}$ in (6.2) we find that $B_{23} \cap B_{14} = \{13, 14\}$, $13 = B_{14} \cap B_{1\,10} \cap B_{4\,10}$ and $14 = B_{14} \cap B_{19} \cap B_{49}$. Similarly, points 15 and 16 may be introduced so as to obtain the following points and parts of blocks.

(6.4)

1	2	3	4	9	10	1	9	8	12	14	15
1	2	5	6	11	12	2	9	7	12	13	16
1	3	5	7	15	16	3	9	6	11	13	15
1	4	6	7	13	14	4	9	5	11	14	16
2	3	5	8	13	14	1	10	8	11	13	16
2	4	6	8	15	16	2	10	7	11	14	15
3	4	7	8	11	12	3	10	6	12	14	16
9	10	5	6	7	8	4	10	5	12	13	15

It is straightforward to check that (6.4) defines a symmetric subdesign $\mathscr{D}^*$ of $\mathscr{D}$ with $\lambda^* = 2$, $k^* = 6$ and $v^* = 16$. The minimality of $\mathscr{D}$ implies that $\mathscr{D} = \mathscr{D}^*$, contradicting the assumption that $k > 6$.

(6.4) defines a design $\mathscr{D}_{16}$ ([12] and [15]) with the property that every permutation of the points of one of the blocks of $\mathscr{D}_{16}$ extends to an automorphism of $\mathscr{D}_{16}$. Thus, $\mathscr{D}_{16}$ satisfies the required conditions, completing the proof of Lemma 6.6.

Lemma 6.7. *Under the hypotheses of Lemma* 6.5, *every four points of B generate a subdesign $\mathscr{D}_{16}$. If S is the set of six points of B of such a subdesign and Δ_S does not act on S as S_6, then $\mathscr{D}$ is $\mathscr{D}_{16}$.*

Proof. The first assertion follows from the preceding lemma. Let $\mathscr{D}_{16}$ be the subdesign of which S is, in effect, a block. Since $\lambda = 2$, any element of Δ moving four points of S to four other points of S fixes $\mathscr{D}_{16}$ and hence also S. By hypothesis, $\Delta_S|_S$ is A_6. If $S = \{1, 2, 3, 4, 5, 6\}$ then Δ_{1234} fixes 5 and 6. Then $\Delta = A_6$ by Lemma 6.5iv, and $\mathscr{D}$ is $\mathscr{D}_{16}$.

Proof of Theorem 6.3. By Lemma 6.7, three points of B belong to $(k-3)/3$ subdesigns $\mathscr{D}_{16}$, so that $3|k$. Two points of B belong to $\binom{n}{2}/\binom{4}{2} = n(n-1)/12$ subdesigns $\mathscr{D}_{16}$ which contain B. We now obtain, successively, $n \equiv 0, 1 \pmod 4$, $k \equiv 2, 3 \pmod 4$ and $v = 1 + k(k-1)/2 \equiv 0 \pmod 2$. By a result of Chowla and Ryser [7, p. 61], n is a square.

7. **Cyclic subgroups of Γ_B.** For k and v prime the following result has been obtained independently by Ito [18].

THEOREM 7.1. *$\mathscr{H}_{11}$ is the only 2-transitive symmetric design, not a projective space, for which k is prime.*

Proof. We will show that, for a 2-transitive automorphism group Γ of such a design $\mathscr{D}$, (2.2iv), (2.2v), (2.2vi) and (2.2i) hold. By (2.1), $k|(v-1)$, so that $v-k>k$ and Γ_B acts faithfully on the block B (Corollary 5.3). Also, if $p\in B$ then $(v-k) \mid |\Gamma_{pB}|$ by Lemma 4.2ii. A theorem of Burnside [2, p. 341] then implies that Γ_B is 2-transitive on B. However, if $q\notin B$, then Γ_{qB} is not 2-transitive on B by Proposition 3.3. Γ_{qB} thus acts faithfully on B as a regular or Frobenius group. By Lemma 4.2viii, Γ is transitive on the ordered quadruples (B, p, p', C) with $p, p'\in B$, $p\in C$ and $p'\notin C$. Γ_{pqB} is thus transitive on the blocks on p and q, so that $\lambda \mid |\Gamma_{pqB}|$. Moreover, Γ_{pqB} is cyclic since k is prime. Thus, if $|\Gamma_{pqB}|>\lambda$, there is a nontrivial element $\gamma\in\Gamma_{pqB}$ fixing all blocks on p and q. If E and E' are two such blocks, then $\gamma\in\Gamma_{qBEE'}=1$ (since Γ_{qB} acts as a Frobenius group on the blocks on q), which is a contradiction. This proves (2.2iv). Moreover, Γ_{pqB} is transitive, regular and faithful on the blocks on p and q, so that $|\Gamma_{pq}|=n\lambda$. If $B'\neq B$ and B' is on p but not on q, then $|\Gamma_{pqBB'}| \mid \lambda$. If $\gamma'\in\Gamma_{pqBB'}$ has prime order then γ' fixes $p\in B\cap B'$; it follows that γ' fixes a second point $p'\in B\cap B'$, and then $\gamma'\in\Gamma_{qBpp'}=1$, a contradiction. This proves (2.2v).

We next prove

(7.1) If p and p' are distinct points of B, then $\Gamma_{pp'B}$ fixes every block on p and p', and dually.

For, by (2.2v), $\Gamma_{pp'}$ has a unique subgroup Σ of order n. Since $\Gamma_{pp'B'}$ has order n it follows that $\Gamma_{pp'B'}=\Sigma$ for all blocks B' on p and p', proving (7.1). *Claim*: If B' is another of these fixed blocks on p and p', then $B\cap B'$ is a line. For otherwise, there is a third point $p''\in B\cap B'$ and a block B'' on p and p' but not on p''. By (7.1), Σ fixes p'' and B'', so that $\Sigma\leqq\Gamma_{p''B''pp'}=1$ (since $\Gamma_{p''B''}$ acts as a Frobenius group on B''). This contradiction implies that lines have λ points.

