Model Theory

no. 2 vol. 3 2024

Independence and bases: theme and variations

Peter J. Cameron

msp

Model Theory
Vol. 3, No. 2, 2024
https://doi.org/10.2140/mt.2024.3.417

Independence and bases: theme and variations

Peter J. Cameron

To Boris Zilber on the occasion of his 75th birthday.

This paper describes a complex of related ideas, ranging from Urbanik's v^*-*algebras*, through Deza's *geometric groups* and Zilber's *homogeneous geometries*, to Sims' *bases* for permutation groups and their use in defining "size" parameters on finite groups, with a brief look at Cherlin's *relational complexity*. It is not a complete survey of any of these topics, but aims to describe the links between them.

1. Introduction

In the 1980s, there was widespread interest in matroids with a large amount of symmetry. Michel Deza was studying *perfect matroid designs*, matroids in which the cardinality of a flat depends only on its dimension: this class includes uniform matroids, classical projective and affine spaces, and Steiner systems. One way to enforce this condition is to assume a large group of automorphisms: for example, it holds if the stabiliser of any subset is transitive on the set of points not dependent on that subset. The tool of choice for many was the recently announced classification of finite simple groups.

In 1988, I attended a Durham Symposium on model theory and groups run by the London Mathematical Society. To my amazement, Boris Zilber spoke at the symposium, giving four lectures on his recent result classifying such geometries with rank at least seven, by geometric methods not using CFSG.

Zilber [1984] had worked on first-order theories which are categorical in all cardinalities. We knew from Morley's theorem that this imposes just two conditions on the theory: countable and uncountable categoricity. The result of Engeler, Ryll-Nardzewski and Svenonius shows that $\aleph_0$-categoricity is equivalent to the existence of a large automorphism group, while categoricity in higher powers forces structural conditions such as the existence of rank functions, which led to the development of stability theory. These nicely combine if both types of categoricity hold. In

MSC2020: primary 20B10; secondary 03C35, 05B35.
Keywords: strictly minimal structures, bases, independence algebras.

particular, strictly minimal countably categorical theories carry geometries of infinite dimension which have analogues of the properties that Deza was interested in.

Zilber's achievement in his lectures at the symposium (described in [Zilber 1988a]) was to observe that methods from the infinite case could be applied also to finite structures. The set of elements independent of a finite subset is infinite in the infinite case, but sufficiently large in the finite case that arguments can be adapted.

Perhaps Zilber's methods have not been sufficiently integrated into finite combinatorics; we still have work to do.

2. Definitions

A family $\mathcal{B}$ of finite subsets of a set is said to have the *exchange property* if, given $B_1, B_2 \in \mathcal{B}$ and $y \in B_2 \setminus B_1$, there exists $x \in B_1 \setminus B_2$ such that $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Clearly all the sets in such a family have the same cardinality. One definition of a *matroid*, in terms of its set of bases, is as a collection of subsets of a finite set having the exchange property. Matroids form an important class of structures, describing subsets of vector spaces, edge sets of graphs (where the bases are spanning forests), transversals to families of sets, and several others. Areas of mathematics in which matroids occur include algebraic and tropical geometry and homotopy theory [Giansiracusa and Giansiracusa 2018].

The set of bases in a vector space V has two properties, which serve as a foundation for linear algebra:

(a) it has the exchange property;

(b) any map from a basis into V has a unique extension to an endomorphism of V.

It is natural to look for further examples of this phenomenon.

Let A be an algebra, in the sense of universal algebra; that is, a set carrying a number of operations of various arities (we interpret 0-ary operations as constants). Suppose that A is finitely generated, and let $\mathcal{B}$ be the set of minimal (under inclusion) generating sets for A. Then A is an *independence algebra* if $\mathcal{B}$ has the above two properties. The definition, and the classification of these algebras, are essentially due to Kazimierz Urbanik [1966] (who called them v^**-algebras*), but his work was not as well known as it deserved to be, and the concept was later rediscovered in the context of semigroup theory. Section 2 of this paper gives some details about independence algebras and their classification, and mentions a recent result on them.

Perhaps unaware of the work of Urbanik, semigroup theorists Fountain and Lewin [1992] and Gould [1995] realised that earlier structural results of Howie, Reynolds and Sullivan, and Erdos on the full transformation semigroup and the semigroup of linear maps on a vector space could be generalised to endomorphism

semigroups of independence algebras. I learned of the topic from John Fountain, and set to work with Csaba Szabó to classify at least the finite independence algebras.

The endomorphisms of a structure form a monoid, and the automorphisms form its group of units. The class of permutation groups arising as automorphism groups of independence algebras is part of a more general class, named "geometric groups" by Michel Deza [Cameron and Deza 1979]. These groups, and the underlying closure systems, were studied by Boris Zilber in the 1980s, in the course of his important researches on countably categorical and $\aleph_0$-stable first-order structures; he called these objects *quasi-Urbanik structures*; see [Zilber 1988b]. Section 3 of this paper discusses some of their theory.

