MATHEMATICAL CENTRE TRACTS 57

M. HALL, Jr. (ed.)
J.H. VAN LINT (ed.)

COMBINATORICS

Part 3: Combinatorial group theory

Proceedings of the Advanced Study Institute on Combinatorics held at Nijenrode Castle, Breukelen, The Netherlands, July 8-20, 1974

2nd edition (revised)

MATHEMATISCH CENTRUM AMSTERDAM 1975

AMS(MOS) subject classification scheme (1970): 05-02, 05B20, 05B05, 05B25, 94A10

1st edition: June 1974
2nd edition (revised): June 1975
ISBN 90 6196 101 7

CONTENTS

PREFACE

Combinatorics has come of age. It had its beginnings in a number of puzzles which have still not lost their charm. Among these are EULER's problem of the 36 officers and the KÖNIGSBERG bridge problem, BACHET's problem of the weights, and the Reverend T.P. KIRKMAN's problem of the schoolgirls. Many of the topics treated in ROUSE BALL's *Recreational Mathematics* belong to combinatorial theory.

All of this has now changed. The solution of the puzzles has led to a large and sophisticated theory with many complex ramifications. And it seems probable that the four color problem will only be solved in terms of as yet undiscovered deep results in graph theory. Combinatorics and the theory of numbers have much in common. In both theories there are many problems which are easy to state in terms understandable by the layman, but whose solution depends on complicated and abstruse methods. And there are now interconnections between these theories in terms of which each enriches the other.

Combinatorics includes a diversity of topics which do however have interrelations in superficially unexpected ways. The instructional lectures included in these proceedings have been divided into six major areas: 1. *Theory of designs*; 2. *Graph theory*; 3. *Combinatorial group theory*; 4. *Finite geometry*; 5. *Foundations, partitions and combinatorial geometry*; 6. *Coding theory*. They are designed to give an overview of the classical foundations of the subjects treated and also some indication of the present frontiers of research.

Without the generous support of the North Atlantic Treaty Organization, this *Advanced Study Institute on Combinatorics* would not have been possible, and we thank them sincerely. Thanks are also due to the National Science Foundation for the support of some advanced students, in addition to the support of those with their own NSF grants. The IBM Corporation has kindly given us financial support to supplement the NATO grant. The Xerox Corporation has helped with donations of material and equipment.

Finally we must acknowledge the extensive activities of the Mathematical Centre of Amsterdam in making all the arrangements necessary for holding this conference and preparing these proceedings.

M. HALL, Jr.
J.H. VAN LINT

COMBINATORIAL GROUP THEORY

MATHEMATICAL CENTRE TRACTS 57, 1974, 1-26

DIFFERENCE SETS *)

M. HALL, Jr.

California Institute of Technology, Pasadena, Cal. 91103, USA

1. INTRODUCTION

A symmetric block design D is a special kind of incidence structure [7,11,21] consisting of v points and v blocks, each block containing k distinct points, each point lying on k distinct blocks, and every pair of distinct points lying on λ different blocks. Counting the point pairs in two ways we have

$$k(k-1) = \lambda(v-1). \tag{1.1}$$

A further consequence [11, p.104] is that any two distinct blocks have λ points in common, so that there is a duality between the points and blocks.

An automorphism α of D is a one-to-one mapping of points onto points and blocks onto blocks preserving incidence. It may happen that D has a group G of automorphisms which is transitive and regular on the points (and as can be shown also transitive and regular on the blocks). Identifying the points with elements of G and a block with the set of k points on it, a single block will determine all the rest. A set of k elements $B = \{d_1,\ldots,d_k\}$ from a group G of order v such that the translates $Bg = \{d_1g,\ldots,d_kg\}$ form a symmetric block design D is called a *difference set*.

At first glance the concept of difference set might appear to be too restrictive to be of much interest. But difference sets are in fact quite numerous and have many interesting properties. For $k \leq 100$ there are at least 85 difference sets with G a cyclic group [1], and there are a number of other cases in this range with G non-cyclic.

---

*) This research was supported in part by NSF grant GP 36230X.

A remarkable fact, first discovered by the author [10] for finite projective planes is that if G is Abelian the design D often has a still larger group of automorphisms. It may happen that there is an integer t, necessarily prime to v, such that the mapping $x \to x^t$ is not only an automorphism of G but is also an automorphism of the design D. Such an integer is called a *multiplier*. There are a number of theorems proving the existence of multipliers. Every known difference set for which G is cyclic has non-trivial multipliers.

Studies of difference sets have led to very interesting connections with finite geometries, algebraic number theory, and group characters among other subjects.

Sections 2, 3, 4 of this paper give some properties of automorphisms of designs, a formal definition of a difference, and the simplest form of the multiplier theorem. Section 5 gives a list of the known types of difference sets and a few sporadic sets. Section 6 gives a brief sketch of the general theory and some of its results.

2. AUTOMORPHISMS OF DESIGNS

A general incidence structure S is a system $(\{p\},\{B\},I)$ with two sets of objects, $\{p\}$ a set of "points" and $\{B\}$ a set of "blocks" together with an incidence relation I such that pIB for certain points p and certain blocks B. If $T = (\{q\},\{C\},J)$ is another incidence structure, then an incidence preserving map of S into T is a mapping ϕ of $\{p\}$ into $\{q\}$ and $\{B\}$ into $\{C\}$ such that pIB implies $p\phi J B\phi$ for all $p \in \{p\}$ and $B \in \{B\}$.

In general the incidence preserving map is a *homomorphism* of S onto T. If ϕ is a one-to-one mapping then it is an *isomorphism* of S onto T. An isomorphism of S onto itself is called an *automorphism*. Clearly the automorphisms of an incidence structure form a group.

The incidence structures which will be considered here are the "partially balanced incomplete block designs" or more briefly "designs". For these if there are v points and b blocks, each block contains k distinct points, every point lies on r blocks, and every pair of distinct points lies on exactly λ blocks.

These parameters satisfy the two well-known relations

$$(2.1) \qquad bk = vr, \quad r(k-1) = \lambda(v-1).$$

To avoid certain trivial designs we assume $2 < k < v-2$. With a design $D = D(v,b,r,k,\lambda)$ we associate an incidence matrix $A = [a_{ij}]$, $i=1,\ldots,v$; $j=1,\ldots,b$ where, if we number the points P_i, $i=1,\ldots,v$ in an arbitrary way and blocks B_j, $j=1,\ldots,b$ also arbitrarily, we put $a_{ij} = 1$ if $P_i \; I \; B_j$ and $a_{ij} = 0$ if $P_i \not I \; B_j$. Then it is well known that A satisfies

$$AA^T = (r-\lambda)I_v + \lambda J_{vv}\,, \quad AJ_{bb} = rJ_{vb}\,, \quad J_{vv}A = kJ_{vb}. \tag{2.2}$$

Here A^T is the transpose of A, I_v is the $v \times v$ identity matrix, and J_{mn} the $m \times n$ matrix all of whose entries are 1's.

Writing $B = (r-\lambda)I_v + \lambda J_{vv}$ we can easily evaluate the determinant of B, obtaining

$$\det B = (r-\lambda)^{v-1}(r+(v-1)\lambda). \tag{2.3}$$

The relations (2.1) together with the assumption $2 < k < v-2$ imply that $r > \lambda$ so that $\det B > 0$. From this it follows that the rank of the $v \times b$ matrix A is v, we obtain FISHER's inequality

$$b \geq v. \tag{2.4}$$

If $b = v$ and so also $r = k$ the design is called a *symmetric design*.

If α is an automorphism of a block design let P_α be the permutation of the points $p \to (p)\alpha$ and Q_α the permutation of the blocks $B \to (B)\alpha$. The fact that α preserves incidences can be expressed in terms of the incidence matrix A

$$P_\alpha^{-1} A Q_\alpha = A. \tag{2.5}$$

For if $A = [a_{ij}]$ the matrix on the left is $[a_{(i)\alpha(j)\alpha}]$ and as incidences are preserved this is identical with A. Conversely permutation matrices P_α and Q_α satisfying (2.5) determine an automorphism of the design with incidence matrix A.

THEOREM 2.1. (PARKER). *An automorphism of a symmetric block design* D *fixes the same number of blocks as points.*

PROOF. From (2.2) and (2.3) the incidence matrix of a symmetric block design is non-singular. Hence from (2.5) we may obtain

$$Q_\alpha = AP_\alpha A^{-1} \tag{2.6}$$

and this gives for the traces

$$\text{(2.7)} \qquad \mathrm{tr}(Q_\alpha) = \mathrm{tr}(P_\alpha).$$

But $\mathrm{tr}(P_\alpha)$ is the number of points fixed by α and $\mathrm{tr}(Q_\alpha)$ is the number of blocks fixed by α and so the theorem is proved. □

COROLLARY. *If* G *is a group of automorphisms of a symmetric block design* D, *then the permutation representations of* $G = \langle \alpha, \beta, \ldots \rangle$ *on the points* $\langle P_\alpha, P_\beta, \ldots \rangle$ *and on the blocks* $\langle Q_\alpha, Q_\beta, \ldots \rangle$ *have the same character.*

A well-known property of symmetric designs is given by the following theorem.

THEOREM 2.2. *If* A *is the incidence matrix of a symmetric design* D *with parameters* v,k,λ, *then* A^T *is the incidence matrix of a dual symmetric design (interchanging points and blocks)* D^* *with the same parameters.*

Thus for A we have

$$\text{(2.8)} \qquad \begin{cases} AA^T = (k-\lambda)I + \lambda J, \quad AJ = kJ, \quad JA = kJ, \\ A^TA = (k-\lambda)I + \lambda J, \quad A^TJ = kJ, \quad JA^T = kJ. \end{cases}$$

Note that this implies that any two distinct blocks of D have exactly λ points in common.

3. DIFFERENCE SETS

Let D be a symmetric block design with parameters $b = v$, $r = k$, and λ. We shall suppose that D has a group G of automorphisms of order v which is transitive and regular on the points. Then if we take an arbitrary point P as a "base point", the points $(P)x = P_x$ as x ranges over G consist of all v points of D, each occurring exactly once. This gives a correspondence between the points of D and the elements of G making an arbitrary point P correspond to the identity of G. From theorem 2.1 and its corollary the same will be true of the blocks where taking an arbitrary block B the blocks $(B)x = B_x$ as x ranges over G will consist of all blocks of D each occurring exactly once.

The parameters v,k,λ necessarily satisfy

(3.1) $k(k-1) = \lambda(v-1)$.

We shall identify the points of D with the elements of G, following the correspondence above. Let B be an arbitrary block and consider the k points in D

(3.2) $B = \{d_1, d_2, \ldots, d_k\}, \quad d_i \in G.$

Then for any block Bx

(3.3) $Bx = \{d_1x, d_2x, \ldots, d_kx\}, \quad x \in G.$

Two points r and s will occur together in Bx if for some d_i and d_j we have $d_ix = r$, $d_jx = s$. Here $d_id_j^{-1} = rs^{-1}$. Conversely if $d_id_j^{-1} = rs^{-1}$ we may determine x uniquely by $d_ix = r$ and it will follow that $d_jx = s$. Hence for any $d \neq 1$ there are exactly λ choices $d_id_j^{-1} = d$ with $d_i, d_j \in \{d_1, \ldots, d_k\}$. Similarly with $d \neq 1$ the blocks B and Bd have exactly λ points in common. This means that for exactly λ choices of d_i there is a d_j with $d_i = d_jd$ or $d_j^{-1}d_i = d$.

THEOREM 3.1. *Let* $B = \{d_1, d_2, \ldots, d_k\}$ *be a set of* k *distinct elements in a group* G *of order* v, *and let* $k(k-1) = \lambda(v-1)$. *If either of the conditions* (1) *or* (2) *holds, both will hold.*

(1) *For every* $d \neq 1$ *there are exactly* λ *choices* $d_i, d_j \in B$ *such that* $d_id_j^{-1} = d$.

(2) *For every* $d \neq 1$ *there are exactly* λ *choices* $d_i, d_j \in B$ *such that* $d_j^{-1}d_i = d$.

Then the sets $Bx = \{d_1x, d_2x, \ldots, d_kx\}$ *will be the blocks of a symmetric block design* D *which has* G *as an automorphism group transitive and regular on the points of* D *and also on the blocks of* D.

PROOF. Clearly the v blocks Bx are all of size k. For a fixed d_i, the elements d_ix as x ranges over G give each element of G exactly once, so that each element of G is in exactly k blocks. For the incidence matrix A of the system D of these points and blocks condition (1) is equivalent to $AA^T = (k-\lambda)I + \lambda J$ while condition (2) is equivalent to $A^TA = (k-\lambda)I + \lambda J$ and as these are equivalent to each other the theorem is proved. □

DEFINITION. A set $B = \{d_1, \ldots, d_k\}$ of distinct elements in a group G of order v, where $k(k-1) = \lambda(v-1)$ is called *a difference set* if for any $d \neq 1$ in G there are exactly λ choices $d_i, d_j \in B$ such that $d_id_j^{-1} = d$.

If G is an Abelian group written additively then the condition is on differences $d_i - d_j$, and this is historically the origin of the term difference set.

4. THE MULTIPLIER THEOREM

The residues 0, 2, 3, 4, 8 (mod 11) are an (11,5,2) difference set in the additive group G of residues modulo 11. We check the difference property

$$
\begin{aligned}
&1 \equiv 3 - 2 \equiv 4 - 3, && 6 \equiv 3 - 8 \equiv 8 - 2,\\
&2 \equiv 2 - 0 \equiv 4 - 2, && 7 \equiv 0 - 4 \equiv 4 - 8,\\
&3 \equiv 0 - 8 \equiv 3 - 0, && 8 \equiv 8 - 0 \equiv 0 - 3, \qquad \text{(modulo 11)}\\
&4 \equiv 4 - 0 \equiv 8 - 4, && 9 \equiv 0 - 2 \equiv 2 - 4,\\
&5 \equiv 2 - 8 \equiv 8 - 3, && 10 \equiv 2 - 3 \equiv 3 - 4.
\end{aligned} \tag{4.1}
$$

The corresponding design D is a symmetric design with parameters $(v,k,\lambda) = (11,5,2)$. We list the blocks and the points on them

$$
\begin{aligned}
&B_0: 0,2,3,4,8, && B_6: 6,8,9,10,3,\\
&B_1: 1,3,4,5,9, && B_7: 7,9,10,0,4,\\
&B_2: 2,4,5,6,10, && B_8: 8,10,0,1,5,\\
&B_3: 3,5,6,7,0, && B_9: 9,0,1,2,6,\\
&B_4: 4,6,7,8,1, && B_{10}: 10,1,2,3,7.\\
&B_5: 5,7,8,9,2,
\end{aligned} \tag{4.2}
$$

Here the design D has further automorphisms. Specifically the mapping $x \to tx$ of residues modulo 11 where t is one of 1,3,4,5,9 is an automorphism of D. Since a mapping $x \to tx$ fixes the point 0, from theorem 2.1 it must also fix a block, and in this case the block B_1 is fixed by all these automorphisms. In this case the full group of automorphisms includes still further elements one being given by the permutations

$$(0)(7)(1,2,8)(3,5,6)(4,10,9)(B_0,B_8,B_9)(B_1,B_2,B_6)(B_3)(B_4,B_{10},B_5)(B_7).$$

The full group of automorphisms of D is the simple group $L_2(11)$ of order 660.

It is a remarkable fact that many difference sets lead to designs D with further automorphisms beyond the given group G of order v. We will define the term *multiplier* in this context.

DEFINITION. An integer t is a *multiplier* of the difference set $\{d_1,d_2,\ldots,d_k\}$ in the Abelian group G of order v if the mapping $x \to x^t$ is an automorphism of the design D determined by the difference set.

Note that multipliers are defined over Abelian groups. With G Abelian of order v, a multiplier t must necessarily be such that $x \to x^t$ is an automorphism of G since every element of G must be of the form x^t with x from G, and so (v,t) = 1. Clearly the multipliers form a multiplicative group of residues modulo v.

THEOREM 4.1. *The integer* t *is a multiplier of the Abelian difference set* $\{d_1,d_2,\ldots,d_k\}$ *if and only if* $\{d_1^t,d_2^t,\ldots,d_k^t\} = \{d_1w,d_2w,\ldots,d_kw\}$ *for some* $w \in G$.

PROOF. If t is a multiplier of $B = \{d_1,\ldots,d_k\}$ then $x \to x^t$ maps B into some block $Bw = \{d_1w,d_2w,\ldots,d_kw\}$. Conversely if $\{d_1^t,d_2^t,\ldots,d_k^t\} = \{d_1w,\ldots,d_kw\}$ then $x \to x^t$ takes an arbitrary block $Bu = \{d_1u,\ldots,d_ku\}$ into Bwu^t, and is an automorphism of the design. □

THEOREM 4.2. Multiplier theorem (HALL & RYSER [14]). *Let* $\{d_1,\ldots,d_k\}$ *be a* (v,k,λ) *difference set over an Abelian group* G *of order* v. *Then if* p *is a prime such that* (i) $p|k-\lambda$, (ii) $(p,v) = 1$ *and* (iii) $p > \lambda$, *then* p *is a multiplier of the difference set.*

PROOF. We assume the group G to be written multiplicatively. We shall work with the group ring ZG over the rational integers Z. The elements of the group ring are formal sums $A = \sum_{g\in G} a(g)g$, $a(g) \in Z$. Addition and multiplication are defined by the rules

$$\sum_g a(g)g + \sum_g b(g)g = \sum_g (a(g) + b(g))g,$$

$$\Big(\sum_g a(g)g\Big)\Big(\sum_g b(g)g\Big) = \sum_k \Big(\sum_{gh=k} a(g)b(h)\Big)k.$$

With these rules ZG is an associative ring with identity.

With the difference set $\{d_1,d_2,\ldots,d_k\}$ we associate the element $\theta(d)$ of the group ring

$$\theta(d) = d_1 + d_2 + \ldots + d_k. \tag{4.3}$$

We also write, using a symbolic notation, for any integer t, defining $\theta(d^t)$

by

$$\theta(d^t) = d_1^t + d_2^t + \ldots + d_k^t. \tag{4.4}$$

Then from theorem 4.1 the proof of theorem 4.2 reduces to proving for some $w \in G$

$$\theta(d^p) = w\theta(d). \tag{4.5}$$

Let us also define the element T of ZG by

$$T = \sum_{x \in G} x. \tag{4.6}$$

With this notation the fact that $\{d_1,\ldots,d_k\}$ is a (v,k,λ) difference set takes the form, writing $k-\lambda = n$,

$$\theta(d)\theta(d^{-1}) = (k-\lambda) + \lambda T = n + \lambda T. \tag{4.7}$$

Here by $k-\lambda$ we mean $(k-\lambda)1$ where 1 is the identity of G. For in the left-hand side of (4.7) the identity appears k times as $d_i d_i^{-1}$, $i=1,\ldots,k$, and every other $d \in G$ appears exactly λ times as $d_i d_j^{-1}$. Since the identity is one of the elements of T, its k occurrences are counted as $(k-\lambda) + \lambda$, and the λ occurrences of every $d \neq 1$ are counted in λT.

Since the binomial coefficients $\binom{p}{j}$, $j=1,\ldots,p-1$ are multiples of the prime p we always have $(A+B)^p = A^p + B^p + pR$ in ZG with R some element of ZG. Hence

$$\theta(d)^p = d_1^p + d_2^p + \ldots + d_k^p + pW = \theta(d^p) + pW. \tag{4.8}$$

Multiplying (4.7) by $\theta(d)^{p-1}$ we have

$$\theta(d)^p\theta(d^{-1}) = n\theta(d)^{p-1} + \lambda\theta(d)^{p-1}T. \tag{4.9}$$

Here since $xT = T$ for any $x \in G$ it follows that $\theta(d)T = kT$, and (4.9) becomes

$$\theta(d)^p\theta(d^{-1}) = n\theta(d)^{p-1} + \lambda(k^{p-1}-1)T + \lambda T. \tag{4.10}$$

Now p divides $n = k-\lambda$. If p does not divide k then p divides $k^{p-1}-1$, while if p divides k, then also p divides λ, so that in all cases p divides $\lambda(k^{p-1}-1)$. Thus (4.10) takes the form

$$\theta(d)^p\theta(d^{-1}) = pV + \lambda T \tag{4.11}$$

with some V in ZG. Combining (4.8) and (4.11) we have

$$\theta(d^p)\theta(d^{-1}) = pS + \lambda T. \tag{4.12}$$

If $x_1,\ldots,x_v$ are the elements of G then the left-hand side takes the form $\sum a_i x_i$ where the a_i are non-negative integers such that

$$\sum_i a_i = k^2. \tag{4.13}$$

Comparison with the right-hand side shows

$$a_i \equiv \lambda \pmod{p}, \qquad i=1,\ldots,v. \tag{4.14}$$

Also since we have assumed $p > \lambda$ it follows that $a_i \geq \lambda$ in every case. Thus if $S = \sum_i s_i x_i$ we have from (4.12)

$$a_i = ps_i + \lambda \tag{4.15}$$

so that $s_i \geq 0$ in every case and also

$$k^2 = \sum_i a_i = \sum_i ps_i + \lambda v. \tag{4.16}$$

But since $k(k-1) = \lambda(v-1)$ we have $k^2-\lambda v = k-\lambda = n$ so that

$$p \sum_i s_i = n, \qquad s_i \geq 0. \tag{4.17}$$

As a consequence

$$pST = p \sum_i s_i T = nT. \tag{4.18}$$

Applying the automorphism $x \to x^p$ of G to the relation (4.7) gives

$$\theta(d^p)\theta(d^{-p}) = n + \lambda T. \tag{4.19}$$

Applying the automorphism $x \to x^{-1}$ of G to (4.12) gives

$$\theta(d^{-p})\theta(d) = pS^* + \lambda T \tag{4.20}$$

where $S^* = \sum_i s_i x_i^{-1}$.

The product of the left-hand sides of (4.7) and (4.19) is the same as the product of the left-hand sides of (4.12) and (4.20). Equating the right-hand sides gives

$$(4.21) \qquad (pS + \lambda T)(pS^* + \lambda T) = (n + \lambda T)^2.$$

Since $pST = nT$ and $pS^*T = nT$ this simplifies to

$$(4.22) \qquad p^2 SS^* = n^2$$

or

$$(4.23) \qquad p^2 \sum_i s_i x_i \sum_j s_j x_j^{-1} = n^2.$$

Since the coefficients s_i are all non-negative we cannot have $s_i > 0$ and $s_j > 0$ for $i \neq j$ since this would give $x_i x_j^{-1} \neq 1$ a positive coefficient on the left of (4.23). Hence only one s_i is different from 0 and as $p\sum s_i = n$ we conclude that for some $w \in G$

$$(4.24) \qquad pS = nw.$$

Now (4.12) takes the simpler form

$$(4.25) \qquad \theta(d^p)\theta(d^{-1}) = nw + \lambda T;$$

multiplying this by $\theta(d)$ we have

$$(4.26) \qquad \theta(d^p)\theta(d^{-1})\theta(d) = nw\theta(d) + \lambda\theta(d)T,$$

which becomes

$$(4.27) \qquad \theta(d^p)(n+\lambda T) = nw\theta(d) + \lambda kT$$

or

$$(4.28) \qquad n\theta(d^p) + \lambda kT = nw\theta(d) + \lambda kT,$$

whence

$$(4.29) \qquad \theta(d^p) = w\theta(d).$$

By theorem 4.1 this proves that p is a multiplier and completes the proof of theorem 4.2. □

This theorem has been very useful in proving that certain difference sets do not exist and in constructing others when they do exist. In this connection the following theorem is useful.

THEOREM 4.3. *If* t *is a multiplier of the design* $D(v,k,\lambda)$ *there is a block fixed by the multiplier. If* $(v,k) = 1$ *there is a block fixed by every multiplier.*

PROOF. The automorphism $x \to x^t$ given by the multiplier fixes the identity element of G. Since this is one of the points of the design, by theorem 2.1 there is a block fixed by this automorphism. Let $\{d_1,\ldots,d_k\}$ be the difference set and write $y = d_1d_2\ldots d_k$. Then in the block Bs the product of the k elements is ys^k. If (v,k) = 1 there is exactly one x with $yx^k = 1$ in G and clearly the block Bx will be fixed by every multiplier. □

Consider the difference set with v = 111, k = 11, λ = 1. Here $k-\lambda = n = 10$ and so 2 and 5 are multipliers. By theorem 4.3 there is a block B fixed by both of these multipliers. If c is a point of this block then c, c^2, c^4, c^5 are all in this block. As $c^2c^{-1} = c^5c^{-4} = c$ and $\lambda = 1$ this is possible only if $c^5 = c^2$ and $c^4 = c$ whence $c^3 = 1$. But in G there are only three elements satisfying $c^3 = 1$ and so we cannot find a block of 11 distinct elements of this kind. Hence no difference set exists for these parameters.

If v = 73, k = 9, λ = 1, as $n = k-\lambda = 8$, p = 2 is a multiplier. Let us write G in additive form as the group of residues modulo 73. Then in the block B fixed by the multiplier let c be an element not the 0 residue. Then the difference set will include

$$c,\ 2c,\ 4c,\ 8c,\ 16c,\ 32c,\ 64c,\ 55c,\ 37c \pmod{73}.$$

These will be all 9 elements of the difference set and without loss of generality we may take c = 1 to obtain the (73,9,1) difference set

(4.30) $$1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 37,\ 55,\ 64 \pmod{73}.$$

In theorem 4.2 the condition (i) $p \mid k-\lambda$ is the source of the multiplier, while condition (ii) (p,v) = 1 is clearly necessary for p to be a multiplier. But in every known case the condition (iii) $p > \lambda$ appears to be unnecessary, though it is required in the proof using (4.15) to show $s_i \geq 0$. Indeed for every known difference set in which G is cyclic, there is a prime dividing $k-\lambda$ but not v and every such prime is a multiplier. There are however Abelian difference sets without multipliers. For example there is an Abelian difference set with parameters (16,6,2) the group G being the elementary Abelian group of order 16.

5. THE KNOWN DIFFERENCE SETS

There are several families of difference sets known. Most of these

depend on arithmical properties of residues modulo primes or on finite fields.

Type S. (Singer difference sets [23]). These are hyperplanes in the n-dimensional projective geometry PG(n,q) over GF(q). The parameters are

$$v = \frac{q^{n+1}-1}{q-1}, \quad k = \frac{q^{n}-1}{q-1}, \quad \lambda = \frac{q^{n-1}-1}{q-1}.$$

Type Q. (Quadratic residues in GF(q), q = 3 (mod 4)).

$$v = q = p^{r} = 4t-1, \quad k = 2t-1, \quad \lambda = t-1.$$

Type H_6. (p is a prime of the form $p = 4x^2+27$). There will exist a primitive root modulo p such that $\mathrm{Ind}_r(3) \equiv 1 \pmod 6$. The (p-1)/2 residues a_i such that $\mathrm{Ind}_r(a_i) \equiv 0, 1$ or 3 (mod 6) will form a difference set with parameters $v = p = 4t-1$, $k = 2t-1$, $\lambda = t-1$.

Type T. (Twin primes). Let p and q = p+2 be primes. Let r be a number such that r is a primitive root of p and also of q. Then r^i (mod pq) i=1,...,(p-1)(q-1)/2 and 0,q,...,(p-1)q (mod pq) form a difference set with $v = pq = 4t-1$, $k = 2t-1$, $\lambda = t-1$.

Type B. (Biquadratic residues of primes $p = 4x^2+1$, x odd). Here $v = p = 4x^2+1$, $k = x^2$, $\lambda = (x^2-1)/4$.

Type B_{Q_2}. (Biquadratic residues and zero modulo primes $p = 4x^2+9$, x odd). Here $v = 4x^2+9$, $k = x^2+3$, $\lambda = (x^2+3)/4$.

Type O. (Octic residues of primes $p = 8a^2+1 = 64b^2+9$ with a, b both odd). Here $v = p$, $k = a^2$, $\lambda = b^2$.

Type O_0. (Octic residues and zero for primes $p = 8a^2+49 = 64b^2+441$, a odd, b even). Here $v = p$, $k = a^2+6$, $\lambda = b^2+7$.

Type W_4. (A generalization of T developed by WHITEMAN [27]). Let p be a prime $p \equiv 1 \pmod 4$ and let q = 3p+2 also be a prime. Suppose also that $pq = v = 1+4x^2$ with x odd. Then take r to be a primitive root of both p and q. Writing d = (p-1)(q-1)/4 the residues $1,r,r^2,\ldots,r^{d-1}$, 0,q,2q,...,(p-1)q (mod pq) are a difference set with $v = pq$, $k = (v-1)/4$, $\lambda = (v-5)/16$.

Type GMW. (GORDON, MILLS & WELCH [9]). The parameters are the same as those of the Singer type.

$$v = \frac{q^{n+1}-1}{q-1}, \quad k = \frac{q^{n}-1}{q-1}, \quad \lambda = \frac{q^{n-1}-1}{q-1}.$$

Here if we can write n+1 in the form n+1 = mM with $m \geq 3$ and if M is the product of r prime numbers, not necessarily distinct, then there are at least 2^r inequivalent difference sets with these parameters.

Type H(2). $v = 2^{2m}$, $k = 2^{2m-1} - 2^{m-1}$, $\lambda = 2^{2m-2} - 2^{m-1}$. Here G is the direct product of m groups of order 4 (some may be the cyclic group, other the four group). These difference sets and designs are most easily described by their relation to Hadamard matrices, as will be done in the next section.

L. BAUMERT [1] has listed the known 85 cyclic difference sets for which $3 \leq k \leq 100$. Most of these are special cases of the types listed above. There are 74 different possible parameters v, k, λ and for no other parameters with k in this range is a cyclic difference set possible. There is a cyclic difference set with v = 133, k = 33, λ = 8 but in all other cases the parameters are those of the listed types. For the projective planes with $v = n^2+n+1$, k = n+1, λ = 1 the writer has shown that the solution is unique when n = 2, 3, 4, 5, 7, 9, 11, 13, 16, 25, 27, 32, and there is certainly a Singer difference set whenever $n = q = p^r$ is a prime power, but for other prime powers in this range it is conceivable that other difference sets exist.

Cyclic difference sets

v = 133, k = 33, λ = 3

(5.1) 1, 4, 5, 14, 16, 19, 20, 21, 25, 38, 54, 56, 57, 64, 66, 70, 76, 80, 83, 84, 91, 93, 95, 98, 100, 101, 105, 106, 114, 123, 125, 126, 131 (mod 133).

For v = 121, k = 4, λ = 13 there is the Singer system of 3 spaces in

121A: (5.2) 1, 3, 4, 7, 9, 11, 12, 13, 21, 25, 27, 33, 34, 36, 39, 44, 55, 63, 64, 67, 68, 70, 71, 75, 80, 81, 82, 83, 85, 89, 92, 99, 102, 103, 104, 108, 109, 115, 117, 119.

There are also three other difference sets with these parameters

121B: 1, 3, 4, 5, 9, 12, 13, 14, 15, 16, 17, 22, 23, 27, 32, 34, 36, 39, 42, 45, 46, 48, 51, 64, 66, 69, 71, 77, 81, 82, 85, 86, 88, 92, 96, 102, 108, 109, 110, 117.

121C: 1, 3, 4, 7, 8, 9, 12, 21, 24, 25, 26, 27, 34, 36, 40, 43, 49,
(5.3) 63, 64, 68, 70, 71, 72, 75, 78, 81, 82, 83, 89, 92, 94, 95, 97,
102, 104, 108, 112, 113, 118, 120.

121D: 1, 3, 4, 5, 7, 9, 12, 14, 15, 17, 21, 27, 32, 36, 38, 42, 45,
46, 51, 53, 58, 63, 67, 68, 76, 79, 80, 81, 82, 83, 96, 100, 103,
106, 107, 108, 114, 115, 116, 119.

For the parameters $v = 127$, $k = 63$, $\lambda = 31$ there are six non-isomorphic difference sets, three corresponding to the listed type, and three others.

127A: Type Q.
1, 2, 4, 8, 9, 11, 13, 15, 16, 17, 18, 19, 21, 22, 25, 26, 30,
31, 32, 34, 35, 36, 37, 38, 41, 42, 44, 47, 49, 50, 52, 60,
61, 62, 64, 68, 69, 70, 71, 72, 73, 74, 76, 79, 81, 82, 84,
87, 88, 94, 98, 99, 100, 103, 104, 107, 113, 115, 117, 120,
121, 122, 124.

127B: Type H_6.
1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 19, 20, 23, 24, 25,
27, 28, 32, 33, 38, 40, 46, 47, 48, 50, 51, 54, 56, 57, 61,
63, 64, 65, 66, 67, 73, 75, 76, 77, 80, 87, 89, 92, 94, 95,
96, 97, 100, 101, 102, 107, 108, 111, 112, 114, 117, 119,
122, 123, 125, 126.

127C: Singer-hyperplanes in PG(6,2).
1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 15, 16, 17, 18, 24, 27, 28,
29, 30, 31, 32, 34, 36, 39, 47, 48, 51, 54, 56, 58, 60, 61,
62, 64, 65, 67, 68, 71, 72, 77, 78, 79, 83, 87, 89, 94, 96,
(5.4) 97, 99, 102, 103, 105, 107, 108, 112, 113, 115, 116, 117,
120, 121, 122, 124.

127D: 1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 16, 17, 18, 19, 24, 25,
26, 27, 28, 31, 32, 34, 35, 36, 38, 47, 48, 50, 51, 52, 54,
56, 61, 62, 64, 65, 67, 68, 70, 72, 73, 76, 77, 79, 81, 87,
89, 94, 96, 97, 100, 102, 103, 104, 107, 108, 112, 115, 117,
121, 122, 124.

127E: 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 17, 18, 19, 20, 24,
25, 27, 29, 30, 32, 33, 34, 36, 38, 39, 40, 48, 50, 51, 54,
55, 58, 59, 60, 64, 65, 66, 68, 71, 72, 73, 76, 77, 78, 80,
83, 89, 91, 93, 96, 99, 100, 102, 105, 108, 109, 110, 113,
116, 118, 120.

127F: 1, 2, 3, 4, 5, 6, 8, 10, 11, 12, 16, 19, 20, 21, 22, 24, 25, 27, 29, 32, 33, 37, 38, 39, 40, 41, 42, 44, 48, 49, 50, 51, 54, 58, 63, 64, 65, 66, 69, 73, 74, 76, 77, 78, 80, 82, 83, 84, 88, 89, 95, 96, 98, 100, 102, 105, 108, 111, 116, 119, 123, 125, 126.

Two difference sets for $v = 36$, $k = 15$, $\lambda = 6$ have been given by P.K. MENON [18]. The non-Abelian group of order 6, isomorphic to the symmetric group S_3 can be given by 1, a, a^2, b, ab, a^2b where $a^3 = 1$, $b^2 = 1$, $ba^2 = ab$.

Taking $G = S_3 \times S_3$ the 15 elements

$$
\begin{array}{lllll}
(1,1), & (1,b), & (b,1), & (b,ab), & (ab,b), \\
(a,a^2), & (a,ab), & (ab,1), & (ab,a^2b), & (a^2b,ab), \\
(a^2,a), & (1,a^2b), & (a^2b,1), & (a^2b,b), & (b,a^2b),
\end{array} \tag{5.5}
$$

form the difference set. This is one of the few known difference sets for which G is non-Abelian.

Also for $G = Z_6 \times Z_6$ where Z_6 is the cyclic group of order 6, taken here as residues modulo 6

$$
\begin{array}{lllll}
(0,0), & (0,1), & (1,0), & (1,3), & (3,1), \\
(2,4), & (0,3), & (3,0), & (3,5), & (5,3), \\
(4,2), & (0,5), & (5,0), & (5,1), & (1,5).
\end{array} \tag{5.6}
$$

The writer has found a simpler form for such a difference set

$$
\begin{array}{lllll}
(1,1), & (2,2), & (3,3), & (4,4), & (5,5), \\
(0,1), & (0,2), & (0,3), & (0,4), & (0,5), \\
(1,0), & (2,0), & (3,0), & (4,0), & (5,0).
\end{array} \tag{5.7}
$$

These are examples of difference sets of Hadamard types.

6. GENERAL THEORY OF DIFFERENCE SETS

Let G be a finite Abelian group of order v. Then from the theory of representation of finite groups [8] it is well-known that over the complex field the irreducible representations are all of degree one. This is to say that if for each $x \in G$ there is a non-singular matrix $M(x)$, and if $M(xy) = M(x)M(y)$, then there is a matrix S such that $S^{-1}M(x)S = A(x)$ and $A(x)$ is

a diagonal matrix for all $x \in G$. Thus $A(x) = \chi_1(x) + \ldots + \chi_m(x)$ where for $x \in G$, $\chi_i(x)$ is a complex number and $\chi_i(xy) = \chi_i(x)\chi_i(y)$, $i=1,\ldots,m$. We call these χ's characters. Since $\chi(1) = 1$, each character $\chi(x)$ is some r-th root of unity if $x^r = 1$ and so for all $x \in G$, $\chi(x)$ is a v-th root of unity. The characters themselves may be multiplied, defining $(\chi_i\chi_j)(x) = \chi_i(x)\chi_j(x)$, all $x \in G$. Under this rule the characters themselves form a group which is in fact isomorphic to G. In particular there are exactly v distinct characters. The character χ_0 with the property $\chi_0(x) = 1$ for all $x \in G$ is called the *principal character*.

The characters may readily be extended to the group ring ZG, where if

$$A = \sum_{g \in G} a(g) \cdot g \tag{6.1}$$

we put

$$\chi(A) = \sum_{g \in G} a(g)\chi(g). \tag{6.2}$$

Clearly for each character χ, $A \to \chi(A)$ is a ring homomorphism of ZG into the complex numbers. A simple but useful property involving all characters is

$$\sum_{\chi} \chi(g) = \begin{cases} v & \text{if } g = 1 \\ 0 & \text{if } g \neq 1. \end{cases} \tag{6.3}$$

A powerful application of this, if A is given by (6.1) is

$$\sum_{\chi} \chi(Ag^{-1}) = va(g). \tag{6.4}$$

Another simple property is

$$\sum_{g \in G} \chi(g) = \begin{cases} v & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0. \end{cases} \tag{6.5}$$

If $\{d_1, d_2, \ldots, d_k\}$ is a difference set in G let us write

$$\begin{aligned} D &= d_1 + d_2 + \ldots + d_k, \\ D^t &= d_1^t + d_2^t + \ldots + d_k^t, \quad t \text{ any integer}, \\ T &= \sum_{g \in G} g \,. \end{aligned} \tag{6.6}$$

Then (4.7) takes the form

(6.7) $$DD^{-1} = n + \lambda T.$$

Hence if χ is any non-principal character of G, then

(6.8) $$\chi(D)\chi(D^{-1}) = n.$$

Here $\chi(D)$ is an algebraic integer in some subfield of the field of v-th roots of unity and $\chi(D^{-1})$ is its complex conjugate. Thus the existence of a difference set is related to the factorization of n in various cyclotomic fields.

An application of these methods is a proof of the following result due to MANN [17]. His original proof was more complicated.

THEOREM 6.1. *A difference set with* $1 < k < v-1$ *over an elementary Abelian 2-group necessarily has parameters*

$$v = 2^{2t+2}, \quad k = 2^{2t+1} - 2^t, \quad \lambda = 2^{2t} - 2^t$$

or the complementary parameters

$$v = 2^{2t+2}, \quad k = 2^{2t+1} + 2^t, \quad \lambda = 2^{2t} + 2^t.$$

PROOF. Let D be a difference set over the elementary Abelian group G of order 2^r. Then since $g^{-1} = g$ for every $g \in G$, in (6.7) we will have $D^{-1} = D$ and so

(6.9) $$D^2 = n + \lambda T.$$

If χ is any non-principal character of G then

(6.10) $$\chi(D)^2 = n.$$

Now $\chi(g) = \pm 1$ for every $g \in G$ and so $\chi(D)$ is a rational integer. Thus

(6.11) $$n = s^2, \quad \chi(D) = \pm s, \quad \chi \neq \chi_0, \quad \chi_0(D) = k.$$

With

(6.12) $$D = \sum_g a(g)g$$

k of the a(g) are +1 and v-k are 0. Using (6.4)

(6.13) $$2^r a(g) = \sum_\chi \chi(Dg^{-1}).$$

From (6.11) this gives for some integer c(g)

(6.14) $2^r a(g) = k + c(g)s.$

Taking some x for which a(x) = 0 we have

(6.15) $0 = k + c(x)s$

so that s divides k. Let us write

(6.16) $k = hs.$

Taking some y for which a(y) = 1 we have

(6.17) $2^r = k + c(y)s = hs + c(y)s$

whence s divides 2^r so that $s = 2^t$ for some exponent t. Here

(6.18) $\lambda = k-n = hs - s^2 = 2^t h - 2^{2t}.$

Also from $k(k-1) = \lambda(v-1)$ we have

(6.19) $2^t h(2^t h-1) = (2^t h-2^{2t})(2^r-1).$

This simplifies to

(6.20) $h^2 - 2^{r-t}h = - 2^r + 1,$

which gives

(6.21) $(h - 2^{r-t-1})^2 = 2^{2r-2t-2} - 2^r + 1.$

Here $2^{2r-2t-2} \geq 2^r$ so that $r \geq 2t+2$. If $r = 2t+2$ then $h = 2^{r-t-1} \pm 1 = 2^{t+1} \pm 1$ and $k = 2^t h = 2^{2t+1} \pm 2^t$, $\lambda = k-n = 2^{2t} \pm 2^t$ and $v = 2^r = 2^{2t+2}$, the parameters of the theorem. If $r > 2t+2$, then $2^{2r-2t-2} - 2^r + 1 \geq 1 + 2^r$, and also $2^{2r-2t-2} - 2^r + 1 \equiv 1 \pmod{2^r}$. But if $z^2 \equiv 1 \pmod{2^r}$ then $z \equiv \pm 1 \pmod{2^{r-1}}$ and if $z \neq \pm 1$, then $|z| \geq 2^{r-1} - 1$. Thus (6.21) yields

(6.22) $|h - 2^{r-t-1}| \geq 2^{r-1} - 1.$

If $h - 2^{r-t-1} \geq 2^{r-1} - 1$ then $h \geq r^{r-1}$ and $k = 2^t h \geq 2^{r+t-1}$, but as $v = 2^r > k$ this is possible only if $t = 0$. On the other hand if $2^{r-t-1} - h \geq 2^{r-1} - 1$, then $2^{r-t-1} \geq 2^{r-1}$ and again this is possible only if $t = 0$. In either case $t = 0$ and $k = h$. Then (6.21) becomes

(6.23) $(k - 2^{r-1})^2 = (2^{r-1} - 1)^2,$

so that $k-2^{r-1} = \pm(2^{r-1}-1)$ giving $k = 1$ or $k = 2^r-1 = v-1$ the trivial solutions excluded by assumption. □

The difference sets of theorem 6.1 all exist. They are special cases of Hadamard difference sets, so called because of their relation to Hadamard matrices. An Hadamard matrix $H = [h_{ij}]$ is a square matrix of order N with $h_{ij} = \pm 1$ which satisfies

$$HH^T = H^TH = NI. \tag{6.24}$$

The matrices

$$\begin{bmatrix} 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix} \tag{6.25}$$

are Hadamard matrices of orders 1, 2, 4 respectively. It is easy to show that the order of an Hadamard matrix is 1, 2, or 4m for m=1,2,... and it is conjectured that Hadamard matrices exist for all these orders. At present the first undecided order is 188 with m = 47.

For square orders $4m^2$, a symmetric block design with $v = 4m^2$, $k = 2m^2-m$, $\lambda = m^2-m$ or its complement with $v = 4m^2$, $k = 2m^2+m$, $\lambda = m^2+m$ can be used to determine a Hadamard matrix of order $N = 4m^2$ by putting $h_{ij} = +1$ if the j-th point is in the i-th block and putting $h_{ij} = -1$ otherwise. And it is not difficult to show that if a Hadamard matrix of order v has exactly k elements which are +1 in every row, the rows will determine a symmetric block design with the parameters above. The third matrix in (6.25) of order 4 is of this type with the trivial design $v = 4$, $k = 1$, $\lambda = 0$.

In particular a difference set in a group G of order $v = 4m^2$ with $k = 2m^2 \pm m$, $\lambda = m^2 \pm m$ determines a Hadamard matrix of this kind. The difference sets with $v = 36$, $k = 15$, $\lambda = 6$ in (5.5), (5.6) and (5.7) are of this kind.

If H and K are Hadamard matrices of orders N and M respectively then the Kronecker product $H \times K$ (sometimes called the direct product or tensor product) is also a Hadamard matrix of order MN. Here

$$(6.26)\qquad H \times K = \begin{bmatrix} h_{11}K & h_{12}K & \dots & h_{1N}K \\ h_{21}K & h_{22}K & \dots & h_{2N}K \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ h_{N1}K & h_{N2}K & \dots & h_{NN}K \end{bmatrix}.$$

The proof of the following theorem is straightforward and will be omitted. It is due to MENON [18] who, however, did not recognize the relation to Hadamard matrices.

THEOREM 6.2. *If* H *and* K *are Hadamard matrices given by difference sets over groups* G_1 *and* G_2 *respectively, then* $H \times K$ *is a Hadamard matrix given by a difference set over* $G_1 \times G_2$. *If* D_1 *is the difference set for* H *over* G_1 *and* D_2 *for* K *over* G_2 *then in the direct product* $G = G_1 \times G_2 = (G_1, G_2)$ *the difference set* D *is the union of* (D_1, D_2) *and* $(\overline{D}_1, \overline{D}_2)$ *where* $\overline{D}_i$, $i=1,2$, *is the complement of* D_i *in* G_i.

COROLLARY. *There are difference sets with* $v = 4m^2$, $k = 2m^2 \pm m$, $\lambda = m^2 \pm m$ *when* $m = 2^{a+b-1}3^b$.

PROOF. This follows from the theorem since such sets exist for $v = 4$ and $v = 36$. □

The designs with $v = 2^{2t+2}$ have been extensively investigated, in particular by BLOCK [2] and recently by KANTOR [15].

In a finite field GF(q), $q = p^r$, p a prime, the multiplicative group H of non-zero elements is cyclic of order p^r-1. If $p^r-1 = ef$ the e-th powers of elements form a subgroup of H of order f and index e in H. If D is a difference set over G, the additive group of GF(q), it may happen that the e-th powers are multipliers of D. Several of the types listed in section 5 are of this kind.

If g is a primitive root of GF(q) the e-th power cyclotomic numbers are the numbers (i,j) where (i,j) is defined to be the number of solutions g^s of

$$(6.27)\qquad g^2 + 1 = g^t, \quad s \equiv i \pmod{e}, \quad t \equiv j \pmod{e}.$$

If D has the e-th powers of elements of GF(q) as multipliers, then (considering D to be the block fixed by these multipliers) D will consist of one or

more cosets of H^e and possibly the zero element. A knowledge of the cyclotomic numbers (i,j) will determine the number of differences in each coset of H^e, and so will determine which combinations will give a difference set. The author [13] has shown that the cyclotomic numbers (i,j) may be determined by the character table of the group G^* of transformations $x \to a^e x+b$, $a \neq 0$ where G^* is of order $p^r f$. For e = 2, 4, 6, 8 difference sets of types Q, B, B_0, H_6, O, O_0 exist when $q = p^r$ satisfies the appropriate conditions. Except for the case Q where e = 2, arithmetical considerations show that for $q = p^r$ the conditions are only satisfied when r = 1 and q = p is a prime. This was shown by the writer for e = 4, 6, and by STORER [24] also for e = 8.

The multiplier theorem can be generalized, though the generalizations would be trivial if the condition $p > \lambda$ could be dropped. One such generalization is

THEOREM 6.3. *Let* D *be a difference set of* k *elements in the Abelian group* G *of order* v. *Let* $n_1 = p_1 p_2 \ldots p_s$ *be a divisor of* $n = k-\lambda$ *where* $p_1, \ldots, p_s$ *are distinct primes. If* $(n_1, v) = 1$, $n_1 > \lambda$ *and if* t *is an integer such that* $t \equiv p_i^{e_i} \pmod{v}$ *for an appropriate power* $p_i^{e_i}$, i=1,...,s, *then the automorphism* α *of* G *defined by* $x \to x^t$ *is a multiplier of the difference set.*

The proof is almost identical with the proof of the multiplier theorem. In other cases for some divisor w of v and for a group G^* of order w which is a homomorphic image of G, it may be possible to find a multiplier t with $\theta^*(d^t) = g^*\theta^*(d)$ holding in G^*, the asterisks denoting homomorphic images. Such a t is called a w-*multiplier*. For example with v = 177, k = 33, λ = 6 it can be shown that 3 is a multiplier for w = 59 and this can be used to show that there is no difference set. There are also non-numerical multipliers α, where α is an automorphism of G which is also an automorphism of the v-k-λ design. This concept was introduced by BRUCK [4] but no multiplier theorem has been found for these.

