JOURNAL OF ALGEBRA 111, 220–247 (1987)

Sharp Sets of Permutations

P. J. CAMERON*

Merton College, Oxford OX1 4JD, United Kingdom

AND

M. DEZA AND P. FRANKL

CNRS, Paris, France

Communicated by Peter M. Neumann

Received January 29, 1984

A set of permutations is sharp if its cardinality is the product of the distinct non-zero Hamming distances between pairs of permutations in the set. We give a number of new results and constructions for sharp sets and groups and for the more special geometric sets and groups, using a mixture of algebraic and combinatorial techniques.

1. INTRODUCTION

Sharp sets of permutations arise in the study of extremal problems for sets of permutations with prescribed Hamming distances. In this paper, we give some new constructions and results about sharp sets and groups and the closely related permutation geometries. A more precise description of the results will be given after the relevant concepts have been defined.

Let S_n be the group of permutations of $\{1, ..., n\}$; for $g \in S_n$, let $\mathrm{fix}(g)$ denote the number of fixed points of g. Given any non-empty subset $L = \{l_0, ..., l_{s-1}\}$ of $\{0, ..., n-1\}$, (where we assume that $l_0 < \cdots < l_{s-1}$), a subset A of S_n is called *L-intersecting* if, for all g, $h \in A$ with $g \neq h$, we have $\mathrm{fix}(g^{-1}h) \in L$. (Note that $n\text{-fix}(g^{-1}h)$ is the Hamming distance between g and h.) Denote by $m(n, L)$ the maximum cardinality of an L-intersecting subset of S_n, and by $m_g(n, L)$ that of an L-intersecting subgroup.

Comparatively little is known about the numbers $m(n, L)$ and $m_g(n, L)$, even though the analogous problem for subsets of a set has been widely studied. A nice general result is due to Kiyota [19].

* Present address: School of Mathematical Sciences, Queen Mary College, London E1 4NS, U.K..

0021-8693/87 $3.00

THEOREM 1.1. $m_g(n, L) \leqslant \prod_{l \in L} (n-l)$.

Although this inequality does not hold in general for $m(n, L)$ (we will give examples later), we will call an L-intersecting set A of S_n a *sharp set* of type (n, L) (or just of type L) if its cardinality is $\prod_{l \in L} (n-l)$. This is partly motivated by the fact that "geometric sets" of permutations (related to permutation geometries, and defined later) are necessarily sharp. A sharp set which is also a group (in other words, a group attaining Kiyota's bound) is called a *sharp group*.

For example, consider the case when $L = \{0, 1, ..., t-1\}$. A set S of permutations is L-intersecting if any two permutations agree in at most $t-1$ positions; S is sharp if and only if it is *sharply t-transitive*, that is, exactly one element of S carries any t-tuple of points to any other. We note that, for $t \geqslant 2$, all sharply t-transitive groups have been determined by Jordan and Zassenhaus (see [25]); there are none for $t \geqslant 6$ apart from the symmetric and alternating groups. On the other hand, the existence of a sharply 2-transitive set of permutations on n points is equivalent to that of a projective plane of order n. Our question can be seen as a generalisation of sharply t-transitive sets or groups.

Among sharp sets or groups, an interesting subclass consists of the geometric ones. We give a recursive definition, equivalent to the usual one (see, e.g., [5]).

First, a geometric set of type $(\varnothing, n)$, is simply a single permutation of $N = \{1, ..., n\}$.

If $L \neq \varnothing$ but $0 \notin L$, a subset A of S_n is geometric of type (L, n) if and only if there exist $i, j \in N$ such that every element of A maps i to j, and if $N \setminus \{i\}$ and $N \setminus \{j\}$ are identified and A regarded as a set of bijections on this set, then it is geometric of type $(L-1, n-1)$, where

$$L - 1 = \{l - 1 \mid l \in L\}.$$

Finally, if $0 \in L$, an L-intersecting set A is geometric if and only if for every $i, j \in N$, the set $A_{ij} = \{g \in A \mid g(i) = j\}$ is geometric of type $(L \setminus \{0\}, n)$.

An easy induction shows that a geometric set A of type (L, n) has size $\prod_{l \in L} (n-l)$, and that it is L-intersecting; so it is sharp of the same type, as we claimed. While every sharply t-transitive set is geometric, not all sharp sets (or groups) are geometric; we will see examples in the next section.

For groups, the definition can be simplified. A group G of permutations of N is geometric of type (L, n), where $L = \{l_0, ..., l_{s-1}\}$ with $l_0 < \cdots < l_{s-1}$, if there is a sequence $(x_1, ..., x_s)$ of points such that

(i) the pointwise stabiliser of $x_1, ..., x_s$ is the identity;

(ii) for $i < s$, the pointwise stabiliser of $x_1, ..., x_i$ fixes l_i points and is transitive on the points that it moves. Thus, if L does not consist of the first

s natural numbers, then a geometric group of type (L, n) is a special kind of Jordan group.

We turn now to the definition of a permutation geometry. This definition is a little more restrictive than the one given in [5], but suffices for our purposes. Let $N = \{1, ..., n\}$. For any $g \in S_n$, let $P(g) = \{(i, g(i)) \mid i \in N\}$, a *diagonal set* of the square $N \times N$. A subset of a diagonal set will be called a *partial diagonal.* Let $\mathscr{L}(\mathscr{F})$ be the meet semilattice (the closure under intersection) generated by the family $\mathscr{F}$ of sets. Given $L = \{l_0, ..., l_{s-1}\} \subseteq \{0, ..., n-1\}$ with $l_0 < \cdots < l_{s-1}$, a *permutation geometry* of type (L, n) is an $(s+1)$-tuple $(\mathscr{F}_0, ..., \mathscr{F}_s)$ of sets of partial diagonals with the following properties:

(i) every element of $\mathscr{F}_i$ has cardinality l_i $(0 \leqslant i \leqslant s)$, where by convention we put $l_s = n$ (so that elements of $\mathscr{F}_s$ are diagonal sets);

(ii) for every $F \in \mathscr{F}_i$ and every $x \in N \times N$ for which $F \cup \{x\}$ is a partial diagonal, there is a unique $F' \in \mathscr{F}_{i+1}$ with $F \cup \{x\} \subseteq F'$;

(iii) $\mathscr{F}_0 \cup \cdots \cup \mathscr{F}_s$ is the meet semilattice generated by $\mathscr{F}_s$.

If $(\mathscr{F}_0, ..., \mathscr{F}_s)$ is a permutation geometry of type (L, n), then $\mathscr{F}_s$ is a geometric set of the same type. Conversely, if A is a geometric set of type (L, n) and, for $0 \leqslant i \leqslant s$, we set

$$\mathscr{F}_i = \{F \in \mathscr{L}(P(A)) \mid |F| = l_i\}$$

with $l_s = n$, then $(\mathscr{F}_0, ..., \mathscr{F}_s)$ is a permutation geometry.

We now outline the main results of this paper.

In Section 2, we prove Kiyota's bound for $m_g(n, L)$ and an equivalent inequality, and also a related but weaker bound for $m(n, L)$, by character-theoretic methods; we give examples, both of non-geometric sharp groups and of L-intersecting sets whose size exceeds Kiyota's bound; and we give some related results.

In Section 3 and 4, we describe a method of obtaining new sharp sets and permutation geometries from old ones: from such sets or geometries of type (L, n) we obtain new ones of type (mL, mn), where $mL = \{ml \mid l \in L\}$. The construction depends on the existence of a certain kind of "transversal design" over an alphabet of size m. We give several examples.

This "blowing-up" construction does not usually produce groups; in Sections 5 and 6, we examine situations where groups are obtained, and find that the structure is much tighter. In Section 5, we show that a sharp group of type (mL, mn), where $L = \{0, ..., k-1\}$, is necessarily a blow-up of a very special kind provided that n is not too small compared to m and $n-k$; some related characterisations are also given. Section 6 contains a detailed discussion of geometric groups for which $|L| = 2$; the "blow-up"

concept emerges naturally in their structure theory. We hope to give a complete description of this class in a subsequent paper.

Any geometric set satisfying some additional conditions (in particular, any geometric group) consists of automorphisms of a basis-transitive matroid (combinatorial geometry) whose flats have cardinalities in the set L. So a natural place to look for such sets is inside the automorphism groups of basis-transitive matroids, noting that Kantor [18] has determined all such matroids (using the classification of finite simple groups). Section 7 shows that such sets do not exist in $\mathrm{Aut}(PG(d-1, q))$ for $d>2$, unless $q=2$; even then, the possibilities are very restricted.

Section 8 considers possible generalisations to the infinite: the definition of an infinite geometric group is clear, although examples are scarce, but that of an infinite sharp group is more problematical.

Finally, we are grateful to M. Laurent for pointing out an error in the definition of a permutation geometry given in [4]—that definition allowed the possibility that some maximal elements are permutations while others are not—and to R. A. Bailey for comments on an earlier draft of this paper.

2. Bounds and Examples

We begin this section with a proof of Kiyota's Theorem 1.1, and then derive some further results using similar techniques.

THEOREM 2.1 (Kiyota). *Let G be a L-intersecting subgroup of S_n. Then $|G|$ divides $\prod_{l\in L}(n-l)$.*

Proof. We represent G by permutation matrices $\{P(g)\,|\,g\in G\}$. The number $\mathrm{fix}(g)$ of fixed points of an element $g\in G$ is given by

$$\mathrm{fix}(g)=\mathrm{trace}(P(g))=\pi(g),$$

where π is the permutation character. Now any power of π is a character of G (the character of the corresponding tensor power of P); so, for any integer polynomial f, $f(\pi)$ is a generalised character of G (the difference of two characters). Taking $f(x)=\prod_{l\in L}(x-l)$, we have

$$f(\pi(g))=\begin{cases}\prod_{l\in L}(n-l) & \text{if } g=1,\\ 0 & \text{otherwise.}\end{cases}$$

Then $d=(f(\pi), 1_G)=\prod_{l\in L}(n-l)/|G|$.

