Base size and separation number

Peter J. Cameron

CSG notes, April 2005

Brief history

The concept of a base for a permutation group was introduced by Sims in the 1960s in connection with computational group theory. It has proved to be of theoretical importance as well. For example, Babai [1] used it in 1981 to give an elementary bound for the order of a primitive but not 2-transitive permutation group. Babai's proof uses only combinatorial and probabilistic methods, although stronger results can be proved using the Classification of Finite Simple Groups.

At the Slovenian Graph Theory conference in 2003, Mohar defined the rigidity number and separation number of a graph. The rigidity number is just the base size of the automorphism group, and the separation number is a related combinatorial invariant. With hindsight, it is actually separation number rather than base size which occurs in Babai's proof. Both of these concepts can be defined for arbitrary permutation groups. Here I say a few words about the relation between them, and pose a couple of problems.

Definitions

Let G be a permutation group on a set X, of degree $n = |X|$. The *minimum base size* $\beta(G)$ is the smallest cardinality of a set of points whose pointwise stabiliser is the identity. (Such a set is called a *base*.) The *separation number* $\sigma(G)$ is the minimum number k for which there exist points $x_1, \ldots, x_k$ such that any two points are in distinct orbits of the stabiliser of at least one of $x_1, \ldots, x_k$. (A set with this property is called a *separating set*.)

For example, let G be the dihedral group of order 8 (the symmetry group of a square). Two vertices on an edge of the square form both a base and a separating set. It is clear that no smaller such sets can exist. So $\beta(G) = \sigma(G) = 2$.

Bases are interesting to permutation group theorists because of the following simple result:

Fact 0 $2^{\beta(G)} \leq |G| \leq n^{\beta(G)}$.

The upper bound holds because the images of a base under different group elements must be different, and there are at most $n^{\beta(G)}$ such images. The lower bound is true because a point which is fixed by its predecessors is 'redundant' and cannot occur in a base of minimal size: so the stabiliser of the first i points of the base is a proper subgroup in the stabiliser of the first $i-1$, and has index at least 2.

Results and problems

Fact 1 For any permutation group G, we have $\beta(G) \leq \sigma(G)$.

For a separating set is clearly a base.

Fact 2 If $H \leq G$, then $\beta(H) \leq \beta(G)$ and $\sigma(H) \leq \sigma(G)$.

For a base, resp. separating set for G is also a base, resp. separating set, for H.

Fact 3 If G_i acts on X_i for $i = 1, 2$, and $G_1 \times G_2$ acts on $X_1 \cup X_2$ (disjoint union), then $\beta(G_1 \times G_2) = \beta(G_1) + \beta(G_2)$ and $\sigma(G_1 \times G_2) = \sigma(G_1) + \sigma(G_2)$.

For fixing points in X_2 does not decrease the size of the group induced on X_1 or *vice versa*; so a base for $G_1 \times G_2$ must contain bases for G_1 and G_2. Similarly, no point in X_2 can separate a pair of points of X_1 in the same G_1-orbit or *vice versa*; so a separating set for G must contain separating sets for both G_1 and G_2. Conversely, the union of two bases (resp. separating sets) is a base (resp. separating set) for G.

Fact 4 If G is not the trivial group, then $\sigma(G) = 1$ if and only if $\beta(G) = 1$.

The forward implication is clear from Fact 1. If $\{x\}$ is a base, then all G_x-orbits are singletons, so any two points lie in different G_x-orbits; that is, $\{x\}$ is separating.

In general, $\sigma(G)$ is not bounded by any function of $\beta(G)$, even for primitive groups, as we will see. (Recall that a permutation group G is *primitive* on X if there is no G-invariant equivalence relation on X apart from equality and the 'universal' relation $X \times X$; and G is *doubly transitive* on X if it is transitive on the set of ordered pairs of distinct elements of X.)

