COMBINATORICA
Akadémiai Kiadó — Springer-Verlag

COMBINATORICA 8 (3) (1988) 249—260

INTERSECTION THEOREMS IN PERMUTATION GROUPS

P. J. CAMERON, M. DEZA and P. FRANKL

Received April 14, 1987

The Hamming distance between two permutations of a finite set X is the number of elements of X on which they differ. In the first part of this paper, we consider bounds for the cardinality of a subset (or subgroup) of a permutation group P on X with prescribed distances between its elements. In the second part. We consider similar results for sets of s-tuples of permutations; the role of Hamming distance is played by the number of elements of X on which, for some i, the ith permutations of the two tuples differ.

1. In the symmetric group

Suppose that X is a finite set with $|X|=n$, and P is a permutation group on X. The Hamming metric is defined on P by

$$d(\pi,\varrho)=\left|\{x\in X:\ \pi(x)\neq\varrho(x)\}\right|$$

for $\pi,\varrho\in P$. Clearly, $n-d(\pi,\varrho)$ is the size of the intersection of π and ϱ, or more exactly, the number of places where π and ϱ coincide; in other words, the number of fixed points of $\pi^{-1}\varrho$. For a set R of permutations, let us define the *type* $d(R)$ of R by

$$d(R)=\{d(\pi,\varrho):\ \pi\varrho\in R,\ \pi\neq\varrho\}.$$

Note that, if R is a group, then

$$d(R)=\{d(1,\varrho):\ \varrho\in R,\ \varrho\neq 1\}.$$

For a fixed subset D of $\{2,3,\dots,n\}$, let $m(n,D,P)$ denote the maximum size of a subset R of P satisfying $d(R)\subseteq D$. (Note that no two permutations have Hamming distance 1.) Analogously, $m_g(n,D,P)$ is the maximal size of a subgroup R of P with $d(R)\subseteq D$.

The function $m(n,D,P)$ was first investigated (in special cases) in [6]; see [3] for a general upper bound for $m(n,D,S_n)$ in terms of n and $|D|$. For $m_g(n,D,P)$, the best general bound is the following theorem of Blichfeldt [1] (see also Kiyota [10]):

Theorem 1.1.

$$m_g(n,D,P)\leqq\prod_{d\in D}d. \tag{1}$$

AMS subject classification (1980): 20B99

A group R satisfying equality in (1) is called a *sharp group.*

For some triples (n, D, P), it can be shown that $m(n, D, P) \leqq \prod_{d \in D} d$. It is an interesting and seemingly difficult problem to decide exactly when this occurs. The simplest such case is the "packing case", when $D = \{n-t+1, n-t+2, ..., n\}$; that is, we require that no two permutations agree in t positions.

Proposition 1.2. *Suppose that* $D = \{n-t+1, ..., n\}$. *Then*

(2) $$m(n, D, P) \leqq \prod_{d \in D} d = n(n-1)...(n-t+1).$$

Proof. Suppose that $R \subseteqq P$, $d(R) \subseteqq D$. Then, for all distinct $\pi, \varrho \in R$, the sequences $(\pi(1), \pi(2), ..., \pi(t))$ and $(\varrho(1), \varrho(2), ..., \varrho(t))$ are distinct. Since the terms of such a sequence are distinct members of X, the number of such sequences is at most the right-hand side of (2).

A set realizing equality in (2) is called *sharply t-transitive.*

Another simple observation is the following.

Proposition 1.3. *Suppose that* $D_1, D_2 \subseteqq \{2, 3, ..., n\}$. *Then we have*

(3) $$m(n, D_1, P)m(n, D_2, P) \leqq |P| m(n, D_1 \cap D_2, P).$$

Proof. Suppose that $R_i \subseteqq P$ satisfies $d(R_i) \subseteqq D_i$ for $i=1, 2$. We claim that for each $\pi \in P$, the equation $\pi = \varrho_1 \varrho_2$ has at most $m(n, D_1 \cap D_2, P)$ solutions with $\varrho_i \in R_i$ for $i=1, 2$. This clearly implies that $|R_1||R_2| \leqq |P| m(n, D_1 \cap D_2, P)$, and thus (3).

To prove the claim, observe that, if $\varrho_1^{(j)} \varrho_2^{(j)} = \pi$ for $j = 1, ..., m$, then

$$d(\varrho_1^{(j)}, \varrho_1^{(k)}) = d(\varrho_2^{(j)}, \varrho_2^{(k)}) \in D_1 \cap D_2$$

for all $j \neq k$; so $\varrho_1^{(1)}, ..., \varrho_1^{(m)}$ has type $D_1 \cap D_2$.

Corollary 1.4. *Suppose that P contains a sharply t-transitive set. Then we have*

(4) $$m(n, \{2, 3, ..., n-t\}, P) = |P|/n(n-1)...(n-t+1).$$

Equality holds, for example, for the stabilizer of t elements of X.

Remark. Corollary 1.4 clearly implies Proposition 1.2. In the other direction, Corollary 1.4 was used in [6] to show that

$$m(n, \{2, 3, ..., n-t\}, S_n) = (n-t)!$$

in the cases

(a) $t=1$, all n;

(b) $t=2$, n a prime power;

(c) $t=3$, $n=q+1$, q a prime power.