In fact, the argument shows that $f(\pi)=d\rho$, where ρ is the regular character of G. By definition, G is sharp if and only if $d=1$.

We re-formulate Theorem 2.1 in a way that will be useful later. First, some notation. Let $f(x)=\prod_{l\in L}(n-l)=\sum_{i=0}^{s} a_i x^i$, where $s=|L|$, and let m_i be the number of orbits of G on ordered i-tuples for $i=1, ..., s$, with $m_0=1$.

PROPOSITION 2.2. *With the above notation,*

$$d=\sum_{i=0}^{s} a_i m_i \geqslant 1,$$

with equality if and only if G is sharp.

Proof. $d=(f(\pi), 1_G) = \sum_{i=0}^{s} a_i(\pi^i, 1_G) = \sum_{i=0}^{s} a_i m_i$. Note that the numbers m_i can be expressed in terms of the numbers of G-orbits on i-tuples of distinct elements; the coefficients are Stirling numbers of the second kind (see [6]).

A sharply t-transitive group is necessarily geometric, but there are many non-geometric sharp groups. We give a simple example.

EXAMPLE 2.3. Let G be a Frobenius group of order lm with Frobenius complement of order l; let M be the Frobenius kernel. Consider the permutation representation of G on $X=X_0\cup X_1\cup\cdots\cup X_l$, where $X_1, ..., X_l$ support the Frobenius representation of G, and X_0 the regular representation of G/M. Then $|X|=l+lm$. A non-identity element of M fixes all l points of X_0 and no others, whereas an element outside M fixes one point in each of $X_1, ..., X_l$, and none in X_0. So G is $\{l\}$-intersecting and hence sharp.

For a deeper study of non-geometric sharp groups, we refer to Ito and Kiyota [16].

There are a few special situations in which any L-intersecting set of permutations necessarily has size at most $\prod_{l\in L}(n-l)$. For example, this is true if $L=\{0, 1, ..., t-1\}$. Also, it is true if there exists a sharp set of type (L', n), where $L'=\{0, ..., n-1\}\backslash L$, in view of the following easy result (see [8]):

PROPOSITION 2.4. *If $L'=\{0, ..., n-1\}\backslash L$, then $m(n, L)\, m(n, L')\leqslant n!$.*

We will see another situation where it holds in Section 7.

In general, however, this bound does not hold. For example, if $n\geqslant 2s$, the set S of all permutations moving at most s points is L-intersecting, where $L=\{n-2s, ..., n-2\}$. In this case, $\prod_{l\in L}(n-l)=(2s)!$ but, for fixed s, $|S|$ tends to infinity with n. See Deza and Frankl [8], where this example is shown to be extremal, and is characterised as such when n is large compared to s; there is a similar example and characterisation for the case $L=$

$\{n-t, ..., n-2\}$, where t is odd. Also, there are examples of L-intersecting sets with $|L|=1$, of size at least cn^2; see [7] and the references cited there.

A simple upper bound for $m(n, L)$ can be derived as follows. If S is such a set, consider the set $P(S)=\{P(g) \mid g \in S\}$ of permutation matrices. These can be regarded as n-subsets of the n^2-set $N \times N$, and clearly form an L-intersecting family of subsets. By the theorem of Ray-Chaudhuri and Wilson [22], $|S| \leqslant \binom{n^2}{s}$, where $s=|L|$. This bound can be improved, using the same techniques as in [22], to the number of partial diagonals of size s in $N \times N$, namely

$$n^2(n-1)^2 \cdots (n-s+1)^2/s!;$$

note that this is a polynomial in n of the same degree $2s$ and with the same leading coefficient $1/s!$ as before.

We present a further improvement, which reduces the leading coefficient to $p(s)/(s!)^2$, where p is the partition function. At the same time, we strengthen the result in the same way that Frankl and Wilson [13] strengthened the result of [22]. Recall the standard bijection between irreducible characters of S_n and partitions of n. A character is said to have *dimension* s if the largest part of the corresponding partition is $n-s$.

THEOREM 2.5. *Suppose that p is a prime number such that no member of L is congruent to n* mod p, *and L is covered by s residue classes* mod p. *Then $m(n, L)$ does not exceed the sum of squares of the degrees of the characters of S_n of dimension s or smaller.*

Remark 2.6. The theorem can always be applied with p a prime greater than n, when $s=|L|$. For $n \geqslant 2s$, a character of S_n of dimension s has degree a polynomial in n of degree s with leading coefficient $1/s!$, and there are $p(s)$ such characters; this justifies the assertion before the theorem.

Proof. Let $m_0, ..., m_{s-1}$ be integers whose residue classes mod p cover L. Consider the generalised character $\theta=f(\pi)$ of S_n, where $f(x)=\prod_{i=0}^{s-1}(x-m_i)$. We have

$$\theta(1) \not\equiv 0 \pmod{p},$$

$$\theta(g) \equiv 0 \pmod{p} \quad \text{whenever } \operatorname{fix}(g) \in L.$$

Now θ is the difference between the characters of representations M_1, M_2 of S_n. Since all representations of S_n are equivalent to rational ones, we may assume that M_1 and M_2 are rational.

Consider the matrices $M(g)=\begin{pmatrix} M_1(g) & 0 \\ 0 & M_2(g) \end{pmatrix}$ for $g \in S$. We claim that these matrices are linearly independent. Suppose that $\sum_{g \in S} a(g) M(g)=0$. We may supppose that the coefficients are integers, and that one of them ($a(h)$, say) is not divisible by p.

The function

$$\left(\begin{pmatrix} A_1 & 0 \\ 0 & B_1 \end{pmatrix}, \begin{pmatrix} A_2 & 0 \\ 0 & B_2 \end{pmatrix}\right) = \text{trace}(A_1^{-t} A_2) - \text{trace}(B_1^{-1} B_2)$$

is a non-singular hyperbolic inner product. We have

$$\begin{aligned}(M(g), M(h)) &= \text{trace}(M_1(g^{-1}h)) - \text{trace}(M_2(g^{-1}h)) \\ &= \theta(g^{-1}h).\end{aligned}$$

Taking the inner product of the dependence relation with $M(h)$, we find that $a(h)\,\theta(1)/p = -\sum_{g \neq h} a(g)\,\theta(g^{-1}h)/p$. This is a contradiction, since p divides $\theta(g^{-1}h)$ but divides neither $a(h)$ nor $\theta(1)$. This establishes our claim.

But the dimension of the span of the matrices $M(g)$, as g runs through S_n, is equal to the sum of squares of the degrees of the irreducible characters of S_n appearing in θ. Since π^i involves all and only characters of dimension i or less (a result of Frobenius), θ involves only characters of dimension s or less, and the theorem follows.

In special cases the bound can be improved still further. For some choices of L, not all characters of dimension less than s will occur in θ, and the sum can be reduced. (Note, however, that all characters of dimension exactly s will occur, and these contribute the leading term.) Also, we have

Remark 2.7. If $0 \in L$, then $m(n, L) \leqslant nm(n, L \setminus \{0\})$. For, if x and y are any two points, then

$$S_{xy} = \{g \in G \mid g(x) = y\}$$

is $L\setminus\{0\}$-intersecting, and, for fixed x, $S = \bigcup_y S_{xy}$.

3. Blowing Up Permutation Geometries

In this section we give a construction which yields geometric sets of type (mL, mn) from geometric sets of type (L, n). The construction requires an auxilliary object, a transversal matroid design, which we proceed to define. Let $N = \{1, ..., n\}$.

Suppose that $X_1, ..., X_n$ are pairwise disjoint m-element sets and that $\mathcal{F}$ is a family of n-element sets which are transversals for $(X_1, ..., X_n)$. Set $\mathcal{F}(A) = \{A \cap A' \mid A' \in \mathcal{F}\}$. Thus $\mathcal{F}(A)$ is a family of subsets of A. Denote by $\mathcal{P}(A)$ its projection on N; that is, $\mathcal{P}(A) = \{P(B) \mid B \in \mathcal{F}(A)\}$, where $P(B) = \{i \mid X_i \cap B \neq \varnothing\}$. Recall the definition of a perfect matroid design (see [9]).

$\mathscr{F}$ is a *transversal matroid design* of type (L, n, m), where $L = l_0, ..., l_{s-1}$, if $|\mathscr{F}| = m^s$ and there exists a perfect matroid design $\mathscr{M}$ of type (L, n) on N such that for all $A \in \mathscr{F}$ we have $\mathscr{P}(A) \subseteq \mathscr{M}$.

Assuming that the elements of each set X_i are enumerated, the members of $\mathscr{F}$ can be identified with sequences $A = (a_1, ..., a_n)$, where $a_i = j$ if $A \cap X_i$ is the jth element of X_i. Note that, in the case $L = \{0, ..., s-1\}$, a transversal matroid design is the same as a transversal s-design: that is, given any s distinct members of N, and any s-tuple of elements of $\{1, ..., m\}$, there is a unique member of $\mathscr{F}$ having that s-tuple in the specified positions.

Suppose that P is a permutation geometry of type (L, n). (Then, in particular, $|P| = \prod_{l \in L} (n-l)$). Let $\mathscr{L}(P)$ be the associated permutation geometry, the meet semilattice generated by P. For each $g \in P$, the set of elements of $\mathscr{L}(P)$ which lie below g are the flats of a perfect matroid design. We may regard the point sets of all these matroids as being N, by identifying an element of $\mathscr{L}(P)$ with its domain (in other words, by projecting onto the first factor of $N \times N$). We make the further assumption that all these matroids coincide, after this identification. (We have no examples where this is not so, but we cannot prove that it must hold.) Let $\mathscr{M}$ be this common matroid. (In the terminology of [10], P is $\mathscr{M}$-unisupported.) Suppose further that there exists a transversal matroid design $\mathscr{F}$ with the matroid $\mathscr{M}$.