It is conjectured that conditions (i) $p|k-\lambda$, (ii) (p,v) = 1 are sufficient for p to be a multiplier, and the condition (iii) $p > \lambda$ is unnecessary If conditions (i) and (ii) are not sufficient for what values of v will p fail to be a multiplier? R. MCFARLAND [16] has proved a theorem which sheds some light on this question.

He defines a quantity M(m) for every positive integer m as follows: $M(1) = 1$, $M(2) = 7$, $M(3) = 3 \cdot 11 \cdot 13$, $M(4) = 2 \cdot 3 \cdot 7 \cdot 31$. For $m \geq 5$ let

$u = (m^2-m)/2$ and let p be a prime divisor of m with p^e the highest power of p dividing m. Then if m is not a square let M(m) be the product of the distinct odd prime factors of

$$(6.28) \qquad m, M(m^2/p^{2e}), p-1, p^2-1, \ldots, p^u-1.$$

If m is a square let M(m) be the product of the distinct prime factors in (6.28), including 2.

THEOREM 6.4. (McFARLAND). *Let* D *be a difference set with parameters* (v,k,λ,n) *in an Abelian group* G *of order* v *and exponent* v^*. *Let*

$$n_1 | n, \qquad (n_1, v) = 1, \quad n_1 = p_1^{e_1} \ldots p_s^{e_s}$$

for some integer n_1 *where the* p_i's *are distinct primes. Suppose there are integers* $t, f_1, \ldots, f_s$ *such that*

$$t \equiv p_1^{f_1} \equiv \ldots \equiv p_s^{f_s} \pmod{v^*}.$$

If either

$$n_1 > \lambda \quad \textit{or} \quad (M(n/n_1), v) = 1$$

then t *is a multiplier of* D.

There are a number of results based on the factorization (6.8) of n in various cyclotomic subfields of the v-th roots of unity. These tend to be highly technical and depend on the theory of the prime ideal factorizations in these fields. Nevertheless, many of the consequences can be described in relatively simple terms. Most of these results are due to work of MANN [17], TURYN [25,26] and YAMAMOTO [28].

These results are best described by some special terminology. If a, b, c are integers ($c \geq 0$) and a^c divides b while a^{c+1} does not, then a^c is said to *strictly divide* b. Let p be a prime and let p^e strictly divide w, so that $w = p^e w_1$ with $(p, w_1) = 1$. If there exists an integer $f > 0$ such that $p^f \equiv -1 \pmod{w_1}$ then p is said to be *self-conjugate modulo* w. If all the prime divisors of an integer m are self-conjugate modulo w, then m is said to be *self-conjugate modulo* w.

THEOREM 6.5. (MANN [17]). *Let* $w > 1$ *be a divisor of* v *and assume a non-trivial* v,k,λ *difference set exists with* w*-multiplier* $t \geq 1$. *Let* p *be a prime divisor of* n *for which* $(p,w) = 1$. *If there exists an integer* $f \geq 0$ *such that* $tpf \equiv -1 \pmod{w}$, *then* n *is strictly divisible by an even power of* p. *If* v^* *is the exponent of* G *and* $v^* = w$, *then there is only the trivial difference set with* $k = v$.

The BRUCK-RYSER-CHOWLA theorem [5,6] asserts that for the existence of a symmetric design with parameters v, k, λ it is necessary that

(i) *if* v *is even,* $n = k-\lambda$ *is a square;*
(ii) *if* v *is odd there exists a solution in integers* x, y, z *not all zero of*

$$x = ny + (-1)^{(v-1)/2}\lambda z^2.$$

Condition (i) was first found by SCHÜTZENBERGER [22].

If there is a v, k, λ difference set then further equations of this type must be solvable.

THEOREM 6.6. (HALL & RYSER [14]). *If there is a cyclic* v, k, λ *difference set then the following equation has solutions in integers* x, y, z *not all zero*

$$x^2 = ny^2 + (-1)^{(w-1)/2}wz^2 \tag{6.29}$$

where w *is any odd divisor of* v.

THEOREM 6.7. (YAMAMOTO [28]). *If there is a* v, k, λ *Abelian difference set, if* q *is an odd divisor of* v, *and if* r *is a prime such that* r^e *strictly divides* n, *then the following equation is solvable in integers* x, y, z *not all zero*

$$x^2 = r^e y^2 + (-1)^{(q-1)/2}qz^2. \tag{6.30}$$

THEOREM 6.8. (TURYN [26]). *Assume a non-trivial Abelian* v, k, λ *difference set exists. Let* m^2 *divide* n *and suppose that* $m > 1$ *is self conjugate modulo* w *for some divisor* $w > 1$ *of* v. *If* $(m,w) > 1$ *then* $m \leq v/w$. *If* $(m,w) > 1$ *then* $m \leq 2^{r-1}v/w$, *where* r *is the number of distinct prime factors of* (m,w).

THEOREM 6.9. (MANN [17]). *If* $p \mid (v,n)$, *and if* $v = p^e v_1$, *and* $p^f \equiv -1 \pmod{v_1}$ *for some* $f \geq 0$ *there is no cyclic* v, k, λ *difference set.*

THEOREM 6.10. (TURYN [26]). *There is no cyclic difference set with* $v = 4m^2$, $k = 2m^2 \pm m$, $\lambda = m^2 \pm m$ *if* m *is a prime power.*

Most of these are non-existence theorems. The author [12] in 1956 studied cyclic difference sets with $3 \le k \le 50$ and was able to determine existence or non-existence in all but 12 cases whose parameters are given here:

(6.31)

v	k	λ	n	v	k	λ	n
45	12	3	9	120	35	10	25
36	15	6	9	288	42	6	36
96	20	4	16	100	45	20	25
64	28	12	16	208	46	10	36
175	30	5	25	189	48	12	36
171	35	7	28	176	50	14	36

These 12 cases in part inspired the efforts to find non-existence theorems. Theorems 6.9 and 6.10 exclude all of these except $(v,k,\lambda,n) = 171,35,7,28$ which is ruled out by theorem 6.5 with $p = 2$, $t = 1$ and the congruence $2^9 \equiv -1 \pmod{171}$ with $w = v^* = v$, and $(v,k,\lambda,n) = 120,35,10,25$ which is ruled out by theorem 6.8 with $m = 5$, $w = 30$ since $5 \equiv -1 \pmod 6$, $(m,w) = 5$ and so $r = 1$, but we do not have $5 \le 2^0 \cdot 120/30 = 4$.

REFERENCES

[1] BAUMERT, L.D., *Cyclic difference sets*, Lecture Notes in Mathematics 182, Springer-Verlag, Berlin etc., 1971.

[2] BLOCK, R.E., *Transitive groups of collineations of certain designs*, Pacific J. Math., 15 (1965) 13-19.

[3] BRAUER, A., *On a new class of Hadamard determinants*, Math. Z., 58 (1953) 219-225.

[4] BRUCK, R.H., *Difference sets in a finite group*, Trans. Amer. Math. Soc., 78 (1955) 464-481.

[5] BRUCK, R.H. & H.J. RYSER, *The non-existence of certain finite projective planes*, Canad. J. Math., 1 (1949) 88-93.

[6] CHOWLA, S. & H.J. RYSER, *Combinatorial problems*, Canad. J. Math., 2 (1950) 93-99.

[7] DEMBOWSKI, P., *Finite geometries*, Ergebnisse der Mathematik 44, Springer-Verlag, Berlin etc., 1968.

[8] FEIT, W., *Characters of finite groups*, Benjamin, New York, 1967.

[9] GORDON, B., W.H. MILLS & L.R. WELCH, *Some new difference sets*, Canad. J. Math., 14 (1962) 614-625.

[10] HALL Jr., M., *Cyclic projective planes*, Duke Math. J., 14 (1947) 1079-1090.

[11] HALL Jr., M., *Combinatorial theory*, Blaisdell, Waltham, Mass., 1967.

[12] HALL Jr., M., *A survey of difference sets*, Proc. Amer. Math. Soc., 7 (1956) 975-986.

[13] HALL Jr., M., *Characters and cyclotomy*, in: Proc. Symp. in Pure Math., vol. 8, Amer. Math. Soc., 1965.

[14] HALL Jr., M. & H.J. RYSER, *Cyclic incidence matrices*, Canad. J. Math., 3 (1951) 495-502.

[15] KANTOR W., *Symplectic groups, symmetric designs, and line ovals*, to appear.

[16] MCFARLAND, R.L., *On multipliers of Abelian difference sets*, thesis, The Ohio State University, 1970.

[17] MANN, H.B., *Balanced incomplete block designs and Abelian difference sets*, Illinois J. Math., 8 (1964) 252-261.

[18] KESAVA MENON, P., *Difference sets in Abelian groups*, Proc. Amer. Math. Soc., 11 (1960) 368-376.

[19] KESAVA MENON, P., *On difference sets whose parameters satisfy a certain relation*, Proc. Amer. Math. Soc., 13 (1962) 739-745.

[20] PARKER, E.T., *On collineations of symmetric designs*, Proc. Amer. Math. Soc., 8 (1957) 350-351.

[21] RYSER, H.J., *Combinatorial mathematics*, Carus Math. Monograph No. 14 Math. Assoc. Amer., Wiley, New York, 1963.

[22] SCHÜTZENBERGER, M.P., *A non-existence theorem for an infinite family of symmetrical block designs*, Ann. Eugenics, 14 (1949) 286-287.

[23] SINGER, J., *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., 43 (1938) 377-385.

[24] STORER, T., *Cyclotomy and difference sets*, Markham, Chicago, 1967.

[25] TURYN, R.J., *The multiplier theorem for difference sets*, Canad. J. Math., 16 (1964) 386-388.

[26] TURYN, R.J., *Character sums and difference sets*, Pacific J. Math., 15 (1965) 319-346.

[27] WHITEMAN, A.L., *A family of difference sets*, Illinois J. Math., 6 (1962) 107-121.

[28] YAMAMOTO, K., *Decomposition fields of difference sets*, Pacific J. Math., 13 (1963) 337-352.

MATHEMATICAL CENTRE TRACTS 57, 1974, 27-43

INVARIANT RELATIONS, COHERENT CONFIGURATIONS AND GENERALIZED POLYGONS *)

D.G. HIGMAN

University of Michigan, Ann Arbor, Mich. 48104, USA

A high point in the combinatorial approach to the theory of finite permutation groups is WIELANDT's theory of invariant relations, culminating in his theorem on groups of degree p^2 [16]. In section 1 we give a few rudiments of WIELANDT's theory in the context of the theory of G-spaces, illustrating the concepts by a proof, which seems first to have been made explicit by R. LIEBLER [12], of a theorem of ALPERIN [1].

In section 2 we axiomatize certain combinatorial aspects of the theory of G-spaces, defining the class of combinatorial structures which we call *coherent configurations* [7,8,9] and listing some results about these from [9]. Association schemes as defined by BOSE & SHIMAMOTO [2] are a special class of coherent configurations.

In section 3 we turn to generalized polygons, which were introduced by J. TITS in connection with the problem of classifying finite groups with (B,N)-pair (cf. [3,6,14]). Here we apply the results listed in section 2 to generalized polygons, obtaining a proof (essentially that of KILMOYER & SOLOMON [11]) of the FEIT-HIGMAN theorem, and a proof that $s \leq t^2$ for generalized quadrangles and octagons having s+1 points on each line and t+1 lines through each point, with $t > 1$.

The author is happy to express thanks to J.E. MCLAUGHLIN for suggestions which simplified section 3, especially for the use of Lagrange interpolation.

1. G-SPACES AND INVARIANT RELATIONS

X and Y will be finite non-empty sets. We regard a subset f of $X \times Y$ as a *relation* from X to Y, and put $f^{\cup} = \{(y,x) \mid (x,y) \in f\}$ (the *converse*

---

*) Research supported in part by the National Science Foundation.

of f) and $f(x) = \{y \in Y \mid (x,y) \in f\}$ for $x \in X$.

An *action* of a group G on X is a map $X \times G \to X$, $(x,g) \mapsto xg$, such that $x(gh) = (xg)h$ and $x1 = x$ for all $x \in X$ and $g,h \in G$, where 1 is the identity element of G. Specifying an action of G on X is equivalent to specifying a homomorphism of G into the symmetric group $\sum_X$ on X.

A G-space is partitioned into its G-*orbits*, which are the equivalence classes under the equivalence relation: $x \sim y$ if and only if $xg = y$ for some $g \in G$. A G-space is *transitive* if there is just one G-orbit.

A subset Y of a G-space X is *invariant* under G if $Yg \subseteq Y$ for all $g \in G$. Then G acts on Y and the G-orbits in Y are G-orbits in X. The G-orbits in a G-space X are transitive G-spaces. For $x \in X$, the subgroup $G_x = \{g \in G \mid xg = x\}$ of G is called the *stabilizer* of x in G.

If X and Y are G-spaces, then so is $X \times Y$ under the componentwise action $((x,y),g) \mapsto (xg,yg)$. A relation $F \subseteq X \times Y$ which is invariant under this action is called an *invariant relation* from X to Y. If $\mathcal{O}$ is the totality of G-orbits in $X \times Y$, then the invariant relations from X to Y are just the unions of members of $\mathcal{O}$.

Assume from now on in this section that X *and* Y *are transitive* G-*spaces.* Choose $x \in X$ and $y \in Y$. Then $\{f(x) \mid f \in \mathcal{O}\}$ is the partition of Y into G_x-orbits and $\{f^\cup(y) \mid f \in \mathcal{O}\}$ is the partition of X into G_y-orbits. Thus

$$f(x) \leftrightarrow f^\cup(y), \qquad (f \in \mathcal{O})$$

is a one-to-one correspondence between the G_x-orbits in Y and the G_y-orbits in X. The *lengths* $|f(x)|$ and $|f^\cup(y)|$ of corresponding orbits are proportional since $|X||f(x)| = |Y||f^\cup(y)| = |f|$.

We illustrate these concepts as follows. Suppose that $F \subseteq X \times Y$ is an invariant relation. Then F is partitioned into G-orbits $F = \bigcup_{f \in \mathcal{O}_F} f$ with $\mathcal{O}_F \subseteq \mathcal{O}$, and $F^\cup = \bigcup_{f \in \mathcal{O}_F} f^\cup$. Taking $(x,y) \in F$ we have that

$$f(x) \leftrightarrow f^\cup(y), \qquad (f \in \mathcal{O}_F)$$

is a one-to-one correspondence between the G_x-orbits in F(x) and the G_y-orbits in $F^\cup(y)$.

To apply this, start with a transitive G-space X, choose $a \in X$ and a subgroup H of G_a, and construct a transitive G-space Y and an invariant relation F as follows:

Y is the totality of conjugates $H^g = g^{-1}Hg$ ($g \in G$) of H in G, with G acting on Y by conjugation,

$$F = \{(x,H^g) \mid x \in X,\ g \in G,\ H^g \subseteq G_x\}.$$

Then $(a,H) \in F$,

$F(a)$ is the totality of conjugates of H which are contained in G_a,

G_H is the normalizer $N_G(H)$ of H in G ($N_G(H) = \{g \in G \mid H^g = H\}$),

and

$F^v(H)$ is the set of fixed points of H in G.

It follows therefore, that

THEOREM 1.1. (ALPERIN [1]). *If* X *is a transitive* G*-space,* $a \in X$, *and* H *is a subgroup of* G_a, *then there is a one-to-one correspondence between the conjugate classes in* G_a *of conjugates of* H *which are contained in* G_a *and the* $N_G(H)$*-orbits of fixed points of* H.

Finiteness plays no essential role in this proof of ALPERIN's theorem. In addition to the corollary in [1], theorems of JORDAN [15; 3.5-3.7], MANNING [15; 3.6'] and WITT [15; 9] are immediate corollaries of theorem 1.1. This proof of ALPERIN's theorem seems first to have been made explicit by R. LIEBLER [12].

2. COHERENT CONFIGURATIONS

As suggested by section 1, we consider *configurations* $(X,\mathcal{O})$ consisting of a (finite) non-empty set X and a set $\mathcal{O}$ of binary relations on X^2. Thus $\mathcal{O}$ is a subset of the power set $\mathcal{P}(X^2)$ of the cartesian square X^2 of X. There is no loss in generality in the restriction to relations on a single set, since, for example, a relation from X to Y can be regarded as a relation on the disjoint union of X and Y. We put $\mathcal{R}$ equal to the boolean subalgebra of $\mathcal{P}(X^2)$ generated by $\mathcal{O}$. If $f_1,f_2,\ldots,f_s \in \mathcal{O}$ and $x,y \in X$, an $(f_1,\ldots,f_s)$-*path* from x to y is an (s+1)-tuple $(x_1,\ldots,x_{s+1})$ such that $x_1 = x$, $x_{s+1} = y$ and $(x_i,x_{i+1}) \in f_i$, $1 \le i \le s$. We call $(X,\mathcal{O})$ *coherent* if the following axioms (I) through (IV) are satisfied.

(I) $\mathcal{O}$ *is a partition of* X^2.

(II) $I = \{(x,x) \mid x \in X\} \in \mathcal{R}$.

(III) $f \in \mathcal{O}$ *implies* $f^{\smile} \in \mathcal{O}$.

(IV) *For all* $f,g,h \in \mathcal{O}$ *and* $(x,y) \in h$, *the number of* (f,g)*-paths from* x *to* y *is independent of the choice of* $(x,y) \in h$.

The number of (f,g)-paths from x to y is $|f(x) \cap g^{\smile}(y)|$ and can be denoted by a_{fgh} for $(x,y) \in h$ if $(X,\mathcal{O})$ is coherent, in which case the non-negative integers a_{fgh} are the *intersection numbers* of $(X,\mathcal{O})$. The number $r = |\mathcal{O}|$ is called the rank.

If X is a G-space for a group G and $\mathcal{O}$ is the set of G-orbits in X^2, then $(X,\mathcal{O})$ is coherent. We refer to this situation as the *group case*.

A coherent configuration is *homogeneous* if $I \in \mathcal{O}$ and *symmetric* if the *pairing* $f \mapsto f^{\smile}$ $(f \in \mathcal{O})$ is trivial, i.e. if every $f \in \mathcal{O}$ is symmetric. A symmetric configuration is necessarily homogeneous. In the group case, homogeneity is equivalent to transitivity of the G-space.

Symmetric coherent configurations are equivalent to *association schemes* as defined by BOSE & SHIMAMOTO [2].

The boolean algebra $\mathcal{R}$ of a coherent configuration is a semigroup under composition and the idempotents in $\mathcal{R}$ are of particular interest. We do not go into this here but turn at once to the *adjacency algebra*, which is the centralizer algebra in the group case.

We denote by $\mathrm{Mat}_{\mathbb{C}} X$ the totality of matrices $\phi\colon X^2 \to \mathbb{C}$, regarded as an algebra over $\mathbb{C}$ with respect to matrix (i.e. pointwise) addition and matrix multiplication. For $f \in \mathcal{O}$, $\Phi_f\colon X^2 \to \mathbb{C}$ will be the characteristic function of f, or, otherwise thought of, Φ_f is the adjacency matrix of the graph (X,f). If $(X,\mathcal{O})$ is coherent, then the set $\mathcal{B} = \{\Phi_f \mid f \in \mathcal{O}\}$ is a basis of a subalgebra $\mathcal{A}$ of $\mathrm{Mat}_{\mathbb{C}} X$, called the *adjacency algebra* of $(X,\mathcal{O})$.

$(X,\mathcal{O})$ will be called *commutative* if $\mathcal{A}$ is commutative. A symmetric configuration is necessarily çommutative and a commutative configuration is necessarily homogeneous. As used by DELSARTE [4], the term association scheme is equivalent to commutative configuration. Section 3 will illustrate the importance of the non-commutative case.

For applications we often need the following translation of the axioms (I) through (IV).

THEOREM 2.1. *Let* $\mathcal{B}$ *be a set of non-zero* $(0,1)$*-matrices in* $\mathrm{Mat}_{\mathbb{C}} X$ *such that*

(1) $\Phi = \sum_{\phi \in \mathcal{B}} \phi$ *is the all 1 matrix,* $\Phi(x,y) = 1$ *for all* $x,y \in X$,

(2) *the identity matrix is a sum of members of* $\mathcal{B}$,

(3) $\phi \in \mathcal{B}$ *implies that* $\phi^t \in \mathcal{B}$, *and*

(4) $\mathcal{B}$ *spans a subalgebra* $\mathcal{A}$ *of* $\mathrm{Mat}_{\mathbb{C}} X$.

Then $(X,\mathcal{O})$ *with* $\mathcal{O} = \{\text{supp } \phi \mid \phi \in B\}$, *is a coherent configuration with adjacency algebra* A.

Now we list some basic facts about A, referring to [9] for proofs.

THEOREM 2.2. *A is semisimple.*

THEOREM 2.3. *There is a unitary matrix* U *effecting a complete reduction of* A, *i.e. such that for all* $\phi \in A$,

$$U^*\phi U = \operatorname{diag}(\Delta_1(\phi) \times I_{z_1}, \ldots, \Delta_m(\phi) \times I_{z_m}),$$

where $\Delta_1, \ldots, \Delta_m$ *are the inequivalent irreducible representations of* A.

We put e_i = degree of Δ_i and call z_i the *multiplicity* of Δ_i. The *character* ζ_i *of* A *afforded by* Δ_i is defined by $\zeta_i(\phi) = \operatorname{trace} \Delta_i(\phi)$. We have $\zeta_i(I) = e_i$ and $\sum_{i=1}^m e_i^2 = r$, $\sum_{i=1}^m e_i z_i = |X|$.

We write $\Delta_\alpha(\phi) = (a_{ij}^\alpha(\phi))$ and list the a_{ij}^α: $a_1, a_2, \ldots, a_r$. If $a_\lambda = a_{ij}^\alpha$, we write $a_{\bar\lambda} = a_{ji}^\alpha$ and $h_\lambda = z_\alpha$. For $f \in \mathcal{O}$ and $x \in$ domain f, $|f(x)|$ is independent of x and we put $v_f = |f(x)|$ and $\tilde\Phi_f = \frac{1}{|f|}\Phi_{f^v}$.

There is a distinguished irreducible character of A of degree 1 called the *principal character*. In the homogeneous case this means that if we choose a notation so that ζ_1 is the principal character, then $e_1 = z_1 = 1$ and $\zeta_1(\Phi_f) = v_f$ for all $f \in \mathcal{O}$.

Of fundamental importance are the Schur relations

$$\sum_{f\in\mathcal{O}} a_\lambda(\tilde\Phi_f)\, a_\mu(\Phi_f) = \delta_{\lambda\bar\mu}\frac{1}{h_\lambda}, \tag{2.1}$$

which imply the orthogonality relations

$$\sum_{f\in\mathcal{O}} \zeta_\alpha(\tilde\Phi_f)\, \zeta_\beta(\Phi_f) = \delta_{\alpha\beta}\frac{e_\alpha}{z_\alpha}. \tag{2.2}$$

Assume that $\Delta_\alpha(\phi^*) = \Delta_\alpha(\phi)^*$ for all α and ϕ, or equivalently, that

$$a_\sigma(\Phi_{f^v}) = a_{\bar\sigma}(\Phi_f) \quad \text{for all } f \in \mathcal{O}, 1 \le \sigma \le r. \tag{2.3}$$

This will hold if the complete reduction of A is afforded by a unitary matrix. Then we have the *Krein condition*

(2.4) Choose λ and μ, $1 \le \lambda, \mu \le r$, such that $\lambda = \overline{\lambda}$ and $\mu = \overline{\mu}$. If $a_\nu = a_{ij}^\alpha$, put

$$c_{ij}^\alpha = \sum_{f \in \mathcal{O}} \frac{a_\lambda(\Phi_f)\, a_\mu(\Phi_f)\, \overline{a_\nu(\Phi_f)}}{|f|^2}.$$

Then $C_\alpha = (c_{ij}^\alpha)$ is hermitian positive semidefinite.

(Actually (2.3) is needed only for the a_σ occurring in the definition of C_α to have this conclusion for a particular C_α.) (2.4) extends a result of L.L. SCOTT Jr. [13].

3. GENERALIZED POLYGONS

An *incidence structure* (P,L,F) consists of two disjoint non-empty sets P and L and a relation $F \subseteq P \times L$. The members of the sets $P \cup L$, P, L and F will be called *elements*, *points*, *lines* and *flags* respectively. Two elements x and y are *incident* if $(x,y) \in F \cup F^\cup$, so the flags are the incident point-line pairs. An incidence structure can be represented by a bipartite graph in which the vertices are the elements and the edges are the flags.

A *path of length* d from an element x to an element y is a (d+1)-tuple $(x_0, x_1, \ldots, x_d)$ of elements such that x_{i-1} and x_i are incident for all i, $1 \le i \le d$. The *distance* $\rho(x,y)$ between two elements is the length of the shortest path from x to y, or ∞ if no such path exists.

A *generalized* n*-gon*, where n is an integer > 0, is an incidence structure (P,L,F) satisfying the following two conditions for all elements x and y:

(A) for each x, the maximum distance $\rho(x,y)$ is n;

(B) if $\rho(x,y) < n$, then there is exactly one path of length < n from x to y.

A *generalized polygon* is a generalized n-gon for some n. The generalized polygons considered here will be assumed to satisfy the following additional condition:

(C) each line is incident with the same number s+1 of points and each point is incident with the same number t+1 of lines.

The generalized polygons with s = t = 1 are just the ordinary polygons. *We assume from now on that* st > 1. According to the FEIT-HIGMAN theorem (to be proved below as theorem 3.1), $n \in \{3,4,6,8,12\}$ and s = 1 or t = 1 if n = 12. A generalized triangle is the same thing as a projective plane. There is a fairly extensive literature about generalized quadrangles, but very little seems to be known about generalized n-gons with n > 4. Simple groups of Lie type of rank 2 act on generalized polygons. These groups are listed at

the end of the section.

Note that the *dual* (L,P,F) of a generalized n-gon is a generalized n-gon.

We now construct a coherent configuration based on the set F of flags of a generalized n-gon (P,L,F), and systematically apply the results outlined in section 2. For this we need to determine the irreducible representations of the adjacency algebra.

If $x \in F$, then $x = (x_1,x_2)$ with $x_1 \in P$ and $x_2 \in L$. We start with the symmetric relations

$$S = \{(x,y) \in F^2 \mid x_1 \neq y_1 \text{ and } x_2 = y_2\}$$

and

$$T = \{(x,y) \in F^2 \mid x_1 = y_1 \text{ and } x_2 \neq y_2\} .$$

Composing relations in the usual way we see that $S^2 = I$ or $S \cup I$ according as $s = 1$ or $s > 1$, $T^2 = I$ or $T \cup I$ according as $t = 1$ or $t > 1$, and that the 2n relations

$$\begin{array}{ll} & S,\ ST,\ STS,\ \ldots,\ \underbrace{STS\ldots}_{n-1}, \\ I & \qquad\qquad \underbrace{STS\ldots}_{n} = \underbrace{TST\ldots}_{n} \\ & T,\ TS,\ TST,\ \ldots,\ \underbrace{TST\ldots}_{n-1}, \end{array}$$

constitute a partition $\mathcal{O}$ of F^2. This uses only the conditions (A) and (B).

Put $A = \Phi_S$ and $B = \Phi_T$. We readily verify that for each $f = \ldots STS\ldots$ in $\mathcal{O}$, $\Phi_f = \ldots ABA\ldots$. In particular, therefore

$$(3.1) \qquad \underbrace{ABA\ldots}_{n} = \underbrace{BAB\ldots}_{n} .$$

At this point we invoke condition (C) to obtain the relations

$$(3.2) \qquad A^2 = (s-1)A + sI \quad \text{and} \quad B^2 = (t-1)B + tI.$$

It follows that the matrices Φ_f, $f \in \mathcal{O}$, constitute a basis of a subalgebra $\mathcal{A}$ of $\mathrm{Mat}_{\mathbb{C}} F$, and hence by theorem 2.1 that $(F,\mathcal{O})$ is a homogeneous coherent configuration with adjacency algebra $\mathcal{A}$. Moreover, $A \mapsto U$ and $B \mapsto V$ will determine a matrix representation of $\mathcal{A}$ if and only if U and V are matrices such that the conditions (3.1) and (3.2) are satisfied with U and V in place of A and B.

First we consider the 1-dimensional representations of $\hat{A}$.

Case n = 2m. In this case $\hat{A}$ has four distinct linear characters $\zeta_1,\dots,\zeta_4$:

(3.3)

	A	B
ζ_1	s	t
ζ_2	-1	-1
ζ_3	s	-1
ζ_4	-1	t

The principal character is ζ_1, so

$$|F| = \sum_{f\in\mathcal{O}} \zeta_1(\Phi_f) ,$$

that is:

(3.4) *if* n = 2m, *then* $|F| = (1+s)(1+t)\,\dfrac{(st)^m - 1}{st - 1}$.

Case n = 2m+1. Here there are two distinct linear characters ζ_1 and ζ_2 as in the first two rows of (3.3). From the relation (3.1),

$$s^{m+1}t^m = \zeta_1((AB)^mA) = \zeta_1(B(AB)^m) = s^mt^{m+1}, \text{ so}$$

(3.5) *if* n *is odd, then* s = t.

Next we determine the 2-dimensional irreducible representations of $\hat{A}$. It turns out to be sufficient to find the real irreducible representations with composition factors affording ζ_1 and ζ_2. Thus we look for real matrices

$$U = \begin{pmatrix} -1 & 0 \\ 0 & s \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} b & u \\ u & c \end{pmatrix} ,$$

with $u \neq 0$, such that V has trace t-1 and determinant -t, i.e. such that

(3.6) $b+c = t-1$ and $u^2 = bc+t$.

Since (3.6) implies (3.2), $A \mapsto U$, $B \mapsto V$ will be a representation if and only if

(3.7) $(UV)^m = (VU)^m$ if n = 2m and $(UV)^mU = V(UV)^m$ if n = 2m+1 .

We need the products

$$UV = \begin{pmatrix} -b & -u \\ su & sc \end{pmatrix}, \qquad VU = \begin{pmatrix} -b & su \\ -u & sc \end{pmatrix},$$

$$UVU = \begin{pmatrix} b & -su \\ -su & s^2c \end{pmatrix}, \qquad VUV = \begin{pmatrix} -b^2+su^2 & (-b+sc)u \\ (-b+sc)u & -u^2+sc^2 \end{pmatrix}.$$

Assume that U and V satisfy (3.6) and (3.7), $u \neq 0$. The matrices UV and VU do not commute, otherwise we would have $b^2+u^2 = b^2+s^2u^2$ and $bsu - usc = bu + s^2uc$, whence $s = t = 1$, contrary to assumption.

By (3.7), $(UV)^r = (VU)^r$ with $r = n/2$ or n according as n is even or odd. But $(UV)^r = aI + b(UV)$, $a,b \in \mathbb{C}$, so $b \neq 0$ would imply that UV and VU commute. Hence $(UV)^r$ is a scalar matrix, so the similar matrices UV and VU have distinct eigenvalues λ and $\mu = \xi\lambda$ with $\xi^r = 1$, $\xi \neq 1$.

Now the determinant of UV is $su^2-bsc = s(u^2-bc) = st$, so $\lambda = \sqrt{st}\,\theta$ and $\mu = \sqrt{st}\,\theta^{-1}$ with $\theta^{2r} = 1$ and $\theta \neq \theta^{-1}$. Since trace $UV = -b+sc = \sqrt{st}(\theta+\theta^{-1})$,

$$(3.8) \qquad \begin{cases} (s+1)b = s(t-1) - \sqrt{st}(\theta+\theta^{-1}), \\ (s+1)c = t-1 + \sqrt{st}(\theta+\theta^{-1}). \end{cases}$$

If X is a 2×2 matrix with distinct eigenvalues λ, μ, then for $k=1,2,\ldots$,

$$X^k = \frac{\lambda^k}{\lambda-\mu}(X-\mu I) + \frac{\mu^k}{\mu-\lambda}(X-\lambda I) =$$

$$= \frac{\lambda^k-\mu^k}{\lambda-\mu}X - \frac{\lambda\mu(\lambda^{k-1}-\mu^{k-1})}{\lambda-\mu}I.$$

In particular, therefore, for X = UV or VU and $k=1,2,\ldots$

$$(3.9) \qquad X^k = \frac{(\sqrt{st})^{k-1}}{\theta-\theta^{-1}}\{(\theta^k-\theta^{-k})X - \sqrt{st}(\theta^{k-1}-\theta^{-(k-1)})I\}.$$

We use (3.9) to determine the character of our representation. We have trace $U = s-1$, trace $V = t-1$, trace UV = trace $VU = -b+sc = \sqrt{st}(\theta+\theta^{-1})$, trace $UVU = b+s^2c = s(t-1) + (s-1)\sqrt{st}(\theta+\theta^{-1})$, and trace $VUV = -b^2 + (s-1)u^2 + sc^2 = -b^2 + (s-1)(bc+t) + sc^2 = (s-1)t + (b+c)(-b+sc) =$

$= (s-1)t + (t-1)\sqrt{st}(\theta+\theta^{-1})$. Hence by (3.9),

$$\text{trace } (UV)^k = \frac{(\sqrt{st})^{k-1}}{\theta - \theta^{-1}} \{(\theta^k-\theta^{-k})\sqrt{st}(\theta+\theta^{-1}) - 2\sqrt{st}(\theta^{k-1}-\theta^{-(k-1)})\} =$$

$$= \frac{(\sqrt{st})^k}{\theta - \theta^{-1}} \{(\theta^{k+1}-\theta^{-(k+1)}) - (\theta^{k-1}-\theta^{-(k-1)})\} =$$

$$= (\sqrt{st})^k(\theta^k+\theta^{-k})$$

and

$$\text{trace } (UV)^k U = \frac{(\sqrt{st})^{k-1}}{\theta - \theta^{-1}} \{(\theta^k-\theta^{-k})(s(t-1)+(s-1)\sqrt{st}(\theta+\theta^{-1})) +$$

$$- \sqrt{st}(\theta^{k-1}-\theta^{-(k-1)})(s-1)\} =$$

$$= \frac{(\sqrt{st})^k}{\theta - \theta^{-1}} \{(s-1)[(\theta^k-\theta^{-k})(\theta+\theta^{-1}) - (\theta^{k-1}-\theta^{-(k-1)})] +$$

$$+ \frac{s}{\sqrt{st}}(t-1)(\theta^k-\theta^{-k})\} =$$

$$= \frac{(\sqrt{st})^k}{\theta - \theta^{-1}} \{(s-1)(\theta^{k+1}-\theta^{-(k+1)}) + \frac{s}{\sqrt{st}}(t-1)(\theta^k-\theta^{-k})\}.$$

The trace of $V(UV)^k$ is obtained from that of $(UV)^k U$ by interchanging s and t. Thus, if ζ is the character afforded by our representation, then

$$(3.10) \qquad \begin{cases} \zeta((AB)^k) = \zeta((BA)^k) = (\sqrt{st})^k(\theta^k+\theta^{-k}) , \\ \zeta((AB)^k A) = \dfrac{(\sqrt{st})^k}{\theta - \theta^{-1}} \{(s-1)(\theta^{k+1}-\theta^{-(k+1)}) + \dfrac{s}{\sqrt{st}}(t-1)(\theta^k-\theta^{-k})\} , \\ \zeta(B(AB)^k) = \dfrac{(\sqrt{st})^k}{\theta - \theta^{-1}} \{(t-1)(\theta^{k+1}-\theta^{-(k+1)}) + \dfrac{t}{\sqrt{st}}(s-1)(\theta^k-\theta^{-k})\} . \end{cases}$$

Now choose b and c according to (3.8), with $\theta^{2r} = 1$, $r = n/2$ or n according as n is even or odd, $\theta = \cos\alpha+i\sin\alpha \neq \pm 1$. Then $-b+sc = \sqrt{st}(\theta+\theta^{-1}) = 2\sqrt{st}\cos\alpha$, so $bc+t = a \leq 0$ would imply that $-b^2 + s(-t+a) = 2b\sqrt{st}\cos\alpha$, or $(b + \sqrt{st}\cos\alpha)^2 - st\sin^2\alpha = sa \leq 0$, and hence $\sin\alpha = 0$, or

$\theta = \pm 1$, contrary to assumption. Hence the solutions of $u^2 = bc+t$ are real. For such a u the matrices U and V satisfy $(UV)^r = (VU)^r$. We consider the cases of even and odd n separately.

Case n = 2m. In this case we have $(UV)^m = (VU)^m = (\sqrt{st})^m \theta^m I$ and hence $A \mapsto U$, $B \mapsto V$ is a representation. We obtain m-1 inequivalent irreducible representations of degree 2 on taking ε a primitive n-th root of unity and $\theta = \varepsilon^i$, $i=1,2,\ldots,m-1$. The sum of the squares of the degrees of the irreducible representations of A obtained so far is $4+4(m-1) = 2n$, the dimension of A, so all irreducible representations are accounted for in this case.

We now apply the orthogonality relations (2.2) to determine the multiplicity z of each irreducible character ρ. In our present case we have

$$\frac{\rho(1)}{z}|F| = \sum_{k=0}^{m-1} \{2\frac{\rho((AB)^k)^2}{(st)^k} + \frac{\rho((AB)^k A)^2}{s(st)^k} + \frac{\rho(B(AB)^k)^2}{(st)^k t}\} + \frac{\rho((AB)^m)^2}{(st)^m} - \rho(1)^2 .$$

For the linear characters $\zeta_1,\ldots,\zeta_4$ the respective multiplicities are

$$(3.11) \quad \begin{cases} z_1 = 1,\ z_2 = (st)^m , \\ z_3 = z_4 = \frac{s}{m} \cdot \frac{s^{2m}-1}{s^2-1} \quad \text{if } s = t , \\ z_3 = t^m \frac{s-t}{s^m - t^m} \frac{(st)^m - 1}{st-1} \\ z_4 = s^m \frac{s-t}{s^m - t^m} \frac{(st)^m - 1}{st-1} \end{cases} \text{if } s \neq t .$$

Now take $\rho = \zeta$ as in (3.10). Then

$$\frac{2|F|}{z} = \sum_{k=0}^{m-1} \{2(\theta^k+\theta^{-k})^2 +$$

$$+ \frac{1}{s} \frac{1}{(\theta-\theta^{-1})^2} [(s-1)(\theta^{k+1}-\theta^{-(k+1)}) + \frac{s}{\sqrt{st}} (t-1)(\theta^k-\theta^{-k})]^2 +$$

$$+ \frac{1}{t} \frac{1}{(\theta-\theta^{-1})^2} [(t-1)(\theta^{k+1}-\theta^{-(k+1)}) + \frac{t}{\sqrt{st}} (s-1)(\theta^k-\theta^{-k})]^2\} +$$

$$+ (\theta^m+\theta^{-m})^2 - 4 =$$

$$= 4m + \frac{1}{(\theta-\theta^{-1})^2}\sum_{k=0}^{m-1}\{[\frac{(s-1)^2}{s}+\frac{(t-1)^2}{t}][(\theta^{k+1}-\theta^{-(k+1)})^2+(\theta^k-\theta^{-k})^2] +$$

$$+ \frac{4(s-1)(t-1)}{\sqrt{st}}(\theta^{k+1}-\theta^{-(k+1)})(\theta^k-\theta^{-k})\}.$$

Hence

$$(3.12)\qquad \frac{|F|}{z} = n\{1 - \frac{1}{(\theta-\theta^{-1})^2}[\frac{(s-1)^2}{s} + \frac{(t-1)^2}{t}] - \frac{\theta+\theta^{-1}}{(\theta-\theta^{-1})^2}\frac{(s-1)(t-1)}{\sqrt{st}}\}.$$

Let ε be a primitive n-th root of unity, take $\theta = \varepsilon$ and $\theta = -\varepsilon$ in (3.12) and add to obtain that

$$\frac{1}{(\varepsilon-\varepsilon^{-1})^2}[\frac{(s-1)^2}{s} + \frac{(t-1)^2}{t}] \in \mathbb{Q}$$

and hence that $(\varepsilon-\varepsilon^{-1})^2 \in \mathbb{Q}$. Since ε is a primitive n-th root of unity with $n = 2m \geq 4$, it follows that $n = 4,6,8$ or 12.

Now

$$\frac{\theta+\theta^{-1}}{(\theta-\theta^{-1})^2}\frac{(s-1)(t-1)}{\sqrt{st}} \in \mathbb{Q}\ .$$

Assume that $s > 1$ and $t > 1$, then $\frac{\theta+\theta^{-1}}{\sqrt{st}} \in \mathbb{Q}$ and we obtain the indicated solution on taking the indicated choice of θ:

	θ	conclusion
$n = 6$	primitive 6-th root	st a square
$n = 8$	primitive 8-th root	2st a square
$n = 12$	primitive 12-th root	3st a square
	primitive 6-th root	st a square

In particular, if $n = 12$, then $s = 1$ or $t = 1$.

The multiplicities of the irreducible characters of degree 2 in the cases n = 4, 6 and 8 are as follows:

n = 4.

$$z = \frac{st|F|}{s^2t + t^2s + s + t} .$$

n = 6.

$$z_{\pm} = \frac{st|F|}{2\{s^2t + t^2s - st + s + t \pm (s-1)(t-1)\sqrt{st}\}} .$$

n = 8.

$$z_{\pm} = \frac{st|F|}{4\{s^2t + st^2 - 2st + s + t \pm (s-1)(t-1)\sqrt{2st}\}}$$

$$z = \frac{st|F|}{2\{s^2t + st^2 + s + t\}} .$$

Now we turn to the case of odd n.

Case n = 2m+1. Here we can verify directly using (3.9) that $(UV)^m U = V(UV)^m$ if and only if $\theta^n = 1$. Taking ε to be a primitive n-th root of unity and $\theta = \varepsilon^i$, i=1,2,...,m, we obtain m inequivalent irreducible representations of degree 2. With the two irreducible representations of degree 1, this accounts for all irreducible representations of A.

Since s = t, the formulas (3.10) become

$$\zeta((AB)^k) = \zeta((BA)^k) = s^k(\theta^k+\theta^{-k}) ,$$

$$\zeta((AB)^kA) = \zeta(B(AB)^k) = \frac{s^k(s-1)}{\theta - \theta^{-1}} (\theta^{k+1}-\theta^{-(k+1)} + \theta^k-\theta^{-k}) .$$

By (2.2)

$$\frac{2|F|}{z} = 2\sum_{k=0}^{m} \frac{\zeta((AB)^k)^2}{s^{2k}} - 4 + 2\sum_{k=0}^{m} \frac{\zeta((AB)^kA)^2}{s^{2k+1}} - \frac{\zeta((AB)^mA)^2}{s^{2m+1}} =$$

$$= 2 \sum_{k=0}^{m} (\theta^k+\theta^{-k})^2 - 4 +$$

$$+ \frac{2}{(\theta-\theta^{-1})^2} \frac{(s-1)^2}{s} \sum_{k=0}^{m} (\theta^{k+1}-\theta^{-(k+1)} + \theta^k-\theta^{-k})^2 +$$

$$- \frac{1}{(\theta-\theta^{-1})^2} \frac{(s-1)^2}{s} (\theta^{m+1}-\theta^{-(m+1)} + \theta^m-\theta^{-m})^2 =$$

$$= 2(n+2) - 4 - \frac{2n}{(\theta-\theta^{-1})^2} (\theta+\theta^{-1}+2) \frac{(s-1)^2}{s} =$$

$$= 2n\{1 - \frac{1}{\theta+\theta^{-1}-2} \frac{(s-1)^2}{s}\} .$$

Hence $\theta+\theta^{-1} \in \mathbb{Q}$, and taking ε to be a primitive n-th root of unity, this implies that n = 3.

Of course the main conclusion from our discussion so far is the celebrated theorem of WALTER FEIT and GRAHAM HIGMAN [5,11].

THEOREM 3.1. *If a generalized* n*-gon has* s+1 *points on each line and* t+1 *lines through each point, with* st > 1, *then* n = 3,4,6,8 *or* 12. *If* s > 1 *and* t > 1, *then*

(1) st *is a square in case* n = 6,

(2) 2st *is a square in case* n = 8, *and*

(3) $n \neq 12$.

The methods under discussion here do not give any results for projective planes, so we assume from now on that n is even.

To apply the Krein condition to the linear character ζ_3 we need the values of ζ_1 and ζ_3:

	n=4							n=6				n=8			
ζ_1	1	s	t	st	st	s^2t	st^2	s^2t^2	s^2t^2	s^3t^2	s^2t^3	s^3t^3	s^3t^3	s^4t^3	s^3t^4	s^4t^4
ζ_3	1	s	-1	-s	-s	$-s^2$	s	s^2	s^2	s^3	$-s^2$	$-s^3$	$-s^3$	$-s^4$	s^3	s^4

The condition is

$$0 \le \sum_{f \in \mathcal{O}} \frac{\zeta_3(\Phi_f)^3}{\zeta_1(\Phi_f)^2} = 1 + \frac{s^3}{s^2} - \frac{1}{t^2} - 2\frac{s^3}{s^2t^2} - \frac{s^6}{s^4t^2} + \frac{s^3}{s^2t^4} + \frac{s^6}{s^4t^4} \quad \Big| \; n = 4$$

$$+ \frac{s^6}{s^4t^4} + \frac{s^9}{s^6t^4} - \frac{s^6}{s^4t^6} - \frac{s^9}{s^6t^6} \quad \Big| \; n = 6$$

$$- \frac{s^9}{s^6t^6} - \frac{s^{12}}{s^8t^6} + \frac{s^9}{s^6t^8} + \frac{s^{12}}{s^8t^8} \quad \Big| \; n = 8$$

where the sum stops as indicated in the respective cases.

In case n = 8 this becomes

$$1 + s - \frac{1}{t^2}(1+s)^2 + \frac{1}{t^4}s(1+s)^2 - \frac{1}{t^6}s^2(1+s)^2 + \frac{1}{t^8}s^3(1+s) \ge 0 ,$$

i.e.

$$t^8 - t^6(1+s) + t^4 s(1+s) - t^2s^2(1+s) + s^3 \ge 0 ,$$

i.e.

$$(t^8-t^6) - (t^6-t^4)s + (t^4-t^2)s^2 - (t^2-1)s^3 \ge 0.$$

Assuming $t > 1$, therefore, $t^6-t^4s+t^2s^2-s^3 \ge 0$, i.e. $(t^2-s)(t^4+s^2) \ge 0$. Hence $s \le t^2$. In case n = 4 we obtain the same inequality, but for n = 6 there is no conclusion. We have proved

THEOREM 3.2. *If a generalized quadrangle or octagon has* s+1 *points on each line and* t+1 *lines through each point, with* $t > 1$, *then* $s \le t^2$.

The simple groups of Lie type of rank 2 act on generalized polygons. We list these groups, their Weyl groups W and the parameters n,s,t for the corresponding generalized polygons which we refer to as generalized polygons of *Lie type*.

type	identification	W	n	s	t
$A_2(q)$	$PSL_3(q)$	$\sum_3$	3	q	q
$B_2(q)$	$PSP_4(q)$	D_8	4	q	q
$A_3'(q)$	$PSU_4(q)$	D_8	4	q^2	q
$A_4'(q)$	$PSU_5(q)$	D_8	4	q^2	q^3
$G_2(q)$	Dickson's group	D_{12}	6	q	q
${}^3D_4(q)$	triality group	D_{12}	6	q^3	q
$F_4'(q)$	Ree group	D_{16}	8	q^2	q

($q = 3^{2a+1}$)

From the table we see that theorem 2 gives the right inequality to quadrangles and octagons. The irreducible representations of A have been obtained in a form satisfying (2.3), and, using (3.9) we can easily write out the full matrix $A = (a_\lambda(\Phi_f))$ and apply the full force of the Krein condition in case $n = 6$. Unfortunately there is no conclusion for this case, and worse yet, we have no way of determining failure short of carrying through the entire procedure. We originally proved theorem 3.2 for quadrangles by a quite different method [10] which can be extended to give the result for octagons, but also gives no result for hexagons. Maybe there are hexagons with $s > t^3$. Although there are many known quadrangles which are not of Lie type, the only known generalized hexagons and octagons (satisfying (C)) seem to be those of Lie type.

REFERENCES

[1] ALPERIN, J.L., *On a theorem of Manning*, Math. Z., 88 (1965) 434-435.