The concept of a *base* can be defined for any permutation group, not just the geometric groups. Permutation group bases do not usually satisfy the exchange property; those which do, the so-called *IBIS groups*, introduced by Dima Fon-Der-Flaass and me [Cameron and Fon-Der-Flaass 1995], form a very interesting class. Bases were introduced by Charles Sims [1970] for use in computation with permutation groups, but raise various interesting questions; among other uses, they form part of László Babai's work on the graph isomorphism problem [Babai 2015], and are connected with Cherlin's notion of *relational complexity* for studying finite homogeneous structures [Cherlin 2016; Cherlin et al. 1996]. This area is seeing renewed activity at present, so I will not give a complete survey, but will highlight some open questions.

The final section draws connections between various "measures" of a finite group with parameters defined in terms of bases in all actions of the group. There are a number of open problems here.

To conclude this section, I give a couple of essential definitions for permutation group theory. Let G be a permutation group acting on Ω. The action is *transitive* if there is no G-invariant subset except for Ω and the empty set (equivalently, any element of Ω can be mapped to any other by some element of G); it is *primitive* if it is transitive and, in addition, there is no G-invariant partition except for the partition into singletons and the partition with a single part. The *stabiliser* of an element $\alpha \in \Omega$ is the subgroup of G consisting of all elements mapping α to itself. The action is *semiregular* or *free* if the stabiliser of every point is the identity; it is *regular* if it is transitive and semiregular.

3. Independence algebras

An *independence algebra* is a finitely generated algebra with the properties

(a) the minimal generating sets have the exchange property;

(b) any map from a minimal generating set into the algebra extends uniquely to an endomorphism of the algebra.

The definition makes no explicit mention of the operations of the algebra; there is some freedom about these, as long as the correct subalgebras and endomorphisms are obtained. (A minimal generating set is a subset minimal with respect to being contained in no proper subalgebra.) Thus a classification up to isomorphism is not possible. Urbanik classified the algebras up to *clone equivalence*, noting that an algebra clone-equivalent to an independence algebra is an independence algebra. Szabó and I used a slightly weaker, but arguably more natural, equivalence. We say that two algebras A and B are *SE-equivalent* if there is a bijection between them which preserves subalgebras and endomorphisms. It turns out that there is one case only where these notions differ (one SE-equivalence class of independence algebras splits into two clone-equivalence classes). For further discussion see [Araújo et al. 2022; 2011; Araújo and Fountain 2004].

There is another small difference also: Urbanik did not allow constants, but used constant-valued unary operations instead. We will see that the presence or absence of constants is crucial to the classification.

First consider the case where A has rank 1. (The rank is the cardinality of a minimal generating set; the exchange property guarantees its invariance.) If there are no constants, then any singleton subset of A is a generating set, and any element can be mapped to any other by a unique automorphism. Thus the automorphism group G of A acts regularly. For any group G, there is an independence algebra of this form; we take $A = G$ and, for each $g \in G$, equip A with a unary operation μ_g given by $\mu_g(x) = gx$. Then G acts regularly on A by right multiplication.

Now suppose that there is a set C of constants. Then the bases are the singletons not contained in C, and any of them can be mapped to any other by a unique automorphism; so we can identify $A \setminus C$ with a group G. There is a unique endomorphism f_c mapping the identity element of G to c, for each $c \in C$. There is a left action of G on C, defined by the rule that the endomorphism $g \circ f_c$ (composed left-to-right) maps the identity of G to an element which we take to be $g(c)$. Conversely, given any group G and left action of G on a set C we obtain an independence algebra on the disjoint union $G \cup C$: it has a constant γ_c for each $c \in C$ (interpreted as c) and a unary operation μ_g for each $g \in G$ given by $\mu_g(h) = gh$ for $h \in G$, $\mu_g(c) = g(c)$.

The phrase "an independence algebra of rank 1" seems to me a remarkably concise way of defining a group with an action on a set.

This construction extends as follows. For any set X, and any group G with a left action on C, define an algebra on the set $A = (X \times G) \cup C$ with C as set of constants, and unary operations μ_g defined by

$$\mu_g((x, h)) = (x, gh), \qquad \mu_g(c) = g(c).$$

This is an independence algebra whose subalgebras are all the sets $(Y \times G) \cup C$

for $Y \subseteq X$, so that the subalgebra lattice is the Boolean algebra $B(X)$ of subsets of X. Every finitely generated independence algebra whose subalgebra lattice is a Boolean algebra is of this form; these are the *trivial* independence algebras. (We could follow the model theorists and call them *disintegrated*.)

Next, it is shown that the subalgebra lattice of a nontrivial independence algebra is a projective or affine space, depending on whether the algebra has constants or not. The arguments for this are quite general, not assuming finiteness or even finite rank; an accessible account is in [Cameron and Szabó 2000].