Fact 5 Let G have degree $n > 2$.Then $\sigma(G) \leq n-1$, with equality if and only if G is doubly transitive.

For all but one point of X clearly forms a separating set. Now suppose that $\sigma(G) = n-1$. Then for any $x_1 \neq x_2$, the set $X \setminus \{x_1, x_2\}$ is not separating; so x_1 and x_2 lie in the same G_{x_3} orbit for any $x_3 \neq x_1, x_2$. Thus G_{x_3} is transitive on $X \setminus \{x_3\}$ for any $x_3 \in X$, and G is doubly transitive.

Fact 6 Let G be transitive of degree n and let G_x have r orbits on $X \setminus \{x\}$. Then

$$n \leq \sigma(G) + r^{\sigma(G)}.$$

For G has r orbits $O_1, \ldots, O_r$ on ordered pairs of distinct points; let

$$O_i(x) = \{y : (x,y) \in O_i\}, \qquad O_i^*(x) = \{y : (y,x) \in O_i\}.$$

Let $\{x_1, \ldots, x_k\}$ be a separating set with $k = \sigma(G)$. Any additional point x can be labelled with the k-tuple $(i_1, \ldots, i_k)$, where $x \in O_{i_j}(x_j)$ (that is, $x_j \in O_{i_j}^*(x)$). By the definition of separating set, distinct points get distinct labels; so $n - k \leq r^k$.

Example Let

$$G = \{x \mapsto a^2 x + b : a, b \in F, a \neq 0\},$$

where F is the Galois field of odd order q. Now G is primitive with $\beta(G) = 2$. In the notation of the preceding fact, $r = 2$, so $\sigma(G) + 2^{\sigma(G)} \geq q$, so $\sigma(G) \geq \log_2 q - 1$.

Bojan Mohar has shown that $\sigma(G)$ is indeed about $\log q$.

Note that adjoining field automorphisms (i.e. taking the full automorphism group of the Paley graph) doesn't change the separation number, while the base size becomes 3 if q is not prime.

Examples There are, on the other hand, many transitive groups with $\sigma(G) = \beta(G)$. Examples include:

- The dihedral group of order $2n$ ($n \geq 3$), acting on the vertices of an n-gon. For two points x_1, x_2, there are at most two points y for which they lie in the same G_y-orbit; if there are two, they are antipodal. So two non-antipodal points form a separating set. (Such sets are precisely the minimal bases.)

- For the symplectic group, preserving a non-degenerate alternating bilinear form on a vector space V over a finite field F, the base size and separation number are both equal to $\dim(V)$. For there is no smaller base: any set of fewer than $\dim(V)$ vectors is contained by a hyperplane, and so fixed by a transvection. But the orbits of G_v (for $v \neq 0$) are the sets

$$\{w \in V : v \cdot w = c\}$$

for $c \in F$, $c \neq 0$, as well as the set

$$\{w \in V \setminus \langle v \rangle : v \cdot w = 0\}.$$

and the singletons $\{\lambda v\}$ for each $\lambda \in F$. Any vector is uniquely determined by its inner products with the vectors of a basis for V; the orbits contain more refined information, so any two points are separated by a basis.

Example If $G = S_m$ acting on 2-element subsets of $\{1,\ldots,m\}$, for $m \geq 3$, we have

$$\sigma(G) = \begin{cases} \beta(G), & \text{if } m = 5 \text{ or if 3 divides } m; \\ \beta(G)+1, & \text{otherwise.} \end{cases}$$

Here is the proof. We represent a set of 2-subsets of $\{1,\ldots,m\}$ as the edge set of a graph on n vertices. It is clear that a graph is a base if and only if it has at most one isolated vertex and no isolated edge. If the graph contains a cycle, then it is not a minimal base, since one edge of the cycle is fixed by the stabilisers of all the others. So a minimal base is a forest. It is clear that the smallest such base is a disjoint union of paths of length 2 together with some 'end effects' as follows: if $m = 3k$, no end effect necessary; if $m = 3k+1$, one isolated vertex; if $m = 3k+2$, join one of the two extra vertices to a vertex in the union of paths. Thus the minimum base size is $2k$ if $m = 3k$ or $m = 3k+1$, and is $2k+1$ if $m = 3k+2$.