(Sharply t-transitive groups are known in these cases.)

Conjecture 1.5 [6]. For $n \geqq n_0(t)$, one has $m(n, \{2, 3, ..., n-t\}, S_n) = (n-t)!$.

Let us remark that to prove the conjecture in the case $t=2$ for any further value of n by using Corollary 1.4 would amount to proving the existence of a projective plane of non-prime-power order; a different method of proof will clearly be necessary in general!

In the case $t=1$, to use Corollary 1.4 it is necessary that P be transitive. However, many transitive groups don't contain sharply transitive subsets. Let us give an example where (4) fails (with $t=1$).

Example 1.6. Consider the permutation group $P \cong A_4$ of degree 6, on the cosets of a subgroup of order 2; P is generated by $(1, 2)(3, 4)$ and $(1, 3, 5)(2, 4, 6)$. The upper bound for $m(6, \{2, 3, 4, 5\}, P)=m(6, \{4\}, P)$ given by (4), were it applicable, would be 2; but the subgroup of P of order 4 has type $\{4\}$.

A necessary condition for a permutation group to contain a sharply transitive subset is given by the following theorem of O'Nan [11].

Theorem 1.7. *Let P be a transitive permutation group on X, with $|X|=n$. Suppose that Y is another set on which P acts transitively, with $|Y|=m$, such that every irreducible constituent of the permutation character of P on Y is contained in its permutation character on X. If P (on X) contains a sharply transitive subset, then m divides n.*

In Example 1.6, we can take Y to be the set of four points affording the usual representation of A_4 (the cosets of a subgroup of order 3).

There is an obvious analogy between Conjecture 1.5 and the Erdős—Ko—Rado theorem [9], which states that, if $\mathscr{F}$ is a family of k-element sets of X satisfying $|F \cap F'| \geqq t$ for all $F, F' \in \mathscr{F}$, then $|\mathscr{F}| \leqq \binom{n-t}{k-t}$ holds provided that $n \geqq n_0(k, t)$.

For $Y \subseteqq X$, $|Y|=r$, define

$$\mathscr{G}(Y) = \{F \subseteqq X\colon\ |F| = k,\ F \cap Y \neq \emptyset\}.$$

Then no $r+1$ sets of $\mathscr{G}(Y)$ can be pairwise disjoint. An old theorem of Erdős [8] states that, for $n \geqq n_0(k, r)$, every family $\mathscr{F}$ of k-element sets satisfying $|\mathscr{F}| > |\mathscr{G}(Y)|$ contains $r+1$ pairwise disjoint members. This, too, has an analogue for permutations:

Theorem 1.8. *Suppose that P contains a sharply t-transitive subset. Let $R \subseteqq P$ have the property that, among any $r+1$ members of R, two coincide in at least t places. Then we have*

(5) $$|R| \leqq \min r,\ n(n-1)\dots(n-t+1)P/n(n-1)\dots(n-t+1).$$

Proof. Let $S \subseteqq P$ be sharply t-transitive. In the same way as in the proof of Proposition 1.3, no element of P can be represented in more than $\min\{r, |S|\}$ ways as a product $\varrho\sigma$ with $\varrho \in R$, $\sigma \in S$. ∎

Corollary 1.9. *Suppose that $R \subseteqq S_n$ and R contains no $r+1$ pairwise disjoint permutations. Then we have $|R| \leqq r(n-1)!$.*

Let us remark that the bound (5) is best possible. More generally, any t-transitive group P contains a set R satisfying the hypothesis of Theorem 1.8, whose cardinality attains the bound (5). This is trivial if $r \geqq n(n-1)\dots(n-t+1)$; otherwise, choose $(r+1)$ t-tuples of distinct elements, say $(x_1^{(i)}, \dots, x_t^{(i)})$, $i=0, \dots, r$, and set

$$R = \{\pi \in P\colon\ \exists i \in \{1, \dots, r\}$$

with

$$\pi(x_j^{(0)}) = x_j^{(i)} \quad \text{for} \quad j = 1, \dots, t\}.$$

We *conjecture* that Theorem 1.8 is valid for $P=S_n$ if the hypothesis on the existence of a sharply t-transitive subset is replaced by the hypothesis $n \geqq n_0(r, t)$. Furthermore, the above example should be the only extremal one.

2. In powers of the symmetric group

A permutation $\pi \in S_n$ can be regarded as an n-element subset $A(\pi) = \{(i, \pi(i)) \colon i \in X\}$ of X^2; it is transversal both to the rows and to the columns of X^2. Similarly, if

$$\bar{\pi} = (\pi_1, \dots, \pi_s) \in S_n \times \dots \times S_n \quad (s \text{ factors}),$$

we may regard $\bar{\pi}$ as a subset

$$A(\bar{\pi}) = \{(i, \pi_1(i), \dots, \pi_s(i)) \colon i \in X\}$$

of X^{s-1}, which is a transversal to each "coordinate hyperplane"

$$C(j, x) = \{(x_0, \dots, x_s) \colon x_j = x\}.$$

The $(n!)^s$ sets $A(\bar{\pi})$ are called *diagonals;* a subset of a diagonal is called a *partial diagonal* or *injective set.*

One can define the distance between $\bar{\pi}, \bar{\varrho} \in S_n^s$ by

$$d(\bar{\pi}, \bar{\varrho}) = n - |A(\bar{\pi}) \cap A(\bar{\varrho})|.$$

Note that $|A(\bar{\pi}) \cap A(\bar{\varrho})|$ is equal to the number of common fixed points of the permutations $\pi_1^{-1}\varrho_1, \dots, \pi_s^{-1}\varrho_s$. The *type* $d(R)$ of a subset R of a group $P \leqq S_n^s$, and the functions $m(n, D, P)$ and $m_g(n, D, P)$, are defined by analogy with the case $s=1$. The value of s should be clear from the representation of $P \leqq S_n^s$.