Since $L=B\cap B'$ is a line, Γ_{BL} is 2-transitive on L and on the blocks $\neq B$ containing L. $|\Gamma_{BL}|=(\lambda-1)|\Gamma_{BB'}|=(\lambda-1)\cdot\lambda n$ then implies that Γ_{BL}/Σ acts on L as a sharply 2-transitive group. The Frobenius kernel of Γ_{BL}/Σ is elementary abelian of order λ. On the other hand, if $p^*\in B-B\cap B'$, then by (2.2iv) $\Gamma_{p^*B'}$ acts as a Frobenius group of order $k\lambda$ on the blocks on p^*, so that $\Gamma_{p^*BB'}\leqq\Gamma_{BL}$ has a cyclic subgroup of order λ. Thus, λ is prime.

k is odd. If λ is odd, then n is even. If p and p' are distinct points of $L=B\cap B'$, then there is an involution $\sigma\in\Sigma\leqq\Gamma_{pp'B}$ fixing no points of $B-L$. By (7.1), σ fixes all blocks containing L. By Proposition 3.3, there is a point x lying on no block containing L. Since σ is an involution, σ fixes either x or the line joining x and x^σ. As k and λ are odd, σ must fix a block X on x. Then σ fixes $B\cap X$. Since λ is odd, σ fixes a point $y\in B\cap X$. By (7.1), $\sigma\in\Gamma_{yBX}$ implies that σ fixes $B\cap X$ pointwise. By the choice of x, $X\not\supseteq L$, so that σ fixes points of $B-L$, contradicting the choice of σ.

Thus, $\lambda=2$. Since $|\Gamma_{BL}|=(\lambda-1)\lambda n=2n$, Γ_B is sharply 3-transitive on B. A result of Zassenhaus [35] now implies that the hypotheses of Lemma 6.1 are satisfied. This proves the theorem.

The main result of the present section is the following generalization of Theorem 7.1.

THEOREM 7.2. *Let $\mathscr{D}$ be a symmetric design with $k|(v-1)$. Suppose that Γ is a 2-transitive automorphism group of $\mathscr{D}$ having a cyclic subgroup fixing a block B and a point $q \notin B$ and sharply transitive on the points on B and the blocks on q. Then $\mathscr{D}$ is a projective space or $\mathscr{H}_{11}$ provided that either*

(i) *k has no proper divisor* $\equiv 1 \pmod{\lambda}$, *or*

(ii) $k<(\lambda+1)^2$.

We begin by proving a lemma which does not require (i) or (ii). The proof uses ideas from [20].

LEMMA 7.3. *Γ_B is 2-transitive on B.*

Proof. If $\Delta=\Gamma_B$ is not 2-transitive on B, then k is not prime (Theorem 7.1) and Δ is imprimitive on B by a result of Schur [34, p. 65]. Fix a system $\mathscr{I}$ of nontrivial imprimitivity classes of Δ on B of maximal length c. $\mathfrak{C}$ will denote a typical member of $\mathscr{I}$. Fix $p \in B$ and let $p \in \mathfrak{C}_1$. Let Π be the elementwise stabilizer of $\mathscr{I}$ in Δ. $\Pi \lhd \Delta$ and Δ/Π is primitive and faithful on $\mathscr{I}$. $\Sigma \cap \Pi$ is transitive on each $\mathfrak{C}$ [34, p. 74], where Σ is the given cyclic group.

Let $\mathscr{B}$ be the set of block-orbits of Π other than $\{B\}$. A typical member of $\mathscr{B}$ will be denoted $\mathfrak{B}$. As Δ is transitive on the blocks $\neq B$, $|\mathfrak{B}|=d$ is independent of $\mathfrak{B} \in \mathscr{B}$.

By Theorem 5.2, Π is transitive on $\mathscr{C}B$. Thus, Π has the following orbits: $\mathscr{C}B$, k/c classes $\mathfrak{C}$, $\{B\}$ and $(v-1)/d$ orbits $\mathfrak{B}$. By Proposition 3.1, $(v-1)/d=|\mathscr{B}|=|\mathscr{I}|=k/c$. By Lemma 2.1,

$$d = sc. \tag{7.2}$$

It follows that

$$|\Pi_p| \geqq d/c > 1. \tag{7.3}$$

By Lemma 4.2ii, Δ_p is transitive on the blocks not on p. Then $|\mathfrak{C}_1 \cap \mathscr{C}X|=t$ is independent of the block X not on p. As Π is transitive on $\mathfrak{C}_1$, while Δ is transitive on $\mathscr{I}$, $t=|\mathfrak{C} \cap \mathscr{C}X|$ for each $\mathfrak{C} \in \mathscr{I}$ and each $X \not\supseteq \mathfrak{C}$.

Define $\mathscr{D}^*$ as follows. $\mathscr{I}$ is the set of points and $\mathscr{B}$ the set of blocks. $\mathfrak{C}$ is on $\mathfrak{B}$ if and only if some point of $\mathfrak{C}$ is *not* on some block of $\mathfrak{B}$. There are k/c points and blocks.

Fix $X \neq B$. There are precisely n/t classes $\not\subseteq X$. That is, each block of $\mathscr{D}^*$ is on n/t points of $\mathscr{D}^*$.