We consider an $nm \times nm$ square partitioned into n^2 subsquares $K(a, b)$ of size $m \times m$. Let

$$\mathscr{G}(a, b) = \{G_1(a, b), ..., G_m(a, b)\}$$

be a family of pairwise disjoint diagonals of $K(a, b)$. (This is equivalent to a Latin square of order m.) Now define

$$\mathscr{C}(P, \mathscr{G}) = \{C(g, A) \mid g \in P, A \in \mathscr{G}\},$$

where

$$C(g, A) = \bigcup_{1 \leq i \leq n} G_{a_i}(i, g(i)).$$

We want to show that $\mathscr{C} = \mathscr{C}(P, \mathscr{G})$ is a permutation geometry.

Let us first determine the cardinalities of the flats, that is, the intersections of members of $\mathscr{C}$. Suppose that $C(g_1, A_1), ..., C(g_l, A_l) \in \mathscr{C}$. Set $B = A_1 \cap \cdots \cap A_l$. Then B is a flat in $\mathscr{F}(A_1)$, whence $|B| \in L$. Also, the projection $P(B)$ is a flat of $\mathscr{M}$.

The meet of $g_1, ..., g_l$ is also a flat of the matroid $(0, g_1)$. Denote by B' its projection on N. Then B', and so also $B \cap B'$, is a flat of $\mathscr{M}$. Now the chosen elements of $\mathscr{C}$ have m common points in each square $(i, g_1(i))$ with

$i \in B \cap B'$, and none in any other square. So the size of the intersection is in the set $mL = \{ml_0, ..., ml_{s-1}\}$.

Obviously,

$$|\mathscr{C}| = |P| \cdot |\mathscr{F}| = m^s \prod_{l \in L} (n - l)$$

$$= \prod_{l \in L} (nm - lm).$$

So $\mathscr{C}$ is a sharp set of type (mL, nm).

To see that it is the hyperplane family of a permutation geometry $(\mathscr{L}_0, ..., \mathscr{L}_s = P)$, let $\mathscr{L} = \mathscr{L}(P)$, the meet semilattice generated by P, and let $\mathscr{L}_i$ be the set of elements of $\mathscr{L}$ with cardinality $l_i m$. From the construction, it is easy to see that, given $D \in \mathscr{L}_i$, the sets $E \setminus D$, for $D \subseteq E \in \mathscr{L}_{i+1}$, form a partition of the points of the $nm \times nm$ square which are "disjoint" from D, in the sense that they do not lie in the rows and columns determined by D. The result follows:

THEOREM 3.1. *Suppose that there exists a permutation geometry of type* (L, n) *in which the matroid below each maximal element is equal to a fixed perfect matroid design* $\mathscr{M}$. *Suppose further that there is a transversal matroid design of type* (L, n, m) *based on the same matroid* $\mathscr{M}$. *Then there exists a permutation geometry of type* (mL, mn).

Since a sharply t-transitive set of permutations is geometric (and is unisupported by the uniform matroid), we obtain an immediate corollary:

THEOREM 3.2. *If there exists a sharp set of permutations of type* $(\{0, 1, ..., t-1\}, n)$ *and a transversal t-design with n classes of size m, then there exists a sharp set of permutations of type* $(\{0, m, ..., (t-1)m\}, nm)$.

Since we have a free choice for each Latin square $\mathscr{G}(a, b)$, the construction produces a large number of sharp sets, most of which are not groups. We give examples in the next section.

4. EXAMPLES OF BLOW-UPS

First, we give some blow-ups of sharply t-transitive sets.

EXAMPLE 4.1. There exist sharp sets of types $(\{0, m, ..., (n-1)m\}, nm)$ and $(\{0, m, ..., (n-2)m\}, nm)$ for all $n \geq 3$, $m \geq 2$.

Proof. The symmetric group S_n is both sharply n-transitive and sharply $(n-1)$-transitive. The set of all transversals is a transversal n-design. For a transversal $(n-1)$-design, we may take each X_i to be a copy of an abelian group of order m, and then consider all those n-tuples of group elements with sum zero.

EXAMPLE 4.2. If n is a prime power, and $m \geqslant m_0(n)$, then there is a sharp set of type $(\{0, m\}, nm)$. For there is a sharply 2-transitive group of degree n, namely the affine group $\mathrm{AGL}(1, n)$; and a transversal 2-design with n blocks of size m is equivalent to a family of $n-2$ mutually orthogonal Latin squares of order m, which exists for all sufficiently large m. (See Wilson [26], e.g.) In particular, this construction gives a sharp set of type $(\{0, m\}, 4m)$ for all m except $m=2$ or 6; but an alternative construction works for these two values (see Sect. 6).

Remark 4.3. The construction of Example 4.2 sometimes yields sharply edge-transitive sets (SETs) of automorphisms of complete multipartite digraphs on n points, which have larger valency than any digraph of the same order admitting a sharply edge-transitive group (SETG). In the notation of [3], these are values of n for which $d^*(n) > d(n)$. For example, blow-ups of A_4 of type $(\{0, 3\}, 12)$ and $(\{0, 7\}, 28)$ demonstrate that $d^*(12) \geqslant 9$ and $d^*(28) \geqslant 21$; but $d(21) = 8$, $d(28) = 18$.

PROBLEM. Find further examples. (Note that the problem of finding the exact value of $d^*(12)$ includes that of the existence of a projective plane of order 12.)

Now we give a construction of some transversal matroid designs, using projective geometry. If $\mathscr{F}$ is a transversal matroid design (TMD) with matroid $\mathscr{M}$, and $\mathscr{M}'$ is obtained from $\mathscr{M}$ by replacing each element by a class of fixed size of "parallel" (i.e., mutually dependent) elements, then we can find a TMD $\mathscr{F}'$ over $\mathscr{M}'$ simply by repeating each coordinate suitably many times. So we concentrate on the case when $\mathscr{M}$ is simple (all rank 1 flats are singletons).

Let $\mathscr{F}$ be a TMD with simple matroid $\mathscr{M}$ on an n-set; we regard $\mathscr{F}$ as a set of n-tuples over a fixed alphabet of size m. Suppose that m is a prime power, and identify the alphabet with the field $\mathrm{GF}(m)$. We say that $\mathscr{F}$ is *linear* if it is $\mathrm{GF}(m)$-subspace of $\mathrm{GF}(m)^n$. (Note that its dimension is necessarily s, the rank of $\mathscr{M}$.)

A *projective representation* of $\mathscr{M}$ over $\mathrm{GF}(m)$ is an injection φ from the point set of $\mathscr{M}$ to $\mathrm{PG}(s-1, m)$ such that every hyperplane section of $\varphi(\mathscr{M})$ is the image under φ of a flat of $\mathscr{M}$. (For simple matroids, projective representations are induced in a natural way by linear representations.)

PROPOSITION 4.4. *There is a linear* TMD *over* GF(m) *with matroid* $\mathcal{M}$ *if and only if* $\mathcal{M}$ *has a projective representation over* GF(m).

Proof. Suppose that φ is a projective that φ is a projective representation of $\mathcal{M}$, with $\varphi(\mathcal{M}) = \{p_1, ..., p_n\}$. Let $V = V(s, m)$ be the underlying vector space, and select vectors $v_1, ..., v_n \in V$ with $\langle v_i \rangle = p_i$. Now

$$\{(f(v_1), ..., f(v_n)) \mid f \in V^*\}$$

is a linear TMD with matroid $\mathcal{M}$; for, given $f, g \in V^*$, $\{p_i \mid f(v_i) = g(v_i)\}$ is the intersection of $\varphi(\mathcal{M})$ with the kernel of $f - g$.

Conversely, a linear TMD $\mathcal{F}$ is a GF(m)-space of dimension s. For $1 \leqslant i \leqslant n$, the projection on the ith coordinate is a linear map $\mathcal{F} \to \mathrm{GF}(m)$, that is, an element of $\mathcal{F}^*$; let p_i be the corresponding point of the projective space PG($s-1, m$) based on $\mathcal{F}^*$. The map $i \mapsto p_i$ is then a projective representation of $\mathcal{M}$.

EXAMPLE 4.5. The uniform matroid of rank t on an n-set (whose hyperplanes are all the $(t-1)$-sets) has a projective representation over GF(m) provided that $n \leqslant m + 1$. (Take the vectors $(1, x, x^2, ..., x^{t-1})$ for $x \in \mathrm{GF}(m)$, together with $(0, 0, ..., 1)$—any t of these are linearly independent.) In the case $t = 3$, if m is even, we may adjoin the vector $(0, 1, 0)$ (the nucleus of the conic formed by the first $m+1$); so the case $n = m + 2$ is covered as well.

These designs can be used to blow up sharply t-transitive sets of permutations. Note that all sharply t-transitive groups of permutations are known; they are:

(i) S_n ($t = n$ and $t = n-1$), A_n ($t = n-2$);

(ii) affine groups over nearfields (n a prime power, $t = 2$);

(iii) PGL(2, $n-1$) and one other if $n-1$ is an odd square ($n-1$ a prime power, $t = 3$);

(iv) M_{11} and M_{12} ($n = 11$, 12, $t = 4$, 5, respectively).

EXAMPLE 4.6. (i) For all d, $s > 1$ and all prime powers q, PG($s-1, q$) and AG($s-1, q$) have projective representations over GF(q^d).

(ii) There exist permutation geometries of type

$$(\{0, q^d, q^{d+1}, ..., q^{d+s-1}\}, q^{d+s})$$

and $(\{0, 2^d, 3.2^d, ..., (2^{s-1}-1)\cdot 2^d\}, (2^s - 1)\cdot 2^d)$.