Before considering these functions, there is one point that must be discussed. The identification of a diagonal of X^{s+1} with an s-tuple of permutations depend on the choice of a distinguished coordinate of X^{s+1} (the 0^{th} coordinate, in our definition). A different choice obviously doesn't affect distances; but it can convert a subgroup of S_n^s into a subset which is not a group. We call this process *translation.* More precisely, for $\bar{\pi} \in S_n^s$ and $1 \leqq j \leqq s$, we define $T_j(\bar{\pi})$ to be the element $(\varrho_1, \dots, \varrho_s)$ for which

$$A(\bar{\pi}) = \{(\varrho_1(i), \dots, \varrho_j(i), i, \varrho_{j+1}(i), \dots) \colon i \in X\}.$$

In the case $s=1$, the unique translation T_1 replaces a permutation by its inverse, since $\{(i, \pi(i) \colon i \in X\} = \{(\pi^{-1}(i), i) \colon i \in X\}$. So a translate of a subgroup is necessarily a subgroup. We give conditions for this to hold in general. Note that, if $T_1(\bar{\pi}) = \bar{\varrho}$, then $\varrho_1 = \pi_1^{-1}$ and $\varrho_k = \pi_k \pi_1^{-1}$ for $k > 1$.

Proposition 2.1. *Let G be a subgroup of S_n^s, and let $\varphi_1, \dots, \varphi_s$ be the projections of G onto the factors of S_n^s. Then the following are equivalent:*

(i) *$T_1(G)$ is also a subgroup of S_n^s;*

(ii) *G is normalized by* $\operatorname{diag}(\varphi_1(G))$, *where* $\operatorname{diag}(P) = \{(\pi, \pi, \dots, \pi) \colon \pi \in P\}$.

Proof. Suppose that (i) holds. Let ψ_i be the function mapping an element $\bar{\pi}\in G$ to the i^{th} projection of $T_1(\bar{\pi})$, and $*$ the group operation on G defined by

$$T_1(\bar{\pi}*\bar{\varrho}) = T_1(\bar{\pi})T_1(\bar{\varrho}) \quad \text{for} \quad \bar{\pi}, \bar{\varrho}\in G.$$

We have $\psi_1(\bar{\pi})=\varphi_1(\bar{\pi})^{-1}$ and

$$\psi_i(\bar{\pi}) = \varphi_i(\bar{\pi})\varphi_1(\bar{\pi})^{-1} \quad \text{for} \quad i \geqq 2.$$

Now $\psi_1, \dots, \psi_s$ are homomorphisms of $(G, *)$. So

$$\begin{aligned}\varphi_1(\bar{\pi}^{-1}\bar{\varrho}^{-1}) &= \varphi_1(\bar{\pi})^{-1}\varphi_1(\bar{\varrho})^{-1}\\ &= \psi_1(\bar{\pi})\psi_1(\bar{\varrho})\\ &= \psi_1(\bar{\pi}*\bar{\varrho})\\ &= \varphi_1(\bar{\pi}*\bar{\varrho})^{-1},\end{aligned}$$

so

(6) $$\varphi_1(\bar{\pi}*\bar{\varrho}) = \varphi_1(\bar{\varrho}\cdot\bar{\pi}).$$

Also, for $i>1$,

$$\begin{aligned}\varphi_i(\bar{\pi}*\bar{\varrho})\varphi_1(\bar{\varrho}\bar{\pi})^{-1} &= \varphi_i(\bar{\pi}*\bar{\varrho})\varphi_1(\bar{\pi}*\bar{\varrho})^{-1}\\ &= \psi_i(\bar{\pi}*\bar{\varrho})\\ &= \psi_i(\bar{\pi})\psi_i(\bar{\varrho})\\ &= \varphi_i(\bar{\pi})\varphi_1(\pi)^{-1}\varphi_i(\bar{\varrho})\varphi_1(\varrho)^{-1},\end{aligned}$$

so

(7) $$\varphi_i(\bar{\pi}*\bar{\varrho}) = \varphi_i(\bar{\pi})\varphi_1(\bar{\pi})^{-1}\varphi_i(\bar{\varrho})\varphi_1(\bar{\pi}).$$

By (6), this holds also for $i=1$. Now $\varphi_i(\bar{\pi}^{-1}\cdot(\bar{\pi}*\bar{\varrho}))=\varphi_i(\varrho)^{\varphi_1(\bar{\pi})}$, so the conjugate of $\bar{\varrho}$ by $\varphi_1(\bar{\pi})$ is $\bar{\pi}^{-1}\cdot(\bar{\pi}*\bar{\varrho})$, which is also in G, proving (ii).