[2] BOSE, R.C. & T. SHIMAMOTO, *Classification and analysis of partially balanced incomplete block designs with two associate classes*, J. Amer. Statist. Assoc., 47 (1952) 151-184.

[3] CARTER, R.W., *Simple groups of Lie type*, J. Wiley & Sons, New York, 1972.

[4] DELSARTE, P., *An algebraic approach to the association schemes of coding theory*, thesis, Univ. Catholique de Louvain, Fac. des Sciences Appliquées, 1973.

[5] FEIT, W. & G. HIGMAN, *The non-existence of certain generalized polygons*, J. Algebra, 1 (1964) 114-138.

[6] FONG, P. & G.M. SEITZ, *Groups with (B,N)-pair of rank 2, I*, Invent. Math., 21 (1973) 1-57.

[7] HIGMAN, D.G., *Coherent configurations*, Rend. Sem. Mat. Univ. Padova, 44 (1970) 22-42.

[8] HIGMAN D.G., *Combinatorial considerations about permutation groups*, Lecture Notes, Oxford, 1972.

[9] HIGMAN, D.G., *Coherent configurations, part I: Ordinary representation theory*, to appear in Geometriae Dedicata.

[10] HIGMAN, D.G., *Partial geometries, generalized quadrangles and strongly regular graphs*, in: Atti Convegno di Geometria e sue Applicazioni, Perugia, 1971.

[11] KILMOYER, R. & L. SOLOMON, *On the theorem of Feit-Higman*, J. Comb. Theory 15 (1973) 310-322.

[12] LIEBLER, R., *On finite planes and collineation groups of low rank*, thesis, Univ. of Michigan, 1970.

[13] SCOTT Jr., L.L., *A condition on Higman's parameters*, Notices Amer. Math. Soc., 20 (1973) A-97.

[14] TITS, J., *Buildings of spherical type*, Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1974.

[15] WIELANDT, H., *Finite permutation groups*, Acad. Press, New York, 1964.

[16] WIELANDT, H., *Permutation groups through invariant relations and invariant functions*, Lecture Notes, Ohio State Univ., 1969.

MATHÉMATICAL CENTRE TRACTS 57, 1974, 44-97

2-TRANSITIVE DESIGNS *)

W.M. KANTOR

University of Oregon, Eugene, Oregon 97403, USA

INTRODUCTION

A great deal of work was done on 2-transitive groups during the last century and the beginning of this one. There has been a recent resurgence of interest in them for several reasons. First of all, many finite simple groups either have 2-transitive permutation representations or are closely related to groups that do. Also, recent work on finite simple groups has made the study of permutation groups more accessible. Finally, the close relationship between these groups and finite geometries has been recognized and has benefitted both group theory and geometry.

This survey will be concerned with designs having 2-transitive automorphism groups. A complete account of the relationship between designs and groups, as it was known in 1968, is contained in the beautiful book of DEMBOWSKI [40]. However, quite a lot has been done since then.

Since this is a combinatorics conference, I will try to minimize the group theory. However, the interplay between the groups and the designs they act on is fundamental to the subject: the fact that the automorphism group G of a design $\mathcal{D}$ permutes both the points and blocks of $\mathcal{D}$ suggests that these two actions should be played off against one another. Moreover, the manner in which designs occur in group-theoretic situations is a basic source for geometric problems and geometric theorems.

The difference between the study of 2-transitive designs and 2-transitive groups seems to be as follows. In the former case, one makes an assumption concerning the set stabilizer (or point-wise stabilizer) of a block: its transitivity properties, index in G, etc. In the latter case, one assumes structural properties of the stabilizer of one or more points. Just how fine a distinction this is can be seen from papers of O'NAN [128, 135], HARADA [63], ASCHBACHER [2,5], SHULT [149], KANTOR, O'NAN & SEITZ [107], and HERING, KANTOR & SEITZ [66], where designs are explicitly or

*) The preparation of this paper was supported in part by NSF Grant GP 37982X.

implicitly obtained in the course of "purely" group-theoretic investigations.

So as not to give a false impression, it should be noted that the relationship between permutation groups, geometry and combinatorics has been known for a long time - see the books of BURNSIDE [18] and CARMICHAEL [32].

There are also important relationships between projective planes and groups. However, I will not discuss collineation groups of projective, affine, or inversive planes at all - that would require a survey paper of its own. Incidentally, most of the problems and methods considered here become meaningless or trivial in the case of such planes. I hope to demonstrate the richness of the geometric nature of a subject spawned in part by, but quite different from, projective planes.

The organization of this paper is as follows. Section 1 consists of little more than geometric and group-theoretic notation. Section 2 discusses the elementary, well-known construction of designs from 2-transitive groups.

In the remaining sections, G will be an automorphism group 2-transitive on the points of a design $\mathcal{D}$. One natural approach is to first try to find $\mathcal{D}$, and then find G. Unfortunately, even if $\mathcal{D}$ is known to be a projective or an affine space, it is still very difficult to determine G (see section 3). This fact is, in turn, undoubtedly partly to blame for the difficulties encountered in the situations described in sections 6-10.

Section 4 contains a brief discussion of the geometry of the Mathieu groups. These designs and groups will arise in later sections.

The subject matter of this survey properly begins in section 5. There, and in the remaining sections, a variety of possible restrictions on 2-transitive designs are discussed. In each case, classical projective or affine spaces satisfy the additional hypothesis and partly motivate its study. With the exception of section 5, the goal will be the determination of $\mathcal{D}$, not of G.

Section 5 is devoted almost exclusively to results of O'NAN. The main geometric application of his striking classification theorems is to the subgroup of G fixing all the blocks through a point of $\mathcal{D}$.

HALL [58] considered the case where the 2-transitive design $\mathcal{D}$ is a Steiner triple system. In section 6, a more general situation is studied: $\lambda = 1$, and the stabilizer of two points fixes all points on the line through them.

In section 7, it is assumed that the pointwise stabilizer of a block of $\mathcal{D}$ is transitive on the complement of the block. An added combinatorial bonus here is the relevance of geometric lattices.

However, the richest combinatorial structure occurs in section 8, where $\mathcal{D}$ is assumed to be a symmetric design. As the length of the section indicates, more work has been done in this case than in any other. There are also several applications, which are discussed in sections 8 and 9; these include difference sets (section 8), Hadamard matrices (section 9), symmetric 3-designs (section 9), the suborbit structure of permutation groups (section 8), and the reducibility of certain complex polynomials (section 8).

Section 9 briefly discusses symmetric 3-designs. Finally, section 10 contains a variety of miscellaneous topics. An appendix lists the known 2-transitive groups.

Throughout the paper -and especially in section 10- I have occasionally digressed slightly from the main topic. In most cases, geometric questions related to 2-transitive groups are raised, even if designs are not involved. In fact, it would be absurd to claim that the only relationship between combinatorics and 2-transitive groups is through designs. The best examples of this, which will not be described here, are the graph extension theorem of SHULT [147] and the growing theory of 2-graphs (SEIDEL [143]; HIGMAN [71]; TAYLOR [155,156]). Also, if G is 2- but not 3-transitive, G_x determines graphs on $S - \{x\}$ which have yet to be studied. Probably the most basic problem in the combinatorial approach to 2-transitive groups is to find ways to use groups, designs, and graphs simultaneously. Thus far, this problem has been considered briefly in only two papers: SIMS [150] and O'NAN [133].

I am indebted to the following people for comments which helped in the preparation of this survey: P. CAMERON, M. FRIED, N. ITO, W. KNAPP, H. NAGAO, P. NEUMANN, and R. NODA.

1. BACKGROUND

A. Designs

A *design* $\mathcal{D}$ consists of a set S of points ("varieties" of wheat in the original statistical context), together with certain subsets called *blocks*,

such that the following conditions hold for some integers v,b,k,r,λ: there are v points, b blocks, k points per block, r blocks per point, and λ blocks through any two distinct points. The following non-degeneracy conditions will also be assumed: $v \geq k+2 > 4$, and some k-subset of S is not a block. The *parameters* v, b, k, r, λ satisfy $vr = bk$ and $\lambda(v - 1) = r(k - 1)$. Also, $b \geq v$ (FISHER's inequality).

$\mathcal{D}$ is a *symmetric design* if $b = v$, or equivalently, if $r = k$. The parameters v, k, λ, and $n = k - \lambda$ then satisfy further restrictions (see DEMBOWSKI [40, § 2.1]), but these will not be needed. A *Hadamard design* is a symmetric design with $v = 2k+1$.

If x is a point of a design $\mathcal{D}$, then $\mathcal{D}_x$ denotes the set $S - \{x\}$ of points together with the sets $B - \{x\}$, where B is a block on x. $\mathcal{D}$ is called an *extension* of $\mathcal{D}_x$.

If B is a block of $\mathcal{D}$, then $\mathcal{D}_B$ denotes the set of points of B and the sets $B \cap C$, where C is any block other than B. This is again a design if $\mathcal{D}$ is symmetric.

The *complementary design* $\mathcal{D}'$ of $\mathcal{D}$ is the design having the same point set as $\mathcal{D}$, and whose blocks are the complements of those of $\mathcal{D}$.

A *t-design* is a design $\mathcal{D}$ such that each set of t points is in the same number $\lambda_t > 0$ of blocks. If $\lambda_t = 1$, $\mathcal{D}$ is also called a *Steiner system* S(t,k,v).

A *line* of $\mathcal{D}$ consists of the intersection of all the blocks containing two given points. Two points are contained in a unique line. While lines of a design can usually have different sizes, they will automatically have the same size in this paper. Note that, when $\lambda = 1$, blocks are lines; in this case, I will use the more suggestive term line. Also, if $\lambda = 1$, a *subspace* of $\mathcal{D}$ is a set Δ of points such that, whenever x and y are distinct points of Δ, their line is contained in Δ.

An *automorphism* of $\mathcal{D}$ is a permutation of the points which also permutes the blocks. The automorphisms of $\mathcal{D}$ form a group Aut $\mathcal{D}$, the *automorphism group* of $\mathcal{D}$. The fact that Aut $\mathcal{D}$ permutes both the points and blocks is crucial.

If $\mathcal{D}$ is a symmetric design, the *dual* design $\tilde{\mathcal{D}}$ has the roles of points and blocks interchanged. $\tilde{\mathcal{D}}$ is symmetric, with the same parameters as $\mathcal{D}$. An *antiautomorphism* (or *correlation*) of $\mathcal{D}$ is an isomorphism $\theta: \mathcal{D} \to \tilde{\mathcal{D}}$. Then θ induces an isomorphism $\tilde{\mathcal{D}} \to \mathcal{D}$, also called θ, by acting on the points and blocks of $\tilde{\mathcal{D}}$ as θ does on the blocks of $\mathcal{D}$. θ is a *polarity* if $\theta^2 = 1$ (i.e. if $x \in y^\theta$ implies $y \in x^\theta$). If g is in Aut $\mathcal{D}$, so is $\theta^{-1}g\theta$. The group

(Aut $\mathcal{D}$) $\langle\theta\rangle$ contains Aut $\mathcal{D}$ as a subgroup of index 2, and contains all anti-automorphisms of $\mathcal{D}$.

The following notation will be used for the classical geometries: $PG_e(d,q)$, $1 \le e \le d-1$, denotes the design of points and e-spaces of $PG(d,q)$; and

$AG_e(d,q)$, $1 \le e \le d-1$, denotes the design of points and e-spaces of $AG(d,q)$.

As usual, $PG(2,q) = PG_1(2,q)$ and $AG(2,q) = AG_1(2,q)$. The automorphism group of $PG(d,q)$ is $P\Gamma L(d+1,q)$.

In section 7, *geometric lattices* will arise. These are (finite) lattices L such that each element is a join of points (i.e., atoms), and which satisfy the exchange condition: if x and y are points, and $X \in L$, then $x \not< X$ and $y < x \vee X$ imply $x < y \vee X$. Each $X \in L$ then has a dimension $\dim(X)$, where $\dim(0) = -1$, $\dim(X) = \dim(Y) - 1$ if $X < Y$ is maximal in Y, and $\dim(X \vee Y) + \dim(X \wedge Y) \le \dim(X) + \dim(Y)$ (for all $X,Y \in L$). Moreover, *bases* of X can be introduced as sets of $\dim(X) + 1$ points of L, none of which is in the join of the rest. The usual replacement conditions then hold for bases.

B. Permutation groups

Let H be a group *inducing* a group of permutations on a finite set S of points. It is essential to allow the possibility that non-trivial elements of H induce the identity on S. $H(S)$ denotes the (normal) subgroup of H consisting of those $h \in H$ fixing every point of S, that is, the pointwise stabilizer of S. H^S denotes the group of permutations of S induced by H. Thus, $H^S \cong H/H(S)$.

x^h denotes the image of $x \in S$ under $h \in H$. X^h denotes the image of $X \subseteq S$ under $h \in H$: $X^h = \{x^h \mid x \in X\}$.

$H_X = \{h \in H \mid X^h = X\}$ is the (set) *stabilizer* of X in H. Clearly, H_X contains the *pointwise stabilizer* $H(X)$ of X, and H_X induces the permutation group $H_X^X \cong H_X/H(X)$ on X. It is convenient to abbreviate $H_{\{x\}} = H_x$. If, say, $X,Y \subseteq S$ then $H_{XY} = H_X \cap H_Y$.

x^H denotes the *orbit* of x under H: $x^H = \{x^h \mid h \in H\}$. The orbits of H partition S.

H is *transitive* if $x^H = S$ for some (and hence each) x. Clearly, H is transitive on each of its orbits. H is *regular* if it is transitive and

$H_x = 1$ for some (and hence each) x. H is *primitive* on S if H is transitive on S and H_x is a maximal subgroup of H. H is t-*transitive* on S if it acts transitively on the ordered t-subsets of S. In this case, H_x is (t-1)-transitive on S - {x}. H is *sharply* t-*transitive* if it is regular on the set of ordered t-subsets of S; for $t \geq 2$, all such H have been determined (ZASSENHAUS [171,172]; JORDAN [89, pp.345-361]; HALL [57, pp.72-73]).

The *rank* of a transitive group H is the number of orbits of H_x. Thus, having rank 2 is the same as being 2-transitive. An *involution* in H is an element of order 2.

C. Preliminary lemmas

(1) ORBIT THEOREM. *If* $G \leq \mathrm{Aut}\ \mathcal{D}$, *then* G *has at least as many block-orbits as point-orbits. If* $\mathcal{D}$ *is symmetric, these numbers are the same* (see DEMBOWSKI [40, p.78]).

(2) *If* $\mathcal{D}$ *is a symmetric design, then each* $g \in \mathrm{Aut}\ \mathcal{D}$ *fixes the same number of points and blocks* (see DEMBOWSKI [40, p.81]).

(3) *If* $\mathcal{D}$ *is symmetric and* $1 \neq g \in \mathrm{Aut}\ \mathcal{D}$, *then* g *fixes at most* $\frac{1}{2}v$ *points* (FEIT [44]). As noted in KANTOR [102], FEIT's proof shows that, if g fixes exactly $\frac{1}{2}v$ points, then g is an involution and $v = 4n$.

(4) *Let* H *act as a permutation group on* S. *Let* $K \leq H$. *Then the normalizer* $N_H(K)$ *of* K *is contained in the set-stabilizer* $H_{\Omega(K)}$ *of the set* $\Omega(K)$ *of fixed points of* K. *Moreover, if* $g \in G$ *then* $\Omega(K^g) = \Omega(K)^g$.

(5) ORBIT LENGTH. *If* $X = x^H$ *is an orbit of* H *on* S, *then* $|X| = |H:H_x|$ *is the index in* H *of the stabilizer of* x.

(6) *Suppose* H *is as in* 1B *and let* X *and* Y *be orbits of* H. *If* d *is the g.c.d of* $|X|$ *and* $|Y|$, *and* $x \in X$, *then each orbit of* H_x *on* Y *has size divisible by* $|Y|/d$. *In particular, if* $d = 1$ *then* G_x *is transitive on* Y.

2. CONSTRUCTIONS

A. Basic construction

(1) *Let* G *be 2-transitive on the finite set* S. *Let* B *be any* k*-subset of* S,

and assume that G *is not transitive on (unordered)* k*-subsets of* S.. *Then the distinct sets* B^g, $g \in G$, *are the blocks of a design* $\mathcal{D} = \mathcal{D}(G,S,B)$.

PROOF. Each B^g has $|B| = k$ points. If $x^g = y$, then g sets up a 1-1-correspondence between the blocks on x and those on y; this provides us with r. The same proof yields λ. □

(2) $G \leq \mathrm{Aut}\,\mathcal{D}(G,S,B)$, *and* G *is transitive on blocks. Hence,* $\mathcal{D}(G,S,B)$ *has* $b = |G:G_B|$ *blocks* (see 1C(5)). *In particular,* $\mathcal{D}(G,S,B)$ *is symmetric if and only if* $|G:G_B| = v$.

Of course, the trouble with this construction is that B, and hence $\mathcal{D}$, may be totally unrelated to the action or structure of G. It is necessary to choose B carefully if $\mathcal{D}$ is to provide information about G. This is what will be done in later sections. One can, for example, assume that B is the set of fixed points of G_{xy}, $x \neq y$, or that G(B) is transitive on S - B.

In almost every case of interest, B is an orbit of some subgroup of G, so that G_B is transitive on B. Note that, *if* $\lambda = 1$, *then necessarily* G_B *is* 2*-transitive on* B.

PROOF. If $x,y,x',y' \in B$, $x \neq y$ and $x' \neq y'$, then any $g \in G$ such that $x^g = x'$ and $y^g = y'$ must fix B. □

If G is t-transitive, then $\mathcal{D}(G,S,B)$ is clearly a t-design.

B. When is $\lambda = 1$?

Suppose $\mathcal{D} = \mathcal{D}(G,S,B)$, where B is the set of fixed points of some subset W of G_{xy} (where $x \neq y$). In this situation (as in the general one) it is natural to ask when $\lambda = 1$. The simplest answer is due to WITT [169]:

(1) $\lambda = 1$ *if* $W^g \subseteq G_{xy}$ *and* $g \in G$ *imply* $W^g = W$.

PROOF. If $x,y \in B^g$, then W^g fixes x and y by 1C(4). That is, $W^g \subseteq G_{xy}$, so $W^g = W$. Thus, $B^g = B$. □

This result has been used in a variety of circumstances. For example, if G_{xy} is cyclic, it applies to every subgroup $W \neq 1$ of G_{xy} fixing more than two points; this was very useful in the determination of all such groups (KANTOR, O'NAN & SEITZ [107]). The designs and groups that arise

here are very interesting. Assume that G does not have a regular normal subgroup and that G_{xy} has such a subgroup W. Then $v = q^3 + 1$, $r = q^2$, and $k = q + 1$ for some prime power q. (In the terminology of DEMBOWSKI [40, p.104], these are the parameters of a *unital*.) There are just two possibilities. One is that G is PSU(3,q) or PGU(3,q), and the design consists of the absolute points and non-absolute lines of a unitary polarity of $PG(2,q^2)$. (See O'NAN [128] for a detailed study of this design.) In the other case, $q = 3^{2e+1}$ for some $e \geq 0$, and G is a group of Ree type (see WARD [163] and KANTOR, O'NAN & SEITZ [107] for some properties of G and the design); the case q = 3 will arise again in section 6, where the design is called $\mathcal{D}(4)$.

There is, of course, an obvious t-design analogue of WITT's result.

There are some other interesting conditions which imply $\lambda = 1$. The most striking one is due to O'NAN [130]:

(2) *Suppose* B *is the set of fixed points of* $W \leq G_{xy}$. *Assume that no element of* $G_{xy} - W$ *is conjugate in* G_x *to an element of* W. *Then* $\lambda = 1$.

It is worthwhile to compare this with 2B(1). The main hypothesis there concerns conjugates of W, while in 2B(2) it concerns conjugates of elements of W. On the other hand, 2B(1) considers *all* conjugates, while 2B(2) only considers conjugates in G_x.

The proof of 2B(2) is elementary, but not straightforward. The main application is as follows:

(3) *Suppose* N *is a normal subgroup of* G_x, $y \neq x$, $N_y \neq 1$, *and* N_y *fixes more than two points. Then* 2B(2) *applies to* $W = N_y$ (O'NAN [130]).

PROOF. Suppose $g \in G_x$. Then $W^g \cap G_{xy} \leq N^g \cap G_{xy} = N_y = W$. □

Note that N fixes every block through x. Both 2B(2) and 2B(3) are crucial in the proofs of the theorems in section 5.

(4) *Suppose* $G_{xy} < K < G_x$ *and* $B = \{x\} \cup y^K$. *Then* $\mathcal{D}(G,S,B)$ *has* $\lambda = 1$ *if either*

(i) *for any three points* x,y,z, G_x *has an element interchanging* y *and* z (O'NAN, unpublished; ATKINSON [6]; a t-design version has been found by NEUMANN [122]); *or*

(ii) $|B| \leq 4$ (O'NAN, unpublished).

A few comments are needed concerning 2B(4). If $\lambda = 1$ for a given $\mathcal{D}(G,S,B)$, let $x,y \in B$, $x \neq y$, and set $K = G_{xB}$. Then $G_{xy} < K < G_x$. This makes the hypothesis of 2B(4) seem more reasonable.

One example of 2B(4i) is provided by the following unpublished result of SHULT (applied to $H = G_x$ acting on $X = S - \{x\}$). Suppose H is transitive on X, and some involution $t \in H$ fixes exactly one point. Then, if $y,z \in X$, $y \neq z$, there is a conjugate of t interchanging y and z.

3. COLLINEATION GROUPS

A. Projective spaces

Let G be a collineation group of PG(d,q) which is 2-transitive on points. The only known examples are: $G \geq PSL(d+1,q)$, the group of projective collineations of determinant 1; and the peculiar but fascinating example $G \cong A_7$ acting on PG(3,2).

It seems unlikely that other examples exist, but this has been verified in only a few cases. WAGNER [162] proved this for $d \leq 4$, D.G. HIGMAN (unpublished) for $d = 5,6$, and KANTOR [102] for $d = 7,8$, or when $d = s^\alpha$ for a prime divisor s of q-1. The same conclusion holds if some non-trivial element of G fixes a (d-2)-space pointwise (WAGNER [162], HIGMAN [68], KANTOR [102]).

Here are two interesting properties of G.

(1) *If* E *is a plane, then* G_E^E *contains* PSL(3,q) (WAGNER [162]).

(2) *If* H *is a hyperplane, then* G_H *is 2-transitive on* S - H (KANTOR [93]).

Additional (but technical) properties of G are found in KANTOR [102].

(3) Since the example $G \cong A_7$ will arise in sections 6-8, it is perhaps worthwhile to discuss it in some detail. By one of the flukes of nature, $A_8 \cong PSL(4,2)$ (see 4A(2) for a proof). Thus, PG(3,2) does indeed have a collineation group $G \cong A_7$. Thus, A_8 can be regarded as acting on the 8 cosets of G, or on the $15 \cdot 14/2$ 2-sets of points of PG(3,2). By 1C(6), G is transitive on these 2-sets. It follows that G is indeed 2-transitive.

By 1C(5), if $x \neq y$ then $|G_{xy}| = 12$. Take a point z not on the line L through x and y. It is easy to see that G cannot contain any non-trivial elation (= transvection), so $G_{xyz} = 1$. Again by 1C(5), G_{xy} must be transitive (and hence even regular) on the 12 points not in L.

It is now not difficult to prove $G_x \cong PSL(3,2)$ and $G_{xy} \cong A_4$.

B. PERIN's results

What happens if some kind of additional transitivity is assumed in 3A? This question was posed and almost completely answered by PERIN [139]:

Suppose G *is transitive on the triangles of points of* PG(d,q). *Then* $G \geq PSL(d+1,q)$, *except perhaps if* $q = 2$ *and* d *is odd.* (In 3A(3), the collineation group A_7 of PG(3,2) was shown to be transitive on triangles.) *If* G *is transitive on tetrahedra, then* $G \geq PSL(d+1,q)$.

The proof is ingenious and surprisingly easy. It depends solely on elementary number theory and elementary group theory.

PERIN's results are certainly the strongest and most useful ones concerning 2-transitive collineation groups of finite projective spaces. They arise several times in later sections of this survey. They have also been useful elsewhere: they were involved in one of the first proofs used for the determination of the 2-transitive permutation representations of the groups PSL(n,q). This in turn led CURTIS, KANTOR & SEITZ [36] to the determination of the 2-transitive representations of all the finite Chevalley groups.

C. Affine spaces

(1) Now let G be a collineation group of AG(d,q) 2-transitive on points. Here, the question is whether G must contain the translation group V of the space. The only known counterexample is $G \cong PSL(3,2) \cong PSL(2,7)$ acting on AG(3,2).

Suppose, for a given d and q, G must contain V. Then by 3A(2), each 2-transitive collineation group of PG(d,q) must contain PSL(d+1,q). The only d and q for which it is known that $G > V$ must hold is $d = s^{\alpha}$ for a prime divisor s of q-1 (KANTOR [102]).

It is important to note that there are many 2-transitive groups $G > V$. The classification of these groups is equivalent to the classification of finite groups of semilinear transformations transitive on non-zero vectors.

(2) If G is also transitive on triangles, it can be shown that $G > V$, except perhaps if $q = 2$ and d is odd. If G is transitive on tetrahedra, then $G > V$.

D. Generalizations

PERIN [139] studied the more general situation in which G is a collineation group of PG(d,q) transitive on e-spaces. When combined with KANTOR [100], the result is that G is 2-transitive on points if $2 \le e \le d-2$, except for groups of order $31 \cdot 5$ line-transitive on PG(4,2); if $3 \le e \le d-3$, then $G \ge PSL(d+1,q)$ except perhaps if $q = 2$ and d is odd; if $4 \le e \le d-4$, then $G \ge PSL(d+1,q)$.

Suppose next that G is a collineation group of AG(d,q) transitive on e-spaces, where $1 \le e \le d-1$. It is then easy to see (by 1C(6)) that G_x is transitive on the e-spaces through x. If $2 \le e \le d-2$, this essentially reduces the problem to the one of the preceding paragraph.

4. THE MATHIEU GROUPS

The Mathieu groups will appear several times in the remainder of this survey. The following brief description of these groups and some of their properties is based primarily on WITT [169,170] and LÜNEBURG [111].

A. M_{22}, M_{23}, and M_{24}

(1) There are unique Steiner systems $\mathcal{W}_{22} = S(3,6,22)$, $\mathcal{W}_{23} = S(4,7,23)$, and $\mathcal{W}_{24} = S(5,8,24)$, discovered by WITT [169]. If x is a point of $\mathcal{W}_v$, then $(\mathcal{W}_v)_x = \mathcal{W}_{v-1}$ for $v = 24, 23$, and $(\mathcal{W}_{22})_x = PG(2,4)$.

Aut $\mathcal{W}_v$ is $(v-19)$-transitive on points and transitive on blocks. Write $M_{24} = \text{Aut } \mathcal{W}_{24}$ and $M_{23} = \text{Aut } \mathcal{W}_{23}$. If x and y are in $\mathcal{W}_{24}$, $x \ne y$, then $(M_{24})_{\{x,y\}} = \text{Aut } \mathcal{W}_{22}$ contains $M_{22} = (M_{24})_{xy}$ as a subgroup of index 2. The three groups M_{24}, M_{23} and M_{22} are simple groups, the "large" Mathieu groups.

If x,y and z are distinct points of $\mathcal{W}_{24}$, then $(M_{24})_x = M_{23}$, $(M_{24})_{xy} = M_{22}$, $(M_{24})_{\{x,y\}} = \text{Aut } \mathcal{W}_{22} = \text{Aut } M_{22}$, $(M_{24})_{xyz} = PSL(3,4)$, and $(M_{24})_{\{x,y,z\}} = P\Gamma L(3,4)$. Suppose B is a block of $\mathcal{W}_{24}$. Then $(M_{24})_B^B \cong A_8$ and $(M_{24})(B)$ is regular on S-B; here, $(M_{24})(B)$ induces an elation group of $(\mathcal{W}_{24})_{xyz} = PG(2,4)$ if $x,y,z \in B$.

(2) M_{24} provides an easy proof that $A_8 \cong PSL(4,2)$. Namely, consider $G = (M_{24})_B$. By 4A(1), $G^B \cong A_8$. But G(B) is elementary abelian of order

16, and is normal in G. It follows readily that A_8 is isomorphic to a subgroup of the automorphism group PSL(4,2) of G(B). Since $|A_8| = |PSL(4,2)|$, this proves $A_8 \cong PSL(4,2)$.

(3) Any two blocks B and C of W_{24} meet in 0, 2 or 4 points. M_{24} is transitive on the ordered pairs of blocks whose intersections have a fixed size. Also, if $|B \cap C| = 4$, then the symmetric difference B + C is a block.

Any two blocks of W_{23} meet in 1 or 3 points. M_{23} is again transitive on the ordered pairs of blocks meeting in 1 or in 3 blocks.

Any two blocks of W_{22} meet in 0 or 2 points. M_{22} is transitive as above.

(4) If B_0 is a block of W_{22}, there are 16 points outside B_0 and 16 blocks missing B_0. These form a symmetric design with parameters v = 16, k = 6, $\lambda = 2$ and full automorphism group $(\mathrm{Aut}\ M_{22})_{B_0} \cong S_6 \cdot V \cong Sp(4,2) \cdot V$, where $V = M_{22}(B_0)$ is an elementary abelian group of order 16. This design is $S^{-1}(4)$ in the notation of 8B(4).

(5) The remarks in 4A(4) can be interpreted in W_{24} as follows (CAMERON [24]). Fix a block B^* of W_{24} and set $S^* = S\text{-}B^*$. If $x,y \in B^*$, $x \neq y$, let S_{xy} be the set of all blocks B such that $B \cap B^* = \{x,y\}$. By 4A(4), $|S^*| = |S_{xy}| = 16$, and S^* and S_{xy} yield a symmetric design.

Let $z \in B^* - \{x,y\}$. Then S_{xy} and S_{xz} also determine a symmetric (16,6,2)-design: call $B \in S_{xy}$ and $C \in S_{xz}$ *incident* if $|B \cap C \cap S^*| = 1$. All the resulting symmetric designs are isomorphic (they are $S^{-1}(4)$ in the notation of 8B(4)).

B. M_{11} and M_{12}

(1) There are unique Steiner systems $W_{11} = S(4,5,11)$ and $W_{12} = S(5,6,11)$. If x, y and z are three points of W_{12}, then $(W_{12})_x = W_{11}$, $(W_{11})_{xy}$ is the miquelian inversive plane of order 3, and $(W_{11})_{xyz} = AG(2,3)$. Write $M_v = \mathrm{Aut}\ W_v$, v = 11,12. Then M_v is sharply (v-7)-transitive on the points of W_v, and is transitive on blocks. M_{11} and M_{12} are both simple; $(M_{12})_{\{x,y\}} = P\Gamma L(2,9)$.

$G_B \cong G_B^B \cong S_6$ if B is a block of W_{12}. Also, S-B is another block, and $G_{\{B,S-B\}} \cong \mathrm{Aut}\ S_6$.

(2) W_{12} is obtained from W_{24} as follows. Let B and C be blocks of the latter design such that $|B \cap C| = 2$. Then their symmetric difference B+C has size 12, and $(M_{24})_{B+C}$ is just M_{12}. Note that $|B \cap (B+C)| = 6$; the blocks of W_{12} are precisely the intersections of size 6 of B+C with blocks of W_{24}.

If $x,y,z \in B+C$, then $(W_{12})_{xyz} = AG(2,3)$ is embedded in $(W_{24})_{xyz} = PG(2,4)$ as the unital preserved by $P\Gamma U(3,2) = (W_{12})_{\{x,y,z\}}$. The latter group is precisely the full collineation group of AG(2,3).

Moreover, the complement of B+C again has the form B_1+C_1 (where $|B_1 \cap C_1| = 2$), and $(M_{24})_{\{B+C,B_1+C_1\}} = \text{Aut } M_{12}$ contains M_{12} as a subgroup of index 2.

(3) In the notation of 4B(2), fix a point $p \notin B+C$. Then $M_{11} = (M_{24})_{B+C,p}$ is 3-transitive on B+C (as well as on $(B_1+C_1) - \{p\}$). The W_{12} determined by B+C has exactly 22 blocks through p. Together with the points of W_{12} (i.e., B+C), these form a 3-design $\mathcal{D}$ with v = 12 and k = 6. If $x \in B+C$, then $\mathcal{D}_x$ is a symmetric (11,5,2)-design. Aut $\mathcal{D} = M_{11}$, and Aut $\mathcal{D}_x = (M_{11})_x \cong PSL(2,11)$. The designs $\mathcal{D}_x$ and $\mathcal{D}$ will reappear in sections 8 and 9.

C. Applications and characterizations

(1) The Mathieu groups are intimately linked to the sporadic simple groups of CONWAY [34,35], HIGMAN & SIMS [72], MCLAUGHLIN [119] and FISCHER [48]. For descriptions of these groups, see the above papers, LÜNEBURG [111], and SEIDEL [143].

Several characterizations of Mathieu groups will appear in sections 7 and 9. The following characterizations do not, however, fit into the framework of those sections.

(2) Let $\mathcal{D}$ be a Steiner system S(t,k,v). Suppose $G \leq \text{Aut } \mathcal{D}$ is transitive on the ordered (t+1)-tuples of points not contained in a block, and also on the ordered (t+2)-tuples of points no t+1 of which are contained in a block. Then $\mathcal{D}$ is PG(2,q), $AG_2(d,2)$, W_{22}, W_{23}, or W_{24} (TITS [158]).

(3) Let $\mathcal{D}$ be a Steiner system S(t,2t-2,v). Assume that, whenever B and C are distinct blocks and $|B \cap C| = t-1$, necessarily B+C is a block. Then $\mathcal{D}$ is $AG_2(d,2)$ or W_{24}. This striking result is due to CAMERON [29]. Actually, CAMERON proves a stronger theorem characterizing $PG_1(d,2)$ and W_{23}.

(4) I know of no satisfactory characterizations of the designs W_{11} or W_{12} in terms of the action of M_{11} or M_{12} on them. These 2-transitive designs do not seem to fit into any known general design setting as do the other three WITT designs. (There is, however, a lattice-theoretic setting; see KANTOR [103].)

5. NORMAL SUBGROUPS OF G_x

A. Situation

G is 2-transitive, and N is a non-trivial normal subgroup of G_x. Of course, I have in mind placing some restrictions on G_x of a geometric nature. Nevertheless, many purely group-theoretic results have been proved recently which are very useful to geometry. Here are two of these: if N is regular on S - {x}, then G is of known type (HERING, KANTOR & SEITZ [66], SHULT [146]); if $|S|$ is odd, $|N|$ is even, and all involutions in N fix only x, then G is either known or has a regular normal elementary abelian subgroup (ASCHBACHER [3]).

B. O'NAN's results

The best work presently being done on 2-transitive groups is due to O'NAN. Some of his general results are described in 5B and then applied in 5C.

(1) *Suppose* N *is abelian and not semiregular* (*i.e.*, $N_y \neq 1$ *for some* $y \in S-\{x\}$). *Then* $P\Gamma L(n,q) \geq G \geq PSL(n,q)$ *for some* $n \geq 3$ *and* q (O'NAN [130]).

(2) *Suppose* $N \cap N^g = N$ *or* 1 *for all* $g \in G$, *and* N *is not semiregular. Then* $P\Gamma L(n,q) \geq G \geq PSL(n,q)$ *for some* $n \geq 3$ *and* q (O'NAN [132]).

(3) *Suppose* N *is cyclic. Then either* G *has a regular normal subgroup, or* $G \geq PSL(2,q)$ *or* $PSU(3,q)$ *for a prime* q, *or* G *is* $P\Gamma L(2,8)$ (O'NAN, unpublished; ASCHBACHER [4]).

(4) *If* N *is abelian, and* $|N|$ *and* $|\Omega|$ *are odd, then* G *has a regular normal subgroup* (O'NAN [135]).

Further beautiful results are found in O'NAN [133]. While these are not strictly geometric, he finds very ingenious ways to use designs and graphs in his arguments.

O'NAN [134] considered the 3-transitive analogue of the above situation. He classified those 3-transitive groups G such that G_{xy} has a non-trivial abelian normal subgroup.

C. Applications

O'NAN's applications of his results are also basic for his proofs. Let $\mathcal{D}$ be a design and suppose $G \leq \mathrm{Aut}\ \mathcal{D}$ is 2-transitive on points.
Let N be the group of $g \in G_x$ fixing all blocks on x. Then N is normal in G_x.

Clearly, N is a very natural geometric subject. It corresponds to groups of central collineations of projective spaces, and dilatation groups of affine ones.

By 5B(2), $\mathcal{D}$ is a projective space if $N_y \neq 1$ for some $y \neq x$. By 5B(3,4), $\mathcal{D}$ is severely restricted if N is cyclic or if N is abelian and $|N|$ and v are both odd. The same is true if $|N|$ is even but each involution in N fixes only x (ASCHBACHER [3]). However, the case N abelian, $|N|$ odd, and v even has not yet been settled.

A slightly different application of 5B(2) is found in 8E(1).

There are, of course, analogous applications to t-designs with $t > 2$.

6. G_{xy} FIXES k POINTS

A. Situation

G is 2-transitive on S. If $x \neq y$, G_{xy} fixes precisely k points, where $2 < k < v$.

Let L be the set of fixed points of G_{xy}. By WITT's result 2B(1) (with $W = G_{xy}$), $\{L^g \mid g \in G\}$ yields a design $\mathcal{D}$ with $\lambda = 1$. Moreover, G_L^L is sharply 2-transitive on L, from which it follows that k is a prime power.

Possibly the main property of $\mathcal{D}$ and G is that the set of fixed points of any subgroup of G is a subspace of $\mathcal{D}$ (defined in 1A). In spite of all the subspaces of $\mathcal{D}$ this usually guarantees, it is very hard to get solid information about $\mathcal{D}$.

B. Known examples of $\mathcal{D}$

(1) $AG_1(d,k)$.

(2) $PG_1(d,2)$.

(3) A unique design $\mathcal{D}(4)$ with $v = 28$, $k = 4$. In this case, necessarily $G \cong P\Gamma L(2,8)$.

Note that, even if $\mathcal{D}$ is $AG_1(d,k)$ or $PG_1(d,2)$, in view of section 3 it is still very difficult to determine G. This fact is undoubtedly one of the major obstacles to the study of $\mathcal{D}$ itself. Note also that $G \cong A_7$ occurs here for $PG_1(3,2)$, in which case $G_{xy} \cong A_4$ is regular on S-L (cf. 3A(3)).

C. Classification theorems

The study of the present situation was initiated by HALL [58] in the case $k = 3$. His and all subsequent results have depended on 2-subgroups of G.

(1) *Suppose* $k = 3$ *and some line is the set of fixed points of an involution. Then* $\mathcal{D}$ *is* $AG_1(d,3)$, $PG(2,2)$, *or* $PG_1(3,2)$. (M. HALL [58] combined with J. HALL [55] or TEIRLINCK [157].)

(2) *Suppose some involution fixes just one point. Then* G *has a regular normal elementary abelian* p*-subgroup, where* p *is an odd prime and* $p|k$. (This is an easy consequence of GLAUBERMAN [53] and FEIT & THOMPSON [46]. The case $k = 3$ is in HALL [58], and is very elementary.)

The best result known is due to HARADA [63]:

(3) *Assume that all involutions fix at most* k *points. Then one of the following holds:*

(i) $\mathcal{D}$ *is* $AG(2,k)$, $PG(2,2)$ *or* $PG_1(3,2)$;

(ii) $\mathcal{D}$ *is* $AG_1(3,k)$ *with* k *odd; or*

(iii) $\mathcal{D}$ *is an affine translation plane of odd order* k.

(Actually, this is slightly different from HARADA's original formulation; see the Appendix of KANTOR [105].)

The only known non-desarguesian examples of (iii) have order $k = 9$. Results of HUPPERT [77] imply that there is a unique such example with G solvable. If G is non-solvable, results contained in CZERWINSKI [37] and HERING [65] show that the "exceptional" nearfield plane of order 9

is the only example possible; unfortunately, as of the writing of the present survey, these results had not quite been completely proved.

(4) *Assume that* G *is transitive on non-incident point-line pairs. Then* $\mathcal{D}$ *is* $AG_1(d,k)$ *or* $PG_1(d,2)$. (HALL and BRUCK for k = 3; see HALL [60] or DEMBOWSKI [40, pp.100-101]; KANTOR [99] in general. Other special cases are due to ITO [84] and OSBORN [136]. A variation on this theme is found in BUEKENHOUT [14].)

(5) *If some non-trivial element of* G_x *fixes all lines through* x, *then either* $\mathcal{D}$ *is* $PG_1(d,2)$ *or* $\mathcal{D}(4)$, *or* G *has a regular normal elementary abelian subgroup.*

PROOF. 5B(2) or 5B(3) applies to a non-trivial normal subgroup of G_x minimal with respect to fixing all lines through x. □

It is easy to see that 6C(5) contains 6C(2); however, 6C(2) is the far more useful result.

D. Subplanes

(1) In [58], HALL showed that, when k = 3, $\mathcal{D}$ has a subspace PG(2,2) or AG(2,3). Because of the 2-transitivity of G, $\mathcal{D}$ has many such concrete subplanes. What is lacking is a way to tie these subplanes together into a projective or affine space.

KANTOR [105] proved the following awkward result, which both generalizes HALL's result and implies 6C(4). $\mathcal{D}$ *must have a subspace such that either*

(i) $|\Delta| = k^i$, $i \geq 2$, *and* G_Δ^Δ *is 2-transitive, has a regular normal subgroup, and has no involution fixing more than one point;*

(ii) k = 3 *and* Δ *is* PG(2,2);

(iii) Δ *is an affine translation plane, and* G_Δ^Δ *contains the translation group and is flag-transitive or has exactly two flag-orbits (of the same size); or*

(iv) k *is a power of 2, and* Δ *is the design* $\mathcal{D}(k)$ *obtained from the dual of the complement of a completed conic in* PG(2,2k).

Note that, if k is prime, Δ is $AG_1(i,k)$ in (i) and AG(2,k) in (iii), so $\mathcal{D}$ must have AG(2,k) as a subplane if k > 3 is prime. As in 6C(2), it is very likely that CZERWINSKI [37] and

HERING [65] will imply that the only non-desarguesian planes which might arise in (iii) are the exceptional nearfield plane of order 9 or the plane obtained from the exceptional solvable 2-transitive group of degree 81 found by HUPPERT [77].

Once again, a method is needed for tying all these subplanes together.

(2) In this context, it is natural to recall the standard methods of gluing planes together to form projective or affine spaces: the axioms of VEBLEN & YOUNG [161], and the theorem of BUEKENHOUT [11]. Groups are not needed for these (nor even finiteness).

Let $\mathcal{D}$ be a design with $\lambda = 1$. If each triangle is contained in a subspace which is a projective plane, then $\mathcal{D}$ consists of the points and lines of a projective space (VEBLEN & YOUNG [161]).

If each triangle of $\mathcal{D}$ is contained in an affine plane of order > 3, then $\mathcal{D}$ consists of the points and lines of an affine space (BUEKENHOUT [11]). This is false if $k = 3$ (see HALL [58]). But here, if Aut $\mathcal{D}$ is primitive on points (e.g., if Aut $\mathcal{D}$ is 2-transitive), then $\mathcal{D}$ is an affine space. (This is contained in FISCHER [47]; it is also an easy consequence of HALL [58] and GLAUBERMAN [53]).

J. HALL [55] and TEIRLINCK [157] have also handled the case where each triangle of $\mathcal{D}$ is in a projective or affine plane (a situation which arises in proving 6C(1)).

There are further interesting geometric questions of this sort that can be asked, with or without a group present; see BUEKENHOUT & DEHERDER [17].

E. Higher transitivity

It is natural to modify the situation under consideration as follows: G is t-transitive on S, and the stabilizer of t points fixes exactly k points, where $2 < t < k < v$. This time, the design $\mathcal{D}$ is a Steiner system $S(t,k,v)$. If B is a block, G_B^B is sharply t-transitive.

(1) Suppose that $t = 3$. The only known examples of $\mathcal{D}$ are:
(i) $AG_2(d,2)$, and (ii) if $PGL(2,q^i)$, $i \geq 2$, is regarded as acting on $GF(q^i) \cup \{\infty\}$, the blocks of $\mathcal{D}$ are the sets $(GF(q) \cup \{\infty\})^g$, $g \in PGL(2,q^i)$. Note that miquelian inversive planes are special cases of (ii).

It is not difficult to prove that the designs in (ii) have $P\Gamma L(2,q^i)$ as their full automorphism groups. For this reason, it seems as if the present situation should be much easier than that of 6A: if $k > 4$, G should be small.

Unfortunately, nothing is known here other than variations on the 2-transitive results of 6C and 6D. Thus, G_x acts on $S-\{x\}$ as a group satisfying the condition 6A. There is a natural definition for subspaces: sets Δ of points such that the block of $\mathcal{D}$ through any three points of Δ is again contained in Δ. There is always a subspace which is $AG_2(3,2)$ or is as in (ii) (where $k = q+1$); see KANTOR [105]. BUEKENHOUT [12,13] has proved other design versions of results related to 6C and 6D.

(2) According to a remarkable result of NAGAO [120], the case $t \geq 4$ does not occur. I will outline a proof, using an approach somewhat simpler than NAGAO's.

Suppose G exists; without loss of generality, $t = 4$. This time, G_B^B is sharply 4-transitive. There are thus just three cases (JORDAN [89, pp.245-361]; HALL [57, pp.72-73]):

(I) $k = 5$, $G_B^B \cong S_5$;

(II) $k = 6$, $G_B^B \cong A_6$; and

(III) $k = 11$, $G_B^B \cong M_{11}$.

(I) Here it is straightforward to use arguments of HALL [58] to find a subspace which is an extension of $AG_2(3,2)$ or the (miquelian) inverse plane of order 3. However, no such extensions exist. (This elementary, highly combinatorial approach was not used by NAGAO. In fact, case (I) was the hardest for him, requiring a complicated argument and involving the FEIT-THOMPSON theorem.)

(II) Let $t \in G$ be an involution and let f be its number of fixed points. Fix a 2-cycle (x,x^t) of t. If (y,y^t) is any other 2-cycle, then $\{x,x^t,y,y^t\}$ belongs to a unique block B, and t fixes B. Since t^B is in A_6, it fixes exactly two points z_1,z_2 of B. Conversely, any two fixed points z_1,z_2 of t uniquely determine a 2-cycle (y,y^t). Hence, t has exactly $\frac{1}{2}(v-f) - 1 = \frac{1}{2}f(f-1)$ 2-cycles other than (x,x^t). Thus, $v = f^2+2$. In particular, $f > 2$.

On the other hand, there are exactly $(v-3)/(k-3)$ blocks containing three fixed points of t, of which $(f-3)/(k-3)$ consist entirely of fixed points. Thus, $f^2+2 = v \equiv 0 \equiv f \pmod 3$, which is impossible.

(III) The same type of argument as in (II) shows that each involution t has exactly $f = \sqrt{v-2}$ fixed points. If (x,x^t) is a 2-cycle, then t commutes with some involution $u \in G_{xy}$. Here, t and u fix exactly $g < f$ common points.

Let Δ be the set of fixed points of t. Then Δ is a subspace of the design, and again as in (II), u fixes exactly $g = \sqrt{f-2}$ points of Δ. Here $g \geq 2$. There are $(v-2)(v-3)/9\cdot 8$ blocks containing two points fixed by t and u, of which $(f-2)(f-3)/9\cdot 8$ are fixed pointwise by t and $(g-2)(g-3)/9\cdot 8$ are fixed pointwise by both involutions. However, the conditions $v = f^2+2$, $f = g^2+2$, and $(v-2)(v-3) \equiv (f-2)(f-3) \equiv (g-2)(g-3) \equiv 0 \pmod 9$ cannot be met.

This contradiction proves NAGAO's theorem. Note that, in (II) and (III), the arguments were purely combinatorial, almost not requiring G.

7. JORDAN GROUPS

A. Situation

$\mathcal{D}$ is a design, $G \leq \mathrm{Aut}\,\mathcal{D}$ is 2-transitive on points and transitive on blocks, and G(B) is transitive on S-B. Intuitively, this means that $\mathcal{D}$ has many "axial automorphisms".

JORDAN [88] (= [89, pp.313-338]) initiated the study of essentially this situation from the point of view of permutation groups. Almost 100 years later, HALL [58] noticed the geometric content of JORDAN's assumptions.

B. Examples

(1) $PG_e(d,q)$, $1 \leq e \leq d-1$.