Proof. (i) For PG($s-1, q$), just take the set of points of PG($s-1, q^d$) whose coordinates lie in GF(q). For AG($s-1, q$), delete the points of a hyperplane.

(ii) The permutation geometries are obtained by blowing up the geometric groups AGL(s, q) or PGL$(s, 2)$.

EXAMPLE 4.7. (i) For all $k \geqslant s$ and all prime powers q, the truncations of PG$(k-1, q)$ and AG$(k-1, q)$ to rank s have projective representations over GF(q^d) for all sufficiently large d.

(ii) There exist permutation geometries of types $(\{0, q, 2q, 4q\}, 16q)$ and $(\{0, q, 3q\}, 3q\}$, whenever q is a sufficiently large power of 2.

Proof. Consider PG$(k-1, q)$. We claim that, for d sufficiently large, GF$(q^d)^s$ has a GF(q)-subspace W of dimension k such that, for any $i < s$ and any GF(q^d)-subspace $\mathcal{U}$ of dimension i, $U \cap W$ has dimension at most i as GF(q)-space. Given this claim, the points of PG$(s-1, q^d)$ spanned by vectors in W clearly provide a projective representation of the truncation of PG$(d-1, q)$.

To establish the claim, note that (for fixed q, s, k, and $d \to \infty$), the number of GF(q)-subspaces of dimension k is $\sim q^{skd}$. For $i < s$, the number of GF(q^d)-subspaces of dimension i is $\sim q^{i(s-i)d}$; and, for each one U of them, the number of GF(q)-spaces of dimension d which contain $i+1$ GF(q)-independent points of U, is $\sim q^{(i+1)id+(k-i-1)sd}$. So only $\sim q^{(i(s-i)+i(i+1)+(k-i-1)s)d}$ spaces are "bad," a proportion $\sim q^{-(s-i)d}$ of the total. So, for sufficiently large d, "good" spaces exist.

For AG$(k-1, q)$, as before, delete the points of a hyperplane.

(ii) The permutation geometries are obtained by blowing up the geometric groups T. A_7 and A_7, for which the supporting matroids are truncations of AG(4, 2) and PG(3, 2), respectively.

Combining these results, we see that all the 2-transitive geometric groups can be blown up in infinitely many different ways.

5. CLASSIFYING SOME SHARP GROUPS

As we noted in the Introduction, in considering geometric groups of type (L, n) with $L = \{l_0, ..., l_{s-1}\}$, where $l_0 < \cdots < l_{s-1}$, we may assume without loss of generality that $l_0 = 0$. Now, if $s > 1$, such a group has a system of blocks of imprimitivity of size l_1, a block being the fixed point set of a point stabiliser, and the induced group of permutations of the block system is doubly transitive. Now that all the finite doubly transitive groups are known, it might seem that we could give a complete list of geometric groups of type (L, n) with $|L| > 1$. However, difficulties remain. The case when $|L| = 2$ is treated in the next section. Here, we give some classifications theorems for geometric or sharp groups of various types. The arguments will require three steps:

(i) establish the existence of a block of imprimitivity of size l_1;

(ii) show that the group permuting the blocks is symmetric or alternating;

(iii) obtain the classification.

We separate these steps to some extent, since they often require slightly different hypotheses. It should be made clear that our results here are not best possible, but that stronger results using these methode would require increased complexity in statement and proof.

THEOREM 5.1. *Let G be a sharp group of type $(\{0, m, ..., (k-1)m\}, nm)$. Assume that*

(a) $n \geqslant \max(m+2, 8)$;

(b) *G has a block of imprimitivity of size m;*

(c) *the only transitive groups of degree n whose order N satisfies*

$$N | m^k n!/(n-k)!\,|\,(m!)^n\, N$$

are the symmetric and alternating groups.

Then either

(i) $k = n$, $G = H$ wr S_n, *where H is regular of degree m or*

(ii) $k = n-1$, $G \leqslant H$ wr S_n, *where H is abelian and regular of degree m, and G contains $M.\ A_n$ as a subgroup of index 2 where $M = \{(h_1, h_2, ..., h_n) \in H^n \mid h_1 \cdots h_n = 1\}$.*

In each case, G is a blow-up of S_n.

Remark 5.2. The complicated hypothesis (c) is not very restrictive. It holds, for example, if there is a prime p satisfying

$$\max(\tfrac{1}{2}(n+1), m+1, n-k+1) \leqslant p \leqslant n-3,$$

since a transitive group of degree n with order divisible by a prime p lying between $\frac{1}{2}(n+1)$ and $n-3$ is necessarily S_n or A_n. In particular, by Bertrand's postulate, it holds if $2m+1 \leqslant n \leqslant 2k-1$ and $n \geqslant 8$.

Remark 5.3. If we strengthen hypothesis (b) by assuming that G is geometric, we may weaken (c) to the assertion that the only k-transitive groups of degree n are S_n and A_n.

Remark 5.4. In conclusion (ii), note that $M \cdot A_n$ is a normal subgroup of H wr S_n with factor group $H \times \langle t \rangle$, where $\langle t \rangle = S_n/A_n \cong C_2$. G may be any group whose image in the factor group is generated by (h, t), for some

$h \in H$ satisfying $h^2 = 1$. In particular, if m is odd then necessarily $G = M \cdot S_n$ but if m is even then there are other possibilities for G.

Proof. We have $|G| = m^k n!/(n-k)!$. Let B be a block of imprimitivity of size m for G, $\mathscr{B}$ the set of translates of B, $H = G_B^B$ (so that $G \leqslant H$ wr S_n), and $L = G \cap H^n$, the kernel of the action of G on. Then $|L|$ divides $(m!)^n$. By hypothesis (c), $G/L = G^{\mathscr{B}} \cong S_n$ or A_n.

Consider the action on $B \times (\mathscr{B} \setminus \{B\})$. It induces H on the first factor and S_{n-1} or A_{n-1} on the second. Since $n-1 > m$ and $n-1 > 5$, either

(i) G_B induces $H \times S_{n-1}$ or $H \times A_{n-1}$ or

(ii) H has a subgroup K of index 2 such that G_B on $B \times (\mathscr{B} \setminus \{B\})$ consists of all (h, σ) with either $h \in K$, $\sigma \in A_{n-1}$, or $h \in H \setminus K$, $\sigma \in S_{n-1} \setminus A_{n-1}$.

Since $n \geqslant 6$, there are both even and odd permutations in S_{n-1} with no fixed point. Any element of H is thus induced by a permutation fixing no further blocks, so its number of fixed points in B is a multiple of m, necessarily 0 or m. Thus H acts regularly on B.

Next we show that for $i \leqslant n-4$, the pointwise stabiliser of i blocks induces at least A'_{n-i} (the commutator subgroup of the alternating group) on the set of remaining blocks. We know this already for $i = 1$. Since $n-i+1 \geqslant 5$, $A'_{n-i+1} = A_{n-i+1}$; and so, given blocks $B_1, ..., B_i$, any even permutation g of the remaining blocks is induced by an element fixing $B_1 ..., B_{i-1}$ pointwise, and any even permutation h by an element fixing $B_2, ..., B_i$ pointwise. Thus (g, h) is induced by an element fixing $B_1, ..., B_i$ pointwise, and the induction proceeds. In particular, G contains an element fixing $n-4$ blocks pointwise, and so $k \geqslant n-3$.

We want to conclude that $k \geqslant n-1$. Note that $|L| = m^k/(n-k)!$ or $2m^k/(n-k)!$. Also, a subgroup of H^n of order greater than m^r contains a non-identity element fixing at least r blocks pointwise. If $m \neq 2$, then $|L| \geqslant m^k/6 > m^{k-2}$, so there is an element $g \neq 1$ fixing at least $k-2$ blocks pointwise. If $k \geqslant 5$, let h fix pointwise all but four blocks and permute these blocks semiregularly, where exactly one of the four contains elements moved by g. Then (g, h) moves points in just two blocks, so $k \geqslant n-1$ as required. If $m = 2$ then $|L| \geqslant m^k/2$ and the same conclusion holds. Thus we have established the claim unless $k \leqslant 4$, $n \leqslant 7$, which violates (a).

If $k = n$ then $|G| = m^n n!$ and so $G = H$ wr S_n.

Suppose that $k = n-1$. Then $|G| = m^{n-1} n!$; $|L| \leqslant m^{n-1}$ by the remark in the preceding paragraph, so in fact $|L| = m^{n-1}$. Let $X \cong S_n$ be the standard complement for H^n in H wr S_n. Then, since $|H \text{ wr } S_n : G| = m < n$, X permutes the m cosets of G, and $X' \cong A_n$ necessarily fixes them. Thus $X' \leqslant G$.

L has the form

$$\{(h_1, ..., h_{n-1}, \varphi(h_1, ..., h_{n-1})) \mid h_1, ..., h_{n-1} \in H\}$$

for some function φ. The map $h \mapsto \varphi(h, 1, ..., 1)$ is one-to-one, hence onto. We conclude:

(i) H is abelian. For

$$\begin{aligned}\varphi(h_1, 1, ..., 1)\, \varphi(1, h_2, ..., 1) &= \varphi(h_1, h_2, ..., 1) \\ &= \varphi(1, h_2, ..., 1)\, \varphi(h_1, 1, ..., 1).\end{aligned}$$

(ii) $L = \{(h_1, ..., h_n) \mid h_1 \cdots h_n = 1\} = M$. For, applying $(1\ 2)(3\ 4) \in X'$ to $(h, 1, ..., \varphi(h, 1, ...)) \in L$ we obtain $(1, h, ..., \varphi(h, 1, ...)) \in L$, whence $(h, h^{-1}, 1, ...)$ L. This holds for any two coordinate positions, and these elements generate M. (Note that $\varphi(h_1, h_2, ...) = (h_1 h_2 \cdots)^{-1}$.)

Thus $MX' \leqslant G$, as required. This completes the proof.