Conversely, if (ii) holds, define $\bar{\pi}*\bar{\varrho}=\bar{\pi}\cdot\bar{\varrho}^{\varphi_1(\bar{\pi})}$. Then $\psi_1, \dots, \psi_s$ are homomorphisms of $(G, *)$; the intersection of their kernels is the identity, so $(G, *)$ is a group, isomorphic to a subgroup of the direct product of its projections.

In view of this, we could define $m_G(n, D, P)=\max\{|R|: d(R)\subseteq D,\ T_i(R)\leqq P$ for all $i\}$. Then, clearly, $m_G(n, D, P)\leqq m_g(n, D, P)\leqq m(n, D, P)$. However, we have no further information about the function m_G.

Problem 2.2. Suppose that R is a subgroup of S_n^s of type D. Is it necessarily the case that

(8) $$|R| \leqq (\prod_{d\in D} d)^s?$$

In the case $s=1$, (8) is simply Blichfeldt's bound (1).

For $D=n-t+1, \dots, n$, one can prove (8) in the same way as (2). Sets realizing equality are again called *sharply t-transitive*. Proposition 1.3, Corollary 1.4, and Theorem 1.8 extend to general s with essentially the same proofs.

The proof of (1) actually shows that $m_g(n, D, P)$ divides $\prod_{d\in D} d$. This is not true in general for $s\geqq 2$:

Example 2.3. Let G be a group of order $n-1$, and let φ_1, φ_2 be two embeddings of G into S_n so that $\varphi_i(G)$ fixes i and acts regularly on the other points for $i=1,2$. Now $P=\{(\varphi_1(\pi), \varphi_2(\pi)) \colon \pi\in G\}$ has type $\{n\}$, but $|P|=n-1\nmid n^2$.

We can prove (8) only under a very restrictive hypothesis, by following Kiyota's proof of (1).

Theorem 2.4. *Suppose that $R\leqq S_n^s$ and R has type D. Suppose further that, for every $(\pi_1, \dots, \pi_s)\in R$, there is some i $(1\leqq i\leqq s)$ with $d(1, \pi_i)\in D$. Then $|R|$ divides $(\prod_{d\in D} d)^s$.*

Proof. Consider the function $f\colon R\to\mathbf{C}$ defined by

$$f(\bar\pi) = \prod_{d\in D}\prod_{1\leqq i\leqq s} (d-d(1,\pi_i)).$$

Clearly $f(\bar\pi)$ is a product of generalized characters of R, whence a generalied character. Consequently, $(f(\bar\pi), 1_R)$ is an integer. However,

$$\begin{aligned}(f(\bar\pi), 1_R) &= \Big(\sum_{\bar\pi\in R} f(\bar\pi)\Big)/|R| \\ &= f(1)/R \\ &= \Big(\sum_{d\in D} d\Big)^S/R,\end{aligned}$$

since $f(\bar\pi)=0$ for $\bar\pi\neq 1$.

A group realising equality in (8) is called *sharp*. Extending the usual notion of a geometric group in the case $s=1$ [2], M. Laurent (personal communication) made the following definition. A sharp group $R\leqq S_n^s$ of type D is called *geometric* if, for all $l\geqq 2$ and all $\bar\varrho_1, \dots, \bar\varrho_l\in R$, $n-|F(\bar\varrho_1)\cap\dots\cap F(\bar\varrho_l)|\in D$ holds. For convenience, we set $L=\{n-d\colon d\in D\}=\{l_0, \dots, l_{t-1}\}$ with $l_0<\dots<l_{t-1}$. For $\bar\varrho_1, \dots, \bar\varrho_l\in R$ with $\bar\varrho_i=(\varrho_i^{(1)}, \dots, \varrho_i^{(s)})$, define $A(\bar\varrho_1\cap\dots\cap\bar\varrho_l)=\{(i, \varrho_1^{(1)}(i), \dots, \varrho_1^{(s)}(i))\colon \bar\varrho_1(i)=\dots=\bar\varrho_l(i)\}$, and let $\mathscr{A}_R=\{A(\bar\varrho_1\cap\dots\cap\bar\varrho_l)\colon l\geqq 1,\ \bar\varrho_1, \dots, \bar\varrho_l\in R\}$. Then $\mathscr{A}_R$ is obviously a meet semilattice in which all maximal sets have cardinality n. Now a sharp group $R\leqq S_n^s$ is geometric if and only if $\mathscr{A}_R$ is the family of flats of an injection design [7]; in other words, for $0\leqq i<t$ and every $A\in\mathscr{A}_R$ with $|A|=l_i$, and every $x\in X^s$ such that $A\cup\{x\}$ is injective, there is a unique $A'\in\mathscr{A}_R$ with $|A'|=l_{i+1}$ and $A\cup\{x\}\subseteqq A'$. (We set $l_t=n$.)

Suppose that R is geometric. For every $\bar\varrho\in R$, the interval $\{A\in\mathscr{A}_R\colon A\subseteqq A(\bar\varrho)\}$ is the family of flats of a perfect matroid design (PMD, for short), and all these PMDs have the same projection onto the 0^{th} coordinate. Let $\mathscr{M}_R$ be this common projection.