Finally it is shown that the algebras are of three types:

(a) Let V be a vector space over a division ring F. Then there is an independence algebra whose elements are those of V; the operations are addition in V and scalar multiplication by elements of F. The subalgebras are the subspaces of V, and so the subalgebra lattice is the projective space built on V. If W is a subspace of V, we obtain an independence algebra by taking the elements of W to be constants; its subalgebra lattice is the projective space on V/W.

(b) Let V be a vector space over a division ring F. For each $c \in F$ with $c \neq 0, 1$, define a binary operation $\beta_c(x, y) = cx + (1-c)y$. (If $|F| = 2$, we use instead the ternary operation $\tau(x, y, z) = x + y + z$.) This defines an independence algebra whose subalgebras are the affine subspaces. If W is a subspace of V, we can add unary operations for translations by elements of W to obtain an algebra whose subalgebras are the unions of cosets of W corresponding to affine subspaces of V/W.

(c) Let G be a *sharply* 2*-transitive group* on Ω: this means that any pair of distinct elements of Ω can be mapped to any other such pair by a unique element of G. Let $\{O_i : i \in I\}$ be the set of orbits of G on triples of distinct elements of Ω. For each $i \in I$, define a binary operation μ_i by

$$\mu_i(a, a) = a, \qquad \mu_i(a, b) = c \text{ if } (a, b, c) \in O_i.$$

This defines an independence algebra; its endomorphisms are the elements of G together with the constant functions, and its rank is 2.

The sharply 2-transitive groups have been of interest for a long time, partly because of their connections with projective planes. It was known to Burnside and Frobenius, and probably earlier, that a finite sharply 2-transitive group has a regular normal subgroup, and so is the group of 1-dimensional affine maps over a finite *nearfield* (this is a structure satisfying the field axioms except possibly the commutativity of multiplication and one distributive law). The finite nearfields were all determined by Zassenhaus [1935]: there are infinitely many *Dickson nearfields* (obtained from Galois fields by "twisting" the multiplication) and seven *exceptional nearfields*.

For a long time it was not known whether all sharply 2-transitive groups are given by nearfields. Several authors [Grätzer 1963; Kerby 1974; Tits 1952; Wilke 1972] defined algebraic structures from such groups, which were given various names and satisfied slightly different sets of axioms. Eventually the question was resolved in [Rips et al. 2017]: infinite sharply 2-transitive groups do not necessarily have regular normal subgroups, and so cannot all be defined from nearfields.

The most recent appearance of independence algebras is in the paper [Araújo et al. 2022]. This gives more details about the relation between Urbanik's v^*-algebras and independence algebras, the relation between clone equivalence and SE-equivalence, and the classification theorem, and goes on to develop matrix theory for most types of independence algebras, though in the case of sharply 2-transitive groups this works only for those defined over nearfields.

4. Geometric groups

The automorphism group of an independence algebra has some remarkable properties:

(a) it acts transitively on (ordered) bases for the algebra;

(b) the stabiliser of any tuple of points fixes pointwise the subalgebra they generate and acts transitively on the points outside this subalgebra.

Forgetting the algebra, the problem of determining the groups with properties like these arises in a couple of places:

- The automorphism group of a strictly minimal set in a totally categorical first-order structure has this property, where the role of subalgebras is taken by definably closed sets; as we saw, Boris Zilber was motivated by this.
- Michel Deza defined an analogue of a matroid in the semilattice of partial permutations rather than the lattice of subsets; he called it a permutation geometry (by analogy with the term "combinatorial geometry", an alternative name for a matroid, proposed by Gian-Carlo Rota).

I will not describe the motivation further, but go straight to the definition. These groups were called "geometric groups" by Deza; not an ideal name, since there are many ways in which a group can be "geometric", and there is no connection with the topic of geometric group theory, but I will stick to this term.

A *geometric group*, then, is a permutation group in which the stabiliser of any finite tuple acts transitively on the points it does not fix (if any).

We see immediately that, in a geometric group, the analogue of a basis for independence algebras can be defined as a sequence of points $(x_1, x_2, \ldots, x_r)$ in which each point is moved by the stabiliser of its predecessors, but the stabiliser

of the whole sequence is the identity. Then the group acts transitively on ordered bases. The number r is the *rank* of the geometric group.

What are the geometric groups? It is clear that a geometric group of rank 1 is an arbitrary group acting regularly, perhaps with some added fixed points. So we can assume that the rank is at least 2.

As noted above, Zilber [1984] determined all geometric groups of rank at least 7: they are stabilisers of sequences of points in the symmetric group, the general linear group, or the affine group (the last two over a finite field). His proof used elementary arguments inspired by model theory. To elaborate a little, [Zilber 1984] analysed the structure of countably categorical $\aleph_0$-stable structures via their strongly minimal sets, showing as a result that totally categorical structures could not be finitely axiomatised. Strictly minimal sets in these structures involve locally finite geometries which are shown to be either disintegrated (all subsets of a set) or projective or affine spaces over finite fields; it is this result which he was able to "finitise", giving the characterisation noted at the start of this paragraph.