The next result gives a sufficient condition for a block of imprimitivity of size m.

THEOREM 5.5. *Let G be a sharp group of type $(\{0, m, ..., (k-1)m\}, nm)$. Assume that $n \geqslant 4m$ and that there is a prime p satisfying $\max(n-k+1, \frac{1}{2}(n+1)) \leqslant p \leqslant n-4$. Then G has a block of primitivity of size m.*

Remark 5.6. Using a slight improvement on Bertrand's postulate, the requirement about the prime p can be replaced by the assumption that $n \leqslant 2k-1$ provided that $n \geqslant 15$.

Proof. Let g be an element of G of order p. The number of p-cycles of g is a multiple of m and is less than nm/p; since $p > \frac{1}{2}n$, the number is exactly m.

For any block of imprimitivity B, and any p-cycle C of g, either $B \supseteq C$ or $|B \cap C| \leqslant 1$. Suppose that $B \supseteq C$. Then every translate of B contains the same number of p-cycles of g. (If not, then G_B would contain non-conjugate subgroups of order p, and so $p^2 \mid |G_B|$, a contradiction.)

Now choose B minimal with respect to containing a p-cycle of g, and B' a block maximal with respect to being properly contained in B. (Either may be a trivial block.) Then we have $|B| = en$, $|B'| = f$, say, where $f \mid e \mid m$. The primitive group X induced by G_B on the set of translates of B' in B contains an element (induced by g) with e/f cycles of length p and at least $4e/f$ fixed points. Since $p > 2e/f$, theorems of Jordan and Manning (13.10 in Wielandt [25]) show that this primitive group is symmetric or alternating. Since $p^2 \nmid |G|$, we have $e = f$.

Now let K be the group which fixes all translates of B. Since G_B acts on B mod B' as S_n or A_n, and $|B^G| < n$, K also induces S_n or A_n on B mod B'. Also since $p^2 \nmid |G|$, and since S_n and A_n have unique permutation represen-

tations of degree n (as $n>6$), we have that K induces isomorphic permutation groups on the set of translates of B' in each translate of B. In particular, the stabilizer of B' in K fixes exactly one translate of B' in each translate of B; the union of all these is a block of impritivity for G, of size $(m/e)f=m$.

From Theorem 5.1 and 5.5 and our remarks about Bertrand's postulate, we obtain

COROLLARY 5.7. *Suppose that G is a sharp group of type $(\{0, m, ..., (k-1)m\}, nm)$, where $4m \leqslant n \leqslant 2k-1$ and $n \geqslant 15$. Then $k=n$ or $n-1$, and G is a blow-up of S_n.*

We conclude this section by describing and characterising some sharp groups of type $(\{0, m, ..., (k-1)m\}, nm)$, which are not of the type described in Theorem 4.1.

EXAMPLE 5.8. (i) In AGL(3, 2), any element fixes 0, 1, 2, or 4 points, and the only elements with just one fixed point are those of order 7. AGL(3, 2) has two conjugacy classes of subgroups of index 7; representatives are the stabiliser of a parallel class of lines, and the stabiliser of a parallel class of planes. Both are sharp groups of type $(\{0, 2, 4\}, 8)$; the first, but not the second, has a block of imprimitivity of size 2.

(ii) In a similar way, the stabiliser of a parallel class of lines, and the stabiliser of a parallel class of solids, in the group $V_{16} \cdot A_7$ (a subgroup of AGL(4, 2)), are both sharp groups of type $(\{0, 2, 4\}, 16)$. The first, but not the second, has a block of imprimitivity of size 2.

PROPOSITION 5.9. *A sharp group of type $(\{0, 2, ..., 2(k-1)\}, 2n)$ $(k \geqslant 3)$ which has a block of imprimitivity of size 2 is one of the following:*

(i) C_2 wr S_n, $k=n$;

(ii) *a subgroup of index 2 in C_2 wr S_n other than C_2 wr A_n (two possibilities), $k=n-1$;*

(iii) *the first group of Example 5.8(ii) above $(k=3, n=8)$.*

Proof. Tsuzuku (24) determined the geometric groups of type $(\{0, 2\}, 2n)$: they have $n=2$, 3, 4, or 7. This is the base step of an induction. It is easy to see that $k=n$ gives (i) while $k=n-1$ gives (ii); it is then enough to show the uniqueness of (iii) and the nonexistence of groups with $(n, k)=(5, 3)$ or $(9, 4)$.

A group of degree 16 and order 16.14.12 must have a normal 2-psubgroup of order 16 admitting a group of automorphisms isometric to GL(3, 2) fixing a non-identity element and acting transitively on the others.

The only such 2-group is the elementary abelian group, and the action is also uniquely determined.

In the case (5, 3), the group induced on the blocks is S_5 of A_5, and the kernel of this action has order 4 or 8 and is thus central. But a central subgroup of a transitive group is semiregular, hence of order 2.

In the case (9, 4), the group induced on the blocks is a transitive extension of AGL(3, 2), which does not exist.

PROBLEM 5.10. Remove the assumption of a block of imprimitivity of size 2. (For $k = 3$, see the next proposition.)

PROPOSITION 5.11. *A sharp group of type* $(\{0, 2, 4\}, 2n)$ *has a block of imprimitivity of size* 2 *unless* $2n = 8$ *or* 16.

Proof. Let r, s be the numbers of orbits on ordered pairs (resp. triples) of distinct points. Then the total number of orbits on ordered pairs, triples is $r+1$ (resp. $s+3r+1$). (As noted in Section 2, the coefficients are Stirling numbers of the second kind.) Proposition 2.2 shows that $s+3r+1-6(r+1)+8=1$ or $s=3r-2$.

Suppose that G has no block of imprimitivity of size 2. The stabiliser of a point has r orbits on the remaining points, all of size greater than one; so the stabiliser of two points has at least r further orbits, giving $s \geqslant r^2$. Thus $(r-1)(r-2) \leqslant 0$, so $r = 1$ or 2. The first is impossible, so $r = 2$, $s = 4$. Now G_x has two orbits other than $\{x\}$ and is doubly transitive on both, the stabiliser of a point in one being transitive on the other; so G is imprimitive, with two blocks of imprimitivity of size n.

The stabiliser of two points in the same block has order $4(n-2)$ and has an orbit of size n; so $n|4(n-2)$, $n|8$, $n = 4$ or 8.

A little further argument shows that the only such groups are those in Example 5.8. So all sharp groups of type $(\{0, 2, 4\}, 2n)$ are known.

PROBLEM 5.12. Suppose that P is a set of permutations of type $(\{0, m, ..., (n-1)m\}, nm)$. Is it true that, for $n \geqslant n_0(m)$ we necessarily have $|P| \leqslant n!\, m^n$? If so, then does equality imply that P is a blow-up of S_n?

Remark 5.13. The corresponding problem for sets is the following. What is the maximum number $f(n, m)$ of subsets of an nm-element set such that all pairwise intersections have size divisible by m? Berlekamp [1] and Graver [14] independently proved that $f(n, 2) = 2^n$ for $n \geqslant 4$. However, for $m \geqslant 3$, $f(n, m)$ is much larger than 2^n, as was shown by Frankl and Odlyzko [13]. However, $\lim f(n, m)^{1/n}$ is unknown.

6. Geometric Groups of Rank 2

Let G be a geometric group of type (L, n), where $|L| = 2$. By deleting fixed points if necessary, we may assume that $0 \in L$; say $L = \{0, m\}$. Then the stabiliser of a point fixes m points, the fixed-point set forming a block of imprimitivity; so m divides n, say $n = km$. If $m = 1$, then G is a sharply 2-transitive group of degree k; all such groups were determined by Zassenhaus [28]. In this section, we present a structure theorem for the general case, and begin the task of determining all geometric groups of rank 2 (i.e., with $|L| = 2$.

The argument will involve examining carefully the structure of such groups which are blow-ups. Accordingly, we begin with a description of these.

Lemma 6.1. *Let G be a geometric group of type $(\{0, m\}, km)$, with $k > 2$. There exists a group which is a blow-up of G of type $(\{0, ms\}, kms)$ if and only if there exists an abelian group R with subgroups $S_1, ..., S_k$ of order s satisfying $S_i \oplus S_j = R$ for $i \neq j$, and an action of G on R with the properties*

(i) *G permutes $S_1, ..., S_k$ among themselves in the same way as it permutes its natural blocks of imprimitivity;*

(ii) *the stabiliser of a point in the ith block acts trivially on R/S_i.*

Proof. First, suppose that $\hat{G}$ is such a blow-up. Then $\hat{G}$ has a system of imprimitivity, with blocks of size s, such that the group induced on the blocks is G, and the kernel R of the action on blocks is a transversal 2-design. Let S_i be the subgroup of R fixing a point in the ith block. Since S_i fixes every point in its orbit, it is a normal subgroup of R. We have $S_i \cap S_j = 1$, and hence $R = S_i \oplus S_j$, for $i \neq j$. Now S_1 centralises S_2 and S_3, and hence centralises $S_2 \oplus S_3 = R$. Similarly S_2 centralises R, and so $R = S_1 \oplus S_2$ is abelian.

Let H and $\hat{H}$ be stabilisers of points in the first block in G and $\hat{G}$, respectively, and H' the preimage of H in $\hat{G}$, so that $H'/R = H$. Since $\hat{H}$ fixes every point of its orbit under R, it is normalised by R, and so $r^{-1}hr \in \hat{H}$ for all $r \in R$, $h \in \hat{H}$. Then $[R, \hat{H}] \leqslant \hat{H} \cap R = S_1$, and H acts trivially on R/S_1.