Theorem 2.5. *Suppose that $R_i\leqq S_n^{s_i}$ is a sharp group of type D for $i=1,2$. Then $R_1\times R_2\leqq S_n^{s_1+s_2}$ is sharp if and only if both R_1 and R_2 are geometric and $\mathscr{M}_{R_1}=\mathscr{M}_{R_2}$. In this case, $R_1\times R_2$ is geometric as well.*

Proof. Suppose that $R_1\times R_2$ is sharp, and let $\bar 1$ be the identity of this group. We apply induction on n, the case $n=1$ being trivial. For $n>1$, we distinguish two cases:

(a) $n\notin D$.

Set $l_0=\min\{n-d\colon d\in D\}$, so $l_0\geqq 1$. Since R_i is sharp, we can find $\bar\pi_i\in R_i$ with $|A(\bar\pi_i\cap\bar 1_i)|=l_0$ for $i=1,2$. We claim that $A(\bar 1\cap(\bar\pi_1,\bar 1_2))=A(\bar 1\cap(\bar 1_1,\bar\pi_2))$, and moreover this set is contained in $A(\bar\varrho_i)$ for all $\bar\varrho_i\in R_i$, $i=1,2$. Indeed, $R_1\times R_2$ has type D by assumption, so $|A(\bar 1\cap(\bar\varrho_1,\bar\varrho_2))|\geqq l_0$ for all $(\bar\varrho_1,\bar\varrho_2)\in R_1\times R_2$.

Thus we have an l_0-element set $Y\subseteq X$ fixed pointwise by both R_1 and R_2. Thus we may consider R_1 and R_2 as subgroups of $S_{n-l_0}^{s_1}$ and $S_{n-l_0}^{s_2}$ respectively, and the statement follows by induction.

(b) $n\in D$.

For every $x\in X$, the stabilisers $R_i(x)$ are sharp of type $D\setminus\{n\}$. The stabiliser of x in $R_1\times R_2$ is $R_1(x)\times R_2(x)$, and is also sharp. By induction, $R_1(x)$ and $R_2(x)$, are geometric and $\mathcal{M}_{R_1(x)}=\mathcal{M}_{R_2(x)}$. The result follows.

The converse, and the final assertion, are checked easily.

The existence question for geometric groups with specified type reduces to the case $s=1$, in view of the following result.

Theorem 2.6. *A geometric subgroup of S_n^s of type D exists for some value of s if and only if such a group exists for $s=1$.*

Proof. If $P\leqq S_n$ is geometric of type D, then so is $P^s\leqq S_m^s$, by Theorem 2.5.

Conversely, suppose that $G\leqq S_n^s$ is geometric of type D, and let $\mathcal{M}=\mathcal{M}_G$ be the matroid supporting G; that is, for any $\bar\pi_1,\ldots,\bar\pi_l\in G$, $F(\bar\pi_1)\cap\ldots\cap F(\bar\pi_l)$ is a flat of $\mathcal{M}$, and every flat of $\mathcal{M}$ is of this form. The number of (ordered) bases of $\mathcal{M}$ is $\prod_{d\in D} d$; so $|G|$ is the number of s-tuples of bases. It follows by an easy induction from the definition of an injection geometry that, if $\beta_0,\ldots,\beta_s$ are bases, there is a unique $\bar\pi=(\pi_1,\ldots,\pi_s)\in G$ with $\pi_i(\beta_0)=\beta_i$ for $i=1,\ldots,s$. Hence, in the action of G on $(X^t)^s$, where $t=|D|$, the orbit of $(\beta_0,\ldots,\beta_0)$ contains $(\beta_1,\ldots,\beta_s)$. Consideration of order shows that this orbit consists precisely of all s-tuples of bases.

It follows that, for any $\bar\pi=(\pi_1,\ldots,\pi_s)\in G$ and any basis β of $\mathcal{M}$, $\pi_i(\beta)$ is a basis for $i=1,\ldots,s$. Since $\mathcal{M}$ is determined by its bases, all projections of G consist of automorphisms of $\mathcal{M}$.

Now let β be a basis, and set $P=\{\pi\in S_n\colon \exists\bar\pi=(\pi_1,\ldots,\pi_s)\in G$ with $\pi_1=\pi$ and $\pi_i(\beta)=\beta$ for $i>1\}$. Then $P\leqq\mathrm{Aut}(\mathcal{M})$, and P is sharply transitive on bases of $\mathcal{M}$. If γ is an independent set contained in β, and $\pi\in P$ fixes γ, then $\gamma\subseteq\bigcap_{1\leqq i\leqq s}F(\pi_i)$; since the set on the right is a flat, we have

$$\langle\gamma\rangle\subseteq\bigcap_{1\leqq i\leqq s}F(\pi_i),$$

and so $\pi=\pi_1$ fixes $\langle\gamma\rangle$ pointwise. By transitivity, the fixedpoint set of any element of P is a flat, and so P is geometric with $\mathcal{M}_P=\mathcal{M}$.

We remark that T. Maund (personal communication) has completed the determination of pairs (n,D) for which geometric groups exist.

Theorem 2.6 does not assert that G is the direct product of its projections, nor that the projections are geometric. The following examples show that this can fail.