At about the same time, Maund [1989] used the recently announced classification of finite simple groups to determine all geometric groups of rank at least 2. The bulk of the work is involved in determining those groups of rank 2, since they occur as building blocks for the groups of larger rank. The list is as follows:

(a) $H \wr S_2$, where H acts regularly.

(b) $M \cdot S_3 \leq H \wr S_3$, where H is abelian and regular and

$$M = \{(h_1, h_2, h_3) \in H^3 : h_1 h_2 h_3 = 1\}.$$

(c) Sharply 2-transitive groups.

(d) $V^2 \cdot \mathrm{AGL}(1, q)$ or $V^2 \cdot \mathrm{GL}(2, q)$, where V is a vector space over $\mathrm{GF}(q)$.

(e) $C_{(q-1)/2} \times \mathrm{PSL}(2, q)$ with $q \equiv 3 \pmod 4$.

(f) $C_{q-1} \times \mathrm{Sz}(q)$, where q is an odd power of 2.

(g) $\mathrm{PGL}(3, 2)$ and $\mathrm{PGL}(3, 3)$.

(In case (d), we regard V^2 as $V \otimes W$, where $\dim(W) = 2$, and $\mathrm{GL}(2, q)$ or its subgroup $\mathrm{AGL}(1, q)$ acts on W.)

Maund used this list and some geometry to determine all finite geometric groups of rank at least 2. Unfortunately this work has never been published.

This list was used in [Cameron and Szabó 2000] to give a determination of finite independence algebras. For each geometric group we have to decide whether or not it is possible to define maps to play the role of endomorphisms, and operations preserved by the group to make the domain into an algebra.

5. Bases for permutation groups

The concept of a base for a permutation group arose in computational group theory. A *base* is a sequence of points in the permutation domain whose pointwise stabiliser is the identity. Thus, for geometric groups, bases in the sense previously defined are bases here also.

The importance of a base is that two elements of a permutation group G which agree on a base for G must coincide: for if g and h are the two elements, then gh^{-1} fixes the base pointwise, so $gh^{-1} = 1$. This can lead to a compact representation of group elements if the base size is small. So it is of interest to find a small base for a permutation group. Let $b_m(G)$ be the size of a smallest base for G.

We can find a base very simply, by choosing points and stabilising them until we reach the identity. This is potentially rather wasteful. Though it is hard to find the base of smallest size for a given group, there are two simple methods which perform rather well, involving choosing base points in order:

- There is no need to include a point which is fixed by the stabiliser of the points already chosen. We call a base *irredundant* if no point is fixed by the stabiliser of its predecessors. We note that bases of geometric groups in the earlier sense are by definition irredundant.
- Motivated by this, a good heuristic is to choose each new base point from an orbit of largest size of the stabiliser of its predecessors. This is a "greedy algorithm", and a base produced by this algorithm is called a *greedy* base. The heuristic is based on the idea that to descend a chain of subgroups to the identity, we should choose the subgroup of largest possible index in its predecessor at each stage, and the index of the stabiliser of a point is the size of the orbit of that point.

Note that bases are ordered sequences, and there is no guarantee that reordering an irredundant or greedy base will result in another with the same property.

Clearly, for a geometric group, irredundant bases and greedy bases are the same, and they have a beautiful geometric structure: they are the bases of a matroid. However, the last condition holds more generally, according to this remarkable theorem of Cameron and Fon-Der-Flaass [1995].

Theorem 1. *For a permutation group G, the following conditions are equivalent*:

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

(b) *the result of reordering an irredundant base is still irredundant*;

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

Proof. Clearly (c) implies (a). Also (a) implies (b), since if reordering a base created a redundancy then a smaller irredundant base could be obtained by removing

some elements. Suppose that (b) holds, and let $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_s)$ be irredundant bases. The stabiliser of $a_1, \ldots, a_{r-1}$ cannot fix all of $b_1, \ldots, b_s$; suppose that it moves b_i. Then $(a_1, \ldots, a_{r-1}, b_i, a_r)$ is a base, which must be redundant since swapping the last two elements gives a redundant base. But the only possible redundancy is that a_r is fixed by the stabiliser of the earlier points, so $(a_1, \ldots, a_{r-1}, b_i)$ is an irredundant base. Thus the exchange property holds. □

Groups satisfying these conclusions are called *IBIS groups* (an acronym for "*I*rredundant *B*ases of *I*nvariant *S*ize". Every geometric group is an IBIS group; the converse is far from true. For a simple example, a *Frobenius group* (a transitive group in which the stabiliser of any two points is trivial but the stabiliser of a single point is not) is an IBIS group of rank 2: the bases are all the 2-element sets. A Frobenius group is a geometric group if and only if it is sharply 2-transitive, and as we saw, all sharply 2-transitive groups are automorphism groups of independence algebras.

A large class of (intransitive) examples is given by the following construction.