Let $\mathfrak{C}$ and $\mathfrak{C}'$ be distinct classes and count in two ways the triples (x, x', X) with $x \in \mathfrak{C}$, $x' \in \mathfrak{C}'$, $x \notin X$, $x' \notin X$. This yields that there are $(v-2k+\lambda)c^2/t^2=(s-1)nc^2/t^2$

blocks X containing neither $\mathfrak{C}$ nor $\mathfrak{C}'$. If X is such a block then so is each block in X^{Π}. Thus, $\mathfrak{C}$ and $\mathfrak{C}'$ are on $[(s-1)nc^2/t^2]d^{-1}=(s-1)nc/st^2$ blocks of $\mathscr{D}^*$. This shows that $\mathscr{D}^*$ is a (possibly degenerate) symmetric design with

$$v^* = k/c, \qquad k^* = n/t, \qquad \lambda^* = (s-1)nc/st^2. \tag{7.4}$$

By (2.1), $[(s-1)nc/st^2](k/c-1)=(n/t)(n/t-1)$. As $sn-1=(s-1)k$, this reduces to

$$(s-1)c = st-1. \tag{7.5}$$

Then also

$$k^* > 1, \tag{7.6}$$

and

$$v^*-k^* = (k-c)/sct = (v^*-1)/st. \tag{7.7}$$

Δ/Π is an automorphism group of $\mathscr{D}^*$ primitive on points. $\Sigma\Pi/\Pi$ is cyclic and transitive. Thus, if Δ/Π is not 2-transitive on points, then results of Burnside [2, p. 341], and Schur [34, p. 65] imply that $|\Delta/\Pi|$ divides $v^*(v^*-1)$ properly. However, as Δ_p is transitive on the blocks not on p, $(\Delta/\Pi)_{\mathfrak{C}_1}$ is transitive on the blocks of $\mathscr{D}^*$ on $\mathfrak{C}_1$. Then $v^*k^* \mid |\Delta/\Pi|$, so that $k^*|(v^*-1)$. By (7.6) and (7.7), $k^*=v^*-1$, whereas $|\Delta/\Pi|$ divides $v^*(v^*-1)$ properly. This contradiction shows that Δ/Π is a 2-transitive automorphism group of $\mathscr{D}^*$. In particular, as $\Delta_{\mathfrak{C}_1}=\Delta_p\Pi$, Δ_p is transitive on the classes $\mathfrak{C}\neq\mathfrak{C}_1$.

Δ_p fixes the set of v^*-k^* blocks of $\mathscr{D}^*$ not containing $\mathfrak{C}_1$. Then Δ_p fixes a set of $d(v^*-k^*)=(k-c)/t$ blocks of $\mathscr{D}$ containing $\mathfrak{C}_1$, by (7.2) and (7.7).

By Lemma 4.2v, our hypotheses and conclusion are self-dual. We may thus define $\tilde{c}$ and $\tilde{t}$ as before, using the blocks on p. Moreover, we may assume that $\tilde{c}\geqq c$.

All previous statements dualize. In particular, $\Delta_p=\Gamma_{pB}$ fixes a set $\mathfrak{p}$ of $(k-\tilde{c})/\tilde{t}$ points of B. By (7.7), $(k-\tilde{c})/\tilde{t}>\tilde{c}\geqq c$, so that $\mathfrak{p}'=\mathfrak{p}-\mathfrak{p}\cap\mathfrak{C}_1\neq\varnothing$. $a=|\mathfrak{p}'\cap\mathfrak{C}|$ is independent of the class $\mathfrak{C}\neq\mathfrak{C}_1$ by the transitivity of Δ_p on these classes. Then $|\mathfrak{p}'|=a(v^*-1)$, so that

$$(k-\tilde{c})/\tilde{t} = |\mathfrak{p}| \geqq a(k/c-1) \geqq a(k/\tilde{c}-1).$$

By (7.5), $a\leqq\tilde{c}/\tilde{t}<2$, so $a=1$.

It follows that the set $\mathfrak{C}^{\#}$ of fixed points of Π_p on B contains $\mathfrak{p}'\cup\{p\}$. By (7.3) and Corollary 5.3, $\mathfrak{C}^{\#}$ is a nontrivial imprimitivity class of Δ on B. The maximality of c, (7.7) and (7.5) imply that

$$c \geqq |\mathfrak{C}^{\#}| > |\mathfrak{p}'| = k/c-1 \geqq st = 1+(s-1)c,$$

a contradiction.

Proof of Theorem 7.2. If $\mathscr{D}$ is neither $\mathscr{H}_{11}$ nor a projective space, then k is composite by Theorem 7.1. $\Lambda=\Gamma_{qB}$ is not 2-transitive on B by Proposition 3.3. Since Λ has a cyclic subgroup transitive on B, Λ is imprimitive on B by Schur's theorem [34, p. 65]. Let $\mathfrak{C}$ be an imprimitivity class of Λ on B; $|\mathfrak{C}|=c$, where $1<c<k$. Let $p\in\mathfrak{C}$. By Lemma 4.2vii, the length of each orbit of Λ_p on $\mathfrak{C}-\{p\}$ is divisible by λ. Then $c-1\equiv 0 \pmod{\lambda}$ and (i) does not hold. Since $k\equiv 1 \pmod{\lambda}$, it follows that $k/c\equiv 1\equiv c \pmod{\lambda}$ and (ii) does not hold. This completes the proof.

We mention without proof a result analogous to Theorem 7.2; the proof is similar to the previous one.

THEOREM 7.3. *Let $\mathscr{D}$ be a symmetric design with $k|(v-1)$. Let Γ be a 2-transitive automorphism group of $\mathscr{D}$ having an abelian subgroup Σ fixing a block B and sharply transitive on B. Suppose that some nontrivial Sylow subgroup of Σ is cyclic and that Σ is centralized by a polarity of $\mathscr{D}$. Then $\mathscr{D}$ is $\mathscr{H}_{11}$ if either* (i) *k has no proper divisor* $\equiv 1 \pmod{\lambda}$, *or* (ii) $k<(\lambda+1)^2$.

8. **Applications to difference set designs.** Let v be an odd prime power and set $F=GF(v)$. Let $B=B(v,k)$ be the subgroup of F^* of order $k=(v-1)/s$, where s is an integer >1. B is a difference set in F^+ if and only if the elements of F and the sets $B+a$, $a\in F$, are the points and blocks of a symmetric design $\mathscr{D}(v,k)$. The designs $\mathscr{D}(v,(v-1)/2)$ are the Paley Hadamard designs [28]; here it is necessary and sufficient that $v\equiv 3 \pmod 4$.

