Europ. J. Combinatorics (1995) **16**, 537–544

Bases for Permutation Groups and Matroids

P. J. Cameron and D. G. Fon-Der-Flaass

In this paper, we give two equivalent conditions for the irredundant bases of a permutation group to be the bases of a matroid. (These are deduced from a more general result for families of sets.) If they hold, then the group acts geometrically on the matroid, in the sense that the fixed points of any element form a flat. Some partial results towards a classification of such permutation groups are given. Further, if G acts geometrically on a perfect matroid design, there is a formula for the number of G-orbits on bases in terms of the cardinalities of flats and the numbers of G-orbits on tuples. This reduces, in a particular case, to the inversion formula for Stirling numbers.

1. Introduction

Let G be a permutation group on an n-set X. A *base* for G is a sequence of points the (pointwise) stabiliser of which is the identity. A sequence of points is *irredundant* if no point is fixed by the stabiliser of its predecessors. In general; irredundant bases do not have the nice properties of matroid bases: they are not preserved by re-ordering, and they can have different lengths (although it is known that the ratio of the lengths of the longest and shortest irredundant bases is at most $\log_2 n$: see Blaha [1]). The first result of this paper asserts that the absence of either of these bad properties is necessary and sufficient for the irredundant bases to be the bases of a matroid. Moreover, if this happens, then G acts in a particular way on the matroid, which we call geometric, since it includes the geometric groups of Cameron and Deza [4].

A group G acts *geometrically* on a matroid M if the fixed points of any element form a flat; that is, if the pointwise stabiliser of any set of points fixes pointwise the flat spanned by that set. In general, this condition does not hold: the full automorphism groups of projective spaces over fields larger than GF(2), and free matroids of rank less than $n-1$ on n points, are examples. Cases which are geometric include any linear or affine group acting on the vector or affine space, any projective group over GF(2), any semiregular group if the empty set is closed (this includes Singer groups of projective spaces), and any Frobenius group if the empty set and singletons are closed.

In Section 2 we prove a general result about families of sets, from which it follows that the irredundant bases of a permutation group are the bases of a matroid iff they all have the same length, or iff they are all preserved by re-ordering. Section 3 concerns the question of finding all permutation groups for which this condition holds: we will see that it is infeasible unless we assume that the group is transitive and the base size is sufficiently large; but some positive results are given. Next, we give a result for counting the number of orbits on bases of a permutation group which acts geometrically on a matroid. In a special case, this becomes the inversion formula for Stirling numbers. The paper concludes with some possible directions for research.

0195-6698/95/060537 + 08 $12.00/0

2. Bases for Set Families and Groups

Let $\mathscr{F} = = \{F_i : i \in I\}$ be a family of subsets of a set X. Set

$$Z = \bigcap_{i \in I} F_i.$$

We say that the sequence $(F_1, F_2,, \ldots, F_k)$ is a *base* for $\mathscr{F}$ if

$$\bigcap_{i=1}^{k} F_i = Z.$$

The sequence is said to be *irredundant* if

$$F_i \not\supseteq \bigcap_{j=1}^{i-1} F_j$$

for $i = 1, \ldots, k$. So an irredundant base for a permutation group G corresponds precisely to an irredundant base for the family of point stabilisers (regarded as subsets of G).

Theorem 2.1. *Let $\mathscr{F}$ be a family of sets. Then the following conditions are equivalent*:
(a) *all irredundant bases of $\mathscr{F}$ have the same size*;
(b) *the irredundant bases of $\mathscr{F}$ are preserved by re-ordering*;
(c) *the index sets for the irredundant bases of $\mathscr{F}$ are the bases of a matroid.*

Proof. Given any base, we obtain from it an irredundant base by discarding 'redundant' sets F_i (those containing the intersection of their predecessors). To show that (a) implies (b), we observe that any re-ordering of an irredundant base is certainly a base; if any of its members were redundant, we would obtain a smaller base.