Conversely, suppose that R, $S_1, ..., S_k$ satisfy the conditions of the lemma. Let $\hat{G}$ be the semidirect product RG, acting on the cosets of $\hat{H} = S_1 H$, where H is the stabiliser of a point in the first block. It is readily checked that the normaliser of $\hat{H}$ in $\hat{G}$ is RK, where $K = N_G(H)$, and that $\hat{H} \cap \hat{H}^g = 1$ for $g \in \hat{G} \setminus RK$; so G is geometric, and is the required blow-up.

Remark 6.2. The proof of the lemma shows that, if any extension of R is a geometric group, then the split extension is geometric. There may be non-split extensions which are geometric too (see Sect. 5, or Tsuzuku [24]).

A geometric group of rank 2 is said to be *deflated* if it is not a blow-up of a smaller geometric group.

THEOREM 6.3. *For given $k \geqslant 2$, there are only finitely many deflated groups of type $(\{0, m\}, km)$; and there are none unless k is a prime power or a prime power plus one.*

Proof. We first recall some facts about subgroups of direct products. Let A_1 and A_2 be groups, N a subgroup of $A_1 \times A_2$. Then there are subgroups B_i, C_i of A_i with $C_i \lhd B_i$ $(i = 1, 2)$, and an isomorphism $\theta: B_1/C_1 \to B_2/C_2$, such that

$$N = \{(g_1, g_2) \in B_1 \times B_2 \mid (C_1 g_1)\theta = C_2 g_2\}.$$

If, moreover, N is a normal subgroup of $A_1 \times A_2$, then B_i and C_i are normal subgroups of A_i $(i = 1, 2)$, and $N/(C_1 \times C_2)$ is in the centre of $(A_1/C_1) \times (A_2/C_2)$; so, in particular, $B_i/C_i \leqslant Z(A_i/C_i)$ for $i = 1, 2$. Finally, if N is also invariant under an automorphism of $A_1 \times A_2$ which interchanges the two direct factors, then A_1/B_1 is isomorphic to A_2/B_2; hence $(A_1 \times A_2)/N$ has a central subgroup, the quotient by which is the direct product of two isomorphic groups. (We call such a group *centre-by-square.*)

Now suppose that G is a *deflated* group of type $(\{0, m\}, km)$. Let $\bar{G}$ be the permutation group induced on the set of k blocks of imprimitivity by G, and N the kernel of the action of G on this set (so that $\bar{G} \cong G/N$). Let H be the subgroup of G fixing two blocks U_1 and U_2. The setwise stabiliser of a block acts regularly on that block; let A_i be the group induded on U_i by its setwise stabiliser.

Then $H \cong A_1 \times A_2$; and $\bar{H}$, the group induced on the set of blocks by H, is a quotient of H, the normal subgroup N being invariant under conjugation by an element of G interchanging the two blocks (and hence the two direct factors). By our remarks above, $\bar{H}$ is centre-by-square.

We now scrutinise the list of 2-transitive groups to find which of them have the property that the stabiliser of two points is centre-by-square. If $\bar{G}$ has a regular normal subgroup, then its degree k is a prime power; if the socle of $\bar{G}$ is PSL(2, q), PSU(3, q), Sz(q), or $R_1(q)$ (in its natural representation), then k is a prime power plus one. For the remaining groups, the only symmetric or alternating groups which can occur have degree at most 5; Sp($2d$, 2), in either 2-transitive representation, is impossible for $d \geqslant 3$; none of the "sporadic" groups can occur; and the socle of $\bar{G}$ cannot be PSL(d, q) with $d \geqslant 4$. There remains only the case when the socle is PSL(3, q), when we find that $\bar{G}$ must be PGL(3, q) (the stabiliser of two points in this group is AGL(1, q) $\times$ AGL(1, q)). For this to occur, AGL(1, q) would have to be quotient of the stabiliser of one point, namely

AGL(2, q), which is only possible if $q=2$ or 3. But both 7 and 13 are primes. (In fact, both PGL(3, 2) and PGL(3, 3) act as geometric groups, of type ($\{0, 2\}$, 14) and ($\{0, 6\}$, 78), resp.—see [3].)

Continuing our analysis, we see that $C_1 \times C_2$ is precisely the set of elements of N whose action on the block U_1 is that of an element of C_1; hence $C_1 \times C_2$ is a normal subgroup of the stabiliser of U_1. Similarly, it is normal in the stabiliser of U_2, and hence in the group which they generate, which is G. Thus G is a blow-up of $G/(C_1 \times C_2)$. Since G is deflated, $C_1 = C_2 = 1$, whence N is semiregular. Furthermore, $|N| \leqslant |A_1| \leqslant |H/N| = |\bar{H}|$; so, for each of the finitely many 2-transitive groups $\bar{G}$ of degree k, there are only finitely many possible deflated groups G. This proves the theorem.

For $k \leqslant 3$, there are geometric groups of type ($\{0, m\}$, km) for all m (the examples in the conclusion of Theorem 5.1). We conclude with two results, one crude and general, the other precise and particular, indicating that examples are rather scarce for $k \geqslant 4$.

THEOREM 6.4. *For any $k \geqslant 4$, the set*

$\{m \mid$ *there is a geometric group of type* ($\{0, m\}$, km)$\}$ *has density zero.*

Proof. By Theorem 6.3, it suffices to show that, if G is a deflated group of type ($\{0, m\}$, km) with $k \geqslant 4$, then the set

$$S = \{s \mid \text{there is a blow-up of } G \text{ of type } (\{0, ms\}, kms)\}$$

has density zero.

Observe first that, if $s \in S$ and $s = tu$ where t and u are coprime, then t, $u \in S$. This is immediate from Lemma 6.1, since the abelian group R of order s^2 is the direct sum of characteristic subgroups of orders t^2 and u^2, each satisfying the conditions of the lemma.

Now we show that, if $k > 3$ and s is a prime in S, then necessarily $s = k$ or $s = k-1$. For G_0 acts on K, of order s^2; and the action is faithful, since a non-identity element moves some subgroup S_i to a disjoint subgroup S_j. So G_0 is a subgroup of $GL(2, s)$. The only 2-transitive groups which are quotients of subgroups of $GL(2, s)$ (where s is prime) are S_2, S_3, A_4, S_4, A_5, AGL(1, s), PSL(2, s), and PGL(2, s). The first two are excluded by the hypothesis $k \geqslant 4$; and A_4 and A_5 occur only as quotients of $SL(2, 3)$ and $SL(2, 5)$, respectively, and so are excluded, since $8 \nmid |G|$ in these cases. If $\bar{G} = S_4$, then there is a set of four 1-dimensional subspaces of $V(2, s)$ (corresponding to the four subgroups S_i) on which the group S_4 is induced. But this is impossible if a $s > 3$, since the s'-part of the stabiliser of a 1-dimensional subspace in GL(2, s) is abelian and cannot involve S_3. Finally, in the last three cases, we have $s = k$ or $k-1$.

So no prime except possibly k or $k-1$ can lie in S; hence no number in S can be divisible by any prime to the first power only, save possibly k or $k-1$. But then S has density at most

$$\prod_{p \neq k, k-1} (1-(p-1)/p^2) = 0.$$

THEOREM 6.5. *A geometric group of type* $(\{0, m\}, 4m)$ *exists if and only if either* $m = 4^d$ *or* $m = 2.3^d$ *for some* $d \geqslant 0$.

Proof. Let G be such a group. Suppose first that G is deflated. The bound in the proof of Theorem 6.3 shows that $m \leqslant 2$; by Tsuzuku's theorem [24], either $m = 1$ and $G = A_4$, or $m = 2$ and $G = \mathrm{GL}(2, 3)$. We consider in turn blow-ups of these two groups.

First, let $G = A_4$, and let R be a G-module affording a blow-up. Set $S = S_1$. The element $a = (1\ 2)(3\ 4)$ of G interchanges S_1 and S_2, and its square acts trivially; so we can represent it by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ over the endomorphism ring of S. Similarly, the element $b = (2\ 3\ 4)$ is represented by $\left(\begin{smallmatrix} 1 & 0 \\ \alpha & \beta \end{smallmatrix}\right)$, where $\alpha, \beta \in \mathrm{End}(S)$. In fact, α and β are automorphisms. (This is clear for β, and follows for α because $S_2 \cap b^{-1}S_2 b = 0$. The 1 in the top left corner reflects (ii) of Lemma 6.1.)

From $b^3 = 1$ we deduce $\beta^2 + \beta + 1 = 0$, while $(ab)^3 = 1$ yields $\alpha\beta = 1$ and $\alpha^2 + \beta = 0$. Then $\alpha^3 = 1$ and $1 + \alpha\beta = 0$, so $1 + 1 = 0$. It follows that α and β generate GF(4), and S is a vector space over this field; so $|S|$ is a power of 4.

Next, suppose that $G = \mathrm{GL}(2, 3)$ and that R affords a blow-up. The central involution z of G is a product of involutions t_1, t_2 fixing points in different blocks (the first and second, say). Then t_1 centralises R/S_1 and normalises S_2; since $R/S_1 \cong S_2$, t_1 centralises S_2. Its centraliser can be no larger, since it interchanges S_3 and S_4. Hence t_1 is fixed-point-free on S_1, which implies that $|S_1|$ is odd, t_1 inverts S_1, and z inverts R.

Suppose that $|S_1|$ is not a power of 3. As in the proof of Theorem 6.4, we can assume that R is an elementary abelian p-group, for some prime $p > 3$. Now the representation of G on R is completely reducible, and the absolutely irreducible representations of G are the same as those in characteristic zero. A brief inspection of the character table of GL(2, 3) shows that there can be no representation in which z acts as -1 while the dimension of the fixed-point space of a subgroup S_3 is at least half the degree.