Example 2.7. (a) ($D=\{n\}$.) A geometric group of type $\{n\}$, with $s=2$, is simply a group G of order n^2 with two subgroups H_1, H_2 of order n such that $H_1\cap H_2=\{1\}$; we embed G in S_n^2 by means of its permutation representations on the cosets of H_1

and H_2. Let P be any group of order n,

$$G = P \times P, \quad H_1 = \{(1, \pi)\colon \pi \in P\}, \quad \text{and} \quad H_2 = \{(\pi, \pi)\colon \pi \in P\}.$$

Then the above conditions hold; but, if P is non-abelian, then H_2 is not a normal subgroup of G, and so G is not the direct product of two regular groups. Moreover, if P admits a fixedpoint-free automorphism θ, then take instead $H_1 = \{(\pi, \theta(\pi))\colon \pi \in P\}$, H_2 as before, to obtain an example where neither projection is regular. We can extend this to an arbitrary $s \geqq 2$ by choosing, for example, $G = P^s$, and

$$H_1 = \{(\pi_1, \ldots, \pi_s) \in P^S\colon \pi_2 = \theta(\pi_1)\} \quad \text{and}$$
$$H_i = \{(\pi_1, \ldots, \pi_s) \in P^S\colon \pi_i = \pi_{i-1}\} \quad \text{for} \quad i > 1.$$

(b) $(D = \{n-2, n-1, n\}.)$ Let us consider the 3-transitive permutation group PGL (2, 9). It contains two sharply 3-transitive subgroups of order 2, namely PGL (2, 9) and M_{10}; theis intersection is PSL (2, 9), which has index 2 in each of them. Let $\alpha \in \mathrm{PGL}(2, 9) \setminus \mathrm{PSL}(2, 9)$ and $\beta \in M_{10} \setminus \mathrm{PSL}(2, 9)$. Consider the following subgroup of the direct product $\mathrm{PGL}(2, 9) \times \mathrm{PGL}(2, 9)$:

$$G = \langle \mathrm{PSL}(2, 9) \times \mathrm{PSL}(2, 9),\ (\alpha, \beta),\ (\beta, \alpha\beta) \rangle.$$

It is not hard to see that G is sharply 3-transitive on $\{1, \ldots, 10\}^2$ but is not a direct product (even as an abstract group). This example can easily be generalised, both replacing 9 by q^2 for any odd prime power q, and replacing the number of factors by any $s \geqq 2$. (The example given depends on the fact that the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ over GF (2) has irreducible characteristic polynomial and so acts indecomposably on GF $(2)^2$. Replace it with a matrix of order s having the same property.)

In spite of this example, there are situations in which we can show that sharp groups must be direct products.

Theorem 2.8. *Suppose that $G \leqq S_n^s$ is sharply t-transitive. Assume that either*

(a) *no sharply t-transitive group of degree n has a nontrivial permutation representation of degree $n-t$ or smaller; or*

(b) *no proper supergroup of a sharply t-transitive group of degree n has order dividing $(n(n-1)\ldots(n-t+1))^s$. Then G is the direct product of its projections.*

Proof. As in the proof of Theorem 2.6, for each j with $1 \leqq j \leqq s$, consider the group $H_j = \{(\pi_1, \ldots, \pi_s) \in G\colon \pi_l(i) = i \text{ for } 1 \leqq i \leqq t,\ 1 \leqq l \leqq s,\ l \neq j\}$. Clearly $\varphi_j(H_j)$ is sharply t-transitive, where φ_j is the j^{th} projection.

If hypothesis (a) holds, then H_j has no non-trivial representation of degree less than $n-t+1$, so $\varphi_l(H_j) = 1$ for all $l \neq j$. Thus the subgroup of G generated by $H_1, \ldots, H_s$ is simply their direct product, and is equal to G (comparing orders).

If hypothesis (b) holds, then $\varphi_j(G) = H_j$, so G is a subdirect product of $H_1, \ldots, H_s$, again their direct product (by comparing orders).

Corollary 2.9. *Suppose that $G \leqq S_n^s$ is sharply t-transitive. Then G is the direct product of its projections in each of the following cases:*

(a) $t \geqq 4$;

(b) $t = 3$, *n odd;*

(c) $t = 1$ *or 2, n prime.*

Proof. If $t=n-1$, then $|G|=(n!)^s$ and consequently $G=S_n^s$.

In the remaining cases of (a) or (b), hypothesis (a) of Theorem 2.8 holds — the possible sharply t-transitive groups are A_n, M_{12}, M_{11} or $\mathrm{PSL}(2, n-1)$.

In case (c) with $t=1$, hypothesis (a) holds trivially. In case (c) with $t=2$, the only sharply 2-transitive group is $\mathrm{AGL}(1, n)$. A theorem of Wielandt ([12], Theorem 27.1) shows that a proper supergroup is 3-transitive and has order divisible by $n-2$, hence not dividing $(n(n-1))^s$.

We conclude with some further conditions which ensure that the bound (8) holds and is met only in injection designs.