(2) $AG_e(d,q)$, $1 \leq e \leq d-1$ if $q \neq 2$, and $2 \leq e \leq d-1$ if $q=2$.
(This restriction is needed to eliminate the degenerate case $q = 2$, $e = 1$, where lines have only two points.)

(3) The Witt designs $\mathcal{W}_{22}$, $\mathcal{W}_{23}$ and $\mathcal{W}_{24}$ (see section 4).

For the latter designs, G must be M_{22}, Aut M_{22}, M_{23}, or M_{24}. By PERIN's results (see 3B), if $\mathcal{D}$ is $PG_e(d,q)$ then $G \geq PSL(d+1,q)$, except perhaps if $e = 1$, $q = 2$, and d is odd. (The collineation group $G \cong A_7$ of $PG(3,2)$ is, in fact, an example of this exceptional situation; see 3A(3).) Similarly, 3C applies when $\mathcal{D}$ is $AG_e(d,q)$.

C. Basic properties

(1) First of all, $v \geq 2k$.

W. KNAPP has been kind enough to look into the history of this result. That $v \leq 2k$ implies the 3-transitivity of G was first proved by JORDAN [88, Théorème 1] (and not by MARGGRAFF [114], as stated on p.34 of WIELANDT [166]). KNAPP found that, in his two inaccessible papers, MARGGRAFF [114,115] proved the impossibility of $v < 2k$ (see WIELANDT [166, pp.34-38] for a proof), and also showed that $v \geq \frac{5}{2}k$ if $v-k$ is not a power of 2 (but obtained no characterizations of this exceptional case). Finally, KNAPP noted inaccuracies in the reference to MARGGRAFF in WIELANDT's bibliography.

For the case $v \leq 6k$, see 7D(2).

(2) *Now let L consist of the set of intersections of families of blocks. Certainly, L is a lattice* (this has nothing to do with $\mathcal{D}$). *In fact, L is a geometric lattice* (see 1A for the terminology). *Moreover, G is transitive on bases of L, and, if $X \in L$, then $G(X)$ is transitive on $S-X$* (KANTOR [105], using different terminology).

PROOF. Let $\emptyset \neq X \in L$ and $X \subset B,C$ with B and C different blocks. Then $|S-(B \cup C)| = v-2k+|B \cap C| > 0$ by (1). Since $G(B)$ is transitive on $S-B$ and $G(C)$ is transitive on $S-C$, $G(B \cap C)$ is transitive on $S-(B \cap C)$. It follows that $G(X)$ is transitive on $S-X$. Consequently, $G(X)$ is transitive on those $Y \in L$ in which X is maximal, so that X is maximal in $X \vee y$ for all $y \in S-X$. This proves that L is a geometric lattice, and the remaining assertions follow easily. □

(3) There is a great deal of information contained in (2). For example, G is 3-transitive if and only if lines have just two points, and is 4-transitive if and only if planes have just three points.

(4) If $X \in L$, $G(X)$ induces an automorphism group $\overline{G(X)}$ on the interval $[X,S] = \{Y \in L \mid X \leq Y\}$. $\overline{G(X)}$ is 2-transitive on those elements of $[X,S]$ of dimension $1 + \dim(X)$. If $\dim(X) \leq \dim(G) - 3$, then $\overline{G(X)}$ and the blocks in $[X,S]$ provide a group and a design satisfying the same conditions as G and $\mathcal{D}$.

Similarly, suppose for simplicity that G is not 3-transitive. Let $X \in L$ be neither $\emptyset$, a point, nor a line. Then G_X^X also acts on the interval $[\emptyset,X]$ as in 7A.

(5) By (4) and some classical geometry (or KANTOR [105], or DOYEN & HUBAUT [43]), if suitable intervals $[X,S]$ or $[\emptyset,X]$ are of known type, $\mathcal{D}$ is essentially known. (See KANTOR [105, 6.5] for a precise statement.) This fact provides very nice inductive possibilities.

D. Characterizations

(1) *If* $k = 3$, *then* $\mathcal{D}$ *is* $PG_1(d,2)$ *or* $AG_1(d,3)$. (This is the HALL-BRUCK theorem; see 6C(4).)

(2) *If* $v \leq 6k$, *then* $\mathcal{D}$ *is a projective or affine space,* W_{22}, W_{23}, *or* W_{24} (KANTOR [105]). *Moreover, in this case,* G *is even known.*

(3) *If* G_B *is 2-transitive on* S-B, *then* $\mathcal{D}$ *is* $PG_{d-1}(d,q)$, $AG_{d-1}(d,2)$, W_{22}, W_{23}, *or* W_{24}, *and* G *is known* (KANTOR [105]).

(4) *If* $G(B)$ *has an abelian subgroup transitive on* S-B, *the conclusions of* (3) *hold.*

PROOF. BY 7C(5), without loss of generality G is not 3-transitive, so lines have $h > 2$ points. Fix $x \in B$. Then the given abelian group $A \leq G(B)$ is transitive on the $(v-k)/(h-1) < |A|$ lines on x not in B. It follows that some $a \neq 1$ in A fixes all lines through x. Now a result of O'NAN [130] (see 5B(2)) completes the proof. □

Special cases of (4) are found in KANTOR [105,106], and MCDONOUGH [117,118].

(5) *If* $v-k$ *is a prime power, the conclusions of* (3) *hold.* (KANTOR [104]; special cases are in KANTOR [105,106], and MCDONOUGH [117,118]. Stronger results are proved in KANTOR [104].)

PROOF. By 7C(5), without loss of generality $\lambda = 1$. Let p be the prime dividing v-k. Let $B \cap C = x$. A Sylow p-subgroup P of G(B) is transitive on S-B. Since $|P:P_C| = r-1 < v-k$, P_C fixes no point of S-B. Since P_C normalizes a Sylow p-subgroup Q of G(C), it centralizes some $q \neq 1$ in the center of Q. Then q fixes the set B of fixed points of P_C. Now the transitivity of Q on S-C implies that q fixes all lines through x. Once again, O'NAN's theorem 5B(2) completes the proof. □

(6) *If* G(B) *has a subgroup normal in* G_B *and regular on* S-B, *then the conclusions of* (3) *hold or* $\mathcal{D}$ *is* $PG_1(3,2)$ *or* $AG_2(4,2)$. (KANTOR [97]; special cases have already been mentioned in 6C(4). This result, and its proof, were motivated by the HERING-KANTOR-SEITZ-SHULT theorem, already mentioned in 5A.)

E. Applications

(1) KANTOR & MCDONOUGH [106] showed that, *if* G *is a permutation group of degree* $v = (q^n-1)/(q-1)$ *containing the 2-transitive group* PSL(n,q), $n \geq 3$, *then either* G *contains the alternating group or* $PSL(n,q) \leq G \leq P\Gamma L(n,q)$.

PROOF. If G is as much as $k = (q^{n-1}-1)/(q-1)$ transitive, results of WIELANDT [164] imply that G is alternating or symmetric. If G is not k-transitive, let $\mathcal{D}$ have as blocks $\{H^g \mid g \in G\}$, where H is a hyperplane. Now use any one of D(3, 4, or 5). □

Unfortunately, the preceding proof does not apply when n = 2. That case is far more interesting than the case $n \geq 3$, since $PSL(2,11) < M_{12} < A_{12}$ and $PSL(2,23) < M_{24} < A_{24}$. In fact, the study of groups G satisfying $PSL(2,p) < G < A_{p+1}$, with p prime, is precisely what led MATHIEU to the discovery of M_{12} and M_{24}. NEUMANN [124] has recently proved that G is necessarily 4-transitive here. For an application of this problem to coding theory, see SHAUGHNESSY [144].

(2) Several of the classification theorems concerning Jordan groups can be interpreted as stating that certain natural attempts at generalizing M_{22}, M_{23} and M_{24} lead to nothing new.

(3) PRAEGER [141] has recently used D(2) in the course of proving some general results concerning 2-transitive groups. Another recent appli-

cation of JORDAN's original situation is made in the beautiful paper of SCOTT [142].

F. Problem

Besides the obvious problem of determining all designs admitting Jordan automorphism groups, there is a natural, interesting type of problem these designs lead to.

First, can G be acting on the set S of points of PG(d,q) or AG(d,q) without $\mathcal{D}$ being $PG_e(d,q)$ or $AG_e(d,q)$ for some e? The answer is no for PG(d,q), q > 2, by results of PERIN [139] (see 3B).

Now let's forget the group, and just consider the remaining geometric situation. Can a design with $\lambda = 1$ be constructed using all the points, and some but not all e-spaces, of a projective or affine space? Such designs are probably rare. There is an obvious generalization of this question in which a generalization of t-designs is involved.

Next, can a design with $\lambda > 1$ be constructed using some but not all e-spaces, in which the lines of the design consist of all the lines of the underlying geometry? I conjecture that this is impossible.

8. 2-TRANSITIVE SYMMETRIC DESIGNS

A. Situation

$\mathcal{D}$ is a symmetric design, and $G \leq \mathrm{Aut}\ \mathcal{D}$ is 2-transitive on points.

2A(2) indicates the group-theoretic interpretation of this situation. Note that the complementary design $\mathcal{D}'$ satisfies the same conditions as $\mathcal{D}$.

B. Examples

There are several very interesting examples of 2-transitive symmetric designs. It is only necessary to describe one of $\mathcal{D},\mathcal{D}'$. In each case, $\mathcal{D}$ has polarities.

(1) Projective spaces: $PG_{d-1}(d,q)$. Of course, $\mathrm{Aut}\ \mathcal{D} = P\Gamma L(d+1,q)$. In view of section 3, from this example it should already be clear that there will be serious obstacles to the study of G.

(2) The unique 11-point Hadamard design W_{11}. Here v = 11, k = 5, λ = 2 (compare 4B(3)). The only possible G is G = Aut $W_{11} \cong$ PSL(2,11). Here, $G_B \cong A_5$ acts as A_5 on B and as PSL(2,5) on S-B. W_{11} has polarities θ, and $G\langle\theta\rangle \cong$ PGL(2,11).

(3) G. HIGMAN's design W_{176} (see G.HIGMAN [73]; SIMS [150]; SMITH [152, 153]; CONWAY [35]). Here, v = 176, k = 50, and λ = 14. The only possible G is G = HS, the sporadic simple group of D.G. HIGMAN & C.C. SIMS [72]. $G_B \cong$ PSU(3,5) has rank 3 on B (and $G_{xB} \cong A_7$ if $x \in B$), while G_B acts on S-B in its usual 2-transitive representation of degree 5^3+1. Also, W_{176} has polarities ϕ, and $G\langle\phi\rangle \cong$ Aut HS.

W_{176} has a fascinating property: there is a 1-1-correspondence θ from 2-sets of points to 2-sets of blocks which is preserved by G. Here, θ is not induced by a polarity of W_{176}. Moreover, $G_{\{x,y\}} = G_{\{x,y\}^\theta} \cong Z_2 \times$ Aut A_6.

(4) The symplectic symmetric designs $S^\varepsilon(2m)$, one for each $m \geq 2$ and $\varepsilon = \pm 1$. Here $v = 2^{2m}$, $k = 2^{m-1}(2^m+\varepsilon)$, $\lambda = 2^{m-1}(2^{m-1}+\varepsilon)$. $S^1(2m)$ and $S^{-1}(2m)$ are complementary designs.

Set G = Aut $S^\varepsilon(2m)$. Then G has a regular normal elementary abelian 2-subgroup V of order $v = 2^{2m}$, and $G = VG_x$, $V \cap G_x = 1$, where $G_x \cong Sp(2m,2)$ is a symplectic group acting on V in the usual way. $G_B \cong Sp(2m,2)$ is 2-transitive on B and S-B. If $x \in B$, then G_{xB} is the orthogonal group $GO^\varepsilon(2m,2)$.

Moreover, by 2A, the preceding properties of G completely determine $S^\varepsilon(2m)$. It is remarkable that these properties were implicitly contained in work of JORDAN 100 years ago (see JORDAN [89, pp.XXI-XXIII] and [90, pp.229-249]).

Any subgroup of G of the form VT, with $T \leq G_x$ transitive on V - {1}, is 2-transitive on $S^\varepsilon(2m)$; for example, T can be $Sp(2e,2^f)$ whenever ef = m. The question of whether every 2-transitive automorphism group necessarily contains V leads to the same difficulties as in 3C.

In view of the action of G_x on V, there is an involution $t \in G_x$ fixing exactly $\frac{1}{2}v$ points (t is a transvection). If x_1 and x_2 are distinct points, there is a unique conjugate of t interchanging x_1 and x_2.

$S^\varepsilon(2m)$ has interesting combinatorial properties. Let + denote the symmetric difference of sets of points. If B, C and D are any blocks,

then B+C+D is either a block or the complement of a block. (This property alone does not quite characterize these designs.) If $B \neq C$, then V_{B+C} is transitive on B+C. (This property does characterize $S^{\epsilon}(2m)$, assuming only that V is an automorphism group of a symmetric design regular on points; see KANTOR [101].)

Here's another description of $S^1(2m)$. Consider the dual of a completed conic in $PG(2,2^m)$. Use the dual of the knot as the line at infinity of $AG(2,2^m)$. Let B be the union (in $AG(2,2^m)$) of the remaining 2^m+1 lines. Then the translates of B are the blocks of $S^1(2m)$.

A similar description of $S^1(4(2e+1))$ can be given in terms of the LÜNEBURG-TITS affine planes of order $2^{2(2e+1)}$ (defined in LÜNEBURG [110,111]): once again, the dual of a suitable oval can be used, in which the dual of the line at infinity is the knot. I know of no other planes which yield any designs $S^1(2m)$ in this manner, but such planes undoubtedly exist (and merit study).

A (-1,1)-incidence matrix of $S^{\epsilon}(2m)$ is a Hadamard matrix known since the last century: the tensor product of m Hadamard matrices of size 4. BLOCK [9] first noticed (using this incidence matrix) that Aut $S^{-1}(2m)$ is 2-transitive on points for each m. He pointed this out to me in 1968. All the properties of $S^{\epsilon}(2m)$ just described were proved at that time, and eventually appeared in KANTOR [101]. The designs were later rediscovered by RUDVALIS (1969, unpublished), HILL [74], and CAMERON & SEIDEL [30]. The latter paper provides an interesting relationship between these designs and coding theory.

C. Basic properties

The most famous result concerning 2-transitive symmetric designs is the beautiful theorem of OSTROM & WAGNER [137]: *if* $\lambda = 1$, *then* $\mathcal{D}$ *is a desarguesian projective plane*. Consequently, I will assume $\lambda > 1$ throughout this section.

(1) G *is 2-transitive on blocks. If* B *is a block, then* G_B *is transitive on* B *and* S-B, *and dually. Moreover, if* (v,k) = 1, *then* G_{xB} *is transitive on* S-B (by 1C(6)), *and dually.*

(2) *If* G_B *is 2-transitive on both* B *and* S-B, *then the dual statements hold and* G_x *has rank* 3 *on* S - {x}. (More generally, in KANTOR [93] it is proved that, *if* G *is an automorphism group of a design 2-transitive on*

points and transitive on blocks, and if G_B *is 2-transitive on both* B *and* S-B, *then the rank* ρ *of* $G_x^{S-\{x\}}$ *satisfies* $\rho \leq 5$, *and even* $\rho \leq 3$ *if* $v \neq 2k$.)

(3) *If* $\mathcal{D}$ *is a Hadamard design,* G_B *is necessarily 2-transitive on* S-B. This will be proved in 8C(5) below. Further special transitivity properties are found in KANTOR [93], especially Lemma 4.2.

(4) In KANTOR [93], a great deal of attention is paid to the case $k|v-1$ (which is equivalent to $(k,\lambda) = 1$, and which holds in $PG_{d-1}(d,q)$ and H_{11}). Assume this condition. *Then* G_B *must be primitive on* S-B. (In view of KANTOR [91, 4.7 and 4.8], the same conclusion holds under much weaker numerical restrictions.) Also, G has a simple normal subgroup 2-transitive on points.

Of course, the example $S^\epsilon(2m)$ shows that the last assertion does not hold in general. KANTOR [93] showed that $\mathcal{D}$ has the parameters of $S^\epsilon(2m)$ for some m,ϵ if G has a regular normal subgroup.

(5) As an example of the proofs of transitivity properties, I will prove: *if* $k-1|v-1$ (*or equivalently, if* $\lambda|k$), *then* G_B *is 2-transitive on* B. (Note that this implies 8C(2) when $\mathcal{D}$ is the complementary design of a Hadamard design.)

PROOF. G_x is transitive on the $v-1$ points $\neq x$, and on the k blocks B on x. By 1C(6), each orbit of G_{xB} on $S - \{x\}$ has size divisible by $(v-1)/(v-1,k)$. But $k = \lambda\cdot(v-1)/(k-1)$ implies that $(v-1,k) = (v-1)/(k-1)$. Thus, G_{xB} has an orbit on $B - \{x\}$ of size divisible by $k-1$. □

In the next section it will be seen how desirable it is to have sufficiently strong transitivity results.

D. The DEMBOWSKI-WAGNER theorem

This theorem provides the basic characterization of projective spaces needed for the study of symmetric designs. Namely:

$\mathcal{D}$ is a projective space if any one of the following holds:

(i) *every line meets every block;*

(ii) *every line has at least* $1 + (v-1)/k$ *points; or*

(iii) G *is transitive on ordered triples of non-collinear points.*

Slightly stronger combinatorial characterizations are found in DEMBOWSKI [40, pp.65-67], and KANTOR [92,93]; in particular, the latter reference describes the relationship with geometric lattices.

PROOF. If L is a line of $\mathcal{D}$ (the intersection of the λ blocks containing two points), there are $v-\lambda-|L|(k-\lambda)$ blocks missing L. Since $(v-\lambda)/(k-\lambda) = 1+(v-1)/k$, this implies that (i) and (ii) are equivalent; assume both of them. If $x \notin L$, and if ρ blocks contain x and L, then there are $k-\rho = |L|(\lambda-\rho)$ blocks on x not containing L. Thus, ρ is a constant, so planes can be defined, and each is determined by any triangle in it. Suppose L and M are distinct lines of a plane E. Then some block $B \supset L$ does not contain E. Since B meets M, $L \cap M = E \cap (B \cap M) \neq \emptyset$. Thus, E is a projective plane, so $\mathcal{D}$ is a projective space (VEBLEN & YOUNG [161]).

Now assume (iii). Then G_L is transitive on L and S-L. By the Orbit Theorem 1C(1), G_L has just two block-orbits. Since these must be the blocks containing L and the blocks meeting L once, (i) holds. □

E. Classification theorems

Many theorems have been proved classifying 2-transitive symmetric designs under suitable additional conditions. A catalogue of these follows.

(1) *If* G(B) ≠ 1, *then* $\mathcal{D}$ *is a projective space* (ITO [81]). Thus, in the remainder of this section it may be assumed that G(B) = 1.

PROOF. G is 2-transitive on blocks. G(B) is a non-trivial normal subgroup of G_B. Each non-trivial element of G(B) fixes more than one point, and hence more than one block (1C(2)). A theorem of O'NAN [132] (see 5B(2)) now applies. (Of course, this wasn't ITO's original proof.) □

(2) *If* $\mathcal{D}$ *has the same parameters as* $PG_{d-1}(d,q)$, *then* $\mathcal{D}$ *is* $PG_{d-1}(d,q)$ (KANTOR [98]).

(3) *If* k *is prime, then* $\mathcal{D}$ *is* $\mathcal{W}_{11}$ *or a projective space* (KANTOR [93]; the case where v and k are prime is due to ITO [3]). From this it follows easily that $\mathcal{D}$ is $\mathcal{W}_{11}$ or a projective space if (v-1)/2 is prime.

(4) *If* $n = k-\lambda$ *is prime,* $\mathcal{D}$ *is* $\mathcal{W}_{11}$, $(\mathcal{W}_{11})'$, *or* PG(2,n)' (KANTOR [93]).

(5) *If* k/2 *is prime, then* $\mathcal{D}$ *is a projective space,* PG(2,2)', $(\mathcal{W}_{11})'$, $S^1(4)$, *or* $S^{-1}(4)$ (ITO & KANTOR [87]).

(6) *If* n/2 *is prime, then* $\mathcal{D}$ *is* $S^1(4)$ *or* $S^{-1}(4)$.

(7) *If* k-1 *is prime and* $\lambda > 2$, *then* $\mathcal{D}$ *is* $(W_{11})'$ *or* $PG_{d-1}(d,2)'$.

PROOF. Write k-1 = p. Then $\lambda(v-1) = p(p+1)$ and $k > \lambda+1$ imply $p \mid v-1$, so $p \mid |G|$. A Sylow p-subgroup of G fixes a block B and a point x, and is transitive on B - {x}. Thus, G_B is 2-transitive on B. By 8E(10) (see below), it may be assumed that G_B is not 3-transitive on B. Also, by 8E(1), G(B) = 1. BURNSIDE [18, p.341] and classification theorems now yield the precise structure of G_B, from which $\mathcal{D} = (W_{11})'$ is readily deduced. □

(8) *If* k-1 *and* v *are prime, then* $\mathcal{D}$ *is* $(W_{11})'$ (ITO [83]).

Note that theorems 8E(2)-(8) all assume nothing more than *numerical* restrictions. In theorems 8E(9)-(14), further *transitivity* conditions will be imposed.

(9) *If* $\mathcal{D}$ *is a Hadamard design, and* G_B *is 2-transitive on* B, *then* $\mathcal{D}$ *is* W_{11} *or a projective space* (KANTOR [93]).

(10) *If* G_B *is 3-transitive on* B *and* $\lambda > 2$, *then* $\mathcal{D}$ *is* $PG_{d-1}(d,2)'$.

This is an unpublished result of CAMERON and KANTOR. The idea of the proof is as follows. As usual, $\mathcal{D}_B$ consists of the points of B and blocks $\neq$ B. Here, $\mathcal{D}_B$ is a 3-design. If $x \in B$, then $\mathcal{D}_B$ has the same number k-1 of points $\neq x$ as blocks on x. Thus, $\mathcal{D}_B$ is a symmetric 3-design, so a theorem of CAMERON [22] (see 10A,B) yields $k = 4\mu+4$, $\lambda = 2\mu+2$ or $k = (\mu+2)(\mu^2+4\mu+2) + 1$, $\lambda = \mu^2+3\mu+2$ (compare CAMERON [25]).

In the first case, $\lambda(v-1) = k(k-1)$ implies $v = 2k-1$, and 8E(9) applies to $\mathcal{D}'$. In the second case, if $x \notin B$ then G_{xB} has rank 3 on the blocks through x, and the parameter restrictions of HIGMAN [69] yield a contradiction.

(11) *If* G_B *is 2-transitive on both* B *and* S-B (compare 8C(2)), $\lambda > 2$, *and* 3 *points exist lying on no block, then* $\mathcal{D}$ *is* PG(d,2)'.

The proof is very similar to that of 8E(10). Note that the desired 3 points are easily shown to exist if $k \geq \lambda^2-\lambda+1$, except when $\mathcal{D}$ is $PG(3,\lambda-1)$.

(12) *If* $\lambda = 2$ *and* G_B *is 2-transitive on* S-B, *then* $\mathcal{D}$ *is* PG(2,2)', W_{11} *or* $S^{-1}(4)$ (CAMERON [29] and KANTOR [93]).

(13) *If* G_B *is 4-transitive on* B, *then* $\mathcal{D}$ *is* PG(2,2)', W_{11} *or* $S^{-1}(4)$. (This easy consequence of 8E(10) and 8E(12) is due to CAMERON [29].)

Further results of these types are found in KANTOR [3]. The following is quite a different sort of result, which (in spite of its technical nature) will be used in 8G.

(14) *Suppose* $k|v-1$, $x \notin B$, *and* G_{xB} *has a cyclic subgroup* A *regular on the points on* B *and the blocks on* x. *Then* $\mathcal{D}$ *is* W_{11} *or a projective space if either* (i) k *has no proper divisor* $\equiv 1 \pmod{\lambda}$, *or* (ii) $k < (\lambda+1)^2$ (KANTOR [93]). (In the projective space case, the given cyclic group is a Singer cycle of B.)

Some characterizations are also known for the designs $S^{\varepsilon}(2m)$ and W_{176}.

(15) *If some* $g \neq 1$ *in* G *fixes at least* $\frac{1}{2}v$ *points, then* $\mathcal{D}$ *is* $S^{\varepsilon}(2m)$ (KANTOR [101]).

(16) *If some* $g \neq 1$ *fixes* S-(B+C) *pointwise for some* $B \neq C$, *then* $\mathcal{D}$ *is* $S^{\varepsilon}(2m)$ *or* $PG_{d-1}(d,2)$ (KANTOR [101]).

Both 8E(15) and 8E(16) rely heavily on FEIT's result 1C(3) and the DEMBOWSKI-WAGNER theorem 8C. The only possible automorphisms g which actually occur in 8E(15) and 8E(16) are elations of the underlying classical geometry.

(17) *If* G *has a regular normal subgroup, and if* G_B *is 2-transitive on both* B *and* S-B, *then* $\mathcal{D}$ *is* $S^{\varepsilon}(2m)$ (KANTOR [101]).

(18) *Suppose* G *preserves a 1-1-correspondence from 2-sets of points to 2-sets of blocks. If* $n = (\lambda-2)^2/4$, *then* $\mathcal{D}$ *is* W_{176} *or* $S^1(4)$. (KANTOR, unpublished; this was proved under additional transitivity assumptions by SMITH [152]).

F. Prime v and linked systems

(1) One of the main sources of interest in 2-transitive symmetric designs is permutation groups G of prime degree v. These are necessarily

solvable or 2-transitive (BURNSIDE [18, p.341]. Very few 2-transitive examples are known: $P\Gamma L(d+1,q) \geq G \geq PSL(d+1,q)$ acting on $PG(d,q)$, for rare pairs d,q; $PSL(2,11)$ with $v = 11$; and A_v, S_v, M_{11} and M_{23}. Here, the first two types yield symmetric designs (see 10A for the sense in which M_{23} produces a generalization of a symmetric design). This naturally leads to the study of symmetric designs with prime v. The reader is referred to NEUMANN [123] for an excellent survey of the general question of 2-transitive groups of prime degree.

(2) If $\mathcal{D}$ is a symmetric design, v is prime, and Aut $\mathcal{D}$ is transitive, then $\mathcal{D}$ is obviously a difference set design. See HALL [56,61] (and his talk at this conference)*), MANN [113], and DEMBOWSKI [40] for the definitions and basic properties of difference set designs.

Of importance in the present context is the well-known fact that, if A is an abelian automorphism group regular on the points of a symmetric design $\mathcal{D}$, and if v is odd, then the map $a \to a^{-1}$, $a \in A$, does not induce an automorphism of $\mathcal{D}$. More generally: *an involutory automorphism of a design cannot fix just one block* (NEUMANN [121]).

Also, if $\mathcal{D}$ and A are as above, then $\mathcal{D}$ admits polarities.

In the case of 2-transitive symmetric designs with v prime, the only other known way of using the primality of v is through modular character theory (as in ITO [82,83]).

(3) In 1955, WIELANDT posed the following problem: can a 2-transitive group of prime degree v have more than two conjugacy classes of subgroups of index v? Certainly, two are possible, as has been noted in 8F(1).

Thus, suppose G is 2-transitive on each of the sets $S_1,\ldots,S_\mu$, $\mu > 2$, $|S_i| = v$ for each i, and the stabilizer of a point x_i in S_i fixes no point in any S_j, $j \neq i$. By 2A(2), each pair (S_i,S_j), $i \neq j$, determines a 2-transitive symmetric design. By 8C(1), G_{x_i} has two orbits on S_j. Thus:

(*) { if $x_i \in S_i$ and $x_j \in S_j$, $i \neq j$, then the number of $x_h \in S_h$, $h \neq i,j$, incident with both x_i and x_j, depends only on i,j,h and whether x_i and x_j are incident or not.

CAMERON [24] considered this situation from a purely combinatorial point of view. *A system of linked symmetric designs* consists of sets $S_1,\ldots,S_\mu$, $\mu > 2$, and an incidence relation between each pair of sets turning each pair into a symmetric design, such that (*) holds.

*) Mathematical Centre Tracts, 57, pp. 1-26.

Needless to say, there is a lot of arithmetic information in this situation. CAMERON rediscovered some such unpublished information due to WIELANDT and to ITO, but in the more general combinatorial setting. The conditions proved there are, however, too technical to reproduce. Additional numerical information has been obtained by ITO. For example, very recently, ITO [68] has shown that if v is prime, then for some design (S_i, S_j) neither k nor v-k can divide v-1.

Furthermore, NEUMANN [123] used a computer to show that WIELANDT's original situation cannot occur if $p < 2{,}000{,}000$. The proof of this provided a test for the available numerical data.

(4) WIELANDT has proved that, in the original situation in 8F(3), G can be the full automorphism group of at most one of the designs. (A proof is found in CAMERON [24].)

(5) The combinatorial setting is as interesting as WIELANDT's group-theoretic one: examples exist.

(a) Let V be a 2m-dimensional vector space over GF(q), $q = 2^e$. Let Sp(2m,q) act on V as usual. Then $G = V \cdot Sp(2m,q)$ has exactly q classes of complements to V (POLLATSEK [140]). Clearly, the scalar transformations act on this family of q sets, and it is not hard to see that Aut G is 2-transitive on these q sets. Since each pair of sets determines an $S^{\epsilon}(2me)$, this is a linked system of designs having $v = 2^{2me}$ and $\mu = q$.

(b) A much larger system is possible for a given $v = 2^{2m}$. Namely, a system of linked symmetric designs with $\mu = 2^{2m-1}$ has been constructed by GOETHALS from the KERDOCK [108] codes (see CAMERON [24] and CAMERON & SEIDEL [30]).

(c) CAMERON [24] notes the following construction for examples (a) and (b) when v = 16. In the notation of 4A(5), S^*, S_{xy}, S_{xz}, S_{yz} (with x,y,z three points of B^*) form example (a) with m = 1, e = 2. S^*, together with the seven sets S_{xy}, $y \in B^* - \{x\}$, for a fixed $x \in B^*$, form example (b) with m = 2.

In each of examples (a)-(c), each symmetric design is isomorphic to $S^{\epsilon}(2\ell)$ for some ℓ. No other examples are known of symmetric designs arising in linked systems.

(6) If $S_1', \ldots, S_\mu$ is a linked system, its *automorphism group* H consists of those permutations of $S_1 \cup \ldots \cup S_\mu$ which preserve both the partition and incidence. In example (a), H is 2-transitive on the q systems; the subgroup of H fixing each set S_i is 2-transitive on each S_i.

In example (b), H is known only for m = 2. Namely, from (c) it is clear that H contains $(M_{24})_{xB^*} \cong A_7 \cdot V$, where $V = M_{24}(B^*)$ is elementary abelian of order 16. In fact (CAMERON & SEIDEL [30]), $H \cong A_8 \cdot V \cong SL(4,2) \cdot V$, where V fixes S^* and each S_{xy}, while A_8 acts as usual on these 8 sets. The subgroup of H fixing 2 of the 8 sets is $A_6 \cdot V$, and induces an automorphism group of the resulting design $S^{-1}(4)$.

Some properties of H for certain types of linked systems (e.g., when v is prime) are found in WIELANDT [167] and CAMERON [24].

G. Some difference set designs

In this section, a special class of difference set designs will be considered. These are of interest for both combinatorial and number-theoretic reasons (see HALL [61] and MANN [113]).

(1) Let v be an odd prime power, and set F = GF(v). Let $1 < k < v-1$ and $k \mid v-1$, and let B = B(v,k) be the subgroup of F^* of order k. Let $\mathcal{D}(v,k)$ have the elements of F as points and the translates B+a, $a \in F$, as blocks. B is a difference set in F^+ if and only if $\mathcal{D}(v,k)$ is a symmetric design.

The designs $\mathcal{D}(v, \frac{1}{2}(v-1))$ are the Hadamard designs of PALEY [138], where $v \equiv 3 \pmod 4$ can be any prime power.

By DEMBOWSKI [40, p.35] (or an easy Singer cycle argument), $\mathcal{D}(v,k)$ cannot be a projective space if $\lambda > 1$. If $\lambda = 1$, the only desarguesian exceptions are PG(2,2) and PG(2,8).

(2) PROBLEM: what is Aut $\mathcal{D}(v,k)$?

Clearly, Aut $\mathcal{D}(v,k)$ contains the group S(v,k) of all mappings $x \to bx^\sigma + a$, $b \in B$, $a \in F$, $\sigma \in$ Aut F. In only three cases is Aut $\mathcal{D}(v,k) > S(v,k)$ known, namely, $\mathcal{D}(11,5) = \mathcal{W}_{11}$, $\mathcal{D}(7,3) = PG(2,2)$ and $\mathcal{D}(73,9) = PG(2,8)$. These are almost certainly the only possibilities.

This problem can be reformulated in terms of permutation polynomials. Let $f(x), g(x) \in F[x]$, and assume that both polynomials act as permutations of F. If

Needless to say, there is a lot of arithmetic information in this situation. CAMERON rediscovered some such unpublished information due to WIELANDT and to ITO, but in the more general combinatorial setting. The conditions proved there are, however, too technical to reproduce. Additional numerical information has been obtained by ITO. For example, very recently, ITO [68] has shown that if v is prime, then for some design (S_i, S_j) neither k nor v-k can divide v-1.

Furthermore, NEUMANN [123] used a computer to show that WIELANDT's original situation cannot occur if $p < 2{,}000{,}000$. The proof of this provided a test for the available numerical data.

(4) WIELANDT has proved that, in the original situation in 8F(3), G can be the full automorphism group of at most one of the designs. (A proof is found in CAMERON [24].)

(5) The combinatorial setting is as interesting as WIELANDT's group-theoretic one: examples exist.

(a) Let V be a 2m-dimensional vector space over GF(q), $q = 2^e$. Let Sp(2m,q) act on V as usual. Then $G = V \cdot Sp(2m,q)$ has exactly q classes of complements to V (POLLATSEK [140]). Clearly, the scalar transformations act on this family of q sets, and it is not hard to see that Aut G is 2-transitive on these q sets. Since each pair of sets determines an $S^{\epsilon}(2me)$, this is a linked system of designs having $v = 2^{2me}$ and $\mu = q$.

(b) A much larger system is possible for a given $v = 2^{2m}$. Namely, a system of linked symmetric designs with $\mu = 2^{2m-1}$ has been constructed by GOETHALS from the KERDOCK [108] codes (see CAMERON [24] and CAMERON & SEIDEL [30]).

(c) CAMERON [24] notes the following construction for examples (a) and (b) when v = 16. In the notation of 4A(5), S^*, S_{xy}, S_{xz}, S_{yz} (with x,y,z three points of B^*) form example (a) with m = 1, e = 2. S^*, together with the seven sets S_{xy}, $y \in B^* - \{x\}$, for a fixed $x \in B^*$, form example (b) with m = 2.

In each of examples (a)-(c), each symmetric design is isomorphic to $S^{\epsilon}(2\ell)$ for some ℓ. No other examples are known of symmetric designs arising in linked systems.

(6) If $S_1,\ldots,S_\mu$ is a linked system, its *automorphism group* H consists of those permutations of $S_1 \cup \ldots \cup S_\mu$ which preserve both the partition and incidence. In example (a), H is 2-transitive on the q systems; the subgroup of H fixing each set S_i is 2-transitive on each S_i.

In example (b), H is known only for m = 2. Namely, from (c) it is clear that H contains $(M_{24})_{xB^*} \cong A_7 \cdot V$, where $V = M_{24}(B^*)$ is elementary abelian of order 16. In fact (CAMERON & SEIDEL [30]), $H \cong A_8 \cdot V \cong SL(4,2) \cdot V$, where V fixes S^* and each S_{xy}, while A_8 acts as usual on these 8 sets. The subgroup of H fixing 2 of the 8 sets is $A_6 \cdot V$, and induces an automorphism group of the resulting design $S^{-1}(4)$.

Some properties of H for certain types of linked systems (e.g., when v is prime) are found in WIELANDT [167] and CAMERON [24].

G. Some difference set designs

In this section, a special class of difference set designs will be considered. These are of interest for both combinatorial and number-theoretic reasons (see HALL [61] and MANN [113]).

(1) Let v be an odd prime power, and set F = GF(v). Let $1 < k < v-1$ and $k \mid v-1$, and let B = B(v,k) be the subgroup of F^* of order k. Let $\mathcal{D}(v,k)$ have the elements of F as points and the translates B+a, $a \in F$, as blocks. B is a difference set in F^+ if and only if $\mathcal{D}(v,k)$ is a symmetric design.

The designs $\mathcal{D}(v, \frac{1}{2}(v-1))$ are the Hadamard designs of PALEY [138], where $v \equiv 3 \pmod 4$ can be any prime power.

By DEMBOWSKI [40, p.35] (or an easy Singer cycle argument), $\mathcal{D}(v,k)$ cannot be a projective space if $\lambda > 1$. If $\lambda = 1$, the only desarguesian exceptions are PG(2,2) and PG(2,8).

(2) PROBLEM: what is Aut $\mathcal{D}(v,k)$?

Clearly, Aut $\mathcal{D}(v,k)$ contains the group S(v,k) of all mappings $x \to bx^\sigma + a$, $b \in B$, $a \in F$, $\sigma \in$ Aut F. In only three cases is Aut $\mathcal{D}(v,k) >$ S(v,k) known, namely, $\mathcal{D}(11,5) = \mathcal{W}_{11}$, $\mathcal{D}(7,3)$ = PG(2,2) and $\mathcal{D}(73,9)$ = PG(2,8). These are almost certainly the only possibilities.

This problem can be reformulated in terms of permutation polynomials. Let $f(x), g(x) \in F[x]$, and assume that both polynomials act as permutations of F. If

$$f(x+b) - g(x) \in B \qquad \forall x \in F,\ \forall b \in B,$$

then the pair (f,g) determines an automorphism of $\mathcal{D}(v,k)$. Conversely, each automorphism determines such a pair (f,g), where f is the permutation induced on blocks and g the one on points.

(3) Write $G = \mathrm{Aut}\,\mathcal{D}(v,k)$, and assume $G > S(v,k)$. If v is prime, then G is 2-transitive on points by BURNSIDE's theorem on groups of prime degree (see BURNSIDE [18, p.341]). If $k = \frac{1}{2}(v-1)$, G must also be 2-transitive (KANTOR [93]; compare CARLITZ [31]; MCCONNEL [116]; BRUEN & LEVINGER [10]).

However, it is not known in any other cases that G must be 2-transitive if $G > S(v,k)$.

(4) *If* $G > S(v,k)$ *and* $k = \frac{1}{2}(v-1)$, *then* $\mathcal{D} = PG(2,2)$ *or* $\mathcal{W}_{11}$ (KANTOR [93]; for some small values of v, this was proved by TODD [159] and F. HERING [67]).

More generally, *if* G *is 2-transitive then* $\mathcal{D} = PG(2,2)$ *or* $\mathcal{W}_{11}$ *provided that either* $1 + \sqrt{k} > (v-1)/k$ *or* k *has no proper divisor* $\equiv 1 \pmod{\lambda}$.

PROOF. 8E(14) applies with $A = \{x \to bx \mid b \in B\}$. □

Further information when G is 2-transitive (but when the above numerical conditions do not hold) is found in KANTOR [93]. The fact that, even for these specific designs, it is not known whether Aut $\mathcal{D}$ can be 2-transitive, indicates the sad state of affairs concerning 2-transitive symmetric designs!

H. An application to the irreducibility of polynomials

A very unexpected sort of occurrence of 2-transitive symmetric designs has recently been found by M. FRIED. Let K be a subfield of the complex field C. If $f(x) \in K[x]$ and $g(x) \in C[x]$, it is natural to study the irreducibility of $f(x) - g(y)$ in $C[x,y]$. This question leads to difference set designs having 2-transitive automorphism groups!

The following discussion is based primarily on FRIED [49,50] (see also CASSELS [33]). f(x) is called *indecomposable* over K if it is not possible to write $f(x) = f_1(f_2(x))$ with $f_i \in K[x]$ and $\deg f_i > 1$, i=1,2; assume that this is the case. Assume further that g(x) cannot be written g(x) = f(ax+b)

for some $a,b \in C$, $a \neq 0$. Finally, assume that $f(x) - g(y) = \prod_{i=1}^{t} h_i(x,y)$ with $h_i(x,y) \in C[x,y]$ irreducible and $t > 1$.

FRIED shows that it may be assumed that deg f = deg g = v, say. Then g(x) is indecomposable over C. Moreover, t = 2. Write k = deg $h_1(x,y)$. Then there is a difference set mod v with k elements. The corresponding symmetric design $\mathcal{D}$ admits a 2-transitive automorphism group G. (Here, G can be interpreted as the Galois group of a suitable extension field of C(x).)

Furthermore, G is generated by permutations $s_1,\ldots,s_\mu$, with $\mu \leq 3$, such that (i) $s_1 \ldots s_\mu$ is a v-cycle on points, and (ii) $\sum_i \ell(s_i) = v-1 = \ell(s_1 \ldots s_\mu)$. (Here, $\ell(s_i)$ is the smallest integer ℓ such that s_i is the product of ℓ transpositions.)

Of course, $PG_{d-1}(d,q)$ and W_{11} are the only known cyclic difference set designs $\mathcal{D}$ for which Aut $\mathcal{D}$ is 2-transitive. (Examples 8B(3) and 8B(4) do not admit transitive cyclic automorphism groups.) FEIT [50] enumerated all cases in which these designs can arise in FRIED's situation; each case produces a pair of polynomials f(x), g(x).

Needless to say, conditions (i) and (ii) are weird from a geometric or group-theoretic point of view. Nevertheless, it should be clear that they merit further study.

Note that the study of the polynomial f(x) - g(y) is remarkably reminiscent of the situation in 8G(2).

In more recent work of FRIED [51], 2-transitive designs have arisen in which b = 2v and some element of order v has one v-cycle on points and two on blocks.

I. 2-transitive suborbits

One recent occurrence of 2-transitive symmetric designs has been in work of CAMERON [19,20,21,26], on multiply-transitive suborbits (i.e., orbits of G_x) of primitive permutation groups. Since these will be discussed in CAMERON's talk at this conference, the reader is referred to that talk *) and the above papers.

---

*) Mathematical Centre Tracts 57, pp. 98-129.

J. Problems

(1) The case $\lambda = 2$ should be feasible. The combinatorial structure here is extremely rich (see HUSSAIN [78,79], HALL [62], and CAMERON [23,29]). So, for that matter, is the permutation structure: G_B must be 2-transitive on B; if $x,y \in B$, $x \neq y$, then either G_B is 3-transitive on B, or G_{xyB} has two orbits of length $(k-2)/2$ on $B - \{x,y\}$ (KANTOR [3], CAMERON [23]). CAMERON [23,29] has indicated a possible approach to this problem.

Note that only three examples are known: PG(2,2)', $\mathcal{W}_{11}$ and $\mathcal{S}^{-1}(4)$.

(2) In the situation of 8C(2), there is a natural strongly regular graph structure on $S - \{x\}$. Unfortunately, the parameter restrictions on this graph and the tactical decomposition relations of DEMBOWSKI [38; 40, pp.60-61] involve too many unknowns. The latter relations were studied by KANTOR [93,101]; the former, in a purely combinatorial setting, by CAMERON [25] (using a method of GOETHALS & SEIDEL [54]). All the results thus far are very inconclusive.

(3) Prove that $\mathcal{D}$ is $\mathcal{S}^{\varepsilon}(2m)$ if G has a regular normal subgroup. As already mentioned in 8C(4), in this case $\mathcal{D}$ has the same parameters as some $\mathcal{S}^{\varepsilon}(2m)$.

(4) No satisfactory characterization of $\mathcal{W}_{176}$ is known. $\mathcal{W}_{176}$ and $(\mathcal{W}_{176})'$ are probably the only 2-transitive symmetric designs with $\lambda > 2$ and $v-2k+\lambda > 2$ in which G preserves a correspondence θ as in 8E(18); no numerical restrictions should be needed. (The main reason for the restriction in 8E(18) is to prevent k from being too large relative to λ.) If such a θ exists, $\mathcal{D}$ can be replaced (if necessary) by $\mathcal{D}'$ in order to obtain $\{x,y\} \subset X \cap Y$ if $\{x,y\}^{\theta} = \{X,Y\}$. Then $2(v-1)/k$ is an integer τ (so this situation is similar to the one considered in KANTOR [93], where $k \mid v-1$). If τ is odd, $G_{\{x,y\}}$ is transitive on $\{x,y\}^{\theta}$, and if $x \in B$, G_{xB} is transitive on the τ points $y \in B - \{x\}$ for which $B \in \{x,y\}^{\theta}$.

SMITH [152] has proposed a reasonable axiom one can assume in addition to the existence of θ in order to try to characterize $\mathcal{W}_{176}$, but this is too technical to state.

(5) Each of the known 2-transitive symmetric designs has polarities. Study these, and find some way to use them in the characterization of self-dual designs.

When v is prime, $\mathcal{D}$ automatically has "natural" polarities. However, no effective use has been found for them.

(6) The proof of 8E(2) in KANTOR [93] indicates that, when n is a power of a prime not dividing λ, $\mathcal{D}$ should be W_{11} or a projective space.

(7) Remove the numerical restrictions (i) and (ii) of 8E(14) and 8G(4).

(8) Answer WIELANDT's question (see 8F(3)). More generally, decide exactly what parameters can occur for linked systems (compare 8F(5)).

9. SYMMETRIC 3-DESIGNS

A. CAMERON's theorem

A *symmetric 3-design* is a 3-design $\mathcal{D}$ such that $\mathcal{D}_x$ is a symmetric design for each x. CAMERON [22] proved that the parameters of $\mathcal{D}$ must satisfy one of the following conditions (where μ is the number of blocks on any three points):

(i) $v = 4\mu + 4$, $k = 2\mu + 2$ (Hadamard 3-design);

(ii) $v = (\mu+2)(\mu^2+4\mu+2) + 1 = (\mu+1)(\mu^2+5\mu+5)$, $k = \mu^2+3\mu+2$;

(iii) $v = 112$, $k = 12$, $\mu = 1$ (extension of a projective plane $\mathcal{D}_x$ of order 10); or

(iv) $v = 496$, $k = 40$, $\mu = 3$.

Note that the λ for $\mathcal{D}$ is given by $\lambda = k-1$. Case (i) occurs if and only if there is a v×v Hadamard matrix. The only other case known to occur is $\mu = 1$ in (ii), when $\mathcal{D}$ is W_{22}.

For a generalization of CAMERON's theorem, see CAMERON [27].

B. 3-transitive automorphism groups

(1) Now suppose $G \leq \mathrm{Aut}\,\mathcal{D}$ is 3-transitive on points. Then G_x is a 2-transitive automorphism group of the symmetric design $\mathcal{D}_x$ (cf. section 8).

It is not hard to show that cases (iii) and (iv) cannot occur. Cases (i) and (ii) remain open. Some special values of μ have, however,

been ruled out by CAMERON [19], such as when $2 \leq \mu < 103$ or $\mu+1$ is a prime power.

For a remarkable occurrence of case (ii) -which originally led CAMERON to his theorem- see CAMERON [20,26].

(2) *If* G_B *is* 3*-transitive on* B*, then* $\mathcal{D}$ *is* $AG_{d-1}(d,2)$*, the unique Hadamard* 3*-design with* 12 *points, or* W_{22}. (This follows readily from 8E(9) and 8E(11).)

(3) Suppose next that $\mathcal{D}$ is a Hadamard 3-design. NORMAN [127] proved that $v = 12$ if μ is even. A slight modification of his argument shows that the same conclusion holds if G is 3-transitive on parallel classes of blocks. Note that, by 5B(4), the unique Hadamard 3-design having 12 points satisfies these conditions. The case n even -where $\mathcal{D}$ should be $AG_{d-1}(d,2)$- remains open.

C. Hadamard matrices

An automorphism of a Hadamard matrix H of size n is a pair (P,Q) of monomial nxn matrices such that PHQ = H. The automorphisms form a group $G = \mathrm{Aut}\, H$ containing $1 = (I,I)$ and $-1 = (-I,-I)$ in its center. $\bar{G} = G/\langle -1 \rangle$ acts faithfully as a permutation group on the union of the sets of rows and columns of H.

It may be assumed that the first row r and column c of H consist of 1's. Deleting columns 1 and n+1 of (H,-H) produces the (-1,1) incidence matrix of a Hadamard 3-design $\mathcal{D}$. Then $\bar{G}_c$ is the automorphism group of $\mathcal{D}$. In view of this, the results in B(2) and B(3) apply to $\mathcal{D}$. These in turn yield results about H. For example, if G is 4-transitive on rows, then n = 4 or 12. Another characterization of the case n = 12 follows from 6G(4) (KANTOR [94]).