(b) implies (c): we just need to verify the exchange axiom for irredundant bases, since clearly no irredundant base contains another. Let $(F_1, \ldots, F_k)$ and $(G_1, \ldots, G_l)$ be irredundant bases. By re-ordering, we may assume that F_k is to be deleted from the first base. Let $Y = \bigcap_{i=1}^{k-1} F_i$. Then, for every $E \in \mathscr{F}$, we have $E \cap Y = Y$ or $E \cap Y = Z$. For, if this were not true, then $(F_1, \ldots, F_{k-1}, E, F_k)$ would be an irredundant base, but $(F_1, \ldots, F_k, E)$ would be redundant, contradicting the assumption. Now it cannot hold that $G_j \cap Y = Y$ for all j, or else $Z = \bigcap_{j=1}^{l} G_j \supseteq Y$. Hence there exists j for which $G_j \cap Y = Z$, and so $(F_1, \ldots, F_{k-1}, G_j)$ is the required base.

(c) implies (a): clear.

We call a family $\mathscr{F}$ of sets an *ibis family* if it satisfies the equivalent conditions of Theorem 2.1 (for 'Irredundant Bases of Invariant Size'). An *ibis*(k) *family* is an ibis family with irredundant base size k.

We can characterise ibis families, using the following result.

Lemma 2.2. *Let $\mathscr{F}$ be an ibis family, and M the corresponding matroid on the index set I. Then, for any $x \in X$, the set*

$$E_x = \{i \in I : x \in F_i\}$$

is a flat of M.

Proof. A point i is dependent on a set J in the matroid iff $F_i \supseteq \bigcap_{j \in J} F_j$. Hence, if J

is a maximal independent set in E_x, we see that the sets containing x are precisely those the index of which is dependent on J □

We call a family $\mathscr{S}$ of flats of a matroid M *separating* if, for any independent set $\{i_1, \ldots, i_l\}$, there is a flat $F \in \mathscr{S}$ containing $i_1, \ldots, i_{l-1}$ but not i_l. Note that a family is separating iff it contains all hyperplanes. The *dual* of a family $\{F_i: i \in I\}$ of subsets of X is the family $\{E_x: x \in X\}$ of subsets of I, where $E_x = \{i \in I: x \in F_i\}$. (For example, the dual of the family of point stabilisers in a permutation group is the family of fixed point sets of elements of the group.)

PROPOSITION 2.3. *Any ibis family of sets is obtained by the following construction. Take a matroid M, and a separating family $\mathscr{S}$ of flats of M (each flat can be repeated arbitrarily many times); then take the dual. In particular, every matroid arises from an ibis family of sets.*

PROOF. Given an ibis family, Theorem 2.1 provides the matroid, and Lemma 2.2 shows that the dual of the family is a family of flats of the matroid. If $\{i_1, \ldots, i_l\}$ is independent, choose $x \in F_{i_1} \cap \cdots \cap F_{i_{l-1}}$, $x \notin F_{i_l}$; then E_x is a flat containing $i_1, \ldots, i_{l-1}$ but not i_l. So $\mathscr{S}$ is separating.

Conversely, let $\mathscr{F}$ be the dual of a separating family $\mathscr{S}$ of flats of the matroid M. If $i_1, \ldots, i_k$ is a basis for M, and $x \in F_{i_1} \cap \cdots \cap F_{i_k}$, then E_x contains $i_1, \ldots, i_k$, so $E_x = I$ and $x \in \bigcap \mathscr{F} = Z$. Conversely, if $l < k$ and $i_1, \ldots, i_l \in I$, choose j not in the span of $i_1, \ldots, i_l$ and a flat E_x containing $i_1, \ldots, i_l$ but not j;; then $x \in F_{i_1} \cap \cdots \cap F_{i_l}$ but $x \notin F_j$, so $x \notin Z$. So any irredundant base has size k, and $\mathscr{F}$ is an ibis family. □

We restate these results for permutation groups.

THEOREM 2.4. *Let G be a permutation group. Then the following conditions are equivalent*:

(a) *all irredundant bases for G have the same size*;

(b) *the irredundant bases for G are preserved by re-ordering*;

(c) *the irredundant bases for G are the bases of a matroid.*

If these conditions hold, then G acts geometrically on the matroid. Moreover, if G acts primitively and is not cyclic of prime order, then the matroid is geometric (the empty set and singletons are closed).