Theorem 2.10. *Suppose that $\mathscr{A}$ is a set of diagonals in X^{s+1} with $s \geqq n+2$. Suppose further that, for all $A, A' \in \mathscr{A}$ with $A \neq A'$, we have $|A \cap A'| \in D$. Then $|\mathscr{A}| \leqq (\prod_{d \in D} d)^s$. Moreover, equality holds if and only if $\mathscr{A}$ is an injection design of type D.*

Proof. We use the notation $\mathscr{A}(B)=\{A \setminus B \colon B \subseteqq A \in \mathscr{A}\}$ for a set $B \subseteqq X$. We use induction on $n+|D|$. The case $D=\emptyset$ is trivial, so we may suppose that $|D| \geqq 1$. Actually, even the case $|D|=1$ follows from a theorem of Deza [4], but we shall not use this fact. We distinguish two cases:

(a) $n \notin D$.

Set $l=\min\{n-d \colon d \in D\}$. Let $A_1, \ldots, A_q$ be a maximal collection of members of $\mathscr{A}$ forming a *sunflower* with kernel of size l, that is, for some l-element set B one has $A_i \cap A_j = B$ for $1 \leqq i < j \leqq q$. We may suppose that $q \geqq 2$. If $q > n-l+1$ then for all $A \in \mathscr{A}$ we have $|A|=n$ and $|A \cap A_j| \geqq l$, whence $B \subseteqq A$ holds. In this case, the statement follows from the induction hypothesis applied to $\mathscr{A}(B)$. From now on, suppose that $q \leqq n-l+1$. The maximality of q implies that

$$A \cap \Big(\bigcup_{i=1}^{q} (A_i \setminus B)\Big) \neq \emptyset$$

for all $A \in \mathscr{A}$ with $B \subseteqq A$. This, in turn, implies that

$$|\mathscr{A}(B)| \leqq q(n-l)m(n-l-1,\ D \setminus \{n-l\}, S_n).$$

Hence, by the induction hypothesis,

$$|\mathscr{A}(B)| \leqq q \prod_{d \in D} d^S/(n-l)^{S-1}.$$

Now

$$|A \cap A_1| \geqq l \quad \text{for all } A \in \mathscr{A}.$$

Using

$$\binom{n}{l} = \binom{n}{n-l} < n^{n-l}/(n-l)! < (ne/(n-l))^{n-l},$$

we infer

$$(9) \qquad |A| \leqq \left[\binom{n}{l} q/(n-l)^{h-1} \prod_{d \in D} d^S < \Big(\prod_{d \in D} d^S\Big)(ne/(n-l))^{n-l} n/(n-l)^{S-1}\right].$$

Substituting $k=n-l \geqq 2$ and using $n<s$ we obtain that, if $k>2$, then $n^{k+1}e^k/k^{n+k+1}=(n^{k+1})/(k^{n+1}) \cdot (e/k)^k < 1$ as $n \geqq k$, and the result holds. If $k=2$ it follows directly from the first part of (9), since $\binom{n}{2} 3/2^{e-1} < 1$ for $n \geqq 1$.

(b) $n \in D$.

Let y be any element of X^{s+1}. Then, by induction, $|\mathscr{A}(y)| \leqq \prod_{d \in D \setminus \{n\}} d^s$ holds. This yields

$$|\mathscr{A}| = \sum_{y \in X} |\mathscr{A}(y)|/n \leqq n^s \prod_{d \in D \setminus \{n\}} d^s = \prod_{d \in D} d^s,$$

as desired. If $\mathscr{A}$ attains the bound, then so does $\mathscr{A}(y)$ for all $y \in X^s$; then, by induction, $\mathscr{A}(y)$ is an injection design, and the same is true for $\mathscr{A}$.

The bound $s \geqq n+2$ is probably too crude; it would be desirable to have better bounds. In the particular case $D = \{2, 3, \ldots, n-t\}$ and $n \geqq n_0(t)$, we show in Theorem 2.12 below that $s \geqq 2$ is sufficient. (We mentioned earlier the conjecture from [6] that the result holds for $s=1$ too.)

Let us recall the "s-version" of Corollary 1.9.

Corollary 2.11. *Suppose that $R \leqq S_n^s$ and R contains no $r+1$ pairwise disjoint diagonal sets, where $r \leqq n^s$. Then $|R| \leqq r((n-1)!)^s$.*

We use this result in the proof of the following.

Theorem 2.12. *Suppose that $s \geqq 2$, $n \geqq n_0(t)$, and $F \subseteqq S_n^s$ satisfies $|A(f) \cap A(f')| \geqq t$ for all $f, f' \in F$. Then*

$$|F| \leqq ((n-t)!)^s$$

with equality holding if and only if $F = \{f \in S_n^s \colon B \subseteqq A(f)\}$ for some injective t-element subset B of S_n^{s+1}.

Proof. Suppose first that, for some t-element injective set B one has $|F(B)| > (n-t)((n-t-1)!)^s$ where $F(B)$ is as defined in the proof of Theorem 2.8. By Corollary 2.11, there exist $n-t+1$ pairwise disjoint sets in $F(B)$, each contained in $(X \setminus B)^{s+1}$.

We claim that $B \subseteqq A(f)$ for all $f \in F$. Indeed, if $A(f) \not\supseteqq B$, then $A(f)$ must intersect each of the $n-t+1$ pairwise disjoint sets in $F(B)$, a contradiction since $|A(f) \cap (X \setminus B)^{s+1}| \leqq n-t$.

Since the number of $f \in S_n^s$ with $B \subseteqq A(f)$ is $((n-t)!)^s$, the proof is complete in this case. Thus we may assume

(10) $\quad |F(B)| \leqq (n-t)((n-t-1)!)^s$ for all t-element injective sets B.