Suppose n = 12. Then B(2) and the discussion of $\bar{G}_c$ imply that $\bar{G}_c \cong M_{11}$, from which $\bar{G} \cong M_{12}$ follows easily. However, $G \not\cong M_{12} \times \langle -1 \rangle$. At the end of 4B(2) it was noted that $|\mathrm{Aut}\, M_{12}| = 2|M_{12}|$. The resulting outer automorphism can be visualized in the present context as follows. $(P,Q) \in G$ implies that PHQ = H, and hence (since H is symmetric) that $Q^tHP^t = H$, so $(Q^t,P^t) \in G$. Thus, $(P,Q) \to (Q^t,P^t)$ is an automorphism of G, and induces one of $\bar{G}$; these are both outer automorphisms (see HALL [59]).

10. FURTHER TOPICS AND PROBLEMS

A. Block intersections

Let $\mathcal{D}$ be a t-design, $t \geq 2$. According to a generalization of FISHER's inequality $b \geq v$, if $v \geq k+\frac{1}{2}t$ then $b \geq \binom{v}{[\frac{1}{2}t]}$ (WILSON & RAY-CHAUDHURI [168]). Equality holds only if $t = 2s$ for an integer s, and then $\mathcal{D}$ is called a *tight t-design*. (This is evidently a generalization of symmetric designs.) WILSON & RAY-CHAUDHURI also proved that, if $\mathcal{D}$ is a 2s-design, then $\mathcal{D}$ is tight if and only if there are at most s different intersection sizes $|B \cap C|$, where B and C run through all pairs of distinct blocks (cf. CAMERON [25]).

It is natural to consider 2s-transitive automorphism groups of tight 2s-designs. Partly motivated by the group-theoretic context, ITO [85] has just completed a proof that the only tight 4-designs are degenerate ($v = k-2$), W_{23}, or its complementary design $(W_{23})'$. The case $s > 2$ remains completely open in both the combinatorial and group-theoretic contexts.

One way to guarantee that a t-design $\mathcal{D}$ has few intersection sizes $|B \cap C|$ is to assume that $G = \mathrm{Aut}\,\mathcal{D}$ is block-transitive and has small block-rank ρ; thus, G_B has exactly ρ block orbits (so there are at most $\rho-1$ different sizes $|B \cap C|$ with $B \neq C$). This was considered by NODA [126] when $\mathcal{D}$ is a Steiner system $S(t,k,v)$. He assumed $t = 3$ or 4 and $\rho = 3$ or 4, and showed $\mathcal{D}$ must be W_{22}, W_{23}, W_{24} or $AG_2(3,2)$. The proofs are very similar to tight design arguments. (In fact, the case $t = 4$, $\rho = 3$ follows from the aforementioned results of WILSON & RAY-CHAUDHURI.)

It should also be possible to handle the case $t = 2$, $\lambda = 1$ and $\rho = 3$. Here, G_B is transitive on the lines disjoint from B, and G_x is 2-transitive on the lines through x. Presumably, $\mathcal{D}$ must be $AG(2,k)$ or $PG_1(d,k-1)$. NODA has observed that $\mathcal{D}$ is $AG(2,k)$ if G is not line-primitive; moreover, in unpublished work, he has used an argument of HIGMAN [70] to show that $\mathcal{D}$ is $PG_1(d,k-1)$ if $v > k^2(k-1)^2(k-2)^2 + k^2 - k + 1$.

B. Parallel relations

Let $\mathcal{D}$ be a design. A parallel relation on $\mathcal{D}$ is an equivalence relation $\parallel$ partitioning the blocks into classes, each of which partitions the points of $\mathcal{D}$. Each parallel class has v/k blocks, and there are exactly r parallel classes.

Relatively little is known about subgroups G of Aut $\mathcal{D}$ which preserve $\|$. If the classical affine space (or plane) case is excluded, little is known beyond NORMAN's theorem (see 9B(3)) and the following result of CAMERON [28].

(1) *Let $\mathcal{D}$ be the degenerate design with* $k = 2$ *and* $\lambda = 1$, *whose blocks are just the 2-sets of points. Assume that* $v > 3$, G *is 3-transitive, and* G *preserves* $\|$. *Then either* $v = 6$ *and* $G \cong PGL(2,5)$, *or* $v = 2^d$ *for some* d *and $\mathcal{D}$ can be regarded as the design* $AG_1(d,2)$ *with the obvious parallel relation.*

PROOF. Let x,y,z be any three points. Then G_{xyz} fixes the block through z parallel to {x,y}. Hence, G_{xyz} fixes $k \geq 4$ points. If $k = v$ then ZASSENHAUS [172] can be used to show that $v = 6$ and G is PGL(2,5). If $k < v$, 6D(1) can be applied to yield $k = 4$. If B and C are two blocks of this S(3,4,v), and if $|B \cap C| = 2$, then $B - B \cap C$, $B \cap C$, and $C - B \cap C$ are parallel. Hence, B+C is a block of the S(3,4,v). It follows easily that the S(3,4,v) is $AG_2(d,2)$ (compare 4C(3)). □

Actually, CAMERON's proof does not use 6D(1). In fact, it was while I was eliminating one case of CAMERON's situation that 6D(1) and 6E(1) were born.

More recently, CAMERON has obtained a generalization of 10B(1) to groups preserving a parallelism of the trivial design of all k-sets of a v-set ($1 < k < v$).

The natural extension of 10B(1) to the case of triangle-transitive automorphism groups of more general designs $\mathcal{D}$ (with $\|$) remains open.

(2) *If $\mathcal{D}$ and $\|$ are as before, then* $b \geq v+r-1$; *moreover,* $b = v+r-1$ *if and only if any two blocks meet in* 0 *or* k^2/v *points* (see DEMBOWSKI [40, pp.72-73]). When $b = v+r-1$, $\mathcal{D}$ is called an *affine design*. Clearly, affine designs provide a common generalization of Hadamard 3-designs and affine spaces. A theorem of DEMBOWSKI [40, p.74] characterizes affine spaces $AG_{d-1}(d,q)$, $q > 2$, among affine designs; this result is similar to the DEMBOWSKI-WAGNER theorem (see 8C). But relatively little attention has been paid to automorphism groups, so perhaps a few additional remarks are worthwhile.

Consider $\mathcal{D}$, $\|$, and $G \leq$ Aut $\mathcal{D}$ preserving $\|$. Let G have t_p point-orbits, t_b block-orbits, and $t_{\|}$ parallel-class orbits. If $\mathcal{D}$ is an

affine design, then $t_b + 1 = t_p + t_{\|}$ (NORMAN [127]). In general, it turns out that one can at least say $t_b + 1 \geq t_p + t_{\|}$. Also, if $\mathcal{D}$ is affine and $g \in G$, then $f_p + 1 = f_b + f_{\|}$, where f_p, f_b and $f_{\|}$ are the numbers of points, blocks and parallel-classes fixed by g. From these facts, further results can be deduced as in KANTOR [91].

Incidentally, it should be noted that the arguments on pp.113-114 of DEMBOWSKI [40] show that the number of non-isomorphic affine designs having the same parameters as $AG_{d-1}(d,q)$, $d \geq 3$, is enormous (and in fact $\to \infty$, as $d \to \infty$ or $q \to \infty$). However, I conjecture that affine spaces are the only affine designs which are not Hadamard 3-designs and whose automorphism groups are transitive on ordered pairs of non-parallel blocks.

C. Transitive extensions

Let H be a given group, possibly given together with a specific transitive permutation representation on a set S'. A *transitive extension* of H is a 2-transitive group G on a set S such that, for some $x \in S$, $G_x \cong H$; if, moreover, H is given as acting on S', then it is also required that $|S| = |S'|+1$ and that G_x acts on $S-\{x\}$ as H does on S'.

A basic open problem concerning 2-transitive groups is: if H is known as an abstract group, find all transitive extensions of H. Needless to say, very few groups H have transitive extensions.

Transitive extensions have been studied geometrically by DEMBOWSKI [39], HUGHES [75,76], and TITS [158]. Their approach was to extend designs associated with groups such as the collineation group of AG(d,q) or PG(d,q), given as acting 2-transitively on the points of the corresponding affine or projective space.

Much more generally, TITS (unpublished) has shown that a Chevalley group over GF(q), acting on a class of parabolic subgroups, has no transitive extensions if q is not very small. Still more generally, SEITZ (unpublished) has obtained the same conclusion if H is isomorphic to a Chevalley group over GF(q) and $(q, |S|-1) = 1$.

D. Some maximal subgroups of alternating or symmetric groups

Let H be a transitive permutation group on S, about which a lot is known. PROBLEM: determine all permutation groups G on S containing H.

Here, I have in mind some "geometric" group H and set S. The case $H = PSL(n,q)$, $n \geq 2$, with S the set of points of $PG(n-1,q)$, has been discussed in 7E(1). In general, if H is chosen "large" enough, and $G > H$, then G will presumably have to be 2-transitive. PROBLEM: handle the case $H = PSL(n,q)$, $n \geq 4$, and S the set of e-spaces of $PG(n-1,q)$, where $1 \leq e \leq n-2$.

I have settled the case $H = Sp(2m,2)$, in its 2-transitive representations of degree $2^{m-1}(2^m \pm 1)$: if $G > H$ then G is alternating and symmetric. The elementary proof uses transvections and the geometry of $GO^{\pm}(2m,2)$.

The reader should have no difficulty in listing many other, similar questions. Perhaps the most intriguing general question of this type concerns a Chevalley group H acting on a set S of parabolic subgroups.

E. Sp(2m,2) and .3

SHULT [148] has obtained some graph-theoretic characterizations of $Sp(2m,2)$ in its 2-transitive representations of degree $2^{m-1}(2^m \pm 1)$. However, no characterization is known in terms of designs. The difficulty is that no really interesting designs seem to have $Sp(2m,2)$ as a 2-transitive automorphism group.

Precisely the same difficulty occurs in the case of CONWAY's smallest group .3, in its 2-transitive representation of degree 276 (see CONWAY [35]). In both cases, the 2-graph approach seems more relevant than the design one (cf. SEIDEL [143]).

APPENDIX

The known 2-transitive groups

The following is a list of all the known 2-transitive groups G having no regular normal subgroup.

(1) $G = A_n$ or S_n, $|S| = n$.

(2) $PSL(d+1,q) \leq G \leq P\Gamma L(d+1,q)$; S is the set of points or hyperplanes of $PG(d,q)$.

(3) $PSU(3,q) \leq G \leq P\Gamma U(3,q)$; S is the set of q^3+1 points of the corresponding unital.

(4) G has a normal Ree subgroup; S is the set of q^3+1 points of the corresponding unital ($q = 3^{2e+1}$). When $e = 0$, $G \cong P\Gamma L(2,8)$, acting on the points of $\mathcal{D}(4)$ (see 6B(3)).

(5) $Sz(2^{2e+1}) \leq G \leq \text{Aut } Sz(2^{2e+1})$; S is the set of $(2^{2e+1})^2 + 1$ points of the corresponding inversive plane or ovoid (see LÜNEBURG [111]).

(6) $G = Sp(2m,2)$, $|S| = 2^{m-1}(2^m \pm 1)$, $G_x = GO^{\pm}(2m,2)$.

(7) $G = PSL(2,11)$ acting on the 11 points or blocks of W_{11} (see 8B(2)).

(8) $G = A_7$ acting on the 15 points or planes of PG(3,2) (see 4A).

(9) The Mathieu groups M_{11}, M_{12}, M_{22}, Aut M_{22}, M_{23} and M_{24} in their usual representations on the points of the corresponding Steiner systems.

(10) $G = M_{11}$ acting 3-transitively on the 12 points of a Hadamard 3-design (see 4B(3), 9B and 9C).

(11) G = HS acting on the 176 points or blocks of W_{176} (see 8B(4)).

(12) G = .3, $|S| = 276$.

REFERENCES

[1] ASCHBACHER, M., *On doubly transitive permutation groups of degree $n \equiv 2 \bmod 4$*, Illinois J. Math., 16 (1972) 276-279.

[2] ASCHBACHER, M., *Doubly transitive groups in which the stabilizer of two points is abelian*, J. Algebra, 18 (1971) 114-136.

[3] ASCHBACHER, M., *A condition for the existence of a strongly embedded subgroup*, Proc. Amer. Math. Soc., 38 (1973) 509-511.

[4] ASCHBACHER, M., *F-Sets and permutation groups*, to appear.

[5] ASCHBACHER, M., *2-Transitive groups whose 2-point stabilizer has 2-rank 1*, to appear.

[6] ATKINSON, M.D., *Doubly transitive but not doubly primitive permutation groups I*, J. London Math. Soc. (2), 7 (1974) 632-634; *II*, ibid., to appear.

[7] BENDER, H., *Endliche zweifache transitive Permutationsgruppen, deren Involutionen keine Fixpunkte haben*, Math. Z., 104 (1968) 175-204.

[8] BENDER, H., *Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festlasst*, J. Algebra, 17 (1971) 527-554.

[9] BLOCK, R.E., *Transitive groups of collineations of certain designs*, Pacific J. Math., 15 (1965) 13-19.

[10] BRUEN, A. & B. LEVINGER, *A theorem on permutations of a finite field*, Canad. J. Math., 25 (1973) 1060-1065.

[11] BUEKENHOUT, F., *Une caractérisation des espaces affins basée sur la notion de droite*, Math. Z., 111 (1969) 367-371.

[12] BUEKENHOUT, F., *A characterization of affine spaces of order two as 3-designs*, Math. Z., 118 (1970) 83-85.

[13] BUEKENHOUT, F., *An axiomatic of inversive spaces*, J. Combinatorial Theory A, 11 (1971) 208-212.

[14] BUEKENHOUT, F., *On 2-designs whose group of automorphisms is transitive on the ordered pairs of intersecting lines*, J. London Math. Soc., 5 (1972) 663-672.

[15] BUEKENHOUT, F., *Transitive groups whose involutions fix one or three points*, J. Algebra, 23 (1972) 438-451.

[16] BUEKENHOUT, F., *Doubly transitive groups in which the maximum number of fixed points of involutions is four*, Arch. Math. (Basel), 23 (1972) 362-369.

[17] BUEKENHOUT, F. & R. DEHERDER, *Espaces linéaires finis à plans isomorphes*, Bull. Soc. Math. Belg., 23 (1971) 348-359.

[18] BURNSIDE, W., *Theory of groups of finite order*, Dover, New York, 1955.

[19] CAMERON, P.J., *Structure of suborbits in some primitive permutation groups*, thesis, Oxford Univ., 1971.

[20] CAMERON, P.J., *Permutation groups with multiply transitive suborbits I*, Proc. London Math. Soc. (3), 25 (1972) 427-440; *II*, Bull. London Math. Soc., to appear.

[21] CAMERON, P.J., *Primitive groups with most suborbits doubly transitive*, Geometriae Dedicata, 1 (1973) 434-446.

[22] CAMERON, P.J., *Extending symmetric designs*, J. Combinatorial Theory A, 14 (1973) 215-220.

[23] CAMERON, P.J., *Biplanes*, Math. Z., 131 (1973) 85-101.

[24] CAMERON, P.J., *On groups with several doubly transitive permutation representations*, Math. Z., 128 (1972) 1-14.

[25] CAMERON, P.J., *Near-regularity conditions for designs*, Geometriae Dedicata, 2 (1973) 213-224.

[26] CAMERON, P.J., *Permutation groups with multiply-transitive suborbits II*, to appear.

[27] CAMERON, P.J., *Locally symmetric designs*, to appear.

[28] CAMERON, P.J., *On groups of degree n and n-1, and highly symmetric edge colourings*, to appear.

[29] CAMERON, P.J., *Characterizations of some Steiner systems, parallelisms, and biplanes*, to appear.

[30] CAMERON, P.J. & J.J. SEIDEL, *Quadratic forms over GF(2)*, Indag. Math., 35 (1973) 1-8.

[31] CARLITZ, L., *A theorem on permutations of a finite field*, Proc. Amer. Math. Soc., 11 (1960) 456-459.

[32] CARMICHAEL, R.D., *Introduction to the theory of groups of finite order*, Dover, New York, 1956.

[33] CASSELS, J.W.S., *Factorization of polynomials in several variables*, in: Proc. 15th Scandinavian Congress 1968, Lecture Notes in Mathematics 118, Springer-Verlag, Berlin, 1970.

[34] CONWAY, J.H., *A group of order 8,315,553,613,086,720,000*, Bull. London Math. Soc., 1 (1969) 79-88.

[35] CONWAY, J.H., *Three lectures on exceptional groups*, in: *Finite simple groups*, Academic Press, New York, 1971, pp.215-247.

[36] CURTIS, C.W., W.M. KANTOR & G.M. SEITZ, *The 2-transitive permutation representations of the finite Chevalley groups*, to appear.

[37] CZERWINSKI, T., *Collineation groups containing no Baer involutions*, Proc. Internat. Conference on Projective Planes, Washington State Univ. Press, Pullman, 1973.

[38] DEMBOWSKI, P., *Verallgemeinerungen von Transitivitätsklassen endlichen projektiver Ebenen*, Math. Z., 69 (1958) 59-89.

[39] DEMBOWSKI, P., *Die Nichtexistenz von transitiven Erweiterungen der endlichen affinen Gruppen*, J. Reine Angew. Math., 220 (1965) 37-44.

[40] DEMBOWSKI, P., *Finite geometries*, Ergebnisse der Mathematik 44, Springer-Verlag, Berlin etc., 1968.

[41] DEMBOWSKI, P. & A. WAGNER, *Some characterizations of finite projective spaces*, Arch. Math. (Basel), 11 (1960) 465-469.

[42] DICKSON, L.E., *Linear groups*, Dover, New York, 1955.

[43] DOYEN, J. & X. HUBAUT, *Finite regular locally projective spaces*, Math. Z., 119 (1971) 83-88.

[44] FEIT, W., *Automorphisms of symmetric balanced incomplete block designs*, Math. Z., 118 (1970) 40-49.

[45] FEIT, W., *On symmetric balanced incomplete block designs with doubly transitive automorphism groups*, J. Combinatorial Theory A, 14 (1973) 221-247.

[46] FEIT, W. & J.G. THOMPSON, *Solvability of groups of odd order*, Pacific J. Math., 13 (1963) 771-1029.

[47] FISCHER, B., *Eine Kennzeichnung der symmetrischen Gruppen von Grade 6 und 7*, Math. Z., 95 (1967) 288-298.

[48] FISCHER, B., *Finite groups generated by 3-transpositions, I*, Invent. Math., 13 (1971) 232-246.

[49] FRIED, M., *On the diophantine equation $f(y)-x = 0$*, Acta Arith., 19 (1971) 79-87.

[50] FRIED, M., *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math., 17 (1973) 128-146.

[51] FRIED, M., *On Hilbert's irreducibility theorem*, J. Number Theory, to appear.

[52] FRIED, M. & D.J. LEWIS, *Solution spaces to diophantine problems*, Bull. Amer. Math. Soc., to appear.

[53] GLAUBERMAN, G., *Central elements in core-free groups*, J. Algebra, 4 (1966) 403-420.

[54] GOETHALS, J.M. & J.J. SEIDEL, *Strongly regular graphs derived from combinatorial designs*, Canad. J. Math., 22 (1970) 597-614.

[55] HALL, J.I., *Steiner triple systems with geometric minimally generated subsystems*, to appear.

[56] HALL, Jr., M., *A survey of difference sets*, Proc. Amer. Math. Soc., 7 (1956) 975-986.

[57] HALL, Jr., M., *The theory of groups*, MacMillan, New York, 1959.

[58] HALL, Jr., M., *Automorphisms of Steiner triple systems*, IBM J. Res. Develop., 4 (1960) 460-472. (Also in Proc. Symp. Pure Math. 6 (1962) 47-66).

[59] HALL, Jr., M., *Note on the Mathieu group* M_{12}, Arch. Math. (Basel), 13 (1962) 334-340.

[60] HALL, Jr., M., *Group theory and block designs*, in: Proc. Internat. Conf. Theory of Groups, Gordon & Breach, New York, 1967, pp.115-144.

[61] HALL, Jr., M., *Combinatorial theory*, Blaisdell, Waltham, Mass., 1967.

[62] HALL, Jr., M., *Symmetric block designs with* $\lambda = 2$, in: *Combinatorial mathematics and its applications*, Univ. of North Carolina Press, 1969, pp.175-186.

[63] HARADA, K., *On some doubly transitive groups*, J. Algebra, 17 (1971) 437-450.

[64] HERING, C., *Zweifach transitive Permutationsgruppen, in denen zwei die maximale Anzahl von Fixpunkten von Involutionen ist*, Math. Z., 104 (1968) 150-174.

[65] HERING, C., *On linear groups which contain an irreducible subgroup of prime order*, in: Proc. Internat. Conf. Projective Planes, Washington State Univ. Press, Pullman, 1973.

[66] HERING, C., W.M. KANTOR & G.M. SEITZ, *Finite groups having a split BN-pair of rank 1*, J. Algebra, 20 (1972) 435-475.

[67] HERING, F., *Über die Kollineationsgruppen einiger Hadamard-Matrizen*, unpublished manuscript.

[68] HIGMAN, D.G., *Flag transitive collineation groups of finite projective spaces*, Illinois J. Math., 6 (1962) 434-446.

[69] HIGMAN, D.G., *Finite permutation groups of rank 3*, Math. Z., 86 (1964) 145-156.

[70] HIGMAN, D.G., *Characterization of families of rank 3 permutation groups by the subdegrees II*, Arch. Math. (Basel), 21 (1970) 353-361.

[71] HIGMAN, D.G., *Remark on Shult's graph extension theorem*, in: *Finite groups '72*, T. GAGEN, M.P. HALE & E.E. SHULT (eds.), North-Holland Publ. Coy., Amsterdam, 1973, pp. 80-83.

[72] HIGMAN, D.G. & C.C. SIMS, *A simple group of order 44,352,000*, Math. Z., 105 (1968) 110-113.

[73] HIGMAN, G., *On the simple group of D.G. Higman and C.C. Sims*, Illinois J. Math., 13 (1969) 74-84.

[74] HILL, R., *Rank 3 permutation groups with a regular normal subgroup*, thesis, Univ. of Warwick, 1971.

[75] HUGHES, D.R., *On t-designs and groups*, Amer. J. Math., 87 (1965) 761-778.

[76] HUGHES, D.R., *Extensions of designs and groups: Projective, symplectic, and certain affine groups*, Math. Z., 89 (1965) 199-205.

[77] HUPPERT, B., *Zweifach transitive, auflösbare Permutationsgruppen*, Math. Z., 68 (1957) 126-150.

[78] HUSSAIN, Q.M., *Impossibility of the symmetrical incomplete block design with $\lambda = 2$, $k = 7$*, Sankhya, 7 (1946) 317-322.

[79] HUSSAIN, Q.M., *Symmetrical incomplete block designs with $\lambda = 2$, $k = 8$ or 9*, Bull. Calcutta Math. Soc., 37 (1945) 115-123.

[80] ITO, N., *Über die Gruppen $PSL_n(q)$, die eine Untergruppe von Primzahlindex enthalten*, Acta Sci. Math. (Szeged), 21 (1960) 206-217.

[81] ITO, N., *On a class of doubly, but not triply transitive permutation groups*, Arch. Math. (Basel), 18 (1967) 564-570.

[82] ITO, N., *On permutation groups of prime degree p which contain (at least) two classes of conjugate subgroups of index p*, Rend. Sem. Mat. Padova, 38 (1967) 287-292.

[83] ITO, N., *On permutation groups of prime degree p which contain at least two classes of conjugate subgroups of index p, II*, Nagoya Math. J., 37 (1970) 201-208.

[84] ITO, N., *A theorem on Jordan groups*, in: *Theory of finite groups*, Benjamin, New York, 1969, pp.47-48.

[85] ITO, N., *Tight 4-designs*, to appear.

[86] ITO, N., *On the Wielandt number of transitive permutation groups of prime degree*, to appear.

[87] ITO, N. & W.M. KANTOR, *2-Transitive symmetric designs with $k = 2p$*, Notices Amer. Math. Soc., 16 (1969) 774.

[88] JORDAN, C., *Théorèmes sur les groupes primitifs*, J. Math. Pures Appl., 16 (1871) 383-408.

[89] JORDAN, C., *Oeuvres*, J. DIEUDONNÉ (ed.), Gauthier-Villars, Paris, 1961.

[90] JORDAN, C., *Traité des substitutions*, (new edition), Gauthier-Villars, Paris, 1957.

[91] KANTOR, W.M., *Automorphism groups of designs*, Math. Z., 109 (1969) 246-252.

[92] KANTOR, W.M., *Characterizations of finite projective and affine spaces*, Canad. J. Math., 21 (1969) 64-75.

[93] KANTOR, W.M., *2-Transitive symmetric designs*, Trans. Amer. Math. Soc., 146 (1969) 1-28.

[94] KANTOR, W.M., *Automorphisms of Hadamard matrices*, J. Combinatorial Theory, 6 (1969) 279-281.

[95] KANTOR, W.M., *Jordan groups*, J. Algebra, 12 (1969) 471-493.

[96] KANTOR, W.M., *Elations of designs*, Canad. J. Math., 22 (1970) 897-904.

[97] KANTOR, W.M., *On a class of Jordan groups*, Math. Z., 118 (1970) 58-68.

[98] KANTOR, W.M., *Note on symmetric designs and projective spaces*, Math. Z., 122 (1971) 61-62.

[99] KANTOR, W.M., *On 2-transitive groups in which the stabilizer of two points fixes additional points*, J. London Math. Soc., 5 (1972) 114-122.

[100] KANTOR, W.M., *Line-transitive collineation groups of finite projective spaces*, Israel J. Math., 14 (1973) 229-235.

[101] KANTOR, W.M., *Symplectic groups, symmetric designs, and line ovals*, to appear.

[102] KANTOR, W.M., *On 2-transitive collineation groups of finite projective spaces*, Pacific J. Math., 48 (1973) 119-131.

[103] KANTOR, W.M., *Some highly geometric lattices*, to appear.

[104] KANTOR, W.M., *Primitive groups having transitive subgroups of smaller, prime power degree*, to appear.

[105] KANTOR, W.M., *Plane geometries associated with certain 2-transitive groups*, to appear.

[106] KANTOR, W.M. & T.P. MCDONOUGH, *On the maximality of PSL(d+1,q), d ≥ 2*, to appear.

[107] KANTOR, W.M., M.E. O'NAN & G.M. SEITZ, *2-Transitive groups in which the stabilizer of two points is cyclic*, J. Algebra, 21 (1972) 17-50.

[108] KERDOCK, A.M., *A class of low-rate nonlinear binary codes*, Information and Control, 20 (1972) 182-187.

[109] KING, J., *Doubly transitive groups in which involutions fix one or three points*, Math. Z., 111 (1969) 311-321.

[110] LÜNEBURG, H., *Über projektive Ebenen, in denen jede Fahne von einer nichttrivialen Elation invariant gelassen wird*, Abh. Math. Sem. Univ. Hamburg, 29 (1965) 37-76.

[111] LÜNEBURG, H., *Die Suzukigruppen und ihre Geometrien*, Lecture Notes in Mathematics 10, Springer-Verlag, Berlin etc., 1965.

[112] LÜNEBURG, H., *Transitive Erweiterungen endlicher Permutationsgruppen*, Lecture Notes in Mathematics 84, Springer-Verlag, Berlin etc., 1969.

[113] MANN, H.B., *Addition theorems*, Tracts in Pure and Applied Math. 18, Interscience, New York, 1965.

[114] MARGGRAFF, B., *Über primitive Gruppen, welche eine transitive Gruppe geringeren Grades enthalten*, thesis, Giessen, 1889.

[115] MARGGRAFF, B., *Primitive Gruppen, welche eine transitive Gruppe geringeren Grades enthalten*, Wiss. Beilage zu den Jahresberichten des Sophiengymnasiums zu Berlin, Berlin, 1895.

[116] MCCONNEL. R., *Pseudo-ordered polynomials over a finite field*, Acta Arith., 8 (1963) 127-151.

[117] MCDONOUGH, T.P., *On Jordan groups*, J. London Math. Soc., 6 (1972) 73-80.

[118] MCDONOUGH, T.P., *On Jordan groups - addendum*, to appear.

[119] MCLAUGHLIN, J.E., *A simple group of order 898,128,000*, in: *Theory of finite groups*, Benjamin, New York, 1969, pp.109-111.

[120] NAGAO, H., *On multiply transitive groups IV*, Osaka J. Math., 2 (1965) 327-341.

[121] NEUMANN, P.M., *Transitive permutation groups of prime degree*, J. London Math. Soc., 5 (1972) 202-208.

[122] NEUMANN, P.M., *Generosity and characters of multiply transitive permutation groups*, to appear.

[123] NEUMANN, P.M., *Transitive permutation groups of prime degree*, in: Proc. Conf. Theory of Groups, Canberra 1973, Lecture Notes in Mathematics, Springer-Verlag, Berlin etc., to appear.

[124] NEUMANN, P.M., *Transitive permutation groups of prime degree IV*, to appear.

[125] NODA, R., *Doubly transitive groups in which the maximal number of fixed points of involutions is four*, Osaka Math. J., 8 (1971) 77-90.

[126] NODA, R., *Steiner systems which admit block-transitive automorphism groups of small rank*, Math. Z., 125 (1972) 113-121.

[127] NORMAN, C.W., *A characterization of the Mathieu group M_{11}*, Math. Z., 106 (1968) 162-166.

[128] O'NAN, M.E., *Automorphisms of unitary block designs*, J. Algebra, 20 (1972) 495-511.

[129] O'NAN, M.E., *A characterization of $U_3(q)$*, J. Algebra, 22 (1972) 254-296.

[130] O'NAN, M.E., *A characterization of $L_n(q)$ as a permutation group*, Math. Z., 127 (1972) 301-314.

[131] O'NAN, M.E., *The normal structure of the one-point stabilizer of a doubly-transitive group*, in: *Finite groups '72*, T. GAGEN, M.P. HALE & E.E. SHULT, (eds.), North-Holland Publ. Coy., Amsterdam, 1973, pp.119-121.

[132] O'NAN, M.E., *Normal structure of the one-point stabilizer of a doubly-transitive permutation group, I*, to appear.

[133] O'NAN, M.E., *Normal structure of the one-point stabilizer of a doubly-transitive permutation group, II*, to appear.

[134] O'NAN, M.E., *Triply-transitive permutation groups whose two-point stabilizer is local*, to appear.

[135] O'NAN, M.E., *Doubly-transitive groups of odd degree whose one point stabilizer is local*, to appear.

[136] OSBORN, J.H., *Finite doubly-transitive permutation groups without subgroups fixing exactly two points*, thesis, Univ. of Wisconsin, 1972.

[137] OSTROM, T.G. & A. WAGNER, *On projective and affine planes with transitive collineation groups*, Math. Z., 71 (1959) 186-199.

[138] PALEY, R.E.A.C., *On orthogonal matrices*, J. Math. Phys., 12 (1933) 311-320.

[139] PERIN, D., *On collineation groups of finite projective spaces*, Math. Z., 126 (1972) 135-142.

[140] POLLATSEK, H., *First cohomology groups of some linear groups over fields of characteristic two*, Illinois J. Math., 15 (1971) 393-417.

[141] PRAEGER, C.E., *Finite permutation groups*, thesis, Oxford Univ., 1973.

[142] SCOTT, L.L., *A double transitivity criterion*, Math. Z., 115 (1970) 7-8.

[143] SEIDEL, J.J., *A survey of two-graphs*, to appear.

[144] SHAUGHNESSY, E.P., *Codes with simple automorphism groups*, Arch. Math. (Basel), 22 (1971) 459-466.

[145] SHULT, E.E., *On the fusion of an involution in its centralizer*, to appear.

[146] SHULT, E.E., *On a class of doubly transitive groups*, Illinois J. Math., 16 (1972) 434-445.

[147] SHULT, E.E., *The graph extension theorem*, Proc. Amer. Math. Soc., 33 (1972) 278-284.

[148] SHULT, E.E., *Characterizations of certain classes of graphs*, J. Combinatorial Theory B, 13 (1972) 142-167.

[149] SHULT, E.E., *On doubly transitive groups of even degree*, to appear.

[150] SIMS, C.C., *On the isomorphism of two groups of order 44,352,000*, in: *Theory of finite groups*, Benjamin, New York, 1969, pp.101-108.

[151] SIMS, C.C., *Computational methods in the study of permutation groups*, in: *Computational problems in abstract algebra*, J. LEECH (ed.), Pergamon Press, London, 1970, pp. 169-183.

[152] SMITH, M.S., *A combinatorial configuration associated with the Higman-Sims simple group*, to appear.

[153] SMITH, M.S., *On the isomorphism of two simple groups of order 44,352,000*, to appear.

[154] SYLVESTER, J.J., *Collected mathematical papers, vol. II*, Cambridge Univ. Press, 1908, pp.615-628.

[155] TAYLOR, D.E., *Some topics in the theory of finite groups*, thesis, Oxford Univ., 1971.

[156] TAYLOR, D.E., *Monomial representations and strong graphs*, in: Proc. First Australian Conf. Combinatorial Math., Univ. of Newcastle, 1972, pp. 197-201.

[157] TEIRLINCK, L., *On linear spaces in which every plane is either projective or affine*, to appear.

[158] TITS, J., *Sur les systèmes de Steiner associés aux trois "grands" groupes de Mathieu*, Rend. Mat. e Appl., 23 (1964) 166-184.

[159] TODD, J.A., *A combinatorial problem*, J. Math. Phys., 12 (1933) 321-333.

[160] TSUZUKU, T., *On doubly transitive permutation groups of degree $1+p+p^2$ where p is a prime number*, J. Algebra, 8 (1968) 143-147.

[161] VEBLEN, O. & J.W. YOUNG, *Projective geometry I*, Ginn, Boston, 1916.

[162] WAGNER, A., *On collineation groups of finite projective spaces, I*, Math. Z., 76 (1961) 411-426.

[163] WARD, H.N., *On Ree's series of simple groups*, Trans. Amer. Math. Soc., 121 (1966) 62-69.

[164] WIELANDT, H., *Abschätzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad*, Schr. Math. Sem. Univ. Berlin, 2 (1934) 151-174.

[165] WIELANDT, H., *Über den Transitivitätsgrad von Permutationsgruppen*, Math. Z., 74 (1960) 297-298.

[166] WIELANDT, H., *Finite permutation groups*, Acad. Press, New York, 1964.

[167] WIELANDT, H., *On automorphism groups of doubly-transitive permutation groups*, in: Proc. Internat. Conf. Theory of Groups, Gordon & Breach, New York, 1967, pp.389-393.

[168] WILSON, R.M. & D.K. RAY-CHAUDHURI, *Generalization of Fisher's inequality to t-designs*, Notices Amer. Math. Soc., 18 (1971) 805.

[169] WITT, E., *Die 5-fach transitiven Gruppen von Mathieu*, Abh. Math. Sem. Univ. Hamburg, 12 (1938) 256-264.

[170] WITT, E., *Über Steinersche Systeme*, Abh. Math. Sem. Univ. Hamburg, 12 (1938) 265-275.

[171] ZASSENHAUS, H., *Über endliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg, 11 (1935) 187-220.

[172] ZASSENHAUS, H., *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg, 11 (1935) 17-40.

MATHEMATICAL CENTRE TRACTS 57, 1974, 98-129

SUBORBITS IN TRANSITIVE PERMUTATION GROUPS

P.J. CAMERON

Merton College, Oxford OX1 4JD, England

With any graph we can associate a group, namely its automorphism group; this acts naturally as a permutation group on the vertices of the graph. The converse idea, that of reconstructing a graph (or a family of graphs) from a transitive permutation group, has been developed by C.C. SIMS, D.G. HIGMAN, and many other people, and is the subject of the present survey. In his lecture notes [23], HIGMAN has axiomatised the combinatorial objects that arise from permutation groups in this way, under the name *coherent configurations*; but I shall discuss only the case where a group is present. My own introduction to the theory was via the unpublished paper of P.M. NEUMANN [30].

In section 1, the construction and some of its basic properties are described. Also in this section I introduce the basis matrices and the centraliser algebra they generate. The theory of this algebra has played an important role in the study of permutation groups and of various combinatorial objects (in such papers as [20],[22],[30],[2],[12],[16]); but here I shall be more concerned with other aspects of the theory, those which may be described as more "graph-theoretic".

Section 2 is about paired suborbits. In graph-theoretic terms, we have a directed graph, and ask about the relations between the actions of the stabiliser G_α of a vertex α on the vertices joined "to" and "from" α.

In section 3 the subject is more group-theoretic. Suppose the action of G_α on the vertices adjacent to α (or perhaps just the number of such vertices) is given. What can be said about the structure of G_α? After pioneering work by TUTTE [41],[42] and SIMS [34], the most powerful results here are due to WIELANDT [47].

Sections 4 and 5 are closely related. In section 4 we take once more the graph-theoretic viewpoint and investigate further transitivity properties of undirected graphs; in the following section these investigations are put back in group-theoretic context, and generalisations of them are studied. One of the themes of this section is the deduction of bounds for the rank of a primitive permutation group from hypotheses about the stabiliser of a point.

Section 6 discusses some aspects of algebraic relations (such as commutativity) between basis matrices. There are no general results here, since none seem to exist, and it appears to be an untilled field full of thorny problems; a special case is considered, to illustrate the ideas.

For the general theory of finite permutation groups, the reader is referred to the book by WIELANDT [45]. It should be mentioned that, unless specifically stated otherwise, all permutation groups are finite.

1. INTRODUCTION AND NOTATION

With the exception of section 4, the point of view throughout these notes is a group-theoretic one. We take a transitive permutation group, associate with it a class of directed or undirected graphs, and use the graphs to get information about the group. All the graphs involved have the property that their automorphism groups act transitively on vertices and on directed edges, and indeed any graph Γ with this property is covered by our remarks (simply by taking $G = \mathrm{Aut}\,\Gamma$ as a permutation group on the vertices of Γ). So the process is essentially a two-way one, and both points of view should be kept in mind. Of course, if we start with a graph, the general machinery produces a whole family of graphs, whose interrelations can be studied.

Suppose G is a transitive permutation group on a set Ω. G has a natural action on $\Omega \times \Omega$, defined by

$$(\alpha,\beta)g = (\alpha g, \beta g)$$

for all $\alpha,\beta \in \Omega$, $g \in G$. So $\Omega \times \Omega$ is partitioned into orbits $\Gamma_0,\Gamma_1,\ldots,\Gamma_{r-1}$ under the action of G. These are called *suborbits* of G, and their number r is the *rank*. (If $|\Omega| > 1$ then $r \geq 2$, since the diagonal $\Gamma_0 = \{(\alpha,\alpha) \mid \alpha \in \Omega\}$ is always an orbit. Note that $r = 2$ if and only if G is

doubly transitive on Ω.) We can regard each suborbit Γ_i as a G-invariant relation on Ω, or alternatively (if $i > 0$) as the edge set of a directed graph which admits G as a group of automorphisms transitive on vertices and directed edges. The suborbit *paired* with a given suborbit Γ (or the *converse* relation to Γ) is

$$\Gamma^* = \{(\beta,\alpha) \mid (\alpha,\beta) \in \Gamma\} .$$

Other notation in common use is Γ' (WIELANDT [45]) and Γ^U (HIGMAN [23]). Γ is *self-paired* or *symmetric* if $\Gamma = \Gamma^*$. If Γ is self-paired, we can regard it as an undirected graph.

The suborbits are the minimal G-invariant binary relations on Ω, and any G-invariant relation is the union of a subcollection of them. (Sometimes I shall call such a relation a *generalized suborbit*.) Of particular importance are the G-invariant equivalence relations. There are always at least two of these, the diagonal Γ_0 and the whole of $\Omega \times \Omega$. Given any non-diagonal suborbit Γ, there is a unique G-invariant equivalence E which is minimal subject to containing Γ. This is "generated" by Γ in a certain sense which we shall make precise. Consider the undirected graph corresponding to Γ (that is, the relation $\Gamma \cup \Gamma^*$). E contains $\Gamma \cup \Gamma^*$ (by symmetry) and so it contains the relation of being connected by a path in $\Gamma \cup \Gamma^*$ (by transitivity). However, this latter relation is an equivalence, and so is equal to E. SIMS showed that we can give a simpler description of E.

THEOREM 1.1. *The smallest* G*-invariant equivalence relation containing* Γ *is the relation of being connected by a directed path in* Γ.

PROOF. For $\alpha \in \Omega$, let $E'(\alpha)$ be the set of points reachable by directed Γ-paths from α. Clearly, if $\beta \in E'(\alpha)$, then $E'(\beta) \subseteq E'(\alpha)$. But if g is an element of G with $\alpha g = \beta$, then $E'(\alpha)g = E'(\beta)$, and so $|E'(\alpha)| = |E'(\beta)|$. It follows that $E'(\alpha) = E'(\beta)$, and in particular $\alpha \in E'(\beta)$. Thus E' is symmetric. It is obviously reflexive and transitive, so it is the minimal equivalence relation E containing Γ. □

G. GLAUBERMAN, who lives in Chicago, formulated this result as follows. The graph Γ (interpreted as a one-way system) has the property that, whenever it is possible to walk from α to β, it is possible to drive. Clearly not all directed graphs have this property! It is a consequence of our transitivity assumption. (This formulation was communicated to me by L. SCOTT.)

We can phrase the result in yet another way. The set of G-invariant relations on Ω, with the operation of composition, forms a semigroup. The union of all members of the subsemigroup generated by Γ is the smallest equivalence relation containing Γ. We may say this is the equivalence relation *generated* by Γ.

It is not difficult to show that if $(\alpha,\beta) \in \Gamma$ and $g \in G$ satisfy $\alpha g = \beta$, then the subgroup of G fixing the equivalence class of E containing α is the subgroup generated by G_α and g. (G_α is the subgroup of G fixing α.) In particular, Γ is connected if and only if $\langle G_\alpha, g\rangle = G$.

The group G is said to be *primitive* if the only G-invariant equivalence relations are the trivial ones Γ_0 and $\Omega \times \Omega$. By theorem 1.1, G is primitive if and only if the graph of every non-diagonal suborbit is connected; this occurs if and only if $\langle G_\alpha, g\rangle = G$ for all $g \notin G_\alpha$; that is, if and only if G_α is a maximal subgroup of G.

As defined in WIELANDT's book [45], a suborbit is an orbit of G_α in Ω. There is a natural one-to-one correspondence between the two concepts: if $\Gamma_0,\ldots,\Gamma_{r-1}$ are the G-orbits in $\Omega \times \Omega$, then $\Gamma_0(\alpha),\ldots,\Gamma_{r-1}(\alpha)$ are the G_α-orbits in Ω, where

$$\Gamma_i(\alpha) = \{\beta \mid (\alpha,\beta) \in \Gamma_i\} = \text{set of points joined "from" } \alpha \text{ in } \Gamma_i.$$

Conversely, Γ_i is the G-orbit containing (α,β), for some $\beta \in \Gamma_i(\alpha)$. The *subdegree* associated with Γ_i is $|\Gamma_i(\alpha)| = |\Gamma_i| \,/\, |\Omega|$, the valency of the graph Γ_i. It follows that paired suborbits have the same subdegree.

The graph-theoretic interpretation of suborbits often provides simple proofs of old theorems on suborbits and subdegrees. As an example I give SIMS' proof of Theorem 17.4 in WIELANDT's book.

THEOREM 1.2. *If G is primitive, with subdegrees* $1=n_0,n_1,\ldots,n_{r-1}$ *(in increasing order), then* $n_1 n_{i-1} \geq n_i$ *for* $i=1,\ldots,r-1$.

PROOF. Let Δ be the generalised suborbit $\Gamma_0 \cup \ldots \cup \Gamma_{i-1}$. Since G is primitive, there is a Γ_1-edge (γ,δ) from a point $\gamma \in \Delta(\alpha)$ to a point $\delta \notin \Delta(\alpha)$; say $\gamma \in \Gamma_j(\alpha)$, $\delta \in \Gamma_k(\alpha)$, with $j < i \leq k$. The number of Γ_1-edges with initial point in $\Gamma_j(\alpha)$ and terminal point in $\Gamma_k(\alpha)$ is at most $n_1 n_j \leq n_1 n_{i-1}$, and also at least $n_k \geq n_i$; so $n_1 n_{i-1} \geq n_i$. □

We do not really need primitivity; connectedness of Γ_1 will suffice. If Γ_1 is self-paired, a simple change in the argument gives the result $(n_1-1)n_{i-1} \geq n_i$ for $i=2,\ldots,r-1$.

If Γ_i and Γ_j are suborbits, their composition $\Gamma_i \circ \Gamma_j$ is the generalised suborbit consisting of the pairs (α,β) for which there exists a point γ with $(\alpha,\gamma) \in \Gamma_i$, $(\gamma,\beta) \in \Gamma_j$. For convenience later on, we make the additional arbitrary assumption that $\alpha \neq \beta$. (This is relevant only if $\Gamma_j = \Gamma_i^*$.)

Since G is transitive on directed edges of each Γ_k, the number of points γ for which $(\alpha,\gamma) \in \Gamma_i$, $(\gamma,\beta) \in \Gamma_j$, depends only on which suborbit contains the pair (α,β); we shall let a_{ijk} denote this number, if $(\alpha,\beta) \in \Gamma_k$. Note that $a_{ijk} = 0$ if $k \neq 0$ and $\Gamma_k \not\subseteq \Gamma_i \circ \Gamma_j$. These intersection numbers satisfy various identities, which can be verified by counting arguments:

$$
(1.1)\qquad \begin{cases} a_{ij0} = n_i\,\delta_{ij^*}\ ; & a_{i0j} = a_{0ij} = \delta_{ij}\ ; \\ a_{ijk} = a_{j^*i^*k^*}\ ; & n_k\,a_{ijk} = n_i\,a_{kj^*i}\ ; \\ \sum_{j=0}^{r-1} a_{ijk} = n_i\ ; & \\ \sum_{t=0}^{r-1} a_{lit}\,a_{tjm} = \sum_{k=0}^{r-1} a_{lkm}\,a_{ijk}\ , & \end{cases}
$$

where n_i is the subdegree of Γ_i, δ_{ij} the Kronecker delta, and $\Gamma_{i^*} = \Gamma_i^*$.

The last of these relations is proved by counting quadrilaterals in two ways, as shown in fig. 1.1.

Fig. 1.1

The *basis matrix* C_i corresponding to Γ_i is the matrix with rows and columns indexed by Ω, with (α,β) entry 1 if $(\alpha,\beta) \in \Gamma_i$, 0 otherwise. The basis matrices (adjacency matrices of the graphs) satisfy

$$(1.2)\quad \begin{cases} C_0 = I, \qquad \sum_{i=0}^{r-1} C_i = J \text{ (the all 1 matrix)}, \\ C_i^T = C_{i^*}\ , \\ C_i\, C_j = \sum_{k=0}^{r-1} a_{ijk}\, C_k\ . \end{cases}$$

The last equation is proved by observing that the (α,β) entry of C_iC_j is a_{ijk} if $(\alpha,\beta) \in \Gamma_k$. It follows that the span of $C_0,\ldots,C_{r-1}$ (over $\mathbb{C}$) is an algebra of dimension r, which is semi-simple (by the second equation). Furthermore, G can be represented as a linear group on the vector space $\mathbb{C}\Omega$ with basis indexed by Ω (elements of G permute the basis vectors in the natural way); it is easy to verify that a given matrix commutes with all the permutation matrices if and only if its (α,β) entry depends only on the suborbit containing (α,β), that is, if and only if it lies in the span of $C_0,\ldots,C_{r-1}$. Thus these matrices span the *centraliser algebra* of the permutation matrices. The fifth equation of (1.1) can be interpreted as the associativity of basis matrices:

$$(C_lC_i)C_j = \sum_{m=0}^{r-1} \Big(\sum_{t=0}^{r-1} a_{lit}a_{tjm}\Big)\, C_m = \sum_{m=0}^{r-1} \Big(\sum_{k=0}^{r-1} a_{lkm}a_{ijk}\Big)\, C_m = C_l(C_iC_j).$$

This is an example of the interaction between the algebra and the graph theory. Another is the fact that C_i and C_j commute if and only if $a_{ijk} = a_{jik}$ for all k (see also section 6).