Finally, we note that the required examples exist. More generally, GL(2, q) possesses a blow-up with $s = q^d$, $d \geqslant 0$. (For $d = 1$, let R be the dual of the natural GL(2, q)-module, with $S_1, \ldots, S_{q+1}$ the 1-dimensional subspaces. In general, take the direct sum of d copies of this module.) Also, AGL(1, q) possesses a blow-up with $s = q^d$, $d \geqslant 0$. (For $d = 1$, take a 2-dimensional GF(q)-space on which the element $x \mapsto a + bx$ of AGL(1, q)

acts as the matrix $\left(\begin{smallmatrix} 1 & 0 \\ a & b \end{smallmatrix}\right)$; in general, take the direct sum of d copies, as before.)

7. Sharp Subsets of Projective Groups

We noted in Section 3 that the elements below any permutation in a permutation geometry form the lattice of flats of a matroid, and that these matroids can be regarded as having the same underlying point set. Furthermore, in the known examples, all these matroids coincide (i.e., the geometry is unisupported [10]), and all the permutations are automorphisms of this matroid. (Both of these conditions hold in the case of a geometric group, see [5].) If this holds, then the automorphism group of the matroid is basis-transitive.

All finite simple basis-transitive matroids are known (see Kantor [18]); they are the free matroids, projective and affine geometries over finite fields, the large Witt designs, the classical unital of order 4, and truncations of all these. So we might look for permutation geometries, or sharp sets, inside the automorphism groups of these examples. In the case of truncations of free matroids, the problem is that of finding sharply t-transitive sets of permutations. For affine geometries, the affine group $\mathrm{AGL}(d, q)$ itself is geometric. We show that, for the projective geometries and the large Witt designs, sharp subsets do not exist, except in the case of projective geometries over GF(2), when the full projective group is geometric. Partial results are obtained for truncations of projective spaces.

For the proof, we require a lemma which has been of some use in another context too, namely the recognition of doubly transitive groups by computer [4].

Lemma 7.1. *The integer f is the number of fixed points of an element of $\mathrm{P\Gamma L}(d, q)$ if and only if, for some r of which q is a power, if f is written to the base r,*

$$f = a_{k-1}r^{k-1} + \cdots + a_1 r + a_0,$$

the digits $a_{k-1}, \ldots, a_1, a_0$ are non-decreasing and have sum at most d. The base r is the order of the fixed field of the field automorphism associated with any such element.

Proof. Let g be any element of $\Gamma\mathrm{L}(d, q)$, acting on the vector space $V = V(d, q)$, and σ the associated field automorphism. Thus we have

$$g(v_1 + v_2) = g(v_1) + g(v_2),$$
$$g(cv) = c^{\sigma} g(v),$$

for all $v_1, v_2, v \in V$ and $c \in F = \mathrm{GF}(q)$. A point $\langle v \rangle$ of $\mathrm{PG}(d-1, q)$ is fixed by g if and only if $g(v) = \lambda v$ for some $\lambda \in F$. Let $K = \mathrm{GF}(r)$ be the fixed field of σ. The set

$$W_\lambda = \{v \in V \mid g(v) = \lambda v\}$$

is a K-subspace of V. Moreover, since

$$g(cv) = c^\sigma g(v) = c^\sigma \lambda v = (c^\sigma/c)\, \lambda cv$$

for $v \in W_\lambda$, we have $cW_\lambda = W_{\lambda c^\sigma/c}$ for all $c \in F$. The set $\{\lambda c^\sigma/c \mid c \in F\}$ is a coset in F^x of the subgroup $\{c^\sigma/c \mid c \in F\}$, of order $(q-1)/(r-1)$; and the union X_λ of all the spaces $W_{\lambda c^\sigma/c}$ is a set of $(r^e-1)/(r-1)$ points of $\mathrm{PG}(d-1, q)$. The entire fixed point set of g is the union of at most $r-1$ such sets, which are linearly independent over F, so the sum of their dimensions is at most d. Thus the number f of fixed points is

$$f = \sum (r^{e_i} - 1)/(r-1),$$

where there are at most $r-1$ terms in the sum, and $\sum e_i \leqslant d$. This is easily seen to be of the form specified in the theorem.

We omit the simple construction which shows that every number of this form occurs as $\mathrm{fix}(g)$ for some $g \in \mathrm{P\Gamma L}(d, q)$.

COROLLARY 7.2. *If the number f of fixed points of an element $g \in \mathrm{P\Gamma L}(d, q)$ satisfies $f \equiv 1 \pmod q$, $f > 1$, then $g \in \mathrm{PGL}(d, q)$ and the fixed-point set of g is a subspace.*

THEOREM 7.3. *Suppose that the subset S of $\mathrm{P\Gamma L}(d, q)$ is of type (L, n), where $n = (q^d-1)/(q-1)$ and $L = \{0, 1, q+1, \ldots, (q^{k-1}-1)/(q-1)\}$, $k > 1$. Then $|S| \leqslant \prod_{l \in L} (n-l)$. If equality holds, then*

(i) *S is geometric;*

(ii) *$q = 2$;*

(iii) *if k is odd, then $d \leqslant \frac{1}{4}(5k+1)$, while if k is even, then $d \leqslant \frac{1}{4}(5k-2)$.*

Remark 7.4. The only known sharp example with $k \neq d$ is $A_7 \leqslant \mathrm{PSL}(4, 2)$, with $k = 3$, $d = 4$; this attains the bound in (iii). As noted earlier, $\mathrm{PSL}(d, 2)$ is itself sharp with $k = d$.

Proof. Let S be such a set. By Corollary 7.2, for any $g, h \in S$, the fixed point set of $g^{-1}h$ is a subspace of dimension at most $k-1$. So, if $g^{-1}h$ fixes k independent points, then $g = h$. Thus $|S|$ is at most the number of

independent k-tuples, which is $\prod_{l \in L} (n-l)$. If equality holds, then S acts sharply transitively on such k-tuples; it follows that S is geometric.

Now suppose that S is sharp. The argument above shows that S is sharply transitive on independent k-tuples. We suppose first that $k = d$.

Let t be any elation in $P\Gamma L(d, q)$ (an element whose fixed point set is a hyperplane), and g any element of S. Choose a basis $x_1, ..., x_d$ such that t fixes $x_1, ..., x_{d-1}$ but not x_d. By basis-transitivity, there exists $h \in S$ such that $h(x_i) = g(t(x_i))$ for $i = 1, ..., d$. Now $g^{-1}h$ fixes $x_1, ..., x_{d-1}$ but not x_d; so $g^{-1}h$ fixes a hyperplane pointwise and is an elation, necessarily t (since the group of elations fixing a given hyperplane pointwise acts sharply transitively on its complement). Thus $gt = h \in S$. So S is closed under right multiplication by all elations, and is a union of left cosets of the group $PSL(d, q)$ generated by the elations. But then S is too large to be sharp, unless $q = 2$.

It follows that $q = 2$ in general. For let H be a $(k-1)$-space, and let $S_0 = \{g \in S \mid g(H) = H\}$, regarded as a set of permutations of the points of H. Clearly S_0 has type (L, n_0), where $n_0 = (q^{k-1})/(q-1)$; and S_0 is sharp, since its size is equal to the number of bases of H.

To complete the proof, we require the following lemmas. The first is due to O'Nan [21] (though O'Nan states a weaker result, this is what he proves).

LEMMA 7.5. *Let G be a group acting transitively on sets X_1 and X_2, having the property that every irreducible constituent of the permutation character of G on X_2 is contained in the permutation character on X_1. Let S be a subset of G which is uniformly transitive on X_1. Then S is uniformly transitive on X_2. In particular, if S is sharply transitive on X_1, then $|X_2|$ divides $|X_1|$.*

(A set S of permutations of X is *uniformly transitive* if $|\{g \in S \mid g(x) = y\}|$ is independent of $x, y \in X$.)

LEMMA 7.6. *Any irreducible constituent of the permutation character of $GL(d, q)$ on k-tuples of nonzero vectors is contained in the permutation character on linearly independent k-tuples of vectors, provided that $k \leqslant d$.*

Proof. Since the stabiliser of an independent r-tuple is a subgroup of the stabiliser of an independent s-tuple for $s \leqslant r$, the permutation character π_s on independent s-tuples is contained in the permutation character π_r on independent r-tuples. Now if π_k^* is the permutation character on k-tuples of nonzero vectors, then

$$\pi_k^* = \sum_{l=0}^{k} \sum_{m=0}^{l} S(k+1, l+1) \begin{bmatrix} l \\ m \end{bmatrix}_q \pi_m$$

(Cameron and Taylor [6]); so every constituent of π_k^* is contained in π_k, as required.

We now conclude the proof of the theorem. Note that the permutation characters of $GL(d, 2)$ on points and hyperplanes are equal; so the character on k-tuples consisting of s points and $t = k - s$ hyperplanes is equal to that on k-tuples of points. Hence, by the Lemma, S is uniformly transitive on any $GL(d, 2)$-orbit consisting of k-tuples of this kind. Take $s = \lfloor \frac{1}{2}k \rfloor$, and let the orbit X consist of k-tuples $(p_1, ..., p_s, H_1, ..., H_t)$ for which $H_1 \cap \cdots \cap H_t$ has codimension t, and $p_1, ..., p_s$ are independent modulo this intersection. Then

$$|X| = ((q^d - 1)/(q-1)) \cdots ((q^d - q^{t-1})/(q-1))\, q^{(d-t)s}$$

divides $((q^d - 1)/(q-1)) \cdots (q^d - q^{s+t-1})/(q-1))$. Considering powers of q, we see that $(d-t)s \leqslant t + (t+1) + \cdots + (t+s-1)$, whence $d \leqslant \frac{1}{2}(4t + s - 1)$, from which the result follows.

We have noted the existence of an example with $d = 4$ and $k = 3$. Here is one small contribution to the nonexistence of larger examples:

PROPOSITION 7.7. *There is no set satisfying the hypotheses of Theorem* 7.3 *with* $k = d - 2$, $d \geqslant 4$.