Let C be a linear code of length n over the finite field F (a subspace of F^n). Let G be the additive group of C, and let $\Omega = \{1, \ldots, n\} \times F$. Define an action of G on Ω by

$$a : (i, x) \mapsto (i, x + a_i)$$

for $a = (a_1, \ldots, a_n) \in C$. This is an IBIS group. It acts on $n|F|$ points, and has rank equal to the dimension of the code; if there is no coordinate in which all codewords are zero, then it has n orbits each of size $|F|$.

The classification problem for primitive IBIS groups is likely to be easier, though even that has not yet been done. In [Cameron and Fon-Der-Flaass 1995], the IBIS groups whose associated matroid is a uniform matroid are determined; these are Frobenius and Zassenhaus groups and their analogues, that is, groups which, for some positive integer t, are t-transitive and have the property that the pointwise stabiliser of any $t + 1$ points is trivial. (The *uniform* matroid of rank r is the one whose bases are all the sets of size r of the ground set.) All such finite groups with $t > 1$ (that is, those which are not Frobenius groups) have been explicitly determined (without using CFSG), by Zassenhaus, Feit, Ito and Suzuki for $t = 2$, and by Gorenstein and Hughes for larger values.

(However, infinite examples are easy to construct and exist in profusion: there is an action of the free group of countable rank with this property for any value of t.)

It is also not known whether there is a similar geometric characterisation of groups in which all greedy bases have the same size.

Blaha [1992] showed that irredundant and greedy bases are not too much larger than the smallest possible:

Theorem 2. *Let G be a permutation group of degree n with minimal base size $b(G)$. Then*

(a) *any irredundant base for G has size at most $b(G)\log n$ (logarithm to base 2)*;

(b) *any greedy base for G has size at most $b(G)(\log\log n + c)$.*

Blaha proved that these bounds are essentially best possible. But for primitive groups, stronger results should be possible. It is conjectured, for example, that if G is primitive, then a greedy base for G has size at most $cb(G)$, where c is a universal constant. Indeed, the limit superior of the ratio of greedy base size to base size, as $b(G) \to \infty$, is conjectured to be $\frac{9}{8}$. The extreme examples involve the symmetric group S_m acting on the set of 2-element subsets of $\{1, \ldots, m\}$. The greedy algorithm chooses disjoint 2-sets until almost all elements of $\{1, \ldots, m\}$ have been covered, and then has to go back and extend two disjoint pairs to a 4-vertex path, giving a base of size roughly $\frac{3}{4}m$; on the other hand, covering most of $\{1, \ldots, m\}$ by 3-vertex paths gives a base of size roughly $\frac{2}{3}m$.

Recently, Coen Del Valle and Colva Roney-Dougal have given the exact value of the base size for the symmetric group of degree n acting on r-sets for $2 \le r \le n/2$. The result is complicated to state, depending on the relative sizes of n and r.

We conclude with two further occurrences of bases.

(a) The first fractional exponential bound for the order of a uniprimitive (primitive but not 2-transitive) permutation group of degree n was found by Babai [1981]. He showed that such a group has a base whose size is bounded by $4\sqrt{n}\log n$. It is clear that a group with degree n and a base of size b has order at most n^b. (Soon after Babai's result appeared, it was observed that much stronger results could be found using the classification of finite simple groups: a bound $n^{c\log n}$ with "known" exceptions. These exceptions are the so-called *large-base groups* which are explained below.)

(b) Graph theorists have considered the *metric dimension* of a connected graph, the smallest d for which there is a d-tuple $(v_1, \ldots, v_d)$ of vertices such that any vertex is uniquely determined by its d-tuple of distances from these vertices. It is clear that such a d-tuple is a base for the automorphism group of the graph. The occurrence of similar concepts in very different fields led to a lot of repetition and rediscovery, which my survey with Robert Bailey [Bailey and Cameron 2011] sets out to clear up.

These two things are related. Babai's proof involved constructing from the group a set of binary relations called a *coherent configuration* and showing that this configuration has relatively small "dimension" (using the relations in the configuration in place of graph distances).

A large-base group is either a symmetric or alternating group S_n or A_n in its action on the set of k-subsets of $\{1, \ldots, n\}$, or a subgroup of the wreath product of such a group with the symmetric group of degree l containing the socle A_n^l of

this group. Their base sizes are fractional powers of the degree, and so their orders are roughly $n^{n^{1/kl}}$. Often in computational group theory it is necessary to treat the large-base groups separately.

There has been a lot of very recent activity around permutation group bases. Scott Harper remarked that the result about IBIS groups gives us powerful information about permutation groups where all irredundant bases have the same size, but the groups for which all minimal bases have the same size has at present no comparable theory. One could ask similar questions about "greedy bases" in Blaha's sense.

It is also appropriate to mention here the work of Gill, Lodà and Spiga [Gill et al. 2022] on a parameter they call *height*, which is the maximum size of an independent set (where a set is *independent* if its pointwise stabiliser is properly contained in the pointwise stabiliser of any subset). They showed that the height of a primitive permutation group of degree n which is not a large-base group is smaller than $9 \log n$. This parameter then gives a bound for the *relational complexity* of a permutation group, a parameter introduced by Cherlin [Cherlin 2016; Cherlin et al. 1996], in connection with the model theory of finite permutation groups: the relational complexity is at most the height plus one.