PROOF. The equivalence of (a)–(c) follows from Theorem 2.1.

Suppose that the conditions hold. By Lemma 2.2, the fixed point set of any element is a flat of the matroid; so G acts geometrically.

If G is primitive but not regular, then the stabiliser of a point fixes no additional points (see Wielandt [16]); so any two points are independent. □

3. IBIS GROUPS

We call a permutation group an *ibis group* if it satisfies the conditions of Theorem 2.4. An *ibis*(k) *group* is an ibis group whose irredundant bases have size k. Not every group acting geometrically on a matroid of rank is an ibis(k) group; those which are ibis groups are characterised by the additional property that any proper flat is the fixed point set of some non-trivial subgroup. (Equivalently, if $\{x_1, \ldots, x_l\}$ is independent, then there is an element of G fixing $x_1, \ldots, x_{l-1}$ but not x_l: this just says that the fixed point sets of the elements of G form a separating family of flats). Since a family of flats is separating if and only if it contains the hyperplanes, we have the following result.

PROPOSITION 3.1. *A group G of automorphisms of a matroid m of rank k is an ibis(k) group associated with M iff G acts geometrically on M and every hyperplane of M is fixed pointwise by a non-trivial element of G.*

An ibis(0) group is trivial, and ibis(1) groups are just groups acting semiregularly on their non-fixed points. Is it possible to classify the ibis(k) groups for sufficiently large k? Note that Maund [14] determined the *geometric* groups—those which permute their irredundant bases transitively—for $k \geq 2$, using the classification of finite simple groups, while Zil'ber [18] determined those of rank $k \geq 7$ by 'elementary' methods, not using the classification.

The next result gives some basic properties of these groups.

PROPOSITION 3.2. (a) *Any transitive constituent of an ibis group is an ibis group.*
(b) *The stabiliser of a point in an ibis group is an ibis group.*
(c) *The direct product of ibis groups, acting on the disjoint union of the underlying sets, is an ibis group.*
(d) *If G is an ibis group on X, then G acts as an ibis group on the disjoint union of any number of copies of X.*

PROOF. (a) Let G be an ibis group and Y an orbit of G. Any irredundant base for the group G^Y induced by G on Y can be extended to an irredundant base for G by appending a fixed irredundant base for the pointwise stabiliser of Y. So any two such bases have the same size.

(b), (c) and (d): clear. □

COROLLARY 3.3. *Let G be an intransitive ibis(k) group, and Y an orbit of G. Then either G acts faithfully on Y, or G^Y is an ibis(l) group for some $l < k$.*

In view of Corollary 3.3, we may (at least initially) reduce the classification problem for ibis groups to the case of transitive groups; and Proposition 3.2(b) allows the possibility of using induction. But starting the induction will be difficult. For example, G is a transitive ibis(2) group iff the point stabiliser H is a proper *TI-subgroup*; that is, $N_G(H) \neq G$ and $H \cap H^x = 1$ for all $x \notin N_G(H)$. This includes, in particular, the Frobenius groups, which satisfy the stronger condition that $H \cap H^x = 1$ for all $x \notin H$. There seems no hope of a complete determination of the transitive ibis(2) groups. For example, any non-normal subgroup of G of prime order is a TI-subgroup.

Perhaps it is more hopeful to attempt to determine the transitive ibis(3) groups. In these cases, there is a rank 3 matroid (a linear space) preserved by G, permitting geometric arguments. Examples of ibis(3) groups include the following:
(a) PSL(2, q), PGL(2, q), Sz(q), degree $q+1$;
(b) groups of the form $A{:}B{:}C$, where A is the additive group of GF(q), B is a subgroup of the multiplicative group, and C a subgroup of prime order of the automorphism group which fixes every B-orbit setwise;
(c) PSL(2, q), where q is a power of q, acting on the cosets of a dihedral subgroup of order $2(q+1)$, degree $q(q-1)/2$;
(d) PSL(3, 2), degree 7;
(e) A_7, degree 15.
Examples (a) are well known; the matroid is trivial (the free matroid of rank 3). In (b),

if $q=r^s$ and $|C|=s$, the condition on B and C is equivalent to requiring that $(q-1)/(r-1)$ divides $|B|$. The matroid is the Desarguesian affine space AG(s,r), truncated to rank 3. In the case $q=16$, $s=2$, $|B|=5$, the permutation group preserves an extremal configuration for Ramsey's theorem, demonstrating that $16 \nrightarrow (3)_3^2$: see Greenwood and Gleason [9]. In (c), the matroid is the so-called Witt–Bose–Shrikhande design (Kantor [13]). In (d), the matroid is PG(2, 2); in (e), it is PG(3, 2), truncated to rank 3.