Since the centraliser algebra is semi-simple, it is a direct sum of matrix algebras of degrees $e_0,\ldots,e_s$ over $\mathbb{C}$. Since its dimension is r, we have $\sum e_i^2 = r$; and we can assume that $e_0 = 1$, since (n_i) is a 1-dimensional direct summand of C_i. $\mathbb{C}\Omega$ is a natural module for this algebra, and is a direct sum of irreducible submodules; suppose the natural module for the i-th summand of the algebra has multiplicity g_i. Then $|\Omega| = \sum e_ig_i$, and $g_0 = 1$ (by the PERRON-FROBENIUS theorem). Double centraliser theory shows that the numbers e_i and g_i are respectively multiplicities and degrees of the irreducible representations of G which occur in the permutation representation on $\mathbb{C}\Omega$.

If we know enough about the algebra (for example, all intersection numbers), we can in principle compute the numbers e_i and g_i. First we compute the irreducible representations of the algebra. This is made easier by the fact that there is an isomorphism from the centraliser algebra to the *intersection algebra* whose elements are r × r matrices (and so in

general much smaller). The intersection matrix M_i of Γ_i is defined to have (l,m) entry a_{lim}. Then

$$(M_iM_j)_{lm} = \sum_{t=0}^{r-1} a_{lit}\, a_{tjm} =$$

$$= \sum_{k=0}^{r-1} a_{lkm}\, a_{ijk} =$$

$$= \left(\sum_{k=0}^{r-1} a_{ijk}\, M_k\right)_{lm} ,$$

so $M_iM_j = \sum_{k=0}^{r-1} a_{ijk}\, M_k$, and the map $C_i \mapsto M_i$ is an algebra isomorphism.

In the case where all e_i are equal to unity (so the centraliser algebra is commutative), an irreducible representation associates with each basis matrix an eigenvalue, and the g_i are the multiplicities of these eigenvalues. The equations $\mathrm{Trace}(C_i) = |\Omega|\delta_{i0}$ are now a set of linear equations for the g_i.

The main applications of the theory are in finding non-trivial "integrality conditions" on the intersection numbers, by computing the degrees and multiplicities and observing that they must be integers. ([20],[22], [4], for example.) Other papers (such as [43],[30]) start with the degrees and multiplicities and compute the intersection numbers. Neither of these will be our chief concern.

There is a little more information that can be gleaned from the permutation character π of G. π is the character of the permutation representation of G on $\mathbb{C}\Omega$, that is, $\pi(g)$ is the number of fixed points of g, for $g \in G$. If the irreducible constituents of π appear with multiplicities $e_1,\ldots,e_s$, we know that $r = \sum e_i^2$ and the principal character 1_G has multiplicity $e_0 = 1$. (Thus, G is doubly transitive if and only if $\pi = 1_G + \chi$, where χ is irreducible.) We can also obtain a formula for the number of self-paired suborbits. The FROBENIUS-SCHUR number n_χ of an irreducible character χ of G is defined to be +1 if χ is of the first kind (the character of a real representation), -1 if χ is of the second kind (a real character not afforded by any real representation), and 0 if χ is of the third kind (complex-valued). This can be extended to an arbitrary character by linearity; thus n_π is the number of constituents of π of the first kind minus the number of the second kind (counted with multiplicity). Now $n_\pi = (|G|)^{-1} \sum_{g\in G} \pi(g^2)$ (see [15; 3.5]), from which it follows that n_π is

the number of self-paired suborbits of G (see [10]). (Note that this number is at least 1.) An irreducible of the second kind must occur with even multiplicity in any real representation. So if all the multiplicities e_i are 1, then # self-paired suborbits = # real irreducible constituents of π, # non-self-paired suborbits = # non-real irreducible constituents of π.

2. PAIRED SUBORBITS

One of our main concerns will be with relations among the different *subconstituents* (transitive constituents of the stabiliser of a point) in a transitive permutation group. In complete generality there can be no relationships at all, as the following example shows. Let H be a permutation group on a set Δ, not necessarily transitive. Let $V = F\Delta$ be a vector space over $F = GF(p)$ (p prime) with basis indexed by Δ; then H acts as a group of linear transformations on V. Let $G = \{x \mapsto xh+v \mid h \in H, v \in V\}$. G is transitive on V, and $G_0 \cong H$ has a union of orbits $\Delta(0)$ on which it acts as H does on Δ. Of course, if H is intransitive on Δ, then none of the graphs corresponding to suborbits in $\Delta(0)$ is connected, and a connected component of one of them contains none of the others. We might expect that two suborbits which generate the same equivalence relation might be better behaved. As shown in theorem 1.1, paired suborbits always fulfil this condition. And indeed paired subsconstituents always share at least one property: they have the same degree.

There is a general machine for producing bad behaviour in paired suborbits. Suppose H is a group, and K and L are isomorphic subgroups of H which are embedded "differently" in H. Embed H in G, the symmetric group of degree $|H|$, by means of its regular representation. K and L are each represented by $|H:K|$ times the regular representation, and so are isomorphic as permutation groups. Thus there is an element $g \in G$ such that $K^g = L$. Indeed there are many such g, and we can usually choose one such that $H \cap H^g = L$ (and then $H \cap H^{g^{-1}} = K$). Represent G as a permutation group on the right cosets of H (acting by right multiplication), and let α, γ, γ' be the cosets H, Hg, Hg^{-1}. Then $G_\alpha = H$, $G_{\alpha\gamma} = L$, $G_{\alpha\gamma'} = K$, and $(\gamma',\alpha)g = (\alpha,\gamma)$. So γ and γ' belong to paired suborbits affording the representations of H on the right cosets of L and K respectively.

EXAMPLES.

1. $H = S_4$, $K = \langle (12),(34)\rangle$, $L = \langle (12)(34),(13)(24)\rangle$. One suborbit affords the (rank 3) representation of S_4 on unordered pairs, while the other is not faithful (since $L \lhd H$) but affords the regular representation of $H/L \cong S_3$.
2. $H = M_{12}$, K and L are non-conjugate subgroups isomorphic to PSL(2,11); one is maximal and the other is not. (Thus one constituent is primitive and the other is imprimitive.)
3. $H = S_n \times S_k$ $(n > 2k)$, $K \cong L \cong S_{n-k} \times S_k$. One constituent is the representation of S_n on ordered k-tuples of distinct elements, while the other is faithful.

These examples, which could be multiplied, indicate that many elementary properties (such as order, rank, primitivity, and regularity) are not necessarily shared by paired subconstituents (or "preserved under pairing"). The first positive result was proved by SIMS (see [31]):

THEOREM 2.1. *If G is transitive on Ω and Γ is a suborbit with subdegree greater than 1, then $G_\alpha^{\Gamma(\alpha)}$ and $G_\alpha^{\Gamma^*(\alpha)}$ have a common non-trivial epimorphic image.*

I shall outline SIMS' proof of this result, which goes by contradiction. First, note that if a group G acts on Γ and Δ, and if K_Γ and K_Δ are the kernels of these actions, then $G^\Gamma \cong G/K_\Gamma$ and $G^\Delta \cong G/K_\Delta$; $G/K_\Gamma K_\Delta$ is a common epimorphic image of G^Γ and G^Δ. If the only such epimorphic image is trivial, then $G = K_\Gamma K_\Delta$, whence $G^\Delta = K_\Gamma^\Delta$ and *a fortiori* $G^\Delta = G_\gamma^\Delta$ for $\gamma \in \Gamma$.

Suppose G, acting on Ω with suborbit Γ, is a counterexample. We prove by induction the statements about the Γ-graph:

A_k : G permutes paths of length k transitively;

B_k : if $(\alpha_1,\ldots,\alpha_k)$ is a path of length k-1, then

$$G_{\alpha_1\ldots\alpha_k}^{\Gamma(\alpha_k)} = G_{\alpha_k}^{\Gamma(\alpha_k)} \text{ and } G_{\alpha_1\ldots\alpha_k}^{\Gamma^*(\alpha_1)} = G_{\alpha_1}^{\Gamma^*(\alpha_1)}.$$

A_1 and B_1 are trivially true. If A_k and B_k hold, and $(\alpha_1,\ldots,\alpha_k)$ is as in B_k, then $G_{\alpha_1\ldots\alpha_k}^{\Gamma(\alpha_k)}$ and $G_{\alpha_1\ldots\alpha_k}^{\Gamma^*(\alpha_1)}$ have no common non-trivial epimorphic image (by B_k and hypothesis), so $G_{\alpha_1\ldots\alpha_k}^{\Gamma(\alpha_k)} = G_{\alpha_0\ldots\alpha_k}^{\Gamma(\alpha_k)}$ and $G_{\alpha_1\ldots\alpha_k}^{\Gamma^*(\alpha_1)} = G_{\alpha_1\ldots\alpha_{k+1}}^{\Gamma^*(\alpha_1)}$ for $\alpha_0 \in \Gamma^*(\alpha_1)$, $\alpha_{k+1} \in \Gamma(\alpha_k)$. Thus A_{k+1} and B_{k+1} hold.

So G acts transitively on paths of length k for all k, a contradiction since the number of such paths is $|\Omega|\ |\Gamma(\alpha)|^k$ and goes to infinity with k.

SIMS' idea was employed by CAMERON [8,I] to show that a variety of properties of transitive groups are "preserved under pairing". The most important of these are double transitivity and the property of containing the alternating group. The first of these can be expressed thus. Let Γ be a directed graph whose automorphism group is transitive on vertices and directed edges. Then the properties of transitivity on the two kinds of figure shown in figure 2.1 are equivalent.

Fig. 2.1

The most general result in [8;I] asserts that a property $\mathcal{P}$ of transitive groups of degree $d > 1$ is preserved under pairing if it satisfies the two conditions

(i) $G^\Omega \in \mathcal{P}$, $G \leq H$ implies $H^\Omega \in \mathcal{P}$;

(ii) if G acts transitively on Γ and Δ, with $|\Gamma| = |\Delta| = d$, $G^\Delta \in \mathcal{P}$, $G^\Gamma \notin \mathcal{P}$, and $\gamma \in \Gamma$, then $G_\gamma^\Delta \in \mathcal{P}$.

More recently I have found a more general necessary condition; it is awkward to state, but implies (for example) that if n is large enough (for given k), the property of acting as S_n or A_n on k-element subsets is preserved under pairing. Compare this with examples 1 and 3 above.

A significant advance was made by KNAPP [26], who found an alternative method of proof. Again I shall illustrate by proving SIMS' result (theorem 2.1). Suppose a group G is a counterexample to the theorem; let Ω be a set affording a permutation representation of G of maximal degree for which the theorem is false, and Γ the suborbit involved. If $(\gamma,\alpha),(\alpha,\beta) \in \Gamma$, then as before $G_{\alpha\gamma}^{\Gamma(\alpha)} = G_\alpha^{\Gamma(\alpha)}$ and $G_{\alpha\beta}^{\Gamma^*(\alpha)} = G_\alpha^{\Gamma^*(\alpha)}$. Thus G is transitive on Γ, and $\Phi = \{((\gamma,\alpha),(\alpha,\beta)) \in \Gamma \times \Gamma\}$ is a suborbit, with $G_{(\gamma,\alpha)}^{\Phi(\gamma,\alpha)} \cong G_{\alpha\gamma}^{\Gamma(\alpha)} = G_\alpha^{\Gamma(\alpha)}$ and $G_{(\alpha,\beta)}^{\Phi^*(\alpha,\beta)} \cong G_{\alpha\beta}^{\Gamma^*(\alpha)} = G_\alpha^{\Gamma^*(\alpha)}$. Thus the theorem is false for the action of G on Γ, and $|\Gamma| = |\Omega||\Gamma(\alpha)| > |\Omega|$, contradicting the maximality of $|\Omega|$.

KNAPP was able to extend the argument to show

THEOREM 2.2. *Suppose* $\mathcal{P}$ *is a property of transitive groups of degree* $d > 1$ *such that*

(i) $\mathcal{P}$ *is preserved under pairing;*

(ii) *groups in* $\mathcal{P}$ *are primitive;*

(iii) *if* Y *is a regular normal subgroup of a group* $X \in \mathcal{P}$, *then* X/Y *has no normal subgroup isomorphic to* Y.

Let G *be a transitive permutation group on* Ω *with suborbit* Γ *such that* $|\Gamma(\alpha)| = d$ *and* $G_\alpha^{\Gamma(\alpha)} \in \mathcal{P}$. *Then* $G_\alpha^{\Gamma(\alpha)} \cong G_\alpha^{\Gamma^*(\alpha)}$ *(as abstract group).*

Note that (ii) is satisfied by most known properties satisfying (i), while (iii) is usually a very weak requirement. Note also that we cannot conclude that the representations of G_α on $\Gamma(\alpha)$ and $\Gamma^*(\alpha)$ are equivalent, even under much stronger hypotheses.

It might be expected that stronger results might hold about paired suborbits in primitive groups. However, nothing seems to be known except for consequences of the more general relations between subconstituents in primitive groups, to be discussed in the next section. Paired subconstituents need not be equivalent, even when they are multiply transitive; but the worst examples I know are very much milder than the general examples discussed previously.

Even when paired constituents are isomorphic as permutation groups, they may look quite different geometrically. For example, let G be a group doubly transitive on Ω, and Δ a fixed set of $G_{\{\alpha,\beta\}}$. Let $S_{(2)}$ denote for the moment the collection of 2-element subsets of a set S. G is transitive on $\Omega_{(2)}$, and has a generalized suborbit Γ defined by $\Gamma(\{\alpha,\beta\}) = \Delta_{(2)}$. We might expect that there would be a fixed set Δ' for $G_{\{\alpha,\beta\}}$ in Ω such that $\Gamma^*(\{\alpha,\beta\}) = \Delta'_{(2)}$, but this need not be the case; it can occur that the members of $\Gamma^*(\{\alpha,\beta\})$ are pairwise disjoint, even when this set is a single suborbit! See ATKINSON [1;II].

In multiply transitive groups there are possibilities of more general kinds of pairing. Suppose G is k-transitive on Ω, and $|\Omega| > k$. As in section 1 there is a natural correspondence between G-orbits on ordered $(k+1)$-tuples of distinct elements of Ω and $G_{\alpha_1 \ldots \alpha_k}$-orbits on $\Omega - \{\alpha_1, \ldots, \alpha_k\}$. Now there are potentially $(k+1)!$ orbits "paired" with a given one, corresponding to the $(k+1)!$ possible rearrangements of a $(k+1)$-tuple. (The number of these which are distinct is the index in S_{k+1} of the group of permutations induced by G on a $(k+1)$-tuple in the given orbit.) The results of this section apply to any two orbits "paired" by a transposition, and so to any two

"paired" orbits, since transpositions generate the symmetric group. However, we might expect that for k > 1 stronger results would hold. This has not been investigated.

It is clear that SIMS' and KNAPP's proofs depend on the finiteness of Ω and G. If Ω is infinite, then any kind of bad behaviour is possible. Thus any two transitive permutation groups (not necessarily of the same degree) can occur as paired subconstituents in a transitive permutation group. The counterexample machine works even better. Instead of embeddings in symmetric groups, we can simply apply the HIGMAN-NEUMANN-NEUMANN construction [24]; BRITTON's lemma [6] guarantees that the element g exists. In bad cases, SIMS' argument often shows that G acts transitively on paths of length k for every k; yet G may have uncountably many orbits on one-way infinite paths. The very simplest example is the directed tree in which every vertex has one edge entering it and two leaving it.

3. MORE GENERAL RELATIONS BETWEEN SUBCONSTITUENTS

Suppose we are concerned with permutation groups with a given subdegree v (or with graphs of a given valency v having automorphism groups transitive on vertices and directed edges). We know then that the stabiliser of a point has a homomorphism into the symmetric group on v letters. It is very important to get hold of the kernel of this homomorphism; but this is a difficult problem. SIMS conjectured that at least the size of the kernel is bounded, provided the group is primitive.

SIMS' CONJECTURE. *There is a function* f *on the natural numbers with the property that, if* G *is a primitive permutation group with a suborbit* Γ *with* $|\Gamma(\alpha)| = v$, *then* $|G_\alpha| \leq f(v)$.

We might expect a similar function to exist under the weaker hypothesis that the Γ-graph is connected; but this is false, as can be seen by considering the directed graph with vertices (i,j), where $0 \leq i \leq n-1$, $0 \leq j \leq m-1$, and edges $((i,j),(i+1,k))$ for all i,j,k, where the first coordinate is taken mod n. Here $|\Gamma(\alpha)| = m$ but $|G_\alpha| = (m!)^{n-1}(m-1)!$ The underlying undirected graph has a similar property.

We observe two simple cases: $f(1) = 1$, $f(2) = 2$. For if $|\Gamma(\alpha)| = 1$ then the Γ-graph is a directed polygon. If $|\Gamma(\alpha)| = 2$ and $\Delta = \Gamma^* \circ \Gamma$, then

$|\Delta(\alpha)| = 2$ and Δ is self-paired, so the Δ-graph is an undirected polygon. SIMS [34;I] showed that $f(3) = 48$, and QUIRIN [31] reports an unpublished result of SIMS and THOMPSON that $f(4) = 2^4\ 3^6$. No other values are known.

However, we can find structural restrictions on G_α when we are given $G_\alpha^{\Gamma(\alpha)}$. The first, discovered by JORDAN, is Theorem 18.4 of WIELANDT:

THEOREM 3.1. *If the Γ-graph is connected and p is a prime dividing $|G_\alpha|$, then p divides $|G_\alpha^{\Gamma(\alpha)}|$.*

PROOF. Suppose $p \nmid |G_\alpha^{\Gamma(\alpha)}|$, and suppose g is an element of order p fixing α. By assumption, g fixes every point of $\Gamma(\alpha)$; then g fixes every point at distance 2 from α; and so on. It follows that $g = 1$, a contradiction. So $p \nmid |G_\alpha|$. □

WIELANDT generalized this result to composition factors, assuming G is primitive; a composition factor of G_α is a composition factor of some subgroup of $G_\alpha^{\Gamma(\alpha)}$. It need not, however, be a composition factor of $G_\alpha^{\Gamma(\alpha)}$ itself. For example, let $G = S_{2n-1}$ act on the set of (n-1)-element subsets. $G_\alpha = S_{n-1} \times S_n$, but if $\Gamma(\alpha)$ is the set of (n-1)-element subsets disjoint from α, then $G_\alpha^{\Gamma(\alpha)} = S_n$, and (if $n \geq 6$) A_{n-1} is a composition factor of G_α but not of $G_\alpha^{\Gamma(\alpha)}$. Note that A_{n-1} is a composition factor of the stabiliser of a point in $G_\alpha^{\Gamma(\alpha)}$. This is quite general, as a result of WIELANDT shows (see [21, Theorem 1.1]).

Suppose K is a stable functor on finite groups, that is, K associates with any group a characteristic subgroup and has the property that $K(X) \leq Y \lhd X$ implies $K(Y) = K(X)$. KNAPP [26] shows

THEOREM 3.2. *If G is primitive with a suborbit Γ, and K is a stable functor such that $K(G_{\alpha\beta})$ acts trivially on both $\Gamma(\alpha)$ and $\Gamma^*(\beta)$ (where $(\alpha,\beta) \in \Gamma$), then $K(G_{\alpha\beta}) = 1$.*

The proof is very similar to that of theorem 3.1: $K(G_{\alpha\beta})$ fixes every point reachable from α by an "alternating" path of type Γ, Γ^*, Γ, Γ^*,..., and this set includes a connected component of $\Gamma \circ \Gamma^*$. Note that connectedness of Γ is not enough here, as the previous example shows.

Examples of stable functors include

(i) O^Λ, where Λ is a set of finite simple groups ($O^\Lambda(X)$ is the smallest normal subgroup Y of X such that all composition factors of X/Y lie in Λ). This includes O^π, for π a set of primes (smallest normal subgroup whose index is a π-number);

(ii) O_Λ, largest normal subgroup whose composition factors belong to Λ. This includes O_π, largest normal π-subgroup;

(iii) F, the Fitting subgroup (largest normal nilpotent subgroup).

Apply theorem 3.2 to O^Λ, where Λ is the set of composition factors of $G_{\alpha\beta}^{\Gamma(\alpha)}$ and $G_{\alpha\beta}^{\Gamma^*(\beta)}$, $(\alpha,\beta) \in \Gamma$. If $K(\alpha)$, $K^*(\alpha)$ are the kernels of the actions of G_α on $\Gamma(\alpha)$, $\Gamma^*(\alpha)$ respectively, then $O^\Lambda(G_{\alpha\beta}) \leq K(\alpha) \cap K^*(\beta)$, so $O^\Lambda(G_{\alpha\beta}) = 1$. In particular, the composition factors of $K(\alpha)$ belong to Λ. This is the cited result of WIELANDT.

Deeper results on the structure of G_α in a primitive group G can be obtained using normaliser and centraliser theorems of WIELANDT for subnormal subgroups. In this way WIELANDT [47] was able to show that, if $M(\alpha)$ is the subgroup of G fixing $\{\alpha\} \cup \Gamma(\alpha) \cup (\Gamma \circ \Gamma^*)(\alpha)$ pointwise, and $M^*(\alpha)$ is similarly defined, then one at least of $M(\alpha)$ and $M^*(\alpha)$ is a p-group, for some prime p. This has the following consequence, closely related to SIMS' conjecture:

THEOREM 3.3. *If* G *is primitive and* Γ *is a suborbit with* $|\Gamma(\alpha)| = v$, *then, for some prime* p, G_α *has a normal* p*-subgroup of index at most* $v!((v-1)!)^v$.

The fact that G has a normal p-subgroup of bounded index (given v) was first proved by THOMPSON [39]. KNAPP [26] has shown that, if $G_\alpha^{\Gamma(\alpha)}$ is 2-homogeneous (transitive on unordered pairs) or if v is prime, then the bound can be improved to $v!(v-1)!$, and we have seen that this is best possible. In several cases KNAPP is able to determine the precise structure of G_α when $G_\alpha^{\Gamma(\alpha)}$ is given.

Sometimes it is possible to prove that the normal p-subgroup referred to must be trivial. Applying theorem 3.2 with $K = F$ (or O_p), we see that, if $G_{\alpha\beta}^{\Gamma(\alpha)}$ and $G_{\alpha\beta}^{\Gamma^*(\beta)}$ have no normal nilpotent subgroup then neither does $G_{\alpha\beta}$; so in this case $M(\alpha)$ or $M^*(\alpha) = 1$, and we deduce that $|G_\alpha| \leq v!((v-1)!)^v$, or (if $G_\alpha^{\Gamma(\alpha)}$ is 2-homogeneous or v is prime) $|G_\alpha| \leq v!(v-1)!$

This is particularly useful when $G_\alpha^{\Gamma(\alpha)}$ and $G_\alpha^{\Gamma^*(\alpha)}$ are 2-primitive, in particular when $v = p+1$ for some prime p dividing $|G_\alpha|$. In this case, if $M(\alpha)$ and $M^*(\alpha)$ are non-trivial, then the stabiliser of a point in $G_\alpha^{\Gamma(\alpha)}$ or $G_\alpha^{\Gamma^*(\alpha)}$ has a regular normal subgroup. Doubly transitive groups with this property have been determined by HERING, KANTOR & SEITZ [19], so we can pin down the structure of $G_\alpha^{\Gamma(\alpha)}$ very precisely. This has been done by GARDINER [17;I] in the case where Γ is self-paired and $v = p+1$;

he was able to determine the structure of G_α. The result will be discussed further in the next section.

Application of these techniques, together with theorems about abstract finite groups, to the problem of primitive permutation groups with small subdegrees has resulted in a complete determination of such groups with a subdegree 3 (SIMS [34;I], WONG [48]), and of such groups with a subdegree 4 under the extra hypothesis that $G_\alpha^{\Gamma(\alpha)}$ is a 2-group (SIMS [34;II]) or the alternating group (QUIRIN [31]); partial results on subdegree 5 are obtained by QUIRIN [31] and KNAPP [26].

There are a number of results which assert that, under certain conditions, G_α acts faithfully on a generalized suborbit $\Delta(\alpha)$. This is true if G is primitive on Ω and one of the following holds:

(i) G_α is primitive on every suborbit not contained in $\Delta(\alpha)$ (MANNING [27]);

(ii) Δ contains Γ or Γ^* for every suborbit Γ (WIELANDT [44]);

(iii) G_α is 2-primitive on $\Delta(\alpha)$, $\Delta = \Delta^*$, and either G_α is primitive on $(\Delta \circ \Delta)(\alpha)$, or $|(\Delta \circ \Delta)(\alpha)| \neq |\Delta(\alpha)|(|\Delta(\alpha)|-1)$ (MANNING [27]).

A curious open conjecture asserts that the same result holds if G is primitive and G_α acts regularly on $\Delta(\alpha)$. This is known to be true if the stabiliser of a point in $\Delta^*(\alpha)$ fixes additional points there ([45, Theorem 18.6]), and so in particular if Δ is self-paired. It is false if we assume only that the Δ-graph is connected, even with the extra hypothesis; see example 1 of section 2.

Finally, I mention an extension of some of these results to doubly transitive groups due to SIMS [35]. Theorems like those of this section hold for the stabiliser of two points in a doubly transitive group G under a weaker assumption than 2-primitivity of G, namely the assumption that G is not an automorphism group of a block design with $\lambda = 1$. For example, suppose G is 2-transitive, $\Gamma(\alpha,\beta)$ is an orbit of $G_{\alpha\beta}$, and p is a prime dividing $|G_{\alpha\beta}|$ but not $|G_{\alpha\beta}^{\Gamma(\alpha,\beta)}|$. Then $O^{p'}(G_{\alpha\beta})$ is weakly closed in $G_{\alpha\beta}$ with respect to G, since it is generated by all the elements of p-power order in $G_{\alpha\beta}$, and it fixes $\Gamma(\alpha,\beta)$ pointwise; then WITT's lemma applies. (See result 2.B.1 of KANTOR's talk at this meeting [25] for discussion, or Theorem 9.4 of WIELANDT [45].)

4. DIGRESSION ON TRANSITIVITY IN GRAPHS

Throughout this section, Γ is a connected undirected graph whose automorphism group G is transitive on vertices and directed edges. (Thus we fix attention on a particular suborbit Γ, replace primitivity of G by connectedness of Γ, but assume that Γ is self-paired.)

Suppose that G is transitive on (ordered) paths of length 2. If Γ contains a triangle, then any two points joined by a path of length 2 are adjacent, and Γ is a complete graph K_{v+1}. We shall ignore this possibility, and assume that Γ contains no triangles. Let Δ be the graph with the same vertex set as Γ, in which two vertices are adjacent if and only if they are joined by a path of length 2 in Γ. (That is, $\Delta = \Gamma \circ \Gamma$.). Then G acts transitively on vertices and directed edges of Δ, and so Δ is regular with valency $v(v-1)/k$, where v is the valency of Γ and $k = |\Gamma(\alpha) \cap \Gamma(\beta)|$ for $(\alpha,\beta) \in \Delta$; k is a measure of "how many quadrilaterals Γ contains". Δ has at most two connected components, with exactly two if and only if Γ is bipartite. The first result shows how conditions on the structure of Δ influence Γ.

THEOREM 4.1. *If a connected component of Δ is a complete graph, then Γ is the incidence graph of a (possibly degenerate) self-dual symmetric design $\mathcal{D}$ satisfying*

(i) Aut $\mathcal{D}$ *is doubly transitive on the points of* $\mathcal{D}$;

(ii) *if* β *is a block, then* $\mathrm{Aut}(\mathcal{D})_\beta$ *is doubly transitive on the points incident with* β.

PROOF. Δ has two components; call the vertices of one component *points*, and those of the other *blocks*, and call a point and block *incident* if they are adjacent in Γ. The conditions are easily verified. □

At this meeting, KANTOR will discuss such designs ([25; section 8]). Of the known symmetric designs with doubly transitive automorphism groups, all are self-dual, and all except one (the HIGMAN design H_{176}) satisfy conclusion (ii) of theorem 4.1. These designs give us examples of such graphs. The degenerate designs have $k = v$ or $k = v-1$; the corresponding graphs are $K_{v,v}$ and the graph obtained from $K_{v+1,v+1}$ by deleting the edges of a matching. (Note: our v and k are the design parameters k and λ.)

Strong conclusions about Δ can be drawn if k is large enough.

THEOREM 4.2. *Either* $k \leq v/2$ *or a connected component of* Δ *is a complete graph.*

PROOF. Suppose $k > v/2$; take $\delta_1, \delta_2 \in \Delta(\alpha)$. Then

$$|\Gamma(\alpha) \cap \Gamma(\delta_1)| = |\Gamma(\alpha) \cap \Gamma(\delta_2)| > \tfrac{1}{2}|\Gamma(\alpha)| ,$$

and so there is a point in $\Gamma(\alpha) \cap \Gamma(\delta_1) \cap \Gamma(\delta_2)$. Then $(\delta_1, \delta_2) \in \Delta$. □

To refine this result, we need to consider more systematically the sets $\Gamma(\alpha) \cap \Gamma(\delta)$. Call elements of $\Gamma(\alpha)$ and $\Delta(\alpha)$ *points* and *blocks* respectively, and call a point and block *incident* if they are adjacent in Γ. Provided $k > 1$, this gives a design $\mathcal{D}$ whose blocks can be identified with the sets $\Gamma(\alpha) \cap \Gamma(\delta)$; v and k agree with the design parameters denoted by the same letters, and $\lambda = k-1$.

THEOREM 4.3. *Either* $v(v-1)k(k^2-3k+v)^2 \leq 2(v-k)^4(v-k-1)^2$ (*which implies* $k < (2v)^{4/5}$), *or a connected component of* Δ *is a complete* m*-partite graph* $K_{n,n,\ldots,n}$ *for some* m,n (*that is,* K_{mn} *with the edges of* m *pairwise vertex-disjoint* K_n*'s deleted.*)

PROOF. Let G_1 and G_2 be the graphs with vertex set $\Delta(\alpha)$ defined thus. Two vertices are adjacent in G_1 if (as blocks) they are not disjoint and no block is disjoint from both; two vertices are adjacent in G_2 if and only if (as blocks) they are disjoint. Both graphs admit the vertex-transitive group $G_\alpha^{\Delta(\alpha)}$, and so are regular, with valencies d_1 and d_2 respectively. Two points which are not adjacent in G_1 are joined by a path of length at most 2 in G_2; so $1+d_2+d_2(d_2-1) \geq v(v-1)/k-d_1$. From design theory we find that $d_2 \leq (v-k)^2(v-k-1)/k(k^2-3k+v)$. (See [8;II].) An easy counting argument shows that, if δ_1 and δ_2 are adjacent in G_1, then $\Delta(\delta_1)-\Delta(\alpha) = \Delta(\delta_2)-\Delta(\alpha)$. If G_1 is connected, then this holds for all δ_1, δ_2, whence the second alternative of theorem 4.3 holds. Otherwise $d_1 \leq v(v-1)/2k - 1$. Putting the three inequalities together gives the result. □

Curiously, only five graphs with $k > 2$ are known which fail to satisfy the second conclusion of theorem 4.3. These are the HIGMAN-SIMS graph on 100 vertices with $v = 22$, $k = 6$, two of its subgraphs (one on 100 vertices with $v = 15$, $k = 5$, obtained by deleting the edges of two vertex-disjoint HOFFMAN-SINGLETON subgraphs; the other on 77 vertices with $v = 16$, $k = 4$, on the vertices not adjacent to a given vertex), and graphs obtained from

the first and third by a "doubling" construction described below. It seems likely that the bound of theorem 4.3 can be improved substantially, and that graphs satisfying the second alternative can be described more precisely. (Note that such graphs must be bipartite.)

In passing, I note that a similar argument gives bounds for certain strongly regular graphs, such as those with no triangles and those associated with generalized quadrangles.

Our hypotheses imply that G_α acts doubly transitively on $\Gamma(\alpha)$. Stronger results can be obtained by increasing the degree of transitivity assumed. To state them, we need some definitions.

If H is a Hadamard matrix, define a graph Γ_H whose vertices are symbols (r_i,ε) and (c_j,ε), where i and j index rows and columns of H respectively and $\varepsilon = \pm 1$; (r_i,ε) and (c_j,ε') are adjacent if and only if the (i,j) entry of H is $\varepsilon\varepsilon'$. Γ_H and $\Gamma_{H'}$ are isomorphic if and only if H and H' are related by permuting and changing of rows and columns and (if necessary) transposing; thus Γ_H is a convenient "equivalence-invariant" of H.

If Γ is a non-bipartite graph satisfying our hypotheses, we can construct a bipartite graph satisfying them, with the same v and k, by the following "doubling" construction: vertices are symbols (α,ε), where α is a vertex of Γ and $\varepsilon = \pm 1$; (α,ε) and (β,ε') are adjacent if and only if α and β are adjacent in Γ and $\varepsilon\varepsilon' = -1$.

THEOREM 4.4. *Suppose that, with the hypotheses of this section,* G_α *is triply transitive on* $\Gamma(\alpha)$. *Then one of the following occurs:*

(i) $k = v$, $\Gamma = K_{v,v}$;

(ii) $k = v-1$, $\Gamma = K_{v+1,v+1}$ *with the edges of a matching removed;*

(iii) $v = 2^d$, $k = v/2$, Γ *is the incidence graph of the complementary design of* $PG_{d-1}(d,2)$;

(iv) $k = v/2$, $\Gamma = \Gamma_H$ *for some Hadamard matrix* H;

(v) $v = (\mu+1)(\mu^2+5\mu+5)$, $k = (\mu+1)(\mu+2)$ *for some positive integer* μ, *and* Γ *is strongly regular on* $(\mu+1)^2(\mu+4)^2$ *vertices, or is obtained from such a graph by "doubling";*

(vi) $k \leq 2$.

The main idea in the proof is this. We may suppose $2 < k < v-1$. The design $\mathcal{D}$ is now a 3-(v,k,μ) design, for some positive integer μ. Also, the number of blocks incident with a point $\gamma (= |\Gamma(\gamma) - \{\alpha\}|)$ is equal to the number of points different from $\gamma (= |\Gamma(\alpha) - \{\gamma\}|)$. So $\mathcal{D}$ is a symmetric

3-design (an extension of a symmetric design), so the main result of CAMERON [9] applies. (See [25; section 9], for this result and discussion of symmetric 3-designs.) If a connected component of Δ is a complete graph, then (iii) holds (see [25; 8.E.10]). Otherwise it can be shown that (iv) or (v) occurs.

THEOREM 4.5. *Suppose, with the hypotheses of this section, that* G_α *acts as the symmetric or alternating group on* $\Gamma(\alpha)$, *and that* Γ *contains a quadrilateral (that is,* $k > 1$*). Then one of the following holds:*

(i) $k = v$, $\Gamma = K_{v,v}$;

(ii) $k = v-1$, $\Gamma = K_{v+1,v+1}$ *with the edges of a matching removed;*

(iii) $k = 2$, $\Gamma = Q_v$ *(the* v*-dimensional cube);*

(iv) $k = 2$, $v \geq 5$, Γ *is obtained from* Q_v *by identifying opposite vertices;*

(v) $k = 2$, $v = 4$, Γ *is a unique graph on* 14 *vertices;*

(vi) $k = 2$, $v = 5$, Γ *is a unique graph on* 22 *vertices.*

The graphs under (v) and (vi) are the incidence graphs of the unique (7,4,2) and (11,5,2) designs. Note that G_α acts on $\Gamma(\alpha)$ as the symmetric group in all cases except (vi). Theorems 4.3-4.5 are proved under the stronger assumption of primitivity in CAMERON [8].

Another direction in which the hypotheses can be strengthened is that of requiring transitivity on longer paths. We say $G = \mathrm{Aut}\,\Gamma$ is s-*path transitive* if it is transitive on paths of length s. If Γ is a circuit, then G is s-path transitive for every s; but for any other finite graph, there is an upper bound on the degree of path-transitivity. It has been conjectured that $s \leq 7$ for any graph which is not a circuit. If $s \geq 3$ and Γ contains a quadrilateral, then it is a complete bipartite graph $K_{v,v}$; so we shall assume that (in the previous notation) $k = 1$. The graph O_v whose vertices are the (v-1)-element subsets of a (2v-1)-element set, adjacent if disjoint, admits the 3-path transitive automorphism group S_{2v-1}; here $G_\alpha^{\Gamma(\alpha)}$ is the symmetric group S_v. However, it appears that s-path transitivity with $s \geq 4$ places severe restrictions on the structure of $G_\alpha^{\Gamma(\alpha)}$.

THEOREM 4.6. *If* $v = 3$ *and* G *is* s-*path transitive then* $s \leq 5$.

This was proved by TUTTE [41], [42]. TUTTE's work provided the inspiration for later research by SIMS on primitive permutation groups with a subdegree 3. SIMS [34] and DJOKOVIC [14] were able to extend it to the

case v = p+1 (p prime) under the hypothesis that G contains a subgroup H which is s-*path regular* (that is, H is s-path transitive and only the identity fixes an s-path). In this case $|G_\alpha| = (p+1)p^{s-1}$, and $G_{\alpha\beta}$ is a p-group (for $\beta \in \Gamma(\alpha)$); calculations in this p-group show that $s \leq 5$ or $s = 7$.

The general problem was attacked by GARDINER [17;I], by combining these methods with those of WIELANDT discussed in section 3. WIELANDT's result (preceding theorem 3.3) is used to produce a p-group, normal in $G_{\alpha\beta}$, in which SIMS' calculations can be carried out. GARDINER's result is

THEOREM 4.7. *If* v = p+1 (p *prime*) *and* G *is* s (*but not* s+1)-*path transitive, then* $s \leq 5$ *or* $s = 7$.

In subsequent papers [18], [17;II], GARDINER has weakened the assumption on v. However, the general conjecture remains open.

EXAMPLES of graphs with s-path transitive groups.

For graphs of valency 3, all those with primitive groups have been determined by WONG [48]. Graphs of valency $v > 3$ with $s \geq 4$ seem much less common. The only known examples are the incidence graphs of certain self-dual generalized (s-1)-gons; in all cases v-1 is a prime power, and if $s = 5$ or $s = 7$ then v-1 is an odd power of 2 or 3 respectively. See TITS [40]. The resemblance of theorem 4.7 to the conclusions of FEIT & HIGMAN [16] is striking, since the methods are completely different.

Another unsolved problem is the exact relation between the degree of path-transitivity of G and the degree of transitivity of G_α on $\Gamma(\alpha)$. GARDINER has conjectured that, if G is 4-path transitive, then G_α is 2-primitive on $\Gamma(\alpha)$. The significance of this conjecture is clear from remarks in section 3.

A further kind of transitivity has been studied by BIGGS [4] and others. A graph Γ is called *distance-transitive* if it is connected and its automorphism group G acts transitively on (ordered) pairs of vertices at distance i for every i with $0 \leq i \leq d$, where d is the diameter of Γ. In particular, G is transitive on vertices and directed edges. However, G may not be 2-path transitive, since Γ may contain triangles. The main technique in the study of distance-transitive graphs is the computation of eigenvalues and multiplicities for the basis matrices. This is simplified by the facts that the basis matrix of Γ generates the centraliser algebra (and so it has d+1 distinct real eigenvalues), and the intersection matrix is

tridiagonal. (Similar remarks apply if the transitivity of G is replaced by appropriate "coherence" or "metric regularity" conditions; graphs such as Moore graphs satisfy these conditions, and this method was used by BANNAI & ITO [2] and DAMARELL [12] to show the non-existence of such graphs with diameter and valency greater than 2. Graphs satisfying these conditions will be discussed at this meeting by DELSARTE [13] under the name of *metric* or P-*polynomial association schemes*. See also [4],[22],[23].)

Two other ideas are relevant to the study of distance-transitive graphs. The first is the observation of D.H. SMITH [36] that if Γ is distance-transitive and $G = \mathrm{Aut}\,\Gamma$ is imprimitive, then Γ is either bipartite or antipodal. (Γ is *antipodal* if the relation of being equal or at distance d is an equivalence relation on the vertex set, where d is the diameter of Γ.) If Γ is antipodal but not bipartite, then by identifying vertices at distance d we obtain another distance-transitive graph with primitive automorphism group. Secondly, if Γ is distance-transitive with given valency, it may be possible to obtain a bound for $|G_\alpha|$ by the methods of section 3. Often such a bound can be converted into a bound for the diameter of Γ. (This is true if Γ has valency 3 [5] or is bipartite [37].) If both steps can be done, the complete determination of such graphs is reduced to a finite amount of calculation.

5. COMBINATORIAL RELATIONS AMONG SUBORBITS

Through this section we shall assume that G is primitive. We are concerned with the consequences of assumptions about the action of G_α on some or all of its orbits. The prototype is a theorem of MANNING [28], which asserts that, *if* G_α *is doubly transitive on* $\Gamma(\alpha)$, *where* $|\Gamma(\alpha)| > 2$, *then* G_α *has an orbit* $\Delta(\alpha)$ *with* $|\Delta(\alpha)| > |\Gamma(\alpha)|$, *or* G *is triply transitive*. The hypothesis implies that G acts transitively on figures of the first kind in figure 2.1 (or on paths of length 2 if Γ is self-paired), and hence that $\Delta = \Gamma^* \circ \Gamma$ is a single suborbit; $|\Delta(\alpha)| = v(v-1)/k$, where $v = |\Gamma(\alpha)|$ and $k = |\Gamma^*(\alpha) \cap \Gamma^*(\delta)|$, $(\alpha,\delta) \in \Delta$. Now our situation is very similar to that of the last section, and by similar arguments we can prove (as in [8]):

THEOREM 5.1. *Either* $v(v-1)k(k^2-3k+v)^2 \leq 2(v-k)^4(v-k-1)^2$ *or* G *is doubly transitive.*

This considerably strengthens MANNING's theorem, but is again probably not best possible; in all known cases except two, $k \leq 2$ or G is doubly transitive. The two exceptions both have rank 3.

THEOREM 5.2. *If* G_α *is triply transitive on* $\Gamma(\alpha)$, *or if* G_α *has rank at most* 3 *on* $\Delta(\alpha)$, *then one of the following holds:*

(i) $k \leq 2$;

(ii) $|\Omega| = (\mu+1)^2(\mu+4)^2$, $v = (\mu+1)(\mu^2+5\mu+5)$, $k = (\mu+1)(\mu+2)$, *for some positive integer* μ, *and* G *has rank* 3;

(iii) G *is doubly transitive.*

THEOREM 5.3. *If* $G_\alpha^{\Gamma(\alpha)}$ *is the symmetric or alternating group, then one of the following holds:*

(i) $k = 1$;

(ii) $|\Omega| = 2^{v-1}$, v *odd*, $G = V_{2^{v-1}} \cdot S_v$ *or* $V_{2^{v-1}} \cdot A_v$;

(iii) $G = S_{v+1}$ *or* A_{v+1}.

These results can be regarded as *rank-bounding theorems*; from a certain hypothesis we deduce either a (stronger) conclusion or a bound for the rank of the primitive group G. (This is valuable because of the existing techniques for studying multiply transitive groups and groups of small rank.) Such theorems have occurred from time to time in the literature; I shall digress to discuss some of them, classified according to the type of hypothesis.

1. *Hypotheses about the degree* $n = |\Omega|$

Let p denote a prime. A classic theorem of BURNSIDE [7] asserts that, if $n = p$, then G is soluble or doubly transitive. (In the former case, G is the group $\{x \mapsto a^m x+b \mid a,b \in GF(p), a \neq 0\}$, where m is a fixed divisor of $p-1$.) Related results are due to WIELANDT [43],[46]: If $n = 2p$ then G has rank at most 3, and G is doubly transitive unless $p = 2a^2+2a+1$ for some integer a; in the latter case, the subdegrees are $a(2a+1)$ and $(a+1)(2a+1)$, and the intersection numbers are also polynomials in a. (S_5 and A_5, acting on 2-element subsets, provide examples with $a = 1$.) Similar results for $n = 3p$ have been found by NEUMANN [30] and SCOTT [33], and for $n = 4p$ by COOPER, incomplete as yet. If $n = p^2$ then one of the following holds: G has a regular normal subgroup (so $G \leq AGL(2,p)$); $G \leq S_p$ wr S_2 (acting on the vertices of the square lattice graph); G is doubly transitive.

2. *Group-theoretic assumptions*

In this class may be put BENDER's theorem [3] on strongly embedded subgroups; a crucial part of it states that, if G_α is strongly embedded in G, then either G has a regular normal subgroup of odd order, or G is doubly transitive. (In the latter case BENDER has determined the possible groups.) Another such result is the FEIT-HIGMAN theorem [16] which asserts that, if G has a BN-pair of rank 2 and G_α is a maximal parabolic subgroup, then $|G_\alpha| = 2$ or G has rank 2, 3, 4, 5 or 7.

3. *Numerical conditions on subdegrees*

It follows from the theorem of BANNAI & ITO [2] and DAMERELL [12] on Moore graphs that, if G has subdegrees 1, a, $a(a-1),\ldots, a(a-1)^{r-2}$, then either $a = 2$ or $r \leq 3$. Similar results are given by HIGMAN [22].

4. *Hypotheses about the action of* G *on some or all of its orbits*

Theorems 5.1-5.3 are of this type, and others follow.

MANNING's theorem implies that, in a primitive permutation group G, if G_α is doubly transitive on every suborbit different from $\{\alpha\}$, then $|G_\alpha| = 2$ or G is doubly transitive. This suggests defining the *subrank* of a transitive permutation group to be the maximum rank of the stabiliser of a point on its orbits, and making the conjecture that in a primitive group of subrank m, either the rank is bounded by a function of m, or $|G_\alpha| = m$. (As originally formulated, the second alternative was that G_α has a non-trivial regular orbit. This is implied by the condition $|G_\alpha| = m$, and is equivalent to it if the conjecture at the end of section 3 is correct. Frobenius groups, and many other examples, show that this possibility must be allowed.) If true, the conjecture implies the existence of functions f and g defined by

$$f(m) = \min\{r \mid G \text{ primitive } \&\ \text{subrank}(G) = m \text{ implies } \text{rank}(G) \leq r \text{ or } |G_\alpha| = m\},$$

$$g(m) = \min\{r \mid \exists \text{ finite set } \mathcal{S} \text{ of permutation groups such that G primitive } \&\ \text{subrank}(G) = m \text{ implies } \text{rank}(G) \leq r \text{ or } |G_\alpha| = m \text{ or G is isomorphic to a group in } \mathcal{S}\}.$$

It would be interesting to have exact values for f(m) and g(m) where they are defined. Clearly $f(2) = g(2) = 2$. Lower bounds for suitable values of m can be obtained from specific groups:

1. Let $F = GF(q^2)$, where $q = 2^n$, and
$G = \{x \mapsto a^{q-1}x^\sigma + b \mid a,b \in F, a \neq 0, \sigma \in \mathrm{Aut}\ F, \sigma^2 = 1\}$.
G_0 is a dihedral group of order $2(q+1)$ and has $q-1$ orbits of length $q+1$, one containing each non-zero element of $GF(q)$. So $f(2^{n-1}+1) \geq 2^n$.

2. Let $G = S_n$ wr S_k, in its representation of degree n^k. G has rank $k+1$ and subrank $[(k+2)(k+3)/6]$, independent of n. So $g([(k+2)(k+3)/6]) \geq k+1$.

For $m = 3$, these bounds are exact [10]:

THEOREM 5.4. *If G is a primitive permutation group with subrank 3, then one of the following holds:*

(i) *G has rank at most 3;*

(ii) *$|G_\alpha| = 3$, G is a Frobenius group;*

(iii) *G is the group of example 1, with rank 4 and degree 16.*

PROOF. If all subdegrees are at most 5, or if $|G_\alpha|$ is odd, then the result can be proved by *ad hoc* arguments. If $|\Gamma(\alpha)| \geq 6$ and $|G_\alpha^{\Gamma(\alpha)}|$ is even for some suborbit Γ, then the complete graph on $\Gamma(\alpha)$ is partitioned into subgraphs corresponding to at most two suborbits; by RAMSEY's theorem, one of these contains a triangle. So $\Delta \subseteq \Delta \circ \Delta$ for some suborbit Δ. Then it is shown that the Δ-graph has diameter at most 2. Regarding the application of RAMSEY's theorem, it is worth noting that the three graphs in case (iii) are non-degenerate with respect to the next case of the theorem (that is, none of them contains a triangle). □

Primitive groups with rank and subrank 3 have been investigated by character-theoretic methods by M.S. SMITH [38], who has found strong restrictions on their parameters. A number of examples exist, including S_n wr S_2, the split extension $V_{2^{2n}} \cdot O^{\pm}(2n,2)$, $P\Gamma U(4,q^2)$ (for prime power q), and the HIGMAN-SIMS and MCLAUGHLIN groups. The graph-theoretic analogue of this situation is a strongly regular graph Γ with the property that the restrictions of Γ to the points adjacent and non-adjacent to any point are both strongly regular. The arguments of [38] extend to this situation, using the algebras associated with "coherent configurations" in place of the centraliser algebras of permutation groups. The result is that either such a graph is of pseudo-Latin square or negative Latin square type [29], or the parameters of it or its complement are given by

$$n = 2(2r-s)^2(r(r-1)-(2r+1)s)/(s+r^2-r)(s-r^2-3r),$$
$$k = (r-s)((2r+1)s-r(3r+1))/(s-r^2-3r),$$
$$l = (r-1-s)((2r+1)s-r(3r+1))/(s+r^2-r),$$
$$\lambda = r(r-1-s)(s+r^2+r)/(s-r^2-3r),$$
$$\mu = (r+1)(r-s)(s+r^2-r)/(s-r^2-3r),$$

where s and r are integers satisfying

$$-s > r(r+1),$$
$$(s-r^2-3r) \mid 2r^2(r+1)^2(r+2),$$
$$(s+r^2-r) \mid 2r^2(r-1)(r+1)^2.$$

(Here, as in [20], n is the degree, k and l the subdegrees, and λ and μ the intersection numbers a_{111} and a_{112}.) SMITH remarks that these conditions have nine infinite families of solutions (with s an integer polynomial in r), and also proves uniqueness (in the group-theoretic situation) for small values of the parameters.