Proof. A simple modification of the proof of Proposition 2.4 shows that, if S and S' are L- and L'-intersecting subsets of $PGL(d, 2)$, where $L' = \{0, 1, 3, ..., 2^{d-1} - 1\} \setminus L$, then $|S| \cdot |S'| \leqslant |PGL(d, 2)|$. Hence it is enough to find a set S' which is $\{2^{d-2} - 1, 2^{d-1} - 1\}$-intersecting and has size greater than 3.2^{2d-3}. The set S' consisting of the identity and all elations in $PGL(d, 2)$ has these properties—it has size $1 + (2^d - 1)(2^{d-1} - 1)$.

Remark 7.8. A virtually identical argument to that in the proof of the theorem shows the nonexistence of sharply 2-transitive subsets of $PGL(2, q)$ for $q \geqslant 4$ (the group $PSL(2, 3)$ is sharply 2-transitive), or of sharp subsets of $Aut(M_{22})$, M_{23} or M_{24} of types $(\{0, 1, 2, 6\}, 22)$, $(\{0, 1, 2, 3, 7\}, 23)$, or $(\{0, 1, 2, 3, 4, 8\}, 24)$, respectively.

Remark 7.9. At the other end of the spectrum, Lorimer [20] and O'Nan [21] showed that most of the known 2-transitive groups cannot contain sharply 2-transitive subsets.

PROBLEM 7.10. Are there any further examples satisfying the hypotheses of Theorem 7.3 with $k < d$? Also, prove an analogous result for the affine groups $A\Gamma L(d, q)$.

8. Infinite Sharp Groups

The definition of an infinite geometric group is just the same as in the finite case: G is geometric if there is a (finite or infinite) sequence $(x_1, x_2, ...)$ of points such that, for any n, the stabiliser of $x_1, ..., x_{n-1}$ acts transitively on the points it does not fix (and x_n, if it exists, lies in the non-trivial orbit), while only the identity fixes the whole sequence. If the sequence is finite (say $(x_1, ..., x_s)$), and if the stabiliser of $x_1, ..., x_{i-1}$ fixes l_i points (where l_i is finite), then G is a geometric group of type

$$L = \{l_0, ..., l_{s-1}\}.$$

Examples of geometric groups having a finite type are comparatively rare. A sharply t-transitive group is geometric of type $\{0, 1, ..., t-1\}$; examples exist, much as in the finite case, for $t = 1, 2, 3$. Note, however, that it is not necessarily true that the type L is the set of cardinalities of fixed-point sets of non-identity elements. For example, $\mathrm{PGL}(2, \mathbb{C})$ is sharply 3-transitive on the projective line over $\mathbb{C}$, but all its elements fix 1 or 2 points.

An old theorem of Tits [23] and Hall [15] asserts that no infinite sharply t-transitive group exists for $t \geqslant 4$. We can deduce a slightly more general result from a recent theorem of Yoshizawa [27], who showed that for $t \geqslant 4$, there is no t-transitive infinite permutation group in which the stabiliser of t points is finite.

Proposition 8.1. *For $t \geqslant 4$, there is no infinite geometric group of type $\{0, m, 2m, ..., (t-1)m\}$.*

Proof. Such a group has a system of blocks of imprimitivity of size m; it acts t-transitively on the block system, and the stabiliser of t blocks has order at most m^t, since the stabiliser of a point in each block is trivial. Now Yoshizawa's theorem applies.

Although sharply t-transitive groups exist for $t = 2, 3$, it is not possible to find permutation geometries of type $\{0, m\}$ or $\{0, m, 2m\}$ by blowing them up, since the required transversal designs cannot exist.

It is not so clear how to define infinite sharp groups. In fact, we do not have a satisfactory definition. Clearly a definition in terms of order will not suffice. A better approach is based on Proposition 2.2, which asserts that a finite group of type (L, n) is sharp if and only if $\sum a_i m_i = 1$, where

$$f(x) = \prod_{i=0}^{s-1} (x - l_i) = \sum_{i=0}^{s} a_i x^i,$$

and m_i is the number of orbits of G on ordered i-tuples for $i = 1, ..., s$, with $m_0 = 1$.

The quantity $d = \sum_{i=0}^{s} a_i m_i$ is well defined for any infinite permutation group for which the number of fixed points of any non-identity element lies in the set L and the number of orbits on ordered s-tuples is finite. It would then be natural to call such a group *sharp* if $d = 1$. One piece of evidence supports this:

PROPOSITION 8.2. *With the above notation, if G is geometric of type L then $\sum_{i=0}^{s} a_i m_i = 1$.*

Proof. Let H be the group induced on a hyperplane by its setwise stabiliser. Then $f(\pi(h)) = 0$ for all $h \in H$, so $\sum_{i=0}^{s} a_i m_i(H) = 0$. But $m_i(G) = m_i(H)$ for $i < s$, and $m_s(G) = m_s(H) + 1$, since any i-tuple for $i \leqslant t$ either is a basis or is contained in a hyperplane, and G is basis-transitive. So $\sum_{i=0}^{s} a_i m_i(G) = 1$.

The unsatisfactory feature is that, for infinite groups, it is no longer true that $d > 0$. For example, let $G = \mathrm{PGU}(2, \mathbb{C})$, acting on the projective line over $\mathbb{C}$. Any element of $\mathrm{GU}(2, \mathbb{C})$ is diagonalizable and (if not a scalar) has distinct eigenvalues, so a non-identity element of G fixes exactly two points. But G is transitive, and so with $L = \{2\}$ we have

$$\sum_{i=0}^{s} a_i m_i = -1.$$

Note added in proof. It has been pointed out to us that Theorem 1.1, which we attribute to Kiyota, was proved by H. F. Blichfeldt, *Trans. Amer. Math. Soc.* **5** (1904), 461–466.—The determination of geometric groups of rank z has been completed by T. Maund (to appear).

REFERENCES

1. E. R. BERLEKAMP, On subsets with intersections of even cardinality, *Canad. Math. Bull.* **12** (1969), 363–366.
2. E. BANNAI AND T. ITO, "Algebraic Combinatorics," Benjamin–Cummings, New York, 1984.
3. L. BABAI, P. J. CAMERON, M. DEZA, AND N. M. SINGHI, On sharply edge-transitive permutation groups, *J. Algebra* **73** (1981), 573–585.
4. P. J. CAMERON AND J. J. CANNON, Recognising S_n and A_n, in preparation.
5. P. J. CAMERON AND M. DEZA, On permutation geometries, *J. London Math. Soc.* (2) **20** (1979), 373–386.
6. P. J. CAMERON AND D. E. TAYLOR, Stirling numbers and affine equivalence, *Utilitas Math.*, in press.
7. M. DEZA, Some new generalizations of sharply t-transitive groups and sets, *Ann. Discrete Math.* **18** (1983), 295–314.
8. M. DEZA AND P. FRANKL, On the maximum number of permutations with given maximal or minimal distance, *J. Combin. Theory Ser. A* **22** (1977), 352–360.

9. M. DEZA AND P. FRANKL, Injection geometries, *J. Combin. Theory Ser. B* **37** (1984), 31–40.
10. M. DEZA AND M. LAURENT, Bouquets of matroids, d-injection geometries and diagrams, submitted.
11. M. DEZA AND S. A. VANSTONE, Bounds for permutation arrays, *J. Statist. Plann. Inference* **2** (1978), 197–209.
12. P. FRANKL AND A. M. ODLYZKO, On subsets with cardinalities of intersections divisible by a fixed integer, *Europ. J. Combin.* **4** (1983), 215–220.
13. P. FRANKL AND R. M. WILSON, Intersection theorems with geometric consequences, *Combinatorica* **1** (1981), 357–368.
14. J. E. GRAVER, Boolean designs and self-dual matroids, *Linear Algebra Appl.* **10** (1975), 111–128.
15. M. HALL JR., On a theorem of Jordan, *Pacific J. Math.* **4** (1954), 219–226.
16. T. ITO AND M. KIYOTA, Sharp permutation groups, *J. Math. Soc. Japan* **33** (1981), 435–444.
17. W. M. KANTOR, 2-transitive designs, Combinatorics (M. Hall Jr. and J. H. van Lint, Eds.), pp. 365–418, Math. Centre Tractsa, Amsterdam, 1975.
18. W. M. KANTOR, Homogeneous designs and geometric lattices, *J. Combin. Theory Ser. A* **38** (1985), 66–74.
19. M. KIYOTA, An inequality for finite permutation groups, *J. Combin. Theory Ser. A* **27** (1979), 119.
20. P. J. LORIMER, Finite projective planes and sharply 2-transitive subsets of finite groups, *in* "Lecture Notes in Math.," No. 372, pp. 432–436, Springer–Verlag, Berlin/Heidelberg/New York, 1974.
21. M. E. O'NAN, Sharply 2-transitive sets of permutations, "Proceddings of the Rutgers Group Theory Year, 1983–1984" (M. Aschbacher *et al.*, Eds.), pp. 63–67, Cambridge Univ. Press, Cambridge, 1985.
22. D. K. RAY-CHAUDHURI AND R. M. WILSON, On t-designs, *Osaka J. Math.* **12** (1975), 737–744.
23. J. TITS, Généralisation des groupes projectifs basée sur leurs propriétés de transitivité, *Acad. Roy. Belg. Cl. Sci. em.* **27** (1952).
24. T. TSUZUKU, On multiple transitivity of permutation groups, *Nagoya Math. J.* **18** (1961), 93–109.
25. H. WIELANDT, "Finite Permutation Groups," Academic Press, New York, 1964.
26. R. M. WILSON, Concerning the number of mutually orthogonal Latin squares, *Discrete Math.* **9** (1974), 181–198.
27. M. YOSHIZAWA, On infinite four-transitive permutation groups, *J. London Math. Soc.* (2) **19** (1979), 437–438.
28. H. ZASSENHAUS, Über endliche Fastkörper, *Abh. Math. Sem. Hamburg* **11** (1935), 187–220.