In a special case, we have a classification:

THEOREM 3.4. *Let G be an ibis(k) group the associated matroid of which is free of rank k, where $k \geqslant 2$. Then G is $(k-1)$-transitive.*

PROOF. It suffices to prove the result when $k=2$. Now the stabiliser of any two points is trivial. This hypothesis implies that G is a Frobenius group, with the Frobenius action on one orbit and the regular action on all the others (Wielandt [16]). But there cannot be a regular orbit, or else G would have a base of size 1. □

For $k=2$, a group satisfying these hypotheses is precisely a Frobenius group (in its Frobenius action). For larger k, we have a complete classification. For $k=3$, G is a Zassenhaus group; the classification is due to Zassenhaus [17], Feit [8], Ito [12] and Suzuki [15]. The classification for $k \geqslant 4$ is due to Gorenstein and Hughes [10], and that for higher k follows. In particular, such a group with $k \geqslant 5$ must be sharply k-transitive, and hence geometric. (See Huppert and Blackburn [11] for these results, which predate the classification of finite simple groups.)

A complete list of ibis(k) groups for $k \geqslant 3$ will probably require the classification of finite simple groups. The following result illustrates a technique that might be useful.

THEOREM 3.5. *There are only finitely many values of n for which the symmetric group S_n or the alternating group A_n acts as a primitive ibis group, not in its natural representation.*

PROOF. It follows from a theorem of Cameron and Kantor [5] (using the classification) that any primitive action of S_n or A_n has base size 2 except in the following cases:

(a) the action on k-sets, $k < \frac{1}{2}n$;
(b) the action on partitions into l sets of size k, $n=kl$, $k, l>1$;
(c) finitely many others.

Now a primitive ibis(2) group is a Frobenius group; but the only symmetric and alternating groups which can act as Frobenius groups are S_3 and A_4 in their natural actions and S_4 with degree 3. So we need only consider actions of types (a) and (b) to prove the theorem. Moreover, the action on 1-sets is the natural one, so we may assume that $k>1$ in (a).

We claim that S_n and A_n on k-sets are not ibis groups for $1<k<\frac{1}{2}n$, with finitely many exceptions. In the case of S_n, there is an irredundant base of size $n-2$: take a fixed $(k-1)$-set Y and a fixed $(k+1)$-set Z with $Y \subset Z$, and let S consist of all but one k-set containing Y and all but one k-set contained in Z, the two k-sets between Y and Z being chosen in both collections. For A_n, omitting one of these gives an irredundant base of size $n-3$. But we can construct bases which are usually smaller, as follows. There is a family $\mathcal{F}_k$ of $\lceil 1+\log_2 k \rceil$ sets of size k the union of which is a $(2k-1)$-set, such that different points of the union lie in different subfamilies of $\mathcal{F}_k$. Taking nearly disjoint copies of $\mathcal{F}_k$ covering all but one of the points, we obtain a base of size

$$\lceil 1+\log_2 k\rceil\cdot\lceil (n-1)/(2k-1)\rceil,$$

which is smaller than $n-3$ with finitely many exceptions, all having $k\leq 5$ and $n\leq 12$. (Note that S_6 and A_6, acting on 2-sets, are ibis groups.)