The group $S(v,k)$ of mappings $x\to bx^\sigma+a$, $a\in F$, $b\in B$ and $\sigma\in \mathrm{Aut}(F)$, is an automorphism group of $\mathscr{D}(v,k)$. It follows from Dembowski [6] that $\mathscr{D}(v,k)$ is not a projective space if $\lambda>1$. If $\lambda=1$ the only desarguesian exceptions are $PG(2,2)$ and $PG(2,2^3)$. In view of Ostrom and Wagner [27], these are the only designs $\mathscr{D}(v,k)$ which will actually be disregarded.

The problem of determining the full automorphism group of $\mathscr{D}(v,k)$ was first raised by Todd [31] in the case $k=(v-1)/2$. $S(v,(v-1)/2)$ is not the full automorphism group if $v=7$ ($PG(2,2)$) or 11 ($\mathscr{H}_{11}$). Todd checked some other cases with small v and found that $S(v,(v-1)/2)$ is the full automorphism group of $\mathscr{D}(v,(v-1)/2)$ in these cases; Hering [13] obtained analogous results for additional small values of v by using a computer. We will prove the following

THEOREM 8.1. *If v is a prime power with* $11<v\equiv 3 \pmod 4$, *then $S(v,(v-1)/2)$ is the full automorphism group of $\mathscr{D}(v,(v-1)/2)$.*

Proof. Suppose that, for some such v, the full automorphism group Γ of $\mathscr{D}(v,(v-1)/2)$ is $>S(v,(v-1)/2)$. By [20, Proposition 6.1], $S(v,(v-1)/2)$ is a maximal subgroup of Γ of odd order. As $S(v,(v-1)/2)$ is 2-homogeneous on points and $|\Gamma|$ is even, it follows that Γ is 2-transitive. As $k=2\lambda+1<(\lambda+1)^2$, Theorem 7.2 applies. This contradiction completes the proof.

COROLLARY 8.2. *Let $v>11$ be an odd prime power and set $F=GF(v)$. If f and g are permutation polynomials such that, for all $x\in F$, $f(x+q)-g(x)$ is a square whenever q is a square, then $f(x)=g(x)=bx^\sigma+a$ for all x, some square $b\neq 0$, some a and some $\sigma\in$* Aut (F).

Proof. Let B be the set of nonzero squares of F. Let $\mathscr{D}$ be the tactical configuration consisting of the elements of F as points and the sets $B+a$, $a \in F$, as blocks. Each pair (f, g) induces an automorphism $\gamma(f, g)$ of $\mathscr{D}$. If $v \equiv 3 \pmod 4$, Theorem 8.1 implies the result. Let $v \equiv 1 \pmod 4$. If $x \in F$ then $B+x=\{y \mid |(B+x) \cap (B+y)| =(v-5)/4\}$. Thus, $(B+x)^{\gamma(f,g)}=B+x^{\gamma(f,g)}$, that is, $g(x)=f(x)$. A result of Carlitz [3] completes the proof.

THEOREM 8.3. *Let v be a prime power, let $k|(v-1)$ and suppose that $B(v, k)$ is a difference set in $GF(v)^+$. If the automorphism group of $\mathscr{D}(v, k)$ is 2-transitive, and if $1+k^{1/2}>(v-1)/k$, then $\mathscr{D}(v, k)=\mathscr{D}(7, 3)$ or $\mathscr{D}(11, 5)$.*

Proof. By (2.1), $\lambda=k(k-1)/(v-1)>k^{1/2}-1$. Theorem 7.2 thus applies.

Note that, if v is prime, then the automorphism group of $\mathscr{D}(v, k)$ is either $S(v, k)$ or 2-transitive. This follows from a theorem of Burnside [2, p. 341], and the fact that $B(v, k)$ is fixed by all multipliers. By Lemma 4.1 we have the

COROLLARY 8.4. *Let Γ be a nonsolvable 2-transitive group of prime degree p having a subgroup of index p with an orbit of length $k\neq 1, p-1$. If the normalizer of a Sylow p-subgroup has order $\geqq pk$ and $1+k^{1/2}>(p-1)/k$, then Γ is similar to $PSL(3, 2)$ in its usual representation or to $PSL(2, 11)$ in its representation of degree 11.*

9. **Automorphisms of prime order** $>\lambda$. Automorphisms of this type are probably rare in symmetric designs for which λ is not small. However, when they occur it is frequently possible to relate them to lines.

LEMMA 9.1. *Let $\mathscr{D}$ be a symmetric design such that n has a prime divisor $p>\lambda>1$. If x and y are distinct points of $\mathscr{D}$, then every two distinct blocks on x and y have the line joining x and y as their intersection, provided that $\mathscr{D}$ admits an automorphism group Δ satisfying one of the following conditions*:

(i) *Δ fixes x and is transitive on the points $\neq x$; or*

(ii) *Δ fixes x and y and is transitive on the blocks on y not on x.*

Proof. Let Σ be a Sylow p-subgroup of Δ_y. Σ fixes all blocks on x and y since $p>\lambda$. Let X and Y be two such blocks whose intersection is not the line joining x and y. Σ fixes $X \cap Y$ pointwise.

(i) Let Z be a block on y but not on x and assume that $|X \cap Y \cap Z| \geqq 2$. Σ fixes $X \cap Y \cap Z$ pointwise, and thus fixes any block containing two points of $X \cap Y \cap Z$. In particular, Σ fixes Z. However $|\Delta|=(v-k)|\Delta_Z|=(v-1)|\Delta_y|$, so that $n|\Delta_Z|=k|\Delta_y|$ and $|\Sigma| \nmid |\Delta_Z|$, a contradiction.

(ii) This time suppose that Z is on both x and y but that there is a point $z \in X \cap Y-X \cap Y \cap Z$, so that x, y and z are not collinear. Then there is a block B on y and z but not on x. Σ fixes y and z and hence also B. Then Σ fixes a certain number $f \geqq 1$ of blocks on y but not on x. Here $f\equiv k-\lambda\equiv 0 \pmod p$. Since $\Delta=\Delta_y$ is transitive on the blocks on y but not on x, Lemma 3.5 implies that $N_\Delta(\Sigma)$, restricted to the fixed blocks of Σ on y but not on x, is a transitive permutation group of degree $f \equiv 0 \pmod p$). This is impossible since this permutation group has a trivial Sylow p-subgroup.