To finish the proof we need two facts about separating sets in this case.

(a) A forest whose components are stars on at least three vertices is a separating set. For suppose that two pairs $\{x,y\}$ and $\{u,v\}$ are not separated. Since the orbits of the stabiliser of $\{x,y\}$ are the singleton $\{\{x,y\}\}$, the pairs meeting $\{x,y\}$ in one point, and the pairs not meeting $\{x,y\}$, it must be the case that $\{x,y\}$ and $\{u,v\}$ are non-edges and every edge meeting $\{x,y\}$ meets $\{u,v\}$ and vice versa. So the two pairs must either be contained in the same component, or must meet the same two components. A short case analysis shows that this is impossible.

This shows that if $m = 3k$, the minimum base is a separating set (necessarily minimal).

(b) A forest containing an isolated vertex a and a path $\{b,c,d\}$ of length 2 is not a separating set. For the pairs $\{a,c\}$ and $\{b,d\}$ are not separated.

If m is not divisible by 3, and $m \neq 5$, then any minimum base contains an isolated vertex and a path of length 2, so is not separating. However, assuming that the base is a union of stars (as we may), joining the isolated vertex to the centre of one of the stars gives a separating set, by (a). So the separation number is one larger than the minimum base size.

For $n = 5$ it is easily checked directly that the minimum base $\{\{1,2\},\{1,3\},\{1,4\}\}$ is a separating set.

Fact 7 If G is primitive but not 2-transitive with degree n, then

$$\sigma(G) \leq 4n^{1/2}\log n.$$

This is the theorem of Babai [1]. The example of S_m acting on 2-sets described above shows that it is best possible apart from a factor $c\log n$. Since $\beta(G) \leq \sigma(G)$ and $|G| \leq n^{\beta(G)}$, we see that

$$|G| \leq n^{4n^{1/2}\log n}.$$

Remark One can define the notion of irredundant separating set as is done for irredundant bases: the points are chosen in order, and each new point strictly decreases the meet of the orbit partitions. There are also versions of the greedy algorithm: choose each new point so that the largest part of the meet is minimised, or so that the number of parts is maximised. (See [4] for irredundant bases and [2] for greedy bases.)

Remark Using the Classification of Finite Simple Groups, very strong results have been proved about the base size of primitive groups. For example:

- Either G is S_m or A_m acting on 2-sets, with $n = m(m-1)/2$, or a subgroup of $S_m \wr S_2$ (in the product action) containing A_m^2, with $n = m^2$, or else $\beta(G) \leq cn^{1/3}\log^2 n$ (this follows easily from the estimates for $|G|$ in [3]);
- if G is almost simple, then either G is a symmetric or alternating group acting on subsets or partitions, or a classical group acting on an orbit of subspaces in its natural module, or $\beta(G)$ is bounded by an absolute constant (a conjecture made in [5], proved in [6]).

It would be interesting to know whether any similar results (perhaps with an extra $\log n$ factor) hold for the separation number. Specifically:

Problem: Is it true that $\sigma(G) \leq C\beta(G)\log n$ for any primitive, not 2-transitive, permutation group G, for some constant C?

References

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

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

[3] P. J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), 1–22.

[4] P. J. Cameron and D. G. Fon-Der-Flaass, Bases for permutation groups and matroids, *Europ. J. Combinatorics* **16** (1995), 537–544.

[5] P. J. Cameron and W. M. Kantor, Random permutations: Some group-theoretic aspects, *Combinatorics, Probability and Computing* **2** (1993), 257–262.

[6] M. W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497–520.