To elaborate: the relational complexity of G is the least k for which G is an automorphism group of a homogeneous relational structure with arity k; more precisely, it is the least k such that, for any $n \geq k$, if $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are two n-tuples of points, they lie in the same G-orbit if and only if all corresponding sub-k-tuples $(a_{i_1}, \ldots, a_{i_k})$ and $(b_{i_1}, \ldots, b_{i_k})$ lie in the same G-orbit.

Gill et al. also proved a similar bound on the maximum size of an irredundant base for a primitive permutation group.

6. Finite group parameters

In this final section I discuss a few "measures" of a finite group which are related to base size of permutation actions of the group. As we will see, some of these can be defined in terms of the subgroup lattice of G, a topic with a long history but still many open problems: see [Schmidt 1994] for a fairly recent account.

The smallest number $d(G)$ of generators of G is not a good measure of size, since arbitrarily large finite groups (such as symmetric groups) are 2-generated. We can avoid this problem as follows. If f is a function from finite groups to natural numbers, let

$$f^{\uparrow}(G) = \max\{f(H) : H \leq G\}.$$

For any f, the function $f^{\uparrow}$ is monotonic (in the sense that $G \leq H$ implies $f^{\uparrow}(G) \leq f^{\uparrow}(H)$). For example, for the symmetric groups, we have $d^{\uparrow}(S_n) = \lfloor n/2 \rfloor$ for $n > 3$ [McIver and Neumann 1987].

Define two other measures as follows:

(a) $\mu(G)$ is the maximal size of a minimal (under inclusion) generating set for G. The parameter $\mu(G)$ is important in the analysis of a random walk on generating sets for G; see [Diaconis and Saloff-Coste 1998]. For the symmetric groups we have $\mu(S_n) = \mu^{\uparrow}(S_n) = n - 1$ [Whiston 2000].

(b) $l(G)$ is the length of the largest subgroup chain in G. This is an interesting measure which bounds various other measures, and was considered by Babai [1986]. It has the nice properties that it is monotonic and, if N is a normal subgroup of G, then $l(G) = l(N) + l(G/N)$; so its value is determined by the composition factors of G. In 1982, I showed that

$$l(S_n) = \left\lceil \frac{3n}{2} \right\rceil - b(n) - 1,$$

where $b(n)$ is the number of 1s in the base 2 representation of n. This appears in a paper with Solomon and Turull [Cameron et al. 1989]; these authors have computed $l(G)$ for various simple groups G.

Given a finite group G, we define three numbers $b_1(G)$, $b_2(G)$, $b_3(G)$ as follows. In each case, the maximum is taken over all permutation representations of G (not necessarily faithful).

- $b_1(G)$ is the maximum, over all representations, of the maximum size of an irredundant base.
- $b_2(G)$ is the maximum, over all representations, of the maximum size of a minimal base.
- $b_3(G)$ is the maximum, over all representations, of the minimum base size.

Clearly we have $b_3(G) \le b_2(G) \le b_1(G)$. These inequalities can be strict. The group $G = \mathrm{PSL}(2, 7)$ has $b_1(G) = 5$, $b_2(G) = 4$, and $b_3(G) = 3$.

Proposition 1. $b_1(G) = l(G)$.

Proof. An irredundant base $(x_1, \ldots, x_k)$ gives a descending chain of subgroups $G = G_0 > G_1 > \cdots > G_k$, where G_i is the pointwise stabiliser of $\{x_1, \ldots, x_i\}$. Conversely, given a chain of subgroups, take the union of the coset spaces of these subgroups, and form a base by choosing the given subgroups in the order given. □

There is a connection between b_2 and μ. Let $B(n)$ denote the Boolean lattice of subsets of an n-set, and $L(G)$ the subgroup lattice of G.

Proposition 2. *Let G be a finite group.*

(a) *The largest n such that $B(n)$ is embeddable as a join-semilattice of $L(G)$ is $\mu^{\uparrow}(G)$.*

(b) *The largest n such that $B(n)$ is embeddable as a meet-semilattice of $L(G)$ in such a way that the minimal element is a normal subgroup of G is $b_2(G)$.*

(c) *$B(n)$ is embeddable as a meet-semilattice in $L(G)$ if and only if it is embeddable as a join-semilattice.*

Proof. (a) If $\{g_1, \ldots, g_n\}$ is an independent set in G, then the subgroups generated by subsets of this set form a join-semilattice isomorphic to $B(n)$. Conversely, given such a semilattice of the subgroup lattice, choose elements g_i contained in all the maximal subgroups except the i-th.