Suppose that $|F|$ is maximal. Then F must contain f_1 and f_2 with $|A(f_1) \cap A(f_2')| = t$ or $t+1$. We treat only the first case; the second is similar and somewhat simpler.

Set $B = A(f_1) \cap A(f_2)$ and $G_i = A(f_i) \setminus B$ for $i=1,2$. Let us classify the sets $A \in \mathscr{A} = \{A(f) \colon f \in F\}$ according to their intersections $A \cap B$, $A \cap G_1$ and $A \cap G_2$.

Since $|A \cap A'| \geqq t$ for $A, A' \in \mathscr{A}$, it follows that

(11) $$|A \cap A(f_i)| = |A \cap B| + |A \cap G_i| \geqq t$$

for $i=1,2$. We distinguish two cases:

(a) there exist an integer b with $0 \leqq b \leqq t$ and subsets $B_0 \subseteqq B$, $C_i \subseteqq G_i$, with $|B_0| = b$, $|C_i| = t-b$ (for $i=1,2$), so that

$$|\mathscr{A}(B_0 \cup C_1 \cup C_2)| > (n-t-b)((n-t-b-1)!).$$

Using Corollary 2.11 and the same argument as above, we infer that $|A \cap H| \geqq t$ for all $A \in \mathscr{A}$, where $H = B_0 \cup C_1 \cup C_2$ (so that $|H| = b+t$). This implies that

$$|\mathscr{A}| \leqq \sum_{E \in \binom{H}{t}} |\mathscr{A}(E)| \leqq \binom{b+t}{t} (n-t)((n-t-1)!)^S \leqq \left[\binom{2t}{t} \Big/ (n-t)^{s-1}\right] ((n-t)!)^S <$$
$$< ((n-t)!)^S$$

for $n > t + \binom{2t}{t}^{1/(s-1)}$.

(b) $|\mathscr{A}(B_0 \cup C_1 \cup C_2)| \leqq (n-t-b)((n-t-b-1)!)^s$ for all b and all b-subsets B_0 of B and $(t-b)$-subsets C_i of G_i, $i=1,2$.

Using (11), we obtain

$$|\mathscr{A}| \leqq \sum_{b=0}^{t} \sum_{B_0 \in \binom{B}{tb}} \sum_{C_1 \in \binom{G_1}{b}} \sum_{C_2 \in \binom{G_2}{b}} |\mathscr{A}(B_0 \cup C_1 \cup C_2)| \leqq$$

$$\leqq \sum_{b=0}^{t} \binom{t}{b} \binom{n-t}{b}^2 (n-t-b)((n-t-b-1)!)^s =$$

$$= \sum_{b=0}^{t} \frac{t!}{b!^3} ((n-t)(n-t-1) \dots (n-t-b))^{2-s} (n-t-b)^{-1} ((n-t)!)^s.$$

Since $s \geqq 2$, $2-s$ is non-positive. Using the fact that $\sum_{b \geqq 0} (1/b!)^3 < e$, we see that the right-hand side does not exceed $((n-t)!)^s \cdot et!/(n-2t)$, which is smaller than $((n-t)!)^s$ for $n > 2t + et!$.

References

[1] H. F. Blichfeldt, A theorem concerning the invariants of linear homogeneous groups, with some applications to substitution-groups, *Trans. Amer. Math. Soc.* **5** (1904), 461—466.

[2] P. J. Cameron, and M. Deza On permutation geometries, *J. London Math. Soc.* **20** (1979), 373—386.

[3] P. J. Cameron, M. Deza and P. Frankl, Sharp sets of permutations, *J. Algebra, to appear.*

[4] M. Deza, Solution d'une probléme de Erdős et Lovász, *J. Combinatorial Theory* (B), **16** (1974), 166—167.

[5] M. Deza, P. Erdős and P. Frankl, On intersection properties of systems of finite sets, *Proc. London Math. Soc.* **36** (1978), 369—384.

[6] M. Deza and P. Frankl, Injection geometries, *J. Combinatorial Theory* (B), **37** (1984), 31—40.

[7] M. Deza and P. Frankl, Squashed designs, *J. Discr. Comput. Geom., to appear.*

[8] P. Erdős, A problem on independent r-tuples, *Ann. Univ. Sci. Budapest,* **8** (1965), 93—95.

[9] P. Erdős, C. Ko and P. Radó, Intersection theorems for systems of finite sets, *Quart. J. Math. Oxford,* **12** (1961), 313—320.

[10] M. Kiyota, An inequality for finite permutation groups, *J. Combinatorial Theory* (A), **27** (1979), 119.

[11] M. E. O'NAN, Sharply 2-transitive of permutations, *Proceedings of the Rutgers Group Theory Year* 1983—198 *(ed. M. Aschbacher et al.)*, 63—67, Cambridge Univ. Press, Cambridge, 1985.
[12] H. WIELANDT, *Finite Permutation Groups*, Acad. Pr., New York, 1964.

P. J. Cameron

School of Mathematical Sciences
Queen Mary College
London El 4NS, U.K.

M. Deza and P. Frankl

C.N.R.S., Université Paris VII, 75005 Paris France