Now consider case (b); assume that $k>3$ and $l>2$. First, choose an irredundant sequence of partitions all cointaining a given part K, and fixing all points outside K. Now we may fix K one point at a time, by choosing additional points one of the parts of which contains $k-1$ points of K; or $\min(k, l-1)$ points at a time, by choosing additional partitions with all but at most one part meeting K in one point. We have the remaining cases as an exercise. (Note that we obtain ibis groups when $k=l=2$, where S_4 and A_4 act unfaithfully as ibis groups of degree 3; $k=3$, $l=2$, where $S_6\simeq \mathrm{P\Gamma L}(2,9)$ and $A_6\simeq \mathrm{PSL}(2,9)$ are ibis groups of degree 10; and $k=2$, $l=3$, where the actions of S_6 and A_6 on partitions are similar to those on 2-sets.) □

REMARK. Among the finitely many exceptions are S_5 and A_5, acting as $\mathrm{PGL}(2,5)$ and $\mathrm{PSL}(2,5)$ of degree 6; S_6 and A_6 in their 'unnatural' actions of degree 6; and A_7 and A_8 with degree 15, explained by $A_8\simeq \mathrm{PSL}(4,2)$.

4. A Counting Theorem

If a group G acts geometrically on a perfect matroid design (a matroid in which the cardinality of a flat depends only on its rank), then the number of orbits of G on bases can be calculated as follows.

THEOREM 4.1. *Let M be a matroid of rank k, in which any flat of rank i has cardinality l_i (with $l_k=n$). Let $f(x)=\prod_{i=0}^{k-1}(x-l_i)$, and let $f(x)=\sum_{i=0}^{k}a_ix^i$. Let G be a group acting geometrically on M, and let m_i be the number of orbits of G on M^i. Then the number of orbits of G on bases is $\sum_{i=0}^{k}a_im_i$.*

PROOF. Since an independent i-tuple can be extended to an independent $(i+1)$-tuple in $n-l_i$ ways, the number of bases is $f(n)$.

Let π be the permutation character of G, and consider the virtual character $\phi=f(\pi)$. We have $\phi(1)=f(n)$. Since the fixed points of any element form a flat, $\phi(g)=0$ for any $g\neq 1$. Thus, ϕ is a multiple of the regular character ρ_G of G, say $\phi=d\rho_G$. Now $d=f(n)/|G|$ is the number of orbits of G on bases, since the stabiliser of a basis is the identity. Using the fact that π^i is the permutation character of G on M^i, we see that the inner product $\langle\pi^i, 1_G\rangle$ is equal to m_i, where 1_G is the principal character. So we have

$$d=\langle\phi, 1_G\rangle=\sum_{i=0}^{k}\langle a_i\pi^i, 1_G\rangle=\sum_{i=0}^{k}a_im_i.$$

Note that the inequality $d>0$ holds, and that G is a geometric group iff $d=1$. □

EXAMPLE. Let G be any permutation group, and k an integer exceeding the number of fixed points of any non-identity element of G. Then G acts geometrically on the free matroid of rank k. For $j\leq k$, an orbit of G on j-tuples can be described uniquely by a partition of $\{1,\ldots,j\}$ (into i parts, say), and an orbit of G on i-tuples of distinct elements (that is, independent i-tuples). Let n_i denote the number of orbits of G on i-tuples of distinct elements. Then $n_k = d$, and we have

$$m_j = \sum_{i=1}^{j} S(j, i) n_i,$$

where $S(j, i)$ is the Stirling number of the second kind (compare Cameron and Taylor [6]). Moreover, $f(x) = \prod_{i=0}^{k-1} (x - i)$, and so a_i is the (signed) Stirling number of the first kind. Thus Proposition 4.1 is an instance of the familiar inversion relation between the two kinds of Stirling numbers.

5. Further Directions

There are at least three possible directions in which to extend these ideas. One is to infinite permutation groups. Theorem 2.4 holds unchanged for groups in which all irredundant bases are finite. (Note that a permutation group has a finite base if and only if it is discrete in the topology of pointwise convergence. However, a group can have both finite and infinite irredundant bases, as examples in Cameron [3] show.) If, in addition, all proper flats are finite, then the analogue of Theorem 4.1 can be proved. The non-existence of geometric groups of rank at least 4 has been proved under the same hypothesis [2]. However, the classification problems appear much harder, partly because of the lack of an infinite version of Frobenius' theorem. Some of these points are discussed in [3].