(b) Given a minimal base of size n, the subgroups stabilising subsets of the base form a meet-semilattice whose minimal element is the kernel of the group action. Conversely, suppose we have an embedding of $B(n)$ as meet-semilattice. Then, reversing order, we have subgroups H_I for each $I \subseteq N = \{1, \ldots, n\}$, with H_N normal in G and $H_i \cap H_J = H_{I \cup J}$. Consider the permutation representation on the union of the coset spaces $H_{\{i\}}$ for $i \in N$. The kernel of this representation is H_N, and the subgroups $H_{\{i\}}$ form a minimal base of size n.

(c) Suppose first that $B(n)$ is a join-semilattice of $L(G)$. Let $N = \{1, \ldots, n\}$. Then, for every subset I of N, there is a subgroup H_I of G, and $H_{I \cup J} = \langle H_I, H_J \rangle$ for any two subsets I and J. Moreover, all these subgroups are distinct. In particular, $H_i \not\leq H_{N \setminus \{i\}}$ for all i (where H_i is shorthand for $H_{\{i\}}$); else

$$H_N = \langle H_i, H_{N \setminus \{i\}} \rangle = H_{N \setminus \{i\}},$$

contrary to assumption.

Let $K_i = H_{N \setminus \{i\}}$, and, for any $I \subseteq N$, put

$$K_I = \bigcap_{i \in I} K_i,$$

with the convention that $K_\emptyset = G$. We claim that all the subgroups K_I are distinct. Suppose that two of them are equal, say $K_I = K_J$. By interchanging I and J if necessary, we may assume that there exists $i \in I \setminus J$. But then $H_i \leq K_J$ while $H_i \not\leq K_I$, a contradiction.

Now it is clear that $K_I \cap K_J = K_{I \cup J}$, so that we have an embedding of $B(n)$ as meet-semilattice (where we have reversed the order-isomorphism to simplify the notation).

The reverse implication is proved by an almost identical argument. □

It is not known whether the extra condition in (b) is really necessary: perhaps $b_2(G) = \mu^\uparrow(G)$ for any G. (Note that $\mu^\uparrow(G)$ is the size of the largest independent set of elements of G.)

Much less is known about $b_3(G)$. If G is a nonabelian finite simple group, then $b_3(G)$ can be computed by looking only at the primitive actions of G.

One could ask similar questions about greedy bases. Nothing is known.

Another question: in which of these results can the use of CFSG be avoided?

Acknowledgement

I am very grateful to two reviewers whose careful and thoughtful reviews have substantially improved this paper.

References

[Araújo and Fountain 2004] J. Araújo and J. Fountain, "The origins of independence algebras", pp. 54–67 in *Semigroups and languages* (Lisbon, 2002), edited by I. M. Araújo et al., World Sci. Publ., River Edge, NJ, 2004. MR Zbl

[Araújo et al. 2011] J. Araújo, M. Edmundo, and S. Givant, "v^*-algebras, independence algebras and logic", *Internat. J. Algebra Comput.* **21**:7 (2011), 1237–1257. MR Zbl

[Araújo et al. 2022] J. Araújo, W. Bentz, P. J. Cameron, M. Kinyon, and J. Konieczny, "Matrix theory for independence algebras", *Linear Algebra Appl.* **642** (2022), 221–250. MR Zbl

[Babai 1981] L. Babai, "On the order of uniprimitive permutation groups", *Ann. of Math.* (2) **113**:3 (1981), 553–568. MR Zbl

[Babai 1986] L. Babai, "On the length of subgroup chains in the symmetric group", *Comm. Algebra* **14**:9 (1986), 1729–1736. MR Zbl

[Babai 2015] L. Babai, "Graph isomorphism in quasipolynomial time", preprint, 2015. arXiv 1512.03547

[Bailey and Cameron 2011] R. F. Bailey and P. J. Cameron, "Base size, metric dimension and other invariants of groups and graphs", *Bull. Lond. Math. Soc.* **43**:2 (2011), 209–242. MR Zbl

[Blaha 1992] K. D. Blaha, "Minimum bases for permutation groups: the greedy approximation", *J. Algorithms* **13**:2 (1992), 297–306. MR Zbl

[Cameron and Deza 1979] P. J. Cameron and M. Deza, "On permutation geometries", *J. London Math. Soc.* (2) **20**:3 (1979), 373–386. MR Zbl

[Cameron and Fon-Der-Flaass 1995] P. J. Cameron and D. G. Fon-Der-Flaass, "Bases for permutation groups and matroids", *European J. Combin.* **16**:6 (1995), 537–544. MR Zbl

[Cameron and Szabó 2000] P. J. Cameron and C. Szabó, "Independence algebras", *J. London Math. Soc.* (2) **61**:2 (2000), 321–334. MR Zbl

[Cameron et al. 1989] P. J. Cameron, R. Solomon, and A. Turull, "Chains of subgroups in symmetric groups", *J. Algebra* **127**:2 (1989), 340–352. MR Zbl

[Cherlin 2016] G. Cherlin, "On the relational complexity of a finite permutation group", *J. Algebraic Combin.* **43**:2 (2016), 339–374. MR Zbl