The preceding lemma has been stated in a form dual to our usual form because the present version can be extended to nonsymmetric designs. For example, in (ii) one would need to assume in the more general situation that $p \mid (r-\lambda)$, $p>\lambda$, and p is greater than the number of points common to any three distinct blocks containing x and y, one of which does not contain the intersection of the other two.

LEMMA 9.2. *Let Δ be an automorphism group of a symmetric design fixing a block B and transitive on the remaining blocks. If n is prime and $>\lambda$, then $\lambda=2$ and, for some prime e, Δ acts on B as $PSL(2, 2^e)$ or $P\Gamma L(2, 2^e)$ in its usual representation.*

Proof. By the dual of Lemma 9.1i, every block $\neq B$ meets B in a line. Then $(\lambda-1)\mid(k-1)$ by Lemma 4.3, so that $(\lambda-1)\mid n$ and $\lambda=2$. By Lemma 6.2, Δ is 3-transitive on B. If Δ is not 4-transitive on B the result follows from [2, p. 341] and [9]. If Δ is 4-transitive, Theorem 6.3 applies. Lemma 6.1 now yields the following

THEOREM 9.3. *$\mathscr{H}_{11}$ is the only 2-transitive symmetric design for which n is a prime $>\lambda>1$.*

THEOREM 9.4. *$\mathscr{H}_{11}$ is the only symmetric design $\mathscr{D}$ admitting an automorphism group Δ fixing a block B and transitive on the remaining blocks, and such that $\lambda^2+1 \geqq k>4$ and n has a prime divisor $p>\lambda$.*

Proof. The dual of Lemma 9.1i implies that every block $\neq B$ meets B in a line. Then $(\lambda-1)\mid(k-\lambda)$ by Lemma 4.3, so that

$$\lambda < p \mid (k-\lambda)(\lambda-1)^{-1} \leqq (\lambda^2+1-\lambda)(\lambda-1)^{-1}.$$

It follows that $\lambda=2$ and $k=5$, so that $\mathscr{D}$ is $\mathscr{H}_{11}$.

Lemma 9.1 involves groups of automorphisms, some of which have prime order $>\lambda$. Some information can also be obtained in the case of a single automorphism of prime order $p>\lambda$, even without the assumption that $p\mid n$. First, we prove a generalization of Bruck's Lemma [10, p. 398].

LEMMA 9.5. *Let $\mathscr{D}^*$ be a proper symmetric subdesign of a symmetric design $\mathscr{D}$ such that $\lambda^*=\lambda$. Then either $n=(k^*-1)^2$ or $\lambda v^* \leqq k$. (The possibility that $k^*=\lambda+1$ is not excluded.)*

Proof. From (2.1), applied to both $\mathscr{D}$ and $\mathscr{D}^*$, it follows that $k>k^*$. Let B be a block of $\mathscr{D}^*$ and x a point of B not in $\mathscr{D}^*$. Since $\lambda^*=\lambda$, B is the only block of $\mathscr{D}^*$ on x. Then there are $\lambda(v^*-k^*)+(\lambda-1)k^*$ blocks on both x and exactly one point of $\mathscr{D}^*$, so that this quantity is at most $k-1$. By (2.1), equality implies that $(k^*-1)^2 = n$. Inequality holds only if some block of $\mathscr{D}$ contains no point of $\mathscr{D}^*$, and dually. Replacing x by a point of $\mathscr{D}$ on no block of $\mathscr{D}^*$ and proceeding as before, we find that $\lambda v^* \leqq k$.

PROPOSITION 9.6. *Let γ be an automorphism of prime order $p>\lambda>1$ fixing more than λ points of a symmetric design $\mathscr{D}$.*

(i) *Either* (a) *every fixed block of γ has $n^{1/2}+1$ fixed points, or* (b) $k\geqq\lambda(\lambda+2)$.

(ii) *If also $p|n$, then* (a) *does not occur and* $k\geqq 4\lambda^2$.

Proof. Let $\mathscr{D}^*$ be the set of fixed points and blocks of γ. Since $p>\lambda$, if x and y are in $\mathscr{D}^*$ then all λ blocks on x and y are in $\mathscr{D}^*$, and dually. As $\mathscr{D}^*$ contains more than λ points it is a symmetric subdesign of $\mathscr{D}$, possibly with $v^*=k^*+1$ (Majumdar [23]; Dembowski [5, p. 269]). Since $v^*\geqq\lambda+2$, the preceding lemma implies (i). If also $p|n$, then $p|(k-k^*)$ and $p\nmid(\lambda-1)$ imply that $p\nmid(k^*-1)$. Then $n\neq(k^*-1)^2$, so that $\lambda v^*\leqq k$ by Lemma 9.5. Since $k^*-\lambda\geqq p>\lambda$, (2.1) implies that $\lambda(v^*-1)=k^*(k^*-1)>2\lambda(2\lambda-1)$, so that $k\geqq\lambda v^*\geqq 4\lambda^2$.

An automorphism of order 3 fixing 3 points of a block of the design in (6.4) provides an example of (ia).

COROLLARY 9.7. *Let $\mathscr{D}$ be a symmetric design for which $\lambda^2+1\geqq k>4$ and n has a prime divisor $p>\lambda$. If there is a block B and a point x on B such that each $y\in B-\{x\}$ is fixed by an automorphism of $\mathscr{D}$ of order p which fixes x, then $\mathscr{D}$ is $\mathscr{H}_{11}$.*

Proof. Let γ be an automorphism of order p fixing x and $y\in B-\{x\}$. Then γ fixes each block on x and y. If C is such a block $\neq B$, then $B\cap C$ is a line. For otherwise, there is a block D on x but not on y such that $|B\cap C\cap D|\geqq 2$. Since γ fixes $B\cap C$ pointwise it fixes all blocks containing $B\cap C\cap D$. Then γ fixes at least $\lambda+1$ blocks, contradicting Proposition 9.6ii. The remainder of the proof is the same as that of Theorem 9.4.