Another possible direction involves sets, rather than groups, of permutations. Some motivation comes from the importance of sharply k-transitive permutation sets in geometry. Extremal problems for sets of permutations are discussed by Cameron and Deza [4], Cameron, Deza and Frankl [7]. We could ask whether there is an analogue of Theorem 2.4 for permutation sets.

Yet another extension would weaken the condition that all irredundant bases have the same size. For example, there is a greedy algorithm for choosing a base: select the next base point from an orbit of maximum size of the stabiliser of its predecessors [1, 14]. Ambiguity results from the fact that there may be several orbits of maximum size. We could ask the following questions: *Which groups have the property that*:

(a) *all greedy bases have the same size*? *or*
(b) *the greedy bases are preserved by re-ordering*? *or*
(c) *the greedy bases are the bases of a matroid*?

Unlike Theorem 2.4, these conditions are not all equivalent. We would expect that, at least among primitive groups, most groups satisfy (a), while (c) is quite restrictive. For example, in the group $\mathrm{PGL}(d, q)$, for $d, q > 2$, (a) and (b) hold but not (c): the greedy bases are the $(d+1)$-tuples such that any d form a basis of the projective geometry.

Finally,

Which groups contain ibis families of subgroups?

If an ibis family of subgroups of G is closed under conjugation, then G acts as an ibis permutation group with the given subgroups as point stabilisers (possibly after adjusting their multiplicities). What if this conjugacy requirement is dropped?

References

1. K. Blaha, Minimum bases for permutation groups: the greedy approximation, *J. Algorithms,* **13** (1992), 297–306.
2. P. J. Cameron, Infinite geometric groups of rank 4, *Europ. J. Combin.*, **13** (1992), 87–88.
3. P. J. Cameron, Cofinitary permutation groups, *Bull. London Math. Soc.*, to appear.
4. P. J. Cameron and M. Deza, On permutation geometries, *J. Lond. Math. Soc.* (2), **20** (1979), 373–386.
5. P. J. Cameron and W. M. Kantor, Random permutations: some group-theoretic aspects, *Combin. Prob. Comput.*, **2** (1994), 257–262.
6. P. J. Cameron and D. E. Taylor, Stirling numbers and affine equivalence, *Ars Combin.*, **20B** (1985), 3–14.
7. P. J. Cameron, M. Deza and P. Frankl, Sharp sets of permutations, *J. Algebra,* **111** (1987), 220–247.
8. W. Feit, On a class of doubly transitive permutation groups, *Illinois J. Math.*, **4** (1960), 170–186.
9. R. E. Greenwood and A. M. Gleason, Combinatorial relations and chromatic graphs, *Can. J. Math.* **7** (1955), 1–7.
10. D. Gorenstein and D. R. Hughes, Triply transitive groups in which only the identity fixes four letters, *Illinois J. Math.*, **5** (1961), 486–491.
11. B. Huppert and N. Blackburn, *Finite Groups III,* Springer-Verlag, Berlin, 1982.
12. N. Ito, On a class of doubly transitive permutation groups, *Illinois J. Math.*, **6** (1962), 341–352.
13. W. M. Kantor, Homogeneous designs and geometric lattices, *J. Combin. Theory, Ser. A,* **38** (1985), 66–74.
14. T. Maund, D.Phil. thesis, Oxford University, 1989.
15. M. Suzuki, On a class of doubly transitive permutation groups, *Ann. Math.* **75** (1962), 241–254.
16. H. Wielandt, *Finite Permutation Groups,* Academic Press, London, 1964.
17. H. Zassenhaus, Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen, *Abh. Math. Sem. Hanburg,* **11** (1935), 17–40.
18. B. I. Zil'ber, Finite homogeneous geometries, in: *Proc. 6th Easter Conf. Model Theory,* B. Dahn and H. Wolter (eds), Humboldt University, Berlin, 1988, pp. 186–208.

Received 11 October 1994 and accepted in revised form 16 March 1995

P. J. Cameron and D. G. Fon-Der-Flaass
School of Mathematical Science,
Queen Mary and Westfield College,
Mile End Road, London E1 4NS, U.K.