[Cherlin et al. 1996] G. L. Cherlin, G. A. Martin, and D. H. Saracino, "Arities of permutation groups: wreath products and k-sets", *J. Combin. Theory Ser. A* **74**:2 (1996), 249–286. MR Zbl

[Diaconis and Saloff-Coste 1998] P. Diaconis and L. Saloff-Coste, "Walks on generating sets of groups", *Invent. Math.* **134**:2 (1998), 251–299. MR Zbl

[Fountain and Lewin 1992] J. Fountain and A. Lewin, "Products of idempotent endomorphisms of an independence algebra of finite rank", *Proc. Edinburgh Math. Soc.* (2) **35**:3 (1992), 493–500. MR Zbl

[Giansiracusa and Giansiracusa 2018] J. Giansiracusa and N. Giansiracusa, "A Grassmann algebra for matroids", *Manuscripta Math.* **156**:1-2 (2018), 187–213. MR Zbl

[Gill et al. 2022] N. Gill, B. Lodà, and P. Spiga, "On the height and relational complexity of a finite permutation group", *Nagoya Math. J.* **246** (2022), 372–411. MR Zbl

[Gould 1995] V. Gould, "Independence algebras", *Algebra Universalis* **33**:3 (1995), 294–318. MR Zbl

[Grätzer 1963] G. Grätzer, "A theorem on doubly transitive permutation groups with application to universal algebras", *Fund. Math.* **53** (1963), 25–41. MR Zbl

[Kerby 1974] W. Kerby, *On infinite sharply multiply transitive groups*, Hamburger Mathematische Einzelschriften (N.F.) **6**, Vandenhoeck & Ruprecht, Göttingen, 1974. MR Zbl

[Maund 1989] T. Maund, *Bases for permutation groups*, D.Phil. thesis, Oxford University, 1989.

[McIver and Neumann 1987] A. McIver and P. M. Neumann, "Enumerating finite groups", *Quart. J. Math. Oxford Ser.* (2) **38**:152 (1987), 473–488. MR Zbl

[Rips et al. 2017] E. Rips, Y. Segev, and K. Tent, "A sharply 2-transitive group without a non-trivial abelian normal subgroup", *J. Eur. Math. Soc.* (*JEMS*) **19**:10 (2017), 2895–2910. MR Zbl

[Schmidt 1994] R. Schmidt, *Subgroup lattices of groups*, De Gruyter Expositions in Mathematics **14**, Walter de Gruyter & Co., Berlin, 1994. MR Zbl

[Sims 1970] C. C. Sims, "Computational methods in the study of permutation groups", pp. 169–183 in *Computational problems in abstract algebra* (Oxford, 1967), edited by J. Leech, Pergamon, Oxford-New York-Toronto, Ont., 1970. MR Zbl

[Tits 1952] J. Tits, "Sur les groupes doublement transitifs continus", *Comment. Math. Helv.* **26** (1952), 203–224. MR Zbl

[Urbanik 1966] K. Urbanik, "Linear independence in abstract algebras", *Colloq. Math.* **14** (1966), 233–255. MR Zbl

[Whiston 2000] J. Whiston, "Maximal independent generating sets of the symmetric group", *J. Algebra* **232**:1 (2000), 255–268. MR Zbl

[Wilke 1972] F. W. Wilke, "Pseudo-fields and doubly transitive groups", *Bull. Austral. Math. Soc.* **7** (1972), 163–168. MR Zbl

[Zassenhaus 1935] H. Zassenhaus, "Über endliche Fastkörper", *Abh. Math. Sem. Univ. Hamburg* **11**:1 (1935), 187–220. MR Zbl

[Zilber 1984] B. I. Zilber, "Strongly minimal countably categorical theories, II", *Sibirsk. Mat. Zh.* **25**:3 (1984), 71–88. MR Zbl

[Zilber 1988a] B. Zilber, "Finite homogeneous geometries", pp. 186–208 in *Proceedings of the 6th Easter Conference on Model Theory* (Wendisch Rietz, Germany, 1988), edited by B. Dahn and H. Wolter, Seminarberichte **98**, Humboldt Univ., Berlin, 1988. MR Zbl

[Zilber 1988b] B. I. Zilber, "Hereditarily transitive groups and quasi-Urbanik structures", *Trudy Inst. Mat.* (*Novosibirsk*) **8** (1988), 58–77. In Russian; translated in *Amer. Math. Soc. Transl. Ser.* 2 **195** (1999), 165–186. MR Zbl

Received 4 Dec 2022. Revised 10 Apr 2023.

PETER J. CAMERON:

pjc20@st-andrews.ac.uk
School of Mathematics and Statistics, University of St Andrews, North Haugh, St Andrews, United Kingdom

Model Theory

msp.org/mt

See inside back cover or msp.org/mt for submission instructions.

Model Theory (ISSN 2832-904X electronic, 2832-9058 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

MT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
https://msp.org/

Model Theory

no. 2 vol. 3 2024

Special issue on the occasion of the 75th birthday of
Boris Zilber