10. **Diophantine conditions.** Let Γ be a 2-transitive automorphism group of a symmetric design $\mathscr{D}$ with $(v-1)/k$ an integer s. Suppose that Γ_B is 2-transitive on the block B, and that $\mathscr{D}$ is not a projective space. In this section we list numerical conditions satisfied by some numbers related to the action of Γ on $\mathscr{D}$.

If all lines have h points, then by Lemmas 2.1, 3.2 and 4.3, and Proposition 3.3,

$$(h-1)|(s,n), \tag{10.1}$$

$$s\geqq h\geqq 2. \tag{10.2}$$

Let p and p' be distinct points of a line L. Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ be the orbits of $\Gamma_{pp'}$ of points not on L. Set $l_i=|\mathfrak{p}_i|$. $|\mathscr{C}B\cap\mathfrak{p}_i|$ is independent of the block B on p and p', and, by Lemma 4.2vi, $|\mathscr{C}B\cap\mathfrak{p}_i|=nx_i$, where x_i is an integer. $x_i>0$, as otherwise every block containing p and p' would contain $\mathfrak{p}_i$, whereas $\mathfrak{p}_i\nsubseteq L$. Clearly,

$$\sum_i l_i = v-h \quad\text{and}\quad \sum_i x_i = s. \tag{10.3}$$

Let $q\in\mathfrak{p}_i$. Since $\Gamma_{pp'}$ is transitive on the blocks on p and p', the number of such blocks not on q is $\lambda n x_i/l_i$, so that

$$nx_i \leqq l_i|\lambda n x_i \quad\text{for all } i. \tag{10.4}$$

Fix B on p and p'. Counting in two ways the pairs (q, B') with B and B' distinct blocks on p and p' but not on q, we obtain

(10.5) $$\sum_i x_i^2/l_i = 1/\lambda.$$

Lemmas 4.4 and 4.5 imply that

(10.6) If Γ_B is 2-transitive on $\mathscr{C}B$, then $t = h = 2$.

Under the hypothesis of (10.6), the number c_i of points of $\mathfrak{p}_i$ on a block X on neither p nor p' is independent of the choice of X. There are $n-\lambda n x_i/l_i$ such blocks X on each point of $\mathfrak{p}_i$. Then by Lemma 2.1, $(s-1)nc_i=(v-2k+\lambda)c_i=l_i(n-\lambda n x_i/l_i)$, so that

(10.7) If Γ_B is 2-transitive on $\mathscr{C}B$, then $(s-1)|(l_i-\lambda x_i)$ for all i.

If $\mathscr{D}$ is $\mathscr{H}_{11}$ then $t=h=2$, $l_1=6$, $l_2=3$ and $x_1=x_2=1$. In the proof of Theorem 11.3 we will encounter a second set of solutions of the conditions (10.1)–(10.7), corresponding to which there is, however, no symmetric design of the desired type: $t=h=2$, $v=506$, $k=101$, $n=81$, $\lambda=20$, $s=5$, $l_1=180$, $l_2=324$, $x_1=2$, and $x_2=3$.

11. **Applications of the Diophantine conditions.**

THEOREM 11.1. *Let $\mathscr{D}$ be a symmetric design having the same parameters as a finite projective space. If $\mathscr{D}$ admits a 2-transitive automorphism group Γ such that Γ_B is 2-transitive on the block B, then $\mathscr{D}$ is a projective space.*

Proof. By Lemma 2.1, the assumption concerning parameters is equivalent to: $k|(v-1)$ and $v-k=sn$ is a power of a prime p. If $\mathscr{D}$ is not a projective space then the results of the preceding section apply. If $s\nmid l_i$ for some i, then $nx_i \leqq l_i|\lambda s p^{-1}x_i$ by (10.4), whereas $\lambda s p^{-1}=(\lambda+n-1)p^{-1}<n$ by Lemma 2.1, a contradiction. Thus,

$$s \Big| \sum_i l_i = v-h = s^2\lambda+s+1-h,$$

so that $s|(h-1)$, contradicting (10.2).

THEOREM 11.2. *Let $\mathscr{D}$ be a symmetric design for which $(v-1)/k$ is an integer s and $(n, 2s-1)=1$. If $\mathscr{D}$ admits a 2-transitive automorphism group Γ such that, for each block B, Γ_B is 2-transitive on B and on $\mathscr{C}B$, then $\mathscr{D}$ is a projective space.*

Proof. If $\mathscr{D}$ is not a projective space then $t=h=2$ by (10.6). By (10.3) and Lemma 2.1,

$$(\lambda, l_1, l_2)|(\lambda, s^2\lambda+s+1-2) = (\lambda, s-1),$$
$$(n, l_1, l_2)|(n, (s^2n-1)(s-1)^{-1}-2) = 1$$

and

$$(x_1, x_2, l_1, l_2)|(s, s^2\lambda+s+1-2) = 1.$$

Since $(l_1, l_2)|\lambda n(x_1, x_2)$ by (10.4), it follows that $(l_1, l_2)|(\lambda, s-1)$. By (10.5), $\lambda(x_1^2 l_2 + x_2^2 l_1) = l_1 l_2$, so that $l_1|\lambda x_1^2(l_1, l_2)$ and thus $l_1|\lambda(\lambda, s-1)x_1^2$. Comparison with $l_1|\lambda n x_1$ shows that $l_1|\lambda x_1(n, (\lambda, s-1)x_1)$. $(n, \lambda)=1$, (10.3) and (10.4) then imply that

$$nx_1 \leqq l_1|\lambda x_1(n, x_1) \leqq \lambda x_1(s-1) = (n-1)x_1,$$

a contradiction.