Another generalization of MANNING's theorem can be obtained by relaxing the condition that G is doubly transitive on all non-trivial suborbits. Thus, it is proved in [11] that

THEOREM 5.5. *If G is primitive on Ω and G_α is doubly transitive on all non-diagonal suborbits except possibly one, with $|G_\alpha| > 2$, then G has rank at most 4. If the rank is 4, then the two doubly transitive suborbits of G are paired with each other, and the degrees, subdegrees, and intersection numbers are polynomials in a single integer parameter.*

The only known example of such a rank 4 group is $PSU(3,3^2)$ acting on 36 points, with subdegrees 1, 7, 7, 21. The stabiliser of a point is PSL(3,2), and the non-trivial suborbits can be identified with the points, lines, and flags of PG(2,2). Indeed, this is the only known primitive rank 4 group with non-trivial pairing of suborbits.

MANNING's theorem in fact implies a stronger statement than the one we have taken as a model for generalization: If G is primitive on Ω, and G_α is doubly transitive on its largest orbit, then $|G_\alpha| = 2$ or G is doubly transitive. Thus it would be desirable to bound the rank of a primitive group G under the assumption that G_α acts with prescribed rank, but not regularly, on its largest orbit. All that is known here is that if $\Delta(\alpha)$ is the largest G_α-orbit and $\Gamma(\alpha)$ any non-trivial G_α-orbit, then the permutation characters of G_α on $\Gamma(\alpha)$ and $\Delta(\alpha)$ must have a non-principal irreducible

constituent in common, provided $|\Delta(\alpha)| > 1$. (For otherwise $G_{\alpha\gamma}$ is transitive on $\Delta(\alpha)$, for $\gamma \in \Gamma(\alpha)$; so $\Delta(\alpha)$ is a G_γ-orbit and hence is fixed by $\langle G_\alpha, G_\gamma \rangle$. But $\langle G_\alpha, G_\gamma \rangle = G$ unless $|G_\alpha| = 1$.)

Another general question, suggested by theorem 5.2, is this. Suppose G is primitive, Γ is a self-paired suborbit, and the actions of G_α on $\Gamma(\alpha)$ and $(\Gamma \circ \Gamma)(\alpha)$ are prescribed. When are these conditions consistent, and when do they imply a bound for the rank? (For example, if $G_\alpha = M_{22}$ acts on $\Gamma(\alpha)$ and $(\Gamma \circ \Gamma)(\alpha)$ as on the points and blocks of the Steiner system, then G has rank 3 and is isomorphic to HS. For $V_{16}Sp(4,2)$ on the points and blocks of the (16,4,3) design, there exists a rank 3 extension, Aut M_{22}; for $V_{64}G_2(2)$ on the points and blocks of the (64,4,3) design, neither answer is known.)

6. ALGEBRAIC RELATIONS AMONG SUBORBITS

We saw in section 1 that the rank of a transitive group is the sum of squares of multiplicities of irreducible constituents of the permutation character, while the number of self-paired suborbits is the sum of multiplicities of irreducibles of the first kind minus the sum for those of the second kind. If the multiplicities are $e_0=1,\ldots,e_s$, then the centraliser algebra (generated by the basis matrices) is a direct sum of matrix algebras of degrees $e_0,\ldots,e_s$ over $\mathbb{C}$. Thus all multiplicities are equal to 1 if and only if all pairs of basis matrices commute. This must be the case if the rank is at most 5, but need not be so for rank 6. (More generally, if $e > 1$, then $1_G + e\chi$ is not a permutation character. For in any transitive group there is an element g with no fixed points; if $\pi = 1_G + e\chi$, then $-1/e = \chi(g)$ is an algebraic integer.)

The case where the centraliser algebra is commutative is very important, and is discussed in section 29 of WIELANDT [45]. Certain group theoretic conditions (such as the existence of a regular abelian subgroup, or the existence of an element interchanging any pair of points, guarantee that this holds. Less trivially, GLAUBERMAN has remarked that if the Sylow 2-subgroups of G are cyclic or generalized quaternion, and G acts by conjugation on its set of involutions, then the centraliser algebra is commutative; he asks if this fact can be used to obtain an alternative proof of the theorem that such a group, if primitive, has a regular normal subgroup.

In other situations we may have only the weaker information that a particular pair C_i, C_j of basis matrices commute. This has the obvious consequence that $a_{ijk} = a_{jik}$ for all k; but sometimes it is possible to go further. I shall illustrate this with a discussion of a normal basis matrix (one which commutes with its transpose) corresponding to a doubly transitive subconstituent.

Suppose G_α is doubly transitive on $\Gamma(\alpha)$, with $\Gamma \neq \Gamma^*$ and $|\Gamma(\alpha)| = v$. Then $\Gamma^* \circ \Gamma$ is a single suborbit, with subdegree $v(v-1)/k$ for some k (section 5). Also, G_α is doubly transitive on $\Gamma^*(\alpha)$ (section 2), and so $\Gamma \circ \Gamma^*$ is a single suborbit, with subdegree $v(v-1)/k'$ for some k'. Counting in two ways quadrilaterals of the first kind in figure 6.1 gives

$$|\Omega| \frac{v(v-1)}{k} k(k-1) = |\Omega| \frac{v(v-1)}{k'} k'(k'-1),$$

so

$$k = k'.$$

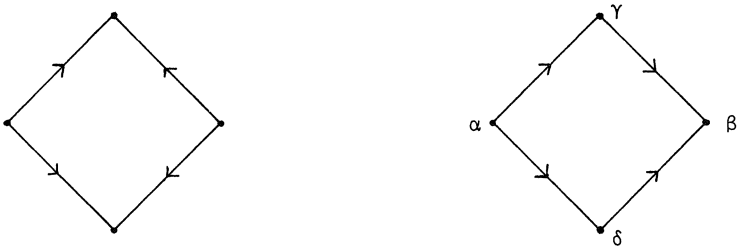


Fig. 6.1

Although the subdegrees are equal, the suborbits $\Gamma^* \circ \Gamma$ and $\Gamma \circ \Gamma^*$ may or may not be equal. An example where they are not equal is given in [8;I]; for one where they are equal, see theorem 5.5. If C, D, D' are the basis matrices of Γ, $\Gamma^* \circ \Gamma$, $\Gamma \circ \Gamma^*$ respectively, we have

$$C^T C = vI + kD, \quad C C^T = vI + kD';$$

so $\Gamma^* \circ \Gamma = \Gamma \circ \Gamma^*$ if and only if C is a normal matrix. We shall call Γ *normal* if this occurs.

THEOREM 6.1. *Γ is normal if and only if $|(\Gamma \circ \Gamma)(\alpha)| < v^2$. If this holds and G is primitive, then G has the same permutation character on $\Gamma(\alpha)$ and $\Gamma^*(\alpha)$.*

PROOF. The Γ-graph contains figures of the second kind in figure 6.1 if and only if Γ is normal (since $(\gamma,\delta) \in (\Gamma^* \circ \Gamma) \cap (\Gamma \circ \Gamma^*)$). Also, the graph contains such figures if and only if $|(\Gamma \circ \Gamma)(\alpha)| < v^2$ (for there are two paths of length 2 from α to β). Suppose Γ is normal and G has different permutation characters on $\Gamma(\alpha)$ and $\Gamma^*(\alpha)$. Then G is transitive on paths of length 2, so $\Gamma \circ \Gamma$ is a single suborbit, with subdegree v^2/l for some integer l. Counting these figures in two ways,

$$|\Omega| \frac{v(v-1)}{k} k^2 = |\Omega| \frac{v^2}{l} l(l-1),$$

so

$$(v-1)k = v(l-1).$$

Since Γ is normal, $l > 1$, and so v divides k; thus $v = k$, and G is imprimitive by theorem 5.1. (The structure of the graph is obvious.) □

If G is primitive, we can push the counting argument further. G_α has the same permutation character on $\Gamma(\alpha)$ and $\Gamma^*(\alpha)$, so these are the points and blocks of a symmetric design with parameters (v,K,Λ), possibly trivial. Then $\Gamma \circ \Gamma$ is the union of two suborbits with subdegrees vK/l and $v(v-K)/l'$ for some l, l'. Now the count gives

$$|\Omega| \frac{v(v-1)}{k} k^2 = |\Omega| \frac{vK}{l} l(l-1) + |\Omega| \frac{v(v-K)}{l'} l'(l'-1),$$

$$(v-1)k = K(l-1) + (v-K)(l'-1).$$

If the representations of G_α on $\Gamma(\alpha)$ and $\Gamma^*(\alpha)$ are equivalent, we can assume $K = 1$, whence it follows that $l = 1$, $l' = k+1$. If G_α is triply transitive on $\Gamma(\alpha)$ then this hypothesis holds, and in addition $k = 1$, $l' = 2$. (If, further, $G_\alpha^{\Gamma(\alpha)}$ is the symmetric or alternating group of sufficiently large degree, it can be shown that G has a regular normal subgroup.) Other solutions which actually occur are $v = 7$, $k = 2$, $K = l = 4$, $l' = 1$ ($PSU(3,3^2)$, degree 36, rank 4) and $v = 11$, $k = 2$, $K = l = 5$, $l' = 1$ (M_{12}, degree 144, rank 5).

The concept of normality has also been used in a rank-bounding theorem [11].

The formulae for the rank and number of self-paired suborbits show that, if the centraliser algebra is non-commutative, then there are non-self-paired suborbits. Is it even true that there will be non-normal suborbits? Does there exist an example of a basis matrix which is not even diagonalisable?

Sometimes it has been shown that there is an absolute bound, greater than 1, on the multiplicities. (For example, in some cases where the Sylow 2-subgroup has rank 2 or 3, and G acts by conjugation on its involutions, the multiplicities are at most 2 or 3.) It is tempting to conjecture that a general result of this kind holds, and it may be worth studying situations where such a bound exists. If the multiplicities are at most d, the centraliser algebra is a sum of matrix algebras with degrees at most d, and so it satisfies certain identities. These identities have combinatorial interpretations in the graphs, similar to that considered for normality; but I do not know how to exploit these conditions.

REFERENCES

[1] ATKINSON, M.D., *Doubly transitive but not doubly primitive permutation groups, I*, J. London Math. Soc. (2), 7 (1974) 632-634; *II*, ibid., to appear.

[2] BANNAI, E. & T. ITO, *On finite Moore graphs*, J. Fac. Sci. Univ. Tokyo, 20 (1973) 191-208.

[3] BENDER, H., *Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festlasst*, J. Algebra, 17 (1971) 527-554.

[4] BIGGS, N., *Finite groups of automorphisms*, London Math. Soc. Lecture Notes 6, C.U.P., 1971.

[5] BIGGS, N. & D.H. SMITH, *On trivalent graphs*, Bull. London Math. Soc., 3 (1971) 155-158.

[6] BRITTON, J.L., *The word problem*, Ann. of Math., 77 (1963) 16-32.

[7] BURNSIDE, W., *On some properties of groups of odd order*, Proc. London Math. Soc. (1), 33 (1901) 162-185.

[8] CAMERON, P.J., *Permutation groups with multiply transitive suborbits, I*, Proc. London Math. Soc. (3), 25 (1972) 427-440; *II*, Bull. London Math. Soc., to appear.

[9] CAMERON, P.J., *Extending symmetric designs*, J. Combinatorial Theory A, 14 (1973) 215-220.

[10] CAMERON, P.J., *Bounding the rank of certain permutation groups*, Math. Z., 124 (1972) 343-352.

[11] CAMERON, P.J., *Primitive groups with most suborbits doubly transitive*, Geometriae Dedicata, 1 (1973) 434-446.

[12] DAMERELL, R.M., *On Moore graphs*, Proc. Cambridge Philos. Soc., 74 (1973) 227-236.

[13] DELSARTE, P., *The association schemes of coding theory*, Mathematical Centre Tracts 55, 1974, pp. 139-157.

[14] DJOKOVIC, D.Z., *On regular graphs, I*, J. Combinatorial Theory, 10 (1971) 253-263; *II*, ibid., 12 (1972) 252-259.

[15] FEIT, W., *Characters of finite groups*, Benjamin, New York, 1967.

[16] FEIT, W. & G. HIGMAN, *The non-existence of certain generalized polygons*, J. Algebra, 1 (1964) 114-138.

[17] GARDINER, A.D., *Arc transitivity in graphs, I*, Quart. J. Math. Oxford Ser. (2), 24 (1973) 399-407; *II*, ibid., to appear.

[18] GARDINER, A.D., *Doubly primitive vertex stabilisers in graphs*, Math. Z., to appear.

[19] HERING, C., W.M. KANTOR & G. SEITZ, *Finite groups with a split* BN-*pair of rank 1*, J. Algebra, 20 (1972) 435-475.

[20] HIGMAN, D.G., *Finite permutation groups of rank 3*, Math. Z., 86 (1964) 145-156.

[21] HIGMAN, D.G., *Primitive rank 3 groups with a prime subdegree*, Math. Z., 91 (1966) 70-86.

[22] HIGMAN, D.G., *Intersection matrices for finite permutation groups*, J. Algebra, 6 (1967) 22-42.

[23] HIGMAN, D.G., *Combinatorial considerations about permutation groups*, Lecture Notes, Oxford, 1972.

[24] HIGMAN, G., B.H. NEUMANN & H. NEUMANN, *Embedding theorems for groups*, J. London Math. Soc. (1), 26 (1949) 247-254.

[25] KANTOR, W.M., *2-transitive designs*, Mathematical Centre Tracts 57, Amsterdam, 1974, 44-97.

[26] KNAPP, W., *On the point stabilizer in a primitive permutation group*, Math. Z., 133 (1973) 137-168.

[27] MANNING, W.A., *Simply transitive primitive groups*, Trans. Amer. Math. Soc., 29 (1927) 815-825.

[28] MANNING, W.A., *A theorem concerning simply transitive primitive groups*, Bull. Amer. Math. Soc., 35 (1929) 330-332.

[29] MESNER, D.M., *A new family of partially balanced incomplete block designs with some Latin square design properties*, Ann. Math. Statist., 38 (1967) 571-581.

[30] NEUMANN, P.M., *Primitive permutation groups of degree 3p*, unpublished.

[31] QUIRIN, W.L., *Primitive permutation groups with small orbitals*, Math. Z., 122 (1971) 267-274.

[32] QUIRIN, W.L., *Extension of some results of Manning and Wielandt on primitive permutation groups*, Math. Z., 123 (1971) 223-230.

[33] SCOTT, L., *Unprimitive permutation groups*, in: *Theory of finite groups*, R. BRAUER & C-H. SAH (eds.), Benjamin, New York, 1969.

[34] SIMS, C.C., *Graphs and finite permutation groups, I*, Math. Z., 95 (1967) 76-86; *II*, ibid., 103 (1968) 276-281.

[35] SIMS, C.C., *Computational methods in the study of permutation groups*, in: *Computational problems in abstract algebra*, J. LEECH, (ed.), Pergamon Press, London, 1970, pp. 169-183.

[36] SMITH, D.H., *Primitive and imprimitive graphs*, Quart. J. Math. Oxford (2), 22 (1971) 551-557.

[37] SMITH, D.H., *Bounding the diameter of a distance-transitive graph*, J. Combinatorial Theory B, to appear.

[38] SMITH, M.S., *On rank 3 permutation groups*, to appear.

[39] THOMPSON, J.G., *Bounds for orders of maximal subgroups*, J. Algebra, 14 (1970) 135-138.

[40] TITS, J., *Sur la trialité et certains groupes qui s'en deduisent*, Publ. Math. IHES, 2 (1969) 14-60.

[41] TUTTE, W.T., *A family of cubical graphs*, Proc. Cambridge Philos. Soc., 43 (1947) 459-474.

[42] TUTTE, W.T., *On the symmetry of cubic graphs*, Canad. J. Math., 11 (1959) 621-624.

[43] WIELANDT, H., *Primitive Permutationsgruppen vom Grad 2p*, Math. Z., 63 (1956) 478-485.

[44] WIELANDT, H., *Subnormale Hülle in Permutationsgruppen*, Math. Z., 74 (1962) 297-298.

[45] WIELANDT, H., *Finite permutation groups*, Acad. Press, New York, 1964.

[46] WIELANDT, H., *Permutation groups through invariant relations and invariant functions*, Lecture Notes, Ohio State Univ., 1969.

[47] WIELANDT, H., *Subnormal subgroups and permutation groups*, Lecture Notes, Ohio State Univ., 1971.

[48] WONG, W.J., *Determination of a class of primitive permutation groups*, Math. Z., 99 (1967) 235-246.

MATHEMATICAL CENTRE TRACTS 57, 1974, 130-161

GROUPS, POLAR SPACES AND RELATED STRUCTURES

E.E. SHULT

University of Florida, Gainesville, Fla. 32611, USA

INTRODUCTION

The purpose of this report is to give a simplified and more or less systematic account of certain developments at the interface between finite group theory and combinatorial theory. At the present time it is virtually possible to characterize the graphs associated with the so-called classical groups on the basis of an exceedingly crude graph-theoretic hypothesis. Such a theorem commands an obvious relevance to finite group theory since it may be used as a tool for diagnosing the presence of a "classical group" -that is, to tell whether a finite group G contains one of the groups $PGU(n,q^2)$, $PSO^{\varepsilon}(n,q),(\varepsilon=\pm 1)$ or $PSp(2n,q)$. Of course in this case, the crudity (or simplicity, if one prefers) of the graph-theoretic hypothesis means that such a graph is more easily realized within a finite group, and this feature serves in making such a diagnostic tool more widely applicable. The phrase "virtually possible to characterize" appears above because certain extremal cases and certain rather tight open cases are also present. To be more specific, graphs which contain a vertex lying on an edge with every remaining vertex, and any generalized quadrangle may also appear along with the "classical-group-graphs" in the conclusion of the theorem. In practice, when the graph is realized in a finite group, say with vertices being a conjugacy class of subgroups and edges some convenient relation between these subgroups, the case that one vertex lies on an edge with each remaining vertex usually implies something very extreme for the group G, and so can usually be handled. Coming to grips with the case of generalized quadrangles is usually more difficult. Nonetheless nice applications of the theorem in finite groups exist (see section 10).

In the hope that this theorem may prove useful in other problems, both inside and outside of finite group theory, I have tried to give a rather simplified presentation of this theorem. (Because some of the deeper results on polar spaces and buildings are necessarily deferred to Professor TITS' forthcoming book, the present treatment will bear a closer resemblance to a boyscout handbook on prepolar spaces and groups, rather than any sort of complete treatise.) The characterization theorem presented is really a linking together of a number of theorems. The chain of theorems begins with VELDKAMP's important work on finite polar spaces fifteen years ago, and this work was subsequently streamlined and extended to infinite polar spaces by TITS [32,29]. It is worth noting, therefore, that the presentation in sections 2 through 7 does not require the structures in question to be finite; but only that they have finite *rank*, a notion in this context roughly analogous to having finite dimension.

Possible variations of the characterization theorem to graphs of non-isotropic or non-singular projective points or to structures associated with other Chevalley groups is discussed in section 9. Section 10 concludes with a few historical notes concerning the origins of the problems and their applications to finite group theory.

1. THE MAIN THEOREMS

We begin with the basic characterization theorem for finite graphs. Throughout, the word "graph" means an undirected graph without loops or double edges. Thus a *graph* is a set V of vertices and a set E (called the *edge set*) which is a subset of $V^{(2)}$, the set of all 2-sets of elements of V. The graph is said to be *finite* if V is a finite set. A graph (V,E) is called *complete* if $E = V^{(2)}$. If X is a subset of V, the *subgraph* X means the graph $(X, E \cap X^{(2)})$. A *clique* means a complete subgraph of (V,E). (Note that in some quarters of this world, "clique" means "maximal complete subgraph"; it does not here.)

THEOREM A. *Let* $G = (V,E)$ *be a finite graph. Suppose, for each edge* (x,y) *in* E *there exists a clique* $C(x,y)$ *containing* x *and* y *such that*

(i) $|C(x,y)| \geq 3$.

(ii) *If* $w \in V - C(x,y)$, *then* w *either lies on an edge with exactly one member of* $C(x,y)$ *or on an edge with every member of* $C(x,y)$.

Then one of the following conclusions holds:

(a) *There exists a vertex in* V *lying on an edge with every other vertex of* V.

(b) $(V,E) \simeq S_\pi$ *where* S_π *is the graph whose vertices are the points of a semiquadric* S_π *with edges being pairs of points of* S_π *which are perpendicular with respect to* π.

(c) *Each* $C(x,y)$ *is uniquely determined by* x *and* y *and* $(V, \{C(x,y) \mid (x,y) \in E\})$ *is a generalized quadrangle.*

(d) (V,E) *is totally disconnected; that is, the edge set* E *is empty.*

In case (b), π is either a non-degenerate polarity of a projective Desarguesian space P and S_π is the set of *absolute points* with respect to π (i.e. points $p \in P$ such that $p \in \pi(p)$) or else π is a (proportionality class of) non-degenerate quadratic form(s) on P and S_π is the set of *singular points* of P with respect to π (i.e. points $p \in P$ such that $\pi(p) = 0$). In either case it makes sense to define "perpendicular with respect to π". Thus S_π denotes the absolute points under a non-degenerate unitary, orthogonal or symplectic polarity, or else the singular points of a non-degenerate quadratic form of a Desarguesian projective space over a field of characteristic 2. The point is that as a graph G is uniquely determined up to isomorphism.

The significance of case (c) is that the $C(x,y)$ are actually maximal cliques, $C(x,y)$ may be viewed as the "line" through x and y, and if L is a line and q a point in V not on L, then q is *collinear* (on a line) with exactly one member of L. It does not follow that all $C(x,y)$'s have the same cardinality as the following example shows: Let A and B be sets of size 3 and 4 respectively. Set $V = A \times B$ and let $(p,q) \in E$ if and only if p and q either agree in their A-coordinate or their B-coordinate, but not both. The graph becomes a 3×4 grid with rows and columns forming the seven "lines". If, however, there exists a vertex lying on at least three lines of a general graph in case (c), then it is not difficult to see that all "lines" -that is, the $C(x,y)$'s- have the same cardinality. Thus the "grids" are the only examples in which $|C(x,y)|$ does not assume a constant value. For this reason (and for the reason that the "grids" are determined up to isomorphism) one frequently excludes these from the definition of generalized quadrangle (see PAYNE [16]).

Case (d) is a graph determined up to isomorphism.

As mentioned in the introduction, this theorem is pieced together from a number of other theorems. Moreover, this piecing together could have been

done so that a version of the above theorem for infinite graphs could have been obtained. How this is done will become apparent (though somewhat clumsy to state) as we break up the above theorem into the pieces which make it work. For this purpose, we introduce an abstract concept designed to mimic the hypotheses of theorem A. This concept is due to BUEKENHOUT [8] (who unfortunately gave it a name rather awkward for me to use. I hope he will forgive me if I rename it for this report.):

DEFINITION 1.1. A *prepolar space* is a set of points P and a collection L of distinguished subsets of P called lines such that

(i) every line contains at least two points,

(ii) for each line L and point $p \in P-L$ either there is exactly one point of L lying on a line with p, or each point of L lies on some line with p.

If P is a prepolar space with the property that every line has cardinality at least 3, and if we let E be the set of collinear pairs of points of P then (P,E) is a graph satisfying the hypothesis of G in theorem A. Note that in the definition of a prepolar space, it is not assumed that different lines have the same cardinality, nor that two points lie in at most one line. This last avenue of generality even makes it appear inappropriate to even have called these blocks "lines". The following theorem shows that in all the interesting cases, we might just as well call them lines. We say a prepolar space is *linear* if every pair of points lies in at most one line.

THEOREM B. (BUEKENHOUT & SHULT [8]). *A prepolar space either contains a point collinear with all other points or is a linear prepolar space.*

In the case that a prepolar space P contains a point collinear with all other points, the space is said to be *degenerate*. If P contains no such point, P is said to be *non-degenerate*.

A *subspace* of a prepolar space (P,L) is a subset of mutually collinear points of P such that any line through two points of the subset lies entirely within the subset. A prepolar space has *rank* n if the greatest lower bound on the length of a tower of subspaces of (P,L) is n+1. (Note that the empty set and the subsets of P containing a single point are subspaces, so, for example, generalized quadrangles are simply prepolar spaces of rank 2.) One next defines a *polar space* S (following TITS' simplification of VELDKAMP's axioms) as a set S of points with a family of distinguished

subsets closed under intersection called *subspaces* (of the polar space S) subject to certain axioms outlined more fully in section 5. One then proves

THEOREM C. (BUEKENHOUT & SHULT [8]). *Let* (P,L) *be a non-degenerate prepolar space of finite rank all of whose lines have cardinality* ≥ 3. *Then* (P,L) *together with its subspaces is a polar space.*

As we shall see shortly, every polar space together with its minimal proper subspaces as its collection of lines, is a prepolar space. We may therefore speak of the rank of a polar space as being its rank as a prepolar space. The next link in the chain is the fundamental theorem of TITS & VELDKAMP [29,32], classifying polar spaces of rank at least three.

THEOREM D. (TITS & VELDKAMP). *Let* S *be a polar space of finite rank* $n \geq 3$. *Then exactly one of the following situations is realized.*

(1) S *is a polar space* $S(\pi)$ *of a projective space with a polarity determined by a trace-valued* σ*-hermitian form.*

(2) S *is a polar space* $S(Q)$ *of a projective space with* Q *a non-degenerate pseudoquadratic form on a division ring* K *of characteristic* 2 *with respect to an antiautomorphism* σ *such that* $\sigma^2 = 1$ *and*

$$\{t \in K \mid t^{\sigma} = t\} \neq \{u + u^{\sigma} \mid u \in K\} .$$

(3) S *is a polar space* $S(\pi)$ *of a Desarguesian projective space coordinitized by a field of characteristic different from* 2, *equipped with a symplectic polarity* π.

(4) S *is a polar space of rank* 3 *whose maximal subspaces are Moufang planes (one polar space for each Cayley division algebra).*

(5) S *is a polar space of rank* 3 *corresponding to a* 3*-dimensional projective space* P *on a non-commutative division ring (*S *corresponds to the classical Klein quadric in the commutative case).*

Most of the technical terms, appearing in the statement of this theorem (for example σ-hermitian and pseudoquadratic) are defined in the next section. In case the polar space contains a finite number of points, cases (4) and (5) of the above theorem do not arise and one is left with a hermitian, symmetric or alternating (symplectic) polarity on a finite projective space, or the totally singular points with respect to a quadratic form on a Desarguesian projective space over a field of characteristic 2. A polar space of rank 2 is precisely a generalized quadrangle and it is now

clear that theorems B, C and D, together, yield theorem A.

The next few sections are devoted to a description of sesquilinear forms, pseudoquadratic forms and their associated polar spaces.

2. SESQUILINEAR FORMS

Let V be a right vector space over a division ring K and let σ be an antiautomorphism of K. Then a *σ-sesquilinear form* is a biadditive mapping $f: V\times V \to K$ such that

$$f(xa,yb) = a^{\sigma} f(x,y)b \tag{2.1}$$

for all $x,y \in V$ and $a,b \in K$. We shall use the term "sesquilinear form" to mean "σ-sesquilinear for some (possibly unspecified) antiautomorphism σ of K". If c is a non-zero scalar in K, the mapping cf defined by $(cf)(x,y) = c\cdot f(x,y)$ is a σ'-sesquilinear form with σ' being the composition of σ with the inner automorphism of K induced by conjugation by c^{-1}. We say cf is *proportional* to f. Obviously proportionality is an equivalence relation on the set of sesquilinear forms.

A σ-sesquilinear form is called *reflexive* if $f(x,y) = 0$ implies $f(y,x) = 0$ for any pair of vectors x,y in V. The first observation is

PROPOSITION 2.1. *A σ-sesquilinear form f is reflexive if and only if there exists a non-zero scalar $\varepsilon \in K$ such that for every pair of vectors $x,y \in V$*

$$f(x,y) = f(y,x)^{\sigma}\cdot\varepsilon \ . \tag{2.2}$$

This is shown by proving that $h(x,y) = f(x,y)^{-1}f(y,x)^{\sigma}$ is a constant function on the subset of $V \times V$ consisting of pairs (u,v) such that $f(u,v) \neq 0$. Clearly if $f(x,v) = 0$, then $h(x,y) = h(x,y+v)$. Similarly if $f(u,y) = 0$, $h(x,y) = h(x+u,y)$. By passing through a chain of translations in each argument in this way, h can be shown to be a constant function on the support of f.

But if f satisfies (2.1), this relation can be iterated to yield the following relations between σ and ε:

$$\varepsilon^{\sigma} = \varepsilon^{-1} \ , \tag{2.3}$$

$$\sigma^2 \text{ is the inner automorphism of K induced by conjugation by } \varepsilon^{-1}. \tag{2.4}$$

A σ-sesquilinear form satisfying (2.2) (and hence (2.3) and (2.4)) is called (σ,ε)-*hermitian*. Several special cases are distinguished: If $\varepsilon = 1$, the form is simply called σ-*hermitian* and if $\varepsilon = -1$, it is called σ-*anti-hermitian*. If $\sigma = 1_K$, σ-hermitian forms are called *symmetric*, and σ-anti-hermitian forms are called *alternating*. Proposition 2.1 states that every reflexive sesquilinear form is a (σ,ε)-hermitian form. Starting with an arbitrary σ-sesquilinear form g we can always construct from it a reflexive form which is (σ,ε)-hermitian (for the same σ) by choosing ε so that (2.3) and (2.4) hold and setting

$$f(x,y) = g(x,y) + g(y,x)^{\sigma}\cdot\varepsilon \ . \tag{2.5}$$

Are all of the reflexive sesquilinear forms obtained by such a semi-symmetrization process? The answer is "no". In case the reflexive (or (σ,ε)-hermitian) form f is obtained from a σ-sesquilinear form g via (2.5) we say that f is *trace-valued*.

PROPOSITION 2.2. *A (σ,ε)-hermitian form* f *is trace-valued if and only if for each vector* $x \in V$, $f(x,x)$ *lies in the subgroup* $\{t + t^{\sigma}\cdot\varepsilon \mid t \in K\}$ *of the additive group of* K.

For certain choices of (σ,ε,K), (σ,ε)-hermitian forms are always trace-valued. Indeed

PROPOSITION 2.3. *Assume σ is an antiautomorphism of a division ring* K *and ε is an element of* K *related to σ by* (2.3) *and* (2.4). *Then a necessary and sufficient condition that* f *be trace-valued is that*

$$\{t + t^{\sigma}\cdot\varepsilon \mid t \in K\} = \{t \in K \mid t^{\sigma}\cdot\varepsilon = t\} \ . \tag{2.6}$$

This condition always holds if char $K \neq 2$, *or if σ acts non-trivially on the center of* K.

If f is a reflexive sesquilinear form, the symmetric relation on V defined by $R_f = \{(x,y) \mid x \in V,\ y \in V,\ f(x,y) = 0\}$ is called the *perpendicular relation* (with respect to f) and we write $x \perp_f y$ or $x \perp y$ if $(x,y) \in R_f$. Then as f is (σ,ε)-hermitian, $x^{\perp} = \{y \in V \mid x \perp y\}$ is a subspace of codimension at most one in V. If X is any subset of V, set $X^{\perp} = \{x \in V \mid f(y,x) = 0,\ \forall y \in X\}$, and write Rad V for $V^{\perp}$. We say f is *non-degenerate* if Rad V = (0). A subspace W of V is called *totally isotropic*

(with respect to f) if $W \leq W^{\perp}$.

PROPOSITION 2.4. *If* X *and* Y *are two maximal totally isotropic subspaces,* $X \cap Y$ *has the same codimension in both* X *and* Y. *Consequently, any two maximal isotropic subspaces of* V (which exist by Zorn's lemma) *have the same dimension,* n.

This invariant cardinal number n is called the *Witt index* of f. To prove the first statement in proposition 2.4 suppose $\dim(Y/X\cap Y) > \dim(X/X\cap Y)$. Then if X_1 and Y_1 are complements of $X\cap Y$ in X and Y respectively, the space $X + (X_1^{\perp} \cap Y_1)$ is a totally isotropic space properly containing X, contrary to the maximality of X.

3. PSEUDOQUADRATIC FORMS

Again let K be a division ring, V a right vector space over K, σ an antiautomorphism of K and ε a non-zero element in K such that (2.3) and (2.4) hold. Following TITS [29], let $K_{\sigma,\varepsilon}$ denote the subgroup of the additive group of K, $\{t - t^{\sigma}\cdot\varepsilon \mid t \in K\}$. Set $K^{(\sigma,\varepsilon)} = K/K_{\sigma,\varepsilon}$, the quotient group.

A function $Q: V \to K^{(\sigma,\varepsilon)}$ is called a (σ,ε)-*quadratic form*, or a *pseudoquadratic form relative to* σ *and* ε if there exists a σ-sesquilinear form $g: V\times V \to K$ such that

$$Q(x) = g(x,x) + K_{\sigma,\varepsilon}, \quad \forall x \in V. \tag{3.1}$$

PROPOSITION 3.1. $Q: V \to K^{(\sigma,\varepsilon)}$ *is a pseudoquadratic form with respect to* σ *and* ε *if and only if there exists a trace-valued* (σ,ε)*-hermitian form* $f: V\times V \to K$ *such that*

$$Q(x + y) = Q(x) + Q(y) + (f(x,y) + K_{\sigma,\varepsilon}), \quad \forall x,y \in V. \tag{3.2}$$

Given Q, the trace-valued form f of (3.2) is uniquely determined. If we write $f = \beta Q$ we may think of β as a map from the set $Q_{\sigma,\varepsilon}$ of all (σ,ε)-quadratic forms into the set $S_{\sigma,\varepsilon}$ of all trace-valued (σ,ε)-hermitian forms.

PROPOSITION 3.2. *The mapping* $\beta: Q_{\sigma,\varepsilon} \to S_{\sigma,\varepsilon}$ *is onto. If* Q *is in* ker β, Q(x) *lies in* $K^{\sigma,\varepsilon}/K_{\sigma,\varepsilon}$ *where* $K^{\sigma,\varepsilon}$ *is the subgroup* $\{t \in K \mid t + t^{\sigma}\cdot\varepsilon = 0\}$. β *is bijective if and only if* (2.6) *holds.*

A subspace X of V is *totally singular* if $Q(X) = 0$ in $K^{(\sigma,\varepsilon)}$. If X is a totally singular subspace for Q, it is clearly isotropic for the (σ,ε)-hermitian form βQ.

PROPOSITION 3.3. *The converse statement, that if* X *is a totally isotropic subspace with respect to* βQ, *then* X *is totally singular with respect to* Q, *is true if* (2.6) *holds.*

It can be shown, by redoing the proof of proposition 2.4, that

PROPOSITION 3.4. *If* X *and* Y *are two maximal totally singular subspaces of* V *then* $\dim(X/X\cap Y) = \dim(Y/X\cap Y)$, *whence* $\dim X = \dim Y$.

This uniform dimension of the maximal totally singular subspaces is called the *Witt index* of the pseudoquadratic form Q.

4. PROJECTIVE SPACES AND POLARITIES

A *projective space* P is a system of points P and a family $\mathcal{L}$ of distinguished subsets called lines such that

1) two points lie on exactly one line,
2) there exist four points, no three of which are collinear,
3) (Pasch's axiom) if L_1 and L_2 are two lines meeting at a point p, and if b and c are two points in $L_1-(p)$ and d and e are two points in $L_2-(p)$, then the line L_3 passing through b and d meets the line L_4 passing through c and e non-trivially.

A *subspace* X of a projective space P is a subset X of points such that every line L in $\mathcal{L}$ either lies in X or meets X in at most one point. Among the subspaces of P can be counted the empty set, called a *subspace of dimension* -1. If the subspace X consists of a single point we say that X is a 0-*dimensional subspace*; if X consists of a single line, X is 1-*dimensional*; and if some line is a maximal subspace of X, then all lines in X meet each other non-trivially, *each* line is a maximal subspace of X and X is called a 2-*dimensional subspace*, or a *projective plane*.

Let V be a right vector space of dimension at least 3 over a division ring K. If we let P denote the collection of 1-dimensional subspaces of V and let $\mathcal{L}$ be the set of 2-dimensional subspaces of V, each such subspace viewed as a collection of 1-dimensional subspaces (i.e. as subsets of P),

then (P,L) is a projective space. Projective spaces constructed in this way are called *Desarguesian*. (Actually, "Desarguesian" is traditionally given an axiomatic definition equivalent to the one given here [31].) One of the most basic theorems of projective spaces is the following:

THEOREM 4.1. *Any projective space properly containing a projective plane as a subspace is Desarguesian.*

Suppose x is a point in the projective space P. Then it is easy to show that subspaces maximal with respect to not containing x (these exist by Zorn's lemma) are in fact maximal subspaces of P. Such subspaces are called *hyperplanes* of P. Let S denote the lattice of all subspaces of P. A mapping $\pi: S \to S$ is called a polarity if π reverses inclusion (that is, $X \leq Y$ implies $Y^\pi \leq X^\pi$) and for each point $x \in P$, x^π is either P or a hyperplane of P. (This definition follows TITS [32, p.128] and generalizes slightly the definition of a polarity given in DEMBOWSKI [10, p.42].) The *rank* of a polarity is the codimension of P^π in P. The polarity π is called *non-degenerate* if $P^\pi = \emptyset$.

If P is a Desarguesian projective space obtained from the right vector space V over a division ring K and f is a (σ,ε)-hermitian form on V, then the perpendicular map $X \to X^\perp$ (the "perpendicular" of X with respect to f) among the subspaces of V induces a polarity $\pi: S \to S$, where S is the set of subspaces of the projective space P. Clearly if f and π correspond in this way, f is non-degenerate if and only if π is. In this case we say that the polarity π is *represented by* f. If f is a trace-valued form we say that π is a polarity of *trace type*.

THEOREM 4.2. *Let* P *be the projective space of a vector space* V. *Every polarity of rank at least* 2 *in* P *is represented by a* (σ,ε)*-hermitian form* f *on* V.

Similarly, a pseudoquadratic form $Q: V \to K^{(\sigma,\varepsilon)}$ defines a perpendicular relation on the vectors of V which also induces a polarity of P. We are now in a position to discuss polar spaces.

5. ABSTRACT POLAR SPACES AND THE THEOREMS OF TITS AND VELDKAMP

The following definition is a simplification (due to TITS) of VELDKAMP's axioms.

DEFINITION 5.1. A *polar space* S is a set of points together with distinguished subsets called *subspaces* such that

(i) a subspace together with the subspaces it contains is a d-dimensional projective space with $-1 < d < n-1$ for some integer n called the *rank* of S;

(ii) given a subspace L of dimension n-1 and a point $p \in S-L$, there exists a unique subspace M containing p such that $\dim(M \cap L) = n-2$; it contains all points of L which lie together with p in some subspace of dimension one;

(iii) the intersection of any two subspaces is a subspace;

(iv) there exist disjoint subspaces of dimension n-1.

Let π be a polarity on a projective space P. Assume P is Desarguesian and π is represented by the trace-valued non-degenerate (σ,ε)-hermitian form f. Let $S(\pi)$ be the set of absolute points of P, so $S(\pi) = \{p \in P \mid p \in p^{\pi}\}$. Then calling the totally isotropic subspaces X of P (that is, those subspaces X such that $X < X$) "subspaces of $S(\pi)$", $S(\pi)$ becomes a polar space.

Similarly, let P be the projective space of a vector space V and let Q be a pseudoquadratic form on P. A singular point of P is a point corresponding to a 1-dimensional subspace of V whose vectors vanish under Q. Let S(Q) be the set of singular points of P and let the subspaces of S(Q) be those subspaces of P lying in S(Q). Then S(Q) becomes a polar space.

A complete proof of theorem D can be obtained from TITS' book [29]. The proof generally seems to proceed in two basic stages (though off in the margin there are exceptional cases for each stage): first one studies what occurs if the polar space can be embedded in a projective space (one reaches a virtual classification here); and second, one proves (with a few exceptions) that almost all polar spaces are embeddable. By an *embedding* of a polar space S into a projective space P we mean a triple (P,π,ϕ) where π is a polarity of P, ϕ is an injection of S into the set $S(\pi)$ of absolute points of P such that

(a) $\phi(S)$ spans P,

(b) for every subspace X of S, $\phi(X)$ is a subspace of P totally isotropic with respect to π.

It then turns out that when an embedding is possible the structure of $S(\pi)$ completely controls the structure of $\phi(S)$ (and hence S). This is because (assuming lines in S contain at least three points) if x and y are not collinear in S but $\phi(x)$ and $\phi(y)$ are perpendicular with respect to

π in P, then $\phi(x)$ is perpendicular to all of $\phi(S)$. As $\phi(S)$ spans P this places $\phi(x)$ in the radical, P^{π}. The classification begins with

THEOREM 5.1. (Part of Theorem 8.6 of TITS [29]). *Let* (P,π,ϕ) *be a projective embedding of a polar space* S *of rank* ≥ 2 *where* π *is represented by a* (σ,ε)*-hermitian form.*

(i) *If* σ *and* ε *satisfy condition* (2.6) (of proposition 2.3 above), π *is non-degenerate and* $\phi(S) = S(\pi)$.

(ii) *Suppose* σ *and* ε *do not satisfy* (2.6). *Then there exists an embedding* $(\overline{P},\overline{\pi},\overline{\phi})$ *of* S, *a morphism* $\mu\colon \overline{P} \to P$ *(as projective spaces) such that* $\overline{\phi}\cdot\mu = \phi$ *and* μ *and* $\overline{\pi}$ *induce* π *on* P, *and a pseudoquadratic form* $\overline{Q}$ *such that* $\overline{\pi} = \beta\overline{Q}$ (the "sesquilinearization" of Q) *and* $\overline{\phi}(S) = S(\overline{Q})$. *The morphism* μ *is unique up to isomorphism.*

Most of the rest of the proof emerges from

THEOREM 5.2. (Due originally to VELDKAMP). *A thick polar space of rank* ≥ 3 *whose maximal subspaces are Desarguesian is embeddable (that is, a* (P,π,ϕ) *exists).*

This gives only a vague idea, to be sure, but the full development will appear in TITS' monumental work [29].

We next describe the other links in the characterization theorem, those showing that non-degenerate prepolar spaces are polar spaces.

6. NON-DEGENERATE PREPOLAR SPACES ARE LINEAR

Let S be a prepolar space. If two points x and y lie together on at least one line of S we say that they are *collinear*. We may thus also regard S as a graph (undirected, without loops) with respect to the relation of being collinear. We write A(x) for the set of all points of S distinct from x but collinear with x, that is, the vertices adjacent to x in the graph. We define the radical of S by

$$\text{(6.1)} \qquad \mathrm{Rad}(S) = \{x \in S \mid \{x\} \cup A(x) = S\} ,$$

simply the set of points collinear with all remaining points. Recall that S is *non-degenerate* if and only if Rad(S) is empty.

We begin with a degeneracy criterion:

PROPOSITION 6.1. *Let* S *be a prepolar space and* L *a line of* S *and* b *some point of* L *such that* S = union A(u), *where* u *ranges over* L - {b}. *Then* Rad(S) *is non-empty.*

PROOF. If L has only 2 points, the result is obvious from the hypothesis on L. So we assume L has at least three points. Let Δ be the intersection of the A(u)'s as u ranges over L - {b}, and set $X_u = \{w \in S \mid A(w) \cap L = \{u\}\}$. Since S is a prepolar space this produces a partition of the points of S as

$$S = (L - \{b\}) + \Delta + \sum_u X_u \quad , \tag{6.2}$$

where, in the last sum, u ranges over L - {b}.

Suppose an element $x \in X_u$ was adjacent to an element $y \in X_v$, where $u \neq v$. Then there exists a line M of S containing x and y. Then M meets Δ trivially since if $z \in M \cap \Delta$, then z is adjacent to u, so u, being adjacent to the two points z and x on M, is adjacent to y, contrary to the assumption that $y \in X_v$, $v \neq u$. By the basic property of a prepolar space, since b is not adjacent to x or y, b is adjacent to a unique point m on M. This point m does not lie in any X_w, $w \in L-\{b\}$. We have just seen that m cannot lie in Δ. So by (6.2) m lies in L - {b}. From the symmetry of u and v in the supposition at the beginning of this paragraph we may assume $m \neq u$. But then u is adjacent to the two points x and m on M and so is adjacent to y, contrary to the assumption that $y \in X_v$, once more. Thus the supposition at the beginning of this paragraph is false and so we may assume henceforward that if $u \neq v$, no element of X_u is adjacent to an element of X_v.

If all of the X_u's were empty then every point of L would lie in the radical of S. If exactly one of the X_u's, say X_v, were non-empty, then v would be an element of L - {b} lying in the radical of S. Thus we may assume that at least two of the X_u's, say X_u and X_v, are non-empty. Select $x \in X_u$, $y \in X_v$ and let M be a line passing through x and y. Then $x \in X_u \cap M$ implies $M \cap L = \{u\}$ and $M-\{u\} \subseteq X_u$. Since y is not adjacent to any member of X_u, by the previous paragraph, the basic axiom for prepolar spaces implies y is adjacent to u. Again, this contradicts $y \in X_v$, proving proposition 6.1. □

Notice that the assumption of proposition 6.1 differs only very slightly from the state of affairs forced by the axioms of a prepolar space, for always, if L is a line, the sets A(u) as u ranges over L, cover S. A glance at the points in the above proof at which Rad(S) is deduced to be non-empty shows that without loss of generality the conclusion of proposition 6.1

could have been sharpened to read "Rad(S) ∩ (L-{b}) is non-empty".

PROPOSITION 6.2. *Let* S *be a prepolar space and let* a,b *be two non-adjacent points of* S. *Then* $A^*(a) = A(a) \cup \{a\}$ *and* $A(a,b) = A(a) \cap A(b)$ *(equipped with those lines of* S *lying entirely inside these sets) are also prepolar spaces. Also*

$$Rad(A(a,b)) \subseteq Rad(A^*(a)).$$

PROOF. The first statement is easily verified. If z is a point in Rad(A(a,b)), and y is any point of A(a) distinct from z, either y lies in A(a,b), z lies on some line through a and y, or b is not adjacent to y and some line M through a and b does not contain z. In the first two cases z is adjacent to y, patently. In the third case, there is a unique point m in $M \cap A(b)$ and since z is adjacent to both m and a (both z and m differ from a since a does not lie in A(a,b)), z is adjacent to all members of M, in particular, to y. Thus in all cases z is adjacent to y and so, from the general choice of y, we have $z \in Rad(A^*(a))$. □

In general if a is not adjacent to b we write A(a,b) for $A(a) \cap A(b)$.

PROPOSITION 6.3. *If* S *is a prepolar space and* a *and* b *are non-adjacent points of* S, *then*

$$Rad(A(a,b)) \subseteq Rad(S) .$$

PROOF. Assume $z \in Rad(A(a,b))$. By proposition 6.2, z is adjacent to every member of $A(a)-\{z\}$. It remains therefore only to show that z is adjacent to any point w which is not adjacent to a. Since $z \in A(a)$, there is at least one line L through z and a and, moreover, w is adjacent to a unique point u on L. If u = z, z is adjacent to w. Suppose $u \neq z$. Then b is not adjacent to u (since it is adjacent to z) and so $z \in A(u,b) \subseteq A^*(b)$ and $z \in Rad(A(a,b)) \subseteq$ $\subseteq Rad(A^*(b))$ (by (6.2)) imply

$$z \in Rad(A(u,b)).$$

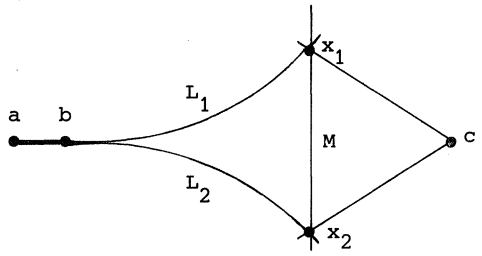
But then by proposition 6.2 once more,

$$z \in Rad(A^*(u)).$$

Since w is an element of $A(u) - \{z\}$, this makes z adjacent to w also. Thus $z \in Rad(S)$. □

PROPOSITION 6.4. *A non-degenerate prepolar space is linear.*

PROOF. Let S be a non-degenerate prepolar space and suppose by way of contradiction that S is not linear. Then there exist two distinct lines L_1 and L_2 such that $L_1 \cap L_2$ contains two points a and b. Since $L_1 \neq L_2$, at least one of the L_i's properly contains $L_1 \cap L_2$ and so if S were the union of the A(u)'s, u ranging over $L_1 \cap L_2$, then by proposition 6.1 Rad(S) would be non-empty, contrary to the assumption that S is non-degenerate. Thus we may assume that there exists a point c not adjacent to any member of $L_1 \cap L_2$. Then c is adjacent to a unique point x_i on $L_i - (L_1 \cap L_2)$, i=1,2. Since $L_1 \cap L_2$ contains two points adjacent to both x_1 and x_2, x_1 and x_2 are adjacent and so lie on some line M. Since c is adjacent to two members of M, c is adjacent to every member of M; thus $M \subseteq A(a,c) \cap A(b,c)$. We now have the configuration:



Choose u in A(a,c). We claim that either (i) u is adjacent to some member of $M - \{x_1\}$, or else (ii) $u = x_2$ and $M = \{x_1, x_2\}$.

If u is not adjacent to x_1 the claim is true.

If $u = x_2$, u is adjacent to some member of $M - \{x_1, x_2\}$ or else $M - \{x_1, x_2\}$ is empty. In either case the claim above is true.

Otherwise we may assume u to be distinct from x_1 and adjacent to both a and x_1. Then u is adjacent to all members of L_1, hence to at least two members of $L_1 \cap L_2$ and hence adjacent to all members of L_2, including x_2 on $M - \{x_1\}$. Thus in all cases the claim is justified.

If $M = \{x_1, x_2\}$ then by the claim x_2 is adjacent to every member of $A(a,c) - \{x_2\}$ so Rad(A(a,c)) contains x_1. Otherwise M contains three points, and the claim asserts that M is a line in the prepolar space A(a,c) and every point of A(a,c) is adjacent to some member of $M - \{x_1\}$. This is precisely the hypothesis of proposition 6.1 and so we may conclude again, that

Rad(A(a,c)) is non-empty. Thus in either case Rad(A(a,c)) is non-empty and so by proposition 6.3, Rad(S) is non-empty, contrary to the assumption that S is non-degenerate. □

REMARK. If one wished to investigate the relation of non-linearity of S with Rad(S) in more detail, one may use the observation following the proof of proposition 6.1. One can then see that M, in the above proof lies entirely inside Rad(S).

7. HOW THEOREM C WORKS

Throughout this section let S be a non-degenerate prepolar space.

PROPOSITION 7.1. *Choose a point* a $\in$ S *and assume* b *and* c *are two points in* S - A^*(a). *Then* A(a,b) *and* A(a,c) *are isomorphic prepolar spaces.*

PROOF. For each $x \in A(a,b)$ let M_x be the unique (by proposition 6.4) line through x and a. Since c is not adjacent to a, $A(c) \cap M_x = \{x'\}$. We claim the mapping $x \to x'$ induces an isomorphism as prepolar spaces $A(a,b) \to A(a,c)$. By proposition 6.4, the "lines" of a non-degenerate prepolar space are the unique graph-theoretic cliques containing an edge and having the "one-or-all" adjacency property with points outside the cliques. Thus, since S is non-degenerate implies both A(a,b) and A(a,c) non-degenerate by proposition 6.3, it suffices merely to show that the mapping $x \to x'$ is a bijection preserving the relation of collinearity. It is easily seen that if the roles of b and c are reversed in the definition of x', the inverse mapping $x' \to x$ is produced. So bijectivity is obvious. Suppose x is adjacent to y in A(a,b). Then every point on M_x is adjacent to every on M_y - {a} and so x' is adjacent to y', completing the proof. □

PROPOSITION 7.2. *Assume the lines of* S *contain at least three points. If* a,b,c,d *are points of* S *such that* (a,b) *and* (c,d) *are non-adjacent pairs, then* A(a,b) *and* A(c,d) *are isomorphic prepolar spaces.*

If a is not adjacent to c, we have from proposition 7.1,

$$A(a,b) \simeq A(a,c) = A(c,a) \simeq A(c,d) .$$

Otherwise, there is a line L through a and c containing at least three points

and so, by proposition 6.1, there is a point f not in $A(a) \cup A(c)$. Then

$$A(a,b) \simeq A(a,f) \simeq A(c,f) \simeq A(c,d) \ ,$$

each isomorphism arising from an application of proposition 7.1.

One can see at this point that proposition 7.2 imposes a far-reaching uniformity across S. It is then not difficult to show

PROPOSITION 7.3. *If the lines of* S *contain at least three points, and* S *has finite rank* $n \geq 2$, *then*

(i) $A(a,b)$ *is a non-degenerate prepolar space of rank* $n-1$, *and*

(ii) *every maximal unrefinable tower of subspaces of* S *(beginning with the empty set) has the same length,* $n+1$.

One then proves

PROPOSITION 7.4. *If the lines of* S *contain at least three points and* S *has finite rank, then* S *contains two maximal subspaces which are disjoint.*

Actually something stronger than this can be proved without using proposition 7.3 and the assumption that all lines contain at least three points (see Proposition 8 of [8]).

Because of proposition 7.4, in proving that a non-degenerate prepolar space whose lines contain at least three elements is a polar space, it remains only to show that a maximal subspace M of S, together with the lines contained in it, form a projective space. We are assuming here that S has rank at least three. Then M contains a line as a proper subspace (proposition 7.3).

If rank S = 3, each line in M is a maximal subspace of M and in that case it is not too difficult to show that any two lines of M meet non-trivially. Since S is linear, this means any two lines in M meet at a unique point, so M with its lines is a (not necessarily Desarguesian) projective space, and so S is a polar space.

If rank S > 3, it suffices to show that Pasch's axiom holds for the lines in M. But if $L_1 \cap L_2 = \{p\}$ for two lines in M, it can be shown that a non-adjacent pair of points b and c exist such that L_1 and L_2 are two lines lying in a subspace of the prepolar space $A(b,c)$. Since $A(b,c)$ is a non-degenerate prepolar space of rank ≥ 3 (by propositions 6.4 and 7.3), induction on the rank shows that $M \cap A(b,c)$ with its lines is a projective space.

Since all lines of M connecting points in $L_1 \cup L_2$ lie in $M \cap A(b,c)$, Pasch's axiom holds for L_1 and L_2. From the general choice of L_1 and L_2, it follows that M is a projective space.

8. THE CASE OF THE GENERALIZED QUADRANGLES

The notion of a generalized quadrangle was first introduced by TITS [30], and precisely corresponds with the notion of a non-degenerate prepolar space of rank 2. Thus a generalized quadrangle is a non-empty collection $\mathcal{L}$ of subsets of a set P such that $p \in P$, $L \in \mathcal{L}$ and $p \notin L$ imply the existence of a unique point f(p,L) on L such that $\{p, f(p,L)\}$ is covered by a member of $\mathcal{L}$, and any two members of $\mathcal{L}$ meet in at most one point, at least two of them being disjoint. We call the members of $\mathcal{L}$ lines, just as we have for all prepolar spaces. Note that f is a mapping from the set of non-incident pairs of $P \times \mathcal{L}$ into P and observe that f is a surjection.

THEOREM 8.1. (BENSON [3]). *Let* $(P,\mathcal{L})$ *be a generalized quadrangle with* P *finite. Assume*

(i) *each point of P lies on at least three lines, and*

(ii) *each line of* $\mathcal{L}$ *contains at least three points.*

Then there exist integers s *and* t *such that every point lies on* 1+t *lines and each line contains* 1+s *points.*

If (ii) fails, each line has 2 points, so (i) alone implies each line contains the same number of points. Similarly (ii) alone implies each point lies on the same number of lines. That (i) or (ii) may fail independently is shown by the examples in figure 8.1. The reader may verify for himself that if (i) or (ii) fails the quadrangle is either a "grid" as in figure 8.1(a) or the line-graph of a "grid", as in figure 8.1(b). If both (i) and (ii) fail, $(P,\mathcal{L})$ is an ordinary quadrangle. We may therefore

(a) (b)

Figure 8.1. Generalized quadrangles in which hypothesis (i) or (ii) fails

assume for the remainder of this section that both (i) and (ii) hold, and (since this is the case of most relevance to finite groups and the casting of theorem A) that P is a finite set. Then the integers s and t of BENSON's theorem are defined. In that case, we shall say $(P,\mathcal{L})$ is a generalized quadrangle of *order* (s,t).

It is easy to see that if $(P,\mathcal{L})$ is a generalized quadrangle of order (s,t) and if we interchange the nomenclature of "point" and "line", we obtain a generalized quadrangle $(P',\mathcal{L}')$ (with $P' = \mathcal{L}, \mathcal{L}' = P$ and incidence matrix the transpose of that for $(P,\mathcal{L})$) of order (t,s) which we call the *dual* of $(P,\mathcal{L})$.

Before going further, I would like to recommend to the reader the beautiful and timely surveys on generalized quadrangles by J.A. THAS [28] and by STANLEY PAYNE [16]. (As far as I know, PAYNE's notes are of more recent vintage and exist so far only in the form of mimeographed notes. It would be nice to see them published soon.)

The generalized quadrangles found among the polar spaces $S(\pi)$ and $S(Q)$ are as follows:

I. $S(\pi)$ when π is the polarity on projective 3-dimensional space obtained from a non-degenerate alternating form. (This quadrangle is associated with the groups $Sp(4,q)$ and has order (q,q).)

II. $S(Q)$ where Q is a non-degenerate quadratic form and P is projective 4-dimensional space. (This quadrangle is associated with the groups $O(5,q)$ and has order (q,q).)

III. $S(Q)$ where Q is a non-degenerate quadratic form of Witt index 2 and P is 5-dimensional projective space. (This quadrangle is associated with the groups $O^+(6,q)$ and has order (q,q^2).)

IV. $S(\pi)$ where π is the polarity on projective 3-dimensional space obtained from a σ-hermitian form over $GF(q^2)$ with σ the field automorphism of order 2. (This quadrangle is associated with the groups $U(4,q^2)$ and has order (q^2,q).)

V. $S(\pi)$ where π is the polarity on projective 4-dimensional space obtained from a σ-hermitian form over $GF(q^2)$ with σ the field automorphism of order 2. (This quadrangle is associated with the groups $U(5,q^2)$ and has order (q^2,q^3).)

Still other generalized quadrangles exist. TITS has constructed quadrangles of orders (q,q) and (q,q^2) which are generalizations of quadrangles of types II and III above. There are also generalized quadrangles of order

(q-1,q+1) when q is a primepower. A special subclass of these, when q is even, was first given by AHRENS & SZEKERES [1] and independently by HALL [13]. It is a theorem of BENSON [4] that types I and II are dual to each other. In addition, types III and IV are also dual to each other. When Q is a non-degenerate quadratic form of Witt index 2 on a 4-dimensional vector space V, the associated totally singular point set S(Q) in $P \simeq PG(3,q)$ is a generalized quadrangle of type (q,1), that is (i) of theorem 8.1 does not hold here.

Now in using theorem A in the context of finite groups, one may frequently assume that the generalized quadrangles which may appear possess a fairly rich group of automorphisms. One then desires a theorem which may be used to characterize the generalized quadrangles. There are a number of theorems allowing one to characterize the quadrangles I through V listed above. Here is a sample:

THEOREM 8.2. (SINGLETON [20], BENSON [4]). *Suppose* (P,L) *is a finite generalized quadrangle such that for every non-collinear pair* x,y *of* P, *any point collinear with two of the set of points collinear with both* x *and* y *is in fact collinear with all* 1+t *points which are collinear with both* x *and* y. *Then* (P,L) *is a generalized quadrangle of type* I.

Dualization of this result yields a characterization of quadrangles of type II. Similarly TALLINI [25] and THAS [28a] have given a characterization of type III which dualizes to a characterization of type IV. There presently seems to be no known characterization of the quadrangles of type V on the basis of intrinsic local geometric properties.

However there is a recent marvelous theorem of BUEKENHOUT & LEFEVRE [7] that may prove useful in obtaining characterizations.

THEOREM 8.3. (BUEKENHOUT & LEFEVRE). *If the quadrangle* (P,L) *is finite and is embeddable in a projective space, then* $(P,L) \simeq S(\pi)$ *or* S(Q) *as polar spaces -i.e.* (P,L) *is one of the types* I-V *or has order* (q,1).

Finally, a recent theorem of TITS (in BUEKENHOUT [5, p.30]) shows that if a generalized quadrangle is exceedingly rich in automorphisms, then it is a quadrangle of "classical" type:

THEOREM 8.4. (TITS). *Let* (P,L) *be a finite generalized quadrangle, and assume the following two properties:*

(i) *If* A *and* B *are two lines through a point* p *and if* b *is any point on* B *distinct from* p, *then the subgroup of* Aut(P,L) *fixing* A *and* B *pointwise and stabilizing all lines through* p, *transitively permutes the lines passing through* $b \in B$ *which are distinct from* B.

(ii) *If* a *and* b *are two points lying on a line* L *and* M *is a line through* b *distinct from* L, *then the subgroup of* Aut(P,L) *fixing* L *pointwise and simultaneously stabilizing all lines through* a *and* b *is transitive on the points of* $M - \{b\}$.

Then either (P,L) *or its dual is an* $S(\pi)$ *or an* S(Q).

Note that conditions (i) and (ii) of this theorem are dual to one another.

THEOREM 8.5. *Let* (P,L) *be a generalized quadrangle of order* (s,t). *Then*

(i) $|P| = (1+s)(1+st)$;

(ii) $|L| = (1+t)(1+st)$;

(iii) *each point is collinear with* s+st *points, and fails to be collinear with* s^2t *points.*

A point x and all the points collinear with it is denoted St(x) and is called the *star at* x (in the prepolar space terminology of section 6, this is just $A^*(x)$). We denote by C(St(x)), the subgroup of those automorphisms of (P,L) which leave St(x) fixed pointwise. We next observe

PROPOSITION 8.1. C(St(x)) *acts semiregularly on the set of points* P - St(x).

The following seems approachable,

CONJECTURE 8.1. *Assume* (P,L) *is a finite generalized quadrangle of order* (s,t), *and, for each* $x \in P$, C(St(x)) *has even order. Then* (P,L) *is type* I, IV *or* V, *with* q *a power of* 2.

Assume the hypothesis of the above conjecture, set G = Aut(P,L), let G_x be the subgroup of G fixing the point x, and write C(x) for C(St(x)). Then the following is easily proved:

(i) G is transitive on unordered pairs of collinear points. In particular G_x is transitive on St(x) - {x} and the stabilizer in G of a line is doubly transitive on the points in the line.

(ii) $G_x = N_G(C(x))$. C(x) is a 2-group, and is a trivial intersection group, that is it meets its G-conjugates which are distinct from itself trivially.

(iii) t is a power of 2, G_x induces a doubly transitive group (H,L_x) on the set of lines passing through x and (H,L_x) contains a normal subgroup (H_0,L_x) which is SL(2,q), Sz(q) or $U(3,q^2)$ acting in its natural representation on $1+t = 1+q$, $1+q^2$, or $1+q^3$ letters, respectively.

(iv) If x and y are non-collinear points, there is a set C(x,y) of 1+w mutually non-collinear points containing x and y with the property that $A(u)\cap A(v) = A(x)\cap A(y)$ for all $u,v \in C(x,y)$. (Here, A(x) is the set of points collinear with x.) The system $L^* = \{C(u,v) \mid (u,v)$ a non-collinear pair in P$\}$ becomes in this way, a second system of lines for P, so that every pair of points in P either lies in a unique line from L or a unique line from L^* but not both. The two line sets are connected by the following interesting property: if $L \in L^*$ and $u \in P$ and u is L-collinear with two points of L, then u is L-collinear with every point of L.

(v) If x and y are not collinear, the subgroup $\langle C(x),C(y)\rangle$ stabilizes C(x,y) and induces on C(x,y) one of the permutation groups SL(2,q), Sz(q) or $U(3,q^2)$ acting doubly transitively on the 1+w points, with $w = q$, q^2 or q^3, respectively. If $w \neq t$ then SL(2,q) is obtained, $t = q^3$ and the subgroup H_0 of (iii) is $U(3,q^3)$.

It may be that the more general assumption that C(St(x)) contains an element of prime order p for each x in P, would also imply that (P,L) is type I, IV or V. In any event if the above conjecture could at least be proved, it would be useful in many instances of determining the 2-Sylow order of $G = Aut(P,L)$. For example, if we assume that $H = G_x$ and $K = Stab(L)$, where L is a line containing x, then $H\cap K$ is the stabilizer of the flag (x,L) and G is an amalgam of H and K. A very pleasant pastime is this: One selects two transitive permutation groups whose one-point stabilizers are either isomorphic, or for which there is a subdirect product of each, which is not direct. These are the candidates for (H,L_x) and (K,L). If H is doubly primitive on the lines through x, then $K_0 = \ker[K \to Sym(L)]$ must coincide with C(St(x)). Similarly, if K is doubly primitive on the points in L, $H_0 = \ker[H \to Sym(L_x)]$ (where L_x is the set of lines through x) must also coincide with C(St(x)). The point is that if (s,t) is chosen so as not to coincide with cases I through V, the conjecture says C(St(x)) must have odd order and this means a 2-Sylow order of G is determined. Choices of H, $H\cap K$ and K giving low values of s and t are easily constructed; samples are:

	H	H∩K	K	(s,t)	|P|	|G|
1a.	E(16)Alt(5)	Alt(5)	Alt(6)	(5,15)	456	$2^9 3^2 5 \cdot 19 \cdot \|C\|$
1b.	E(16)Sym(5)	Sym(5)	Sym(6)	(5,15)	456	2 times case 1a
1c.	E(16)D_{10}	D_{10}	PSL(2,5)	(5,15)	456	$2^8 3 \cdot 5 \cdot 19 \cdot \|C\|$
2a.	Alt(6)	D_{10}	PSL(2,5)	(5,35)	1056	$2^8 3^2 5 \cdot 11 \cdot \|C\|$
2b.	Sym(6)	$Z_5 Z_4$	PGL(2,5)	(5,35)	1056	2 times case 2a
3.	E(16)Sym(6)	Sym(6)	Sym(7)	(6,15)	567	$2^8 3^2 5 \cdot 7^2 13 \cdot \|C\|$
4.	Alt(8)	E(8)L(3,2)	E(8^2)L(3,2)	(7,14)	1485	$2^9 3^4 5 \cdot 7 \cdot 11 \cdot \|C\|$
5.	U(3,3^2)	L(3,2)	E(8)L(3,2)	(7,35)	1944	$2^9 3^4 5 \cdot 7 \cdot 41 \cdot \|C\|$
6.	E(16)Alt(6)	Alt(6)	Sym(7)	(13,15)	2744	$2^{10} 3^2 5 \cdot 7^3 \cdot \|C\|$
7.	Alt(8)	Sym(6)	E(16)Sym(6)	(15,27)	6496	$2^{11} 3^2 5 \cdot 7^2 11 \cdot \|C\|$

... and so on. If the conjecture is true, $|C| = |C(St(x))|$ is odd and the 2-Sylow order of G is known. In addition, part of the 2-fusion pattern is already prescribed in the two subgroups H and K, so one is presumably on his way to determining G.

9. VARIATIONS ON A THEME; OPEN QUESTIONS

A few open questions remain concerning prepolar spaces.

(1) *What is the exact relation between lines which meet at two or more points* (we call these "neighbor lines") *and the radical of* (P,L)*?*

One may consider the equivalence relation R defined on P by xRy if and only if $A^*(x) = A^*(y)$. Then one can show that $A^*(x) \subseteq A^*(y)$ implies either xRy or $y \in \mathrm{Rad}(P)$. From this it follows that on the set $\bar{P}$ of equivalence classes under R, the structure of a prepolar space $\bar{L}$ can unambiguously be defined from L. The theorem is that $(\bar{P},\bar{L})$ is non-degenerate [8, Proposition 14]. Then from proposition 6.4, $(\bar{P},\bar{L})$ is linear. This means that if two lines L_1 and L_2 meet at two points, then at least one of the two points lies in Rad(P). From this one sees that lines meeting at three points must lie in Rad(P). Do lines meeting at exactly two points necessarily lie in Rad(P) also?

(2) *Can the structure of non-degenerate prepolar spaces containing lines of cardinality* 2 *be described?*

It is clear that if (P,L) is such a prepolar space then it contains many lines of cardinality 2. To see this, let $L = \{a,b\}$ be a line containing just two points. Then we have a decomposition $P = L+\Delta+X_a+X_b$ into disjoint sets, where $\Delta = A(a)\cap A(b)$, $X_a = A(a)-\Delta$, $X_b = A(b)-\Delta$. From non-degeneracy, both X_a and X_b are non-empty. Then the lines through point a either lie entirely inside $X_a \cup \{a\}$, or $\Delta \cup \{a\}$. Let M be a line through a lying in $X_a \cup \{a\}$. Then any point p in X_b is collinear with some point p' in M. Then if N is a line containing p and p' we see that $N\cap X_a = \{p'\}$, $N\cap X_b = \{p\}$ and $N \cap (\Delta\cup\{a,b\})$ is empty. Thus $N = \{p,p'\}$. There are thus $|X_b|$ such lines meeting M.

(3) *All of the graphs of theorem* A *corresponding to prepolar spaces of rank at least three involve structures associated with the groups* $Sp(2n,q)$, $O(2n+1,q)$, $O^{\varepsilon}(2n,q)$, $\varepsilon=\pm1$, *and* $U(n,q^2)$. *These are the non-abelian simple sections of the finite Chevalley groups of types* B_n, C_n, D_n *and the twisted types* ${}^2D_n$ *and* ${}^2A_n$. *Does there exist a similar simple (and local) graph-theoretic hypothesis which could be used to characterize structures associated with other Chevalley and Steinberg groups?*

Those which come to mind are the groups of types A_n (the PSL(n,q)'s), ${}^3D_4$, G_2, F_4, E_6, E_7, E_8. Presumably ${}^2F_4$, ${}^2G_2$, ${}^2B_2$ are of such low rank as to be below the level of such a theorem. What does one use as a replacement for $S(\pi)$ or $S(Q)$ in these cases? One suspects that in the case of PSL(n,q) one would use the line-graph of PG(n-1,q), suggesting a hypothesis of the form:

HYPOTHESIS H. *If* (x,y) *is an edge in the graph* G, *there exists a clique* $C(x,y)$ *containing* $1+q+q^2$ *vertices such that every vertex* $z \in G-C(x,y)$ *is adjacent to* 0 *or* $1+q$ *members of* $C(x,y)$. *The sets* $A(z) \cap C(x,y)$ *which are non-empty as* z *ranges over* $G - C(x,y)$ *define a projective plane on* $C(x,y)$.

Possibly one can weaken hypothesis H. If q = 1, the socalled "triangular graphs" also have this property. But these correspond to the symmetric groups which may be thought of as what would be groups of type A_n if there were such a thing as a field containing one element.

Some work has already begun [6] on prepolar-like spaces that might be characteristic for the Chevalley groups of type E_6.

This point of view suggests still another question.

(4) *Is there an analogue of theorem* A *that could be used to characterize the graph of non-singular points in a projective space with a non-degenerate unitary polarity or the graph of non-singular points with square (or non-square) values under a non-degenerate quadratic form* Q*?*

That such a theorem may be possible is indicated by the following result:

THEOREM 9.1. *Let* G *be a finite graph satisfying the following hypothesis:*

(9.1) *(Cotriangle property) Given any non-adjacent pair of vertices* x *and* y*, there exists at least one third vertex* z *not adjacent to either* x *or* y*, such that any vertex in* $G - \{x,y,z\}$ *is adjacent to one or three members of* $\{x,y,z\}$.

Then the graphs G *are determined up to isomorphism.*

The graphs include the graphs $N(2n,2)$ of non-singular vectors with respect to a non-degenerate quadratic form in 2n-variables over GF(2).

Suppose G is a graph with the cotriangle property (9.1) and $G = X_1 + X_2 + \ldots + X_m$ is a partition of the vertices of G with each X_i non-empty and if $i \neq j$, every vertex of X_i being adjacent to every vertex of X_j. Then as subgraphs, each X_i has the cotriangle property. Clearly G is determined up to isomorphism by the isomorphism types of the X_i. We say G is *indecomposable* if no non-trivial partition of this type exists.

THEOREM 9.2. *If* G *has property* (9.1)*, the following are equivalent:*

(i) $A(x) \cup \{x\} = A(y) \cup \{y\}$ *implies* $x = y$*, for all* $x,y \in G$.

(ii) *The vertex* z *of* (9.1) *is uniquely determined by* x *and* y.

The relation $A(x) \cup \{x\} = A(y) \cup \{y\}$ is clearly an equivalence relation on the vertices of G and if $\bar{G} = \{C_j\}$ is the family of equivalence classes of G with respect to this relation, and $i \neq j$, then either

(a) every vertex of C_i is adjacent to every vertex of C_j, or

(b) no vertex of C_i is adjacent to any vertex of C_j.

We can then make a graph on $\bar{G}$ by the relation (a). Then if G is indecomposable, so is $\bar{G}$. If G has the cotriangle property, so does $\bar{G}$, except now property (b) also holds. Finally G is determined up to isomorphism by the isomorphism type of $\bar{G}$ and the assignment of cardinalities $|C_i|$ to the vertices i of G.

Thus in proving theorem 9.1 we need only show

THEOREM 9.3. *If G is a finite indecomposable graph with the cotriangle property* (9.1) *for which* (b) *of theorem* 9.2 *holds, then either*

(i) $G \simeq N(2n,2)$,

(ii) $G \simeq Sp(2n,2)$,

(iii) $G \simeq T^*(n)$,

where $N(2n,2)$ is the graph of non-singular vectors with respect to a non-degenerate quadratic form in 2n *variables over* GF(2), *$Sp(2n,2)$ is the graph of non-zero vectors under the perpendicular relation of a non-degenerate symplectic form over* GF(2), *and $T^*(n)$ is the complement of the triangular graph on* n *letters.*

The proof is merely a modification of a theorem of J.J. SEIDEL [17]. Because of property (b) we may write $z = x+y$ unambiguously in the statement of the cotriangle property. (In SEIDEL's situation, the graph is already embedded in a symplectic space with "+" being ordinary vector addition, hence associative in his proof; also case (ii) is not possible in his situation.) SEIDEL's inspiration was in noticing that if X_a is the subgraph of vertices adjacent only to a in a cotriangle $\{a,b,c = a+b\}$, then X_a has the *triangle property* (that is, the hypothesis of theorem A with the $C(x,y)$'s all having just 3 points). The structure of $\Delta = A(a) \cap A(b) \cap A(c)$ is a little more difficult to see, but is determined up to isomorphism by X_a.

10. SOME GROUP-THEORETIC BACKGROUND AND SOME APPLICATIONS

Historically speaking theorem A is the coming together of two independent lines of development: on the one side, the development of the theory of polar spaces beginning with VELDKAMP's important work [32]; on the other side, the need to characterize graphs which arose in certain group-theoretic problems, eventually reaching the prepolar spaces. The comments in this section are confined to the group-theoretic side of the picture.

In one sense the dim beginnings are noticeable in the graph extension theorem. A well-known problem that arises in the theory of permutation groups is that of constructing a transitive extension. By saying that (G,X) is a permutation group, we mean that we have an injection $f: G \to Sym(X)$. If x and y are two elements of X, the ability to reach y from x *via* a permutation in $f(G)$ is an equivalence relation on X, the equivalence classes being called G-*orbits*. We say G is *transitive* on X if G acts in one orbit on X.

Always, if Y is a subset of X, the permutations leaving Y fixed point-wise form a subgroup G_Y of G and by custom we write G_y for $G_{\{y\}}$. If G is transitive on X, all subgroups G_x, $x \in X$, form one conjugacy class of subgroups of G. We say G is *rank* n on X if G is transitive on X and G_x acts in n distinct orbits on X; a rank 2 group is called *doubly transitive* and is transitive on the set of ordered 2-sets from X. If (G,X) is doubly transitive, then G is called a *transitive extension* of $(G_x, X - \{x\})$. The problem is to reverse this process; find for which transitive groups $(G_x, X - \{x\})$, the doubly transitive group (G,X) exists.

As an example, there are 35 ways to partition 8 letters into two 4-sets and Sym(8) is a rank 3 permutation group (H,X) on the set X of partitions. The subgroup H_x fixing a partition x is $\mathrm{Sym}(4)\backslash Z_2$ acting with orbits of lengths 1, 18 and 16, so $H = H_x + H_x t_1 H_x + H_x t_2 H_x$. We can adjoin a new letter a to X and define a permutation z on $\{a\} \cup X$, transposing a and x, such that zt_1z and zt_2z lie in the set $G = H+HzH$. Then the set G is closed under composition of permutations and so G is a doubly transitive group on 36 letters and is a transitive extension of H. As it turns out H is also the full automorphism group of a graph which can be defined on X. The graph has valence 18 and is defined by the translates of the orbit of length 18 for H_x. Moreover, z can be chosen to centralize the subgroup H_x and induces automorphisms of the subgraphs defined by the H_x-orbits and A and B of lengths 18 and 16 respectively. However if $(x,y) \in AB$, then (x,y) is an edge if and only if (x^z, y^z) is not an edge.

This was the prototype of the so-called "graph extension theorem" [22] which gave a sufficient condition (involving graph-theoretic concepts) that a group (H,X) have a transitive extension $(G, \{a\} \cup X)$, namely

HYPOTHESIS 10.1. *X is a graph and* $H = \mathrm{Aut}(X)$ *is transitive on the vertices* X. *There exist automorphisms* h_1 *and* h_2 *of the subgraphs* $\Gamma = A(b)$ *and* $\Sigma = X - (\{b\} \cup A(b))$ *such that* $h_1 \times h_2$ *interchanges the set of adjacent pairs with the set of non-adjacent pairs in* $\Gamma \times \Sigma$.

Transitive extensions which arise in this way include PSL(2,q), $q \equiv 1 \pmod 4$, $U(3,q^2)$, q odd, groups of Ree type, the symmetric groups, the two 2-transitive representations of Sp(2n,2) and two doubly transitive sporadic groups, HS and (.3). Any doubly transitive group whose one-point-stabilizer contains a strongly closed subgroup of index two arises by virtue of hypothesis 10.1 [12,26]. The problem of classifying the doubly transitive

groups which are transitive extensions coming from hypothesis 10.1 is still unsolved.

However, if one of the two automorphisms h_1 or h_2 of hypothesis 10.1 can be taken to be the identity (say, by composing them with the restriction of an automorphism of X fixing b) then the graph X is either a pentagon, or else has the "triangle property" -that is, the hypothesis of theorem A with C(x,y) assumed always to contain exactly three points. Regular graphs with this property were characterized in [23] (in fact SEIDEL proves a version of this result with the regularity of X relaxed [17]) before theorem A was ever proved. Because of this result the doubly transitive groups which arise from hypothesis 10.1 in this case must be PSL(2,5) on 6 letters, Sp(2n,2) on $2^{n-1}(2^n \pm 1)$ letters or the semidirect product V(2n,2)Sp(2n,2) on 2^{2n} letters. We thus have (logically, if not actually historically) an application of theorem A to doubly transitive groups.

A more general way of looking at the above construction is obtained by considering a new combinatorial object, the 2-graph, first introduced by GRAHAM HIGMAN in order to study the Conway group (.3) as a doubly transitive group on 276 letters. A *2-graph* (Ω,Δ) is a set of letters Ω and a family Δ of 3-sets from Ω such that any 4-set of Ω contains an even number of 3-sets belonging to Δ (the cases in which Δ contains all 3-sets or is empty, are regarded as *trivial* 2-graphs). A 2-graph is called *regular* if every pair of letters lies in the same number of sets in Δ. The transitive extensions obtained from the graph extension theorem are in 1-1-correspondence with the class of doubly transitive 2-graphs. Let X be the graph in hypothesis 10.1 and let a be the "new" point, and regard $\{a\} \cup X$ as a graph with $\{a\}$ as an isolated vertex and X as a subgraph. Then the 2-graph in question has $\{a\} \cup X$ as its set of letters, and all 3-sets of $\{a\} \cup X$ containing an odd number of edges as the family of 3-sets Δ. Because of hypothesis 10.1, the transitive extension constructed is in the automorphism group of the 2-graph $(\{a\} \cup X, \Delta)$. Because $G_b = H = \mathrm{Aut}(X)$, it is the *full* automorphism group. Those graphs G, for which the family Δ of 3-sets of vertices of G containing an odd number of edges defines a regular 2-graph (G,Δ) are characterized among all graphs by the fact that their (-1,0,1) adjacency matrices possess only two distinct eigenroots [17, Theorem 2.5]. If G is such a graph, and Y is a subgraph of G, we may switch with respect to Y; that is, obtain a new graph G' with Y and G-Y as subgraphs, by erasing all edges in $Y \times (G-Y)$ and declaring all non-adjacent pairs of $Y \times (G-Y)$ in G to be edges of G'. Then the 3-sets of G' possessing an odd number of edges is

still Δ, so the same 2-graph is defined by G'. We may thus associate a 2-graph with a switching class of graphs, and SEIDEL [19] has made this association precise by showing that any two graphs which lead to the same 2-graph are actually switching-equivalent. It is interesting to note that SEIDEL first introduces the switching concept into graph theory in [18], well before its relevance to 2-graphs became known. The mathematical muse seems mysteriously to bring things forth at the right time!

I should mention that 2-graphs are interesting combinatorial objects to study in their own right. SEIDEL & GOETHALS [19] have shown that there is a unique regular 2-graph on 276 letters and in doing so have produced an elementary construction of this 2-graph from first principles. This gives us an elementary construction of Conway's group (.3) without the use of the Leech lattice, or even the existence of the larger Mathieu groups. Although there is an excellent development of 2-graphs in TAYLOR's thesis [27], I would recommend the reader to the more accessible and current survey of 2-graphs by SEIDEL [20].

Another application of theorem A stems originally from an earlier version [24] of the "triangle property" theorem [23] in which the vertices of the graph were actually involutions in a group, and edges were commuting pairs of involutions. As a corollary of that theorem (and GLAUBERMAN's Z^*-theorem [11]) one obtains the following non-simplicity criterion for a finite group.

THEOREM 10.1. *Let* K *be a non-empty union of classes of involutions in a finite group* G. *Suppose that if* t *and* s *are commuting members of* K, *then*

(i) $ts \in K$, *and*

(ii) *any element of* K *commutes with at least one involution in* $\langle t,s\rangle$.

Then either no two members of K *commute and* $Z^*(G)$ *is non-trivial, or else* G *has a normal elementary abelian 2-group. In either case* G *contains a non-trivial normal solvable subgroup.*

ALPERIN [2] generalized this theorem and gave a direct group-theoretic proof of it.

THEOREM 10.2. (ALPERIN) *Let* A *be a fours group in* G, *and set* $K = (A^\#)^G$, *and suppose* $C_G(x) \cap A > 1$ *for all* $x \in K$. *Then* $A \cap O_2(G) > 1$.

By using theorem A one can prove an "odd p" version of theorem 10.1, namely:

THEOREM 10.4. (SHULT [24a]). *Let* K *be a union of classes of cyclic groups of prime order* p *in* G. *Suppose that whenever* X *and* Y *are distinct members of* K *which commute with one another, then*

(i) *at least three* Z_p*'s in* $\langle X,Y\rangle$ *lie in* K, *and*

(ii) $C_G(P) \cap \langle X,Y\rangle \cap K$ *is non-trivial for each* P *in* K.

Suppose, further, that at least two members of K *commute with one another. Then* G *contains a non-trivial normal elementary* p*-group* N, *central in* $\langle K\rangle$.

Does there exist a similar "odd p" version of ALPERIN's generalization of hypothesis 10.1? Such a theorem would have a hypothesis referring to a fixed subgroup A of type $Z_p \times Z_p$, with $C_G(X) \cap A > 1$ for each X in K, the set of G-conjugates of Z_p's in A. Indeed, this suggests a variation on the theorems of BRODKEY [9] and LAFFEY [14]: Suppose A is a subgroup of G of type $Z_p \times Z_p$ and suppose A meets all of its G-conjugates non-trivially. Then show $O_p(G)$ is non-trivial. So far these generalizations remain to be proved.

These are meagre beginnings, but it is the author's belief that the applications of theorem A (and similar theorems) to group-theoretic problems has just begun.

REFERENCES

[1] AHRENS, B.W. & G. SZEKERES, *On a combinatorial generalization of 27 lines associated with a cubic surface*, J. Austral. Math. Soc., 10 (1969) 485-492.

[2] ALPERIN, J.L., *On fours groups*, Illinois J. Math., 16 (1972) 349-351.

[3] BENSON, C., *On the structure of generalized quadrangles*, J. Algebra, 15 (1970) 443-454.

[4] BENSON, C., *Generalized quadrangles and (B,N)-pairs*, thesis, Cornell University, 1965.

[5] BUEKENHOUT, F., *Characterizations of semi-quadrics; a survey*, preprint.

[6] BUEKENHOUT, F., Personal communication.

[7] BUEKENHOUT, F. & C. LEFEVRE, *Generalized quadrangles in projective spaces*, to appear.

[8] BUEKENHOUT, F. & E.E. SHULT, *On the foundations of polar geometry*, to appear in Geomtriae Dedicata.

[9] BRODKEY, J.S., *A note on finite groups with an abelian Sylow subgroup*, Proc. Amer. Math. Soc., 14 (1963) 132-133.

[10] DEMBOWSKI, P., *Finite geometries*, Ergebnisse der Mathematik 44, Springer-Verlag, Berlin etc., 1968.

[11] GLAUBERMAN, G., *Central elements in core-free groups*, J. Algebra, 4 (1966) 403-420.

[12] HALL Jr., M. & E.E. SHULT, *Equiangular lines, the graph extension theorem and transfer in triply transitive groups*, to appear in Math. Z.

[13] HALL Jr., M., *Affine generalized quadrilaterals*, in: *Studies in pure mathematics*, L. MIRSKY (ed.), Academic Press, London, 1971, pp. 113-116.

[14] LAFFEY, T.J., *A problem on cyclic subgroups of finite groups*, Proc. Edinburgh Math. Soc., 18 (Series II) (1973) 247-250.

[15] LINT, J.H. VAN & J.J. SEIDEL, *Equilateral point sets in elliptic geometry*, Kon. Nederl. Akad. Wetensch. Proc. A, 69 (= Indag. Math. 28) (1966) 335-348.

[16] PAYNE, S., *Finite generalized quadrangles; a survey*, mimeographed notes.

[17] SEIDEL, J.J., *On 2-graphs and Shult's characterization of symplectic and orthogonal geometries over* GF(2), Tech. University Eindhoven, T.H. Report 73-WSK-02, 1973.

[18] SEIDEL, J.J., *Strongly regular graphs of* L_2*-type and of triangular type*, Kon. Nederl. Akad. Wetensch. Proc. A, 70 (= Indag. Math. 29) (1967) 188-196.

[19] SEIDEL, J.J., Personal communication.

[20] SEIDEL, J.J., *Survey of 2-graphs*, preprint for an address before the Boca Raton Conference, 1974.

[21] SINGLETON, R.R., *Minimal regular graphs of maximal even girth*, J. Combinatorial Theory, 1 (1966) 306-332.

[22] SHULT, E.E., *The graph extension theorem*, Proc. Amer. Math. Soc., 33 (1972) 278-284.

[23] SHULT, E.E., *Characterizations of certain classes of graphs*, J. Combinatorial Theory B, 13 (1972) 1-26.

[24] SHULT, E.E., *A characterization of the groups* Sp(2n,2), J. Algebra, 15 (1970) 543-553.

[24a] SHULT, E.E., *On subgroups of type* $Z_p \times Z_p$, to appear in J. Algebra.

[25] TALLINI, G., *Ruled graphic systems*, in: Atti Convegno Geometria e sue Applicazioni, Perugia, 1971, pp. 403-411.

[26] TAYLOR, D.E., *Monomial representations and strong graphs*, in: Proc. First Autralian Conf. Combinatorial Math., Univ. of Newcastle, 1972, pp. 197-201.

[27] TAYLOR, D.E., *Some topics in the theory of finite groups*, thesis, Oxford Univ., 1971.

[28] THAS, J.A., *4-gonal configurations*, to appear in Geometriae Dedicata.

[28a] THAS, J.A., *4-gonal configurations with parameters* $r = q^2+1$ *and* $k = q+1$. To appear.

[29] TITS, J., *Buildings and* B,N*-pairs of spherical type*, Lecture Notes in Mathematics, Springer-Verlag, Berlin etc., 1974.

[30] TITS, J., *Sur la trialité et certains groups que s'en deduisent*, Publ. Math. I.H.E.S., Paris, 2 (1959) 14-60.

[31] VEBLEN, O. & J.W. YOUNG, *Projective geometry I*, Ginn, Boston, 1916.

[32] VELDKAMP, F.D., *Polar geometry I-V*, Kon. Nederl. Akad. Wet. Proc. A, 62 (1959) 512-551; A 63 (1960) 207-212 (= Indag. Math. 21 resp. 22).

OTHER TITLES IN THE
SERIES MATHEMATICAL CENTRE TRACTS

A leaflet containing an order-form and abstracts of all publications mentioned below is available at the Mathematical Centre, 2e Boerhaavestraat 49, Amsterdam-1005, The Netherlands. Orders should be sent to the same address.

MCT 1 T. VAN DER WALT, *Fixed and almost fixed points*, 1963.

MCT 2 A.R. BLOEMENA, *Sampling from a graph*, 1964.

MCT 3 G. DE LEVE, *Generalized Markovian decision processes, part I: Model and method*, 1964.

MCT 4 G. DE LEVE, *Generalized Markovian decision processes, part II: Probabilistic background*, 1964.

MCT 5 G. DE LEVE, H.C. TIJMS & P.J. WEEDA, *Generalized Markovian decision processes, Applications*, 1970.

MCT 6 M.A. MAURICE, *Compact ordered spaces*, 1964.

MCT 7 W.R. VAN ZWET, *Convex transformations of random variables*, 1964.

MCT 8 J.A. ZONNEVELD, *Automatic numerical integration*, 1964.

MCT 9 P.C. BAAYEN, *Universal morphisms*, 1964.

MCT 10 E.M. DE JAGER, *Applications of distributions in mathematical physics*, 1964.

MCT 11 A.B. PAALMAN-DE MIRANDA, *Topological semigroups*, 1964.

MCT 12 J.A.TH.M. VAN BERCKEL, H. BRANDT CORSTIUS, R.J. MOKKEN & A. VAN WIJNGAARDEN, *Formal properties of newspaper Dutch*, 1965.

MCT 13 H.A. LAUWERIER, *Asymptotic expansions*, 1966, out of print; replaced by MCT 54.

MCT 14 H.A. LAUWERIER, *Calculus of variations in mathematical physics*, 1966.

MCT 15 R. DOORNBOS, *Slippage tests*, 1966.

MCT 16 J.W. DE BAKKER, *Formal definition of programming languages with an application to the definition of ALGOL 60*, 1967.

MCT 17 R.P. VAN DE RIET, *Formula manipulation in ALGOL 60, part 1*, 1968.

MCT 18 R.P. VAN DE RIET, *Formula manipulation in ALGOL 60, part 2*, 1968.

MCT 19 J. VAN DER SLOT, *Some properties related to compactness*, 1968.

MCT 20 P.J. VAN DER HOUWEN, *Finite difference methods for solving partial differential equations*, 1968.

MCT 21 E. WATTEL, *The compactness operator in set theory and topology*, 1968.

MCT 22 T.J. DEKKER, *ALGOL 60 procedures in numerical algebra, part 1*, 1968.

MCT 23 T.J. DEKKER & W. HOFFMANN, *ALGOL 60 procedures in numerical algebra, part 2*, 1968.

MCT 24 J.W. DE BAKKER, *Recursive procedures*, 1971.

MCT 25 E.R. PAERL, *Representations of the Lorentz group and projective geometry*, 1969.

MCT 26 EUROPEAN MEETING 1968, *Selected statistical papers, part I*, 1968.

MCT 27 EUROPEAN MEETING 1968, *Selected statistical papers, part II*, 1969.

MCT 28 J. OOSTERHOFF, *Combination of one-sided statistical tests*, 1969.

MCT 29 J. VERHOEFF, *Error detecting decimal codes*, 1969.

MCT 30 H. BRANDT CORSTIUS, *Excercises in computational linguistics*, 1970.

MCT 31 W. MOLENAAR, *Approximations to the Poisson, binomial and hypergeometric distribution functions*, 1970.

MCT 32 L. DE HAAN, *On regular variation and its application to the weak convergence of sample extremes*, 1970.

MCT 33 F.W. STEUTEL, *Preservation of infinite divisibility under mixing and related topics*, 1970.

MCT 34 I. JUHASZ a.o., *Cardinal functions in topology*, 1971.

MCT 35 M.H. VAN EMDEN, *An analysis of complexity*, 1971.

MCT 36 J. GRASMAN, *On the birth of boundary layers*, 1971.

MCT 37 G.A. BLAAUW a.o., *MC-25 Informatica Symposium*, 1971.

MCT 38 W.A. VERLOREN VAN THEMAAT, *Automatic analysis of Dutch compound words*, 1971.

MCT 39 H. BAVINCK, *Jacobi series and approximation*, 1972.

MCT 40 H.C. TIJMS, *Analysis of (s,S) inventory models*, 1972.

MCT 41 A. VERBEEK, *Superextensions of topological spaces*, 1972.

MCT 42 W. VERVAAT, *Success epochs in Bernoulli trials (with applications in number theory)*, 1972.

MCT 43 F.H. RUYMGAART, *Asymptotic theory of rank tests for independence*, 1973.

MCT 44 H. BART, *Meromorphic operator valued functions*, 1973.

MCT 45 A.A. BALKEMA, *Monotone transformations and limit laws*, 1973.

MCT 46 R.P. VAN DE RIET, *ABC ALGOL, A portable language for formula manipulation systems, part 1: The language*, 1973.

MCT 47 R.P. VAN DE RIET, *ABC ALGOL, A portable language for formula manipulation systems, part 2: The compiler*, 1973.

MCT 48 F.E.J. KRUSEMAN ARETZ, P.J.W. TEN HAGEN & H.L. OUDSHOORN, *An ALGOL 60 compiler in ALGOL 60, Text of the MC-compiler for the EL-X8*, 1973.

MCT 49 H. KOK, *Connected orderable spaces*, 1974.

* MCT 50 A. VAN WIJNGAARDEN, B.J. MAILLOUX, J.E.L. PECK, C.H.A. KOSTER, M. SINTZOFF, C.H. LINDSEY, L.G.L.T. MEERTENS & R.G. FISKER (eds.), *Revised report on the algorithmic language ALGOL 68*.

MCT 51 A. HORDIJK, *Dynamic programming and Markov potential theory*, 1974.

MCT 52 P.C. BAAYEN (ed.), *Topological structures*, 1974.

MCT 53 M.J. FABER, *Metrizability in generalized ordered spaces*, 1974.

MCT 54 H.A. LAUWERIER, *Asymptotic analysis, part 1*, 1974.

MCT 55 M. HALL JR. & J.H. VAN LINT (eds.), *Combinatorics, part 1: Theory of designs, finite geometry and coding theory*, 1974.

MCT 56 M. HALL JR. & J.H. VAN LINT (eds.), *Combinatorics, part 2: Graph theory; foundations, partitions and combinatorial geometry*, 1974.

MCT 57 M. HALL JR. & J.H. VAN LINT (eds.), *Combinatorics, part 3: Combinatorial group theory*, 1974.

MCT 58 W. ALBERS, *Asymptotic expansions and the deficiency concept in statistics*, 1975.

A star (*) before the number means "to appear".