THEOREM 11.3. *Let $\mathcal{D}$ be a symmetric design for which $k|(v-1)$, n is a prime power and $\lambda > 2$. If $\mathcal{D}$ admits a 2-transitive automorphism group Γ such that, for each block B, Γ_B is 2-transitive on B and on $\mathcal{C}B$, then $\mathcal{D}$ is a projective space.*

Proof. Suppose that $\mathcal{D}$ is not a projective space. Then $t=h=2$ by (10.6). We may assume that $(l_1, l_2, n)=(l_1, n)$. As in the proof of the preceding theorem, this divides $(n, \lambda, s-1)(n, 2s-1)=(n, 2s-1)$. Lemma 2.1 and (10.4) imply that

$$\{1+\lambda(s-1)\}x_1 = nx_1 \leqq l_1|\lambda(n, 2s-1)x_1 \leqq \lambda(2s-1)x_1.$$

It follows that $l_1 = \varepsilon\lambda(2s-1)x_1$, $\varepsilon=1$ or $1/2$, and $(2s-1)/(l_1, n) \leqq 2$. Then (l_1, l_2, n) $=2s-1$. Substituting in (10.5),

$$x_2^2\varepsilon\lambda(2s-1) = l_2\{\varepsilon(2s-1)-s+x_2\}. \tag{11.1}$$

Case 1. $\varepsilon=1$. By (10.3), (10.4) and Lemma 2.1,

$$\{1+\lambda(s-1)\}x_2 \leqq l_2 = (s^2\lambda+s+1)-2-\lambda(2s-1)(s-x_2),$$

or $(\lambda s-1)x_2 \geqq (\lambda s-1)(s-1)$. Then by (10.3), $x_2=s-1$, $x_1=1$ and $l_2=(s-1)n$. By (11.1), $\lambda(2s-1)=2n$, so that $\lambda|2$, a contradiction.

Case 2. $\varepsilon=1/2$ and $(x_2, n)=1$. By (11.1), $x_2=1$ and thus $l_2=\lambda(2s-1)$. Since $l_1=\lambda(2s-1)(s-1)/2$ this contradicts (10.3).

Case 3. $\varepsilon=1/2$ and $(x_2, n)\neq 1$. Let p be the prime dividing n. By (11.1), $l_2 = x_2^2\lambda(2s-1)/(2x_2-1)$, so that $x_2|n$ by (10.4). By (10.3) and Lemma 2.1,

$$\lambda x_1/2 + \lambda x_2^2/(2x_2-1) = \{s^2 n(2s-1)^{-1}-1\}/(s-1). \tag{11.2}$$

Since $\lambda\neq 2$, $n\neq 2s-1$ and so $p|n(2s-1)^{-1}$. If $n(2s-1)^{-1}\equiv x_2\equiv 0 \pmod{p^2}$, then (11.2) implies that $\lambda x_1/2 \equiv -1/(s-1) \pmod{p^2}$, so that, by (10.3), $s\equiv x_1\equiv -2/(n-1)$ $\equiv 2 \pmod{p^2}$; since $2s-1$ is a power of p this is impossible. Thus, either (i) $n=p(2s-1)$ or (ii) $x_2=p$. The same argument also shows that $s\equiv 2 \pmod{p}$, so that $p=3$.

(i) $n=3(2s-1)$ implies that $\lambda=2(3s-2)/(s-1)$ (by Lemma 2.1). Then $(s-1)|2$, contradicting the fact that $s>x_2=p=3$.

(ii) $x_2=3$, (10.3), (11.2) and Lemma 2.1 imply that $x_1=s-3$ and

$$\lambda(2s-1)(s-3)/2+3^2\lambda(2s-1)/(2\cdot 3-1) = s^2\lambda+s-1.$$

Then $\lambda=10(s-1)/(s-3)$. Since $2s-1$ is a power of 3 it follows that $s=5$ and $\lambda=20$. Then $k=101$ is prime, contradicting Theorem 7.1. This proves the theorem.

THEOREM 11.4. *Let $\mathcal{D}$ be a symmetric design with $k|(v-1)$ and $\lambda>2$ admitting a 2-transitive automorphism group Γ. If, for each block B, Γ_B is 2-transitive on $\mathcal{C}B$*

and transitive on the ordered triples of noncollinear points of B, then $\mathcal{D}$ is a projective space.

Proof. If $\mathcal{D}$ is not a projective space then $t=h=2$ by (10.6). In particular, Γ_B is 3-transitive on B. However, $t=2$ means that Γ has precisely 2 orbits of ordered triples of points. Thus, Γ is transitive on those triples contained in some block and on those triples contained in no block. In the preceding section we may thus assume that $\lambda=\lambda n x_2/l_2$. A straightforward calculation using (10.3) and (10.5) yields

$$(l_1-\lambda x_1)/(s-1) = \lambda^2(k-2)/(\lambda^2-2\lambda+n).$$

Since $(n, \lambda)=1$, (10.7) implies that $\{(\lambda-1)(\lambda-2)+(k-2)\}|(k-2)$, which contradicts $\lambda>2$.

THEOREM 11.5. *Let Γ be a 2-transitive automorphism group of a Hadamard design $\mathcal{D}$. If Γ_B is 2-transitive on the block B, then $\mathcal{D}$ is either a projective space or $\mathcal{H}_{11}$.*

Proof. Suppose that $\mathcal{D}$ is not a projective space. Since $t>1$ by Proposition 3.3, (10.3) implies that $t=2$ and $x_1=x_2=1$ (compare Lemma 4.2iv). $h=2$ by (10.2). Then (10.3) and (10.5) imply that $l_1l_2=(n-1)(4n-3)$, so that $l_1\cdot(-l_1)\equiv 0 \pmod{4n-3}$. Then by (10.4), $n=3$, as claimed.

Note that Theorem 11.6 can be used in place of Theorem 7.1 in the proof of Theorem 8.1.

12. ***n* a prime power.** The conditions given in §10 may be generalized somewhat. The resulting numerical conditions do not, however, seem useful unless n is a prime power (compare Theorems 11.1 and 11.3). In this case we can prove the following simple characterization of projective spaces over prime fields.

THEOREM 12.1. *Let $\mathcal{D}$ be a 2-transitive symmetric design with $(v-1)/k$ an integer s. If n is a prime power relatively prime to every number of the form $as+s-a$ with $1\leqq a<s$ and $a|(n, s)$, then $\mathcal{D}$ is a projective space.*

Proof. Assume that $\mathcal{D}$ is not a projective space. By Lemma 3.2 and Proposition 3.3, all lines have the same number $h\leqq s$ of points. Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ be the orbits of $\Gamma_{pp'}$ of points not on the line joining the points p and p'. Set $l_i=|\mathfrak{p}_i|$. By Lemma 4.2ii, $\Gamma_{pp'}$ is transitive on the blocks C on p but not on p'. Then $y_i=|\mathfrak{p}_i\cap C|$ is independent of C. By Lemma 2.1,

$$\sum_i l_i = v-h = \{s^2n-1-h(s-1)/(s-1)\}.$$

Since $(h-1)|(n, s)$ by Lemmas 2.1 and 4.3, our hypothesis implies that $(n, v-h)=1$. Then $(n, l_i)=1$ for some i. As in §10, there are ny_i/l_i blocks C on each point of $\mathfrak{p}_i$. Since $l_i\geqq y_i$ it follows that $l_i=y_i$. Then each of the n blocks on p but not on p' contains $\mathfrak{p}_i\cup\{p\}$. Since $n>\lambda$ this is impossible.

COROLLARY 12.2. *A 2-transitive symmetric design is a projective space if* $(v-1)/k$ *is a prime s, n is a prime power and* $(n, 2s-1)=1$.

This corollary applies to Hadamard designs in which n is a power of a prime $\neq 3$, and to designs with the same parameters as $PG(d, p)$ with p prime.

REFERENCES

1. N. Burgoyne and P. Fong, *The Schur multipliers of the Mathieu groups*, Nagoya Math. J. **27** (1966), 733–745.

2. W. Burnside, *The theory of groups of finite order*, Dover, New York, 1955.

3. L. Carlitz, *A theorem on permutations in a finite field*, Proc. Amer. Math. Soc. **11** (1960), 456–459.

4. P. Dembowski, *Verallgemeinerungen von Transitivitätsklassen endlicher projektiver Ebenen*, Math. Z. **69** (1958), 59–89.

5. ———, *Kombinatorische Eigenschaften endlicher Inzidenzstrukturen*, Math. Z. **75** (1961), 256–270.

6. ———, *Scharf transitive and scharf fahnentransitive Kollineationsgruppen*, Math. Ann. **149** (1963), 217–225.

7. ———, *Finite geometries*, Springer-Verlag, Berlin, 1968.

8. P. Dembowski and A. Wagner, *Some characterizations of finite projective spaces*, Arch. Math. **11** (1960), 465–469.

9. D. Gorenstein and D. R. Hughes, *Triply transitive groups in which only the identity fixes four letters*, Illinois J. Math. **5** (1961), 486–491.

10. M. Hall, Jr., *The theory of groups*, Macmillan, New York, 1959.

11. ———, *Combinatorial theory*, Ginn, Waltham, Mass., 1967.

12. ———, *Note on symmetric block designs with* $\lambda=2$, (to appear).

13. F. Hering, *Über die Kollineationsgruppen einiger Hadamard-Matrizen* (unpublished manuscript).

14. D. R. Hughes, *Collineations and generalized incidence matrices*, Trans. Amer. Math. Soc. **86** (1957), 284–296.

15. Q. M. Hussain, *On the totality of the solutions for the symmetrical incomplete block designs*: $\lambda=2$, $k=5$ or 6, Sankhyā **7** (1945), 204–208.

16. ———, *Impossibility of the symmetrical incomplete block design with* $\lambda=2$, $k=7$, Sankhyā **7** (1946), 317–322.

17. N. Ito, *On a class of doubly, but not triply transitive permutation groups*, Arch. Math. **18** (1967), 564–570.

18. ———, *On permutation groups of prime degree p which contain (at least) two classes of conjugate subgroups of index p*, Rend. Sem. Mat. Univ. Padova **38** (1967), 287–292.

19. W. M. Kantor, *Characterizations of finite projective and affine spaces*, Canad. J. Math. **21** (1969), 64–75.

20. ———, *Automorphism groups of designs*, Math. Z. **109** (1969), 246–252.

21. ———, *4-homogeneous groups*, Math. Z. **103** (1968), 67–68. Correction, ibid. **109** (1969), 86.

22. D. Livingstone and A. Wagner, *Transitivity of finite permutation groups on unordered sets*, Math. Z. **90** (1965), 393–403.

23. K. N. Majumdar, *On some theorems in combinatorics relating to incomplete block designs*, Ann. Math. Statist. **24** (1953), 377–389.

24. H. B. Mann, *Difference sets in elementary abelian groups*, Illinois J. Math. **9** (1965), 212–219.

25. H. B. Mann, *Addition theorems*, Interscience, New York, 1965.

26. H. Nagao, *On multiply transitive groups*. IV, Osaka J. Math. **2** (1965), 327–341.

27. T. G. Ostrom and A. Wagner, *On projective and affine planes with transitive collineation groups*, Math. Z. **71** (1959), 186–199.

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

29. E. T. Parker, *On collineations of symmetric designs*, Proc. Amer. Math. Soc. **8** (1957), 350–351.

30. H. J. Ryser, *Combinatorial mathematics*, Wiley, New York, 1963.

31. J. A. Todd, *A combinatorial problem*, J. Math. and Phys. **12** (1933), 321–333.

32. A. Wagner, *On collineation groups of projective spaces*. I, Math. Z. **76** (1961), 411–426.

33. ———, *On finite affine line transitive planes*, Math. Z. **87** (1965), 1–11.

34. H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.

35. H. Zassenhaus, *Kennzeichnung endlicher linearen Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 17–40.

University of Wisconsin,
Madison, Wisconsin