Bases for permutation groups

Lecture 1

Tim Burness, University of Bristol

Overview

- **Lecture 1.**
  - Introduction, examples and connections
  - Base size bounds for primitive groups
  - Pyber's conjecture and related problems

- **Lecture 2.** Pyber's base size conjecture

- **Lecture 3.** Cameron's base size conjecture

- **Lecture 4.** Applications (e.g. generation, extreme primitivity)

- **Lecture 5.** Base-two groups and the Saxl graph

t.burness@bristol.ac.uk

https://seis.bristol.ac.uk/∼tb13602/padova2021.html

▸ Link

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group.

Definition

A subset B of Ω is a **base** for G if the pointwise stabilizer of B is trivial, i.e. $\bigcap_{\alpha \in B} G_\alpha = 1$.

The **base size** of G, denoted by $b(G)$, is the minimal cardinality of a base.

- If G is transitive and $H = G_\alpha$, then $b(G)$ is the minimal cardinality of a subset $S \subseteq G$ such that
$$\bigcap_{g \in S} H^g = 1.$$
- Note that Ω itself is a base for G.
- $b(G) = 1 \iff G$ has a regular orbit on Ω.

Examples

(1) $G = S_n$, $\Omega = \{1, \ldots, n\}$: $b(G) = n - 1$

(2) $G = A_n$, $\Omega = \{1, \ldots, n\}$: $b(G) = n - 2$

(3) $G = D_{2n}$, $\Omega = \{1, \ldots, n\}$: $b(G) = 2$

(4) $G = \mathrm{GL}(V)$, $\Omega = V$:

A subset of V is a base iff it contains a basis for V, so $b(G) = \dim V$.

(5) Similarly, if $G = \mathrm{PGL}(V)$, $d = \dim V > 1$ and $\Omega = P(V)$ (the set of 1-dimensional subspaces of V), then $b(G) = d + 1$:

If $\{v_1, \ldots, v_d\}$ is a basis for V, then $\{\langle v_1 \rangle, \ldots, \langle v_d \rangle, \langle v_1 + \cdots + v_d \rangle\}$ is a base of minimal size.

A historical perspective

Notice that each group element is uniquely determined by its action on a base B: if $x, y \in G$ then

$$\alpha^x = \alpha^y \text{ for all } \alpha \in B \iff xy^{-1} \in \bigcap_{\alpha \in B} G_\alpha \iff x = y.$$

In particular, if Ω is finite then $|G| \leqslant |\Omega|^{b(G)}$.

The problem of bounding $|G|$ in terms of $|\Omega|$ attracted significant interest in the 19th century, and the above observation motivated early investigations of bases.

This is related to the ambitious problem set by the Paris Academy for the Grand Prix de Mathématiques of 1860, which asked for a classification of the subgroups of S_n of index k.

A computational connection

The **base and strong generating set** (BSGS) concept was introduced by **Sims (1970)** as a fundamental data structure for calculating with finite permutation groups on a computer.

Let $B = \{\alpha_1, \dots, \alpha_b\}$ be a base for G and consider the chain of stabilizers

$$G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots \geqslant G^{(b-1)} \geqslant G^{(b)} = 1,$$

where $G^{(k)} = \bigcap_{i=1}^{k} G_{\alpha_i}$. A subset $S \subseteq G$ is a **strong generating set** relative to B if $G^{(k)} = \langle S \cap G^{(k)} \rangle$ for all k.

Example

If $G = S_n$ and $\Omega = \{1, \dots, n\}$, then

$$S = \{(1,2), (2,3), \dots, (n-1, n)\}$$

is a strong generating set relative to the base $B = \{1, \dots, n-1\}$.

The **Schreier–Sims algorithm** provides an efficient way to construct a BSGS from a given generating set.

A BSGS allows basic tasks such as computing $|G|$ and testing membership in G to be achieved in polynomial time. For example

$$|G^{(b-1)}| = |\alpha_b^{G^{(b-1)}}|, \ |G^{(b-2)}| = |G^{(b-1)}||\alpha_{b-1}^{G^{(b-2)}}|, \ldots, |G| = \prod_{i=1}^{b} |\alpha_i^{G^{(i-1)}}|$$

As a consequence, this concept plays a fundamental role in computer algebra systems such as **GAP** and **Magma**.

The associated algorithms will be more efficient if $|B| \ll |\Omega|$.

A small base B also provides an efficient way to store the elements of G, using $|B|$-tuples, rather than $|\Omega|$-tuples.

Further connections

Abstract group theory. Let G be a group and let H be a core-free subgroup: view G as a permutation group on the set of cosets of H.

In this setting,

$$b(G) = \text{minimal cardinality of a subset } S \subseteq G \text{ with } \bigcap_{g \in S} H^g = 1$$

Graph theory. Let Γ be a graph with vertex set V and automorphism group G, viewed as a permutation group on V. Then

$$\begin{aligned} b(G) &= \text{the } \textbf{fixing number} \text{ of } \Gamma \\ &= \text{the } \textbf{determining number} \text{ of } \Gamma \\ &= \text{the } \textbf{rigidity index} \text{ of } \Gamma \end{aligned}$$

is a well-studied graph invariant.

Some related concepts

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with $|\Omega|$ finite.

Definition

A base $B \subseteq \Omega$ is **minimal** if no proper subset of B is a base. Let $B(G)$ be the maximal size of a minimal base.

Example

Let $G = S_m$ and $\Omega = \{$2-element subsets of $\{1, \ldots, m\}\}$. Assume $m \equiv 1 \pmod 3$ and observe that

$$B_1 = \{\{1,2\},\{2,3\},\ \ \{4,5\},\{5,6\},\ \ldots,\ \{m-2,m-1\}\}$$
$$B_2 = \{\{1,2\},\{1,3\},\ldots,\{1,m-1\}\}$$

are both minimal bases, where $|B_1| = \frac{2}{3}(m-1)$ and $|B_2| = m-2$.

Fact. $b(G) = \frac{2}{3}(m-1)$ (Halasi, 2012), $B(G) = m-2$ (Gill & Loda, 2021)

Definition

A subset $S \subseteq \Omega$ is **independent** if

$$\bigcap_{\alpha \in S} G_\alpha < \bigcap_{\beta \in T} G_\beta$$

for every proper subset T of S. The **height** of G, denoted $H(G)$, is the maximum size of an independent set.

Definition

An ordered sequence $[\alpha_1, \ldots, \alpha_t]$ of points in Ω is an **irredundant base** if $\{\alpha_1, \ldots, \alpha_t\}$ is a base and every inclusion in the chain

$$G = G^{(0)} > G^{(1)} > G^{(2)} > \cdots > G^{(t-1)} > G^{(t)} = 1$$

is proper, where $G^{(k)} = \bigcap_{i=1}^{k} G_{\alpha_i}$.

The size of the longest irredundant base is denoted $I(G)$.

Further connections

Note. $b(G) \leqslant B(G) \leqslant H(G) \leqslant I(G) \leqslant b(G) \log_2 |\Omega|$.

The invariants $B(G), H(G)$ and $I(G)$ have not been intensively studied, but an interesting connection to **relational complexity** has recently emerged via the bound

$$\mathrm{RC}(G) \leqslant H(G) + 1.$$

This concept has origins in the model theory of relational structures.

For more details, see

- **Gill, Loda, Spiga:** *On the height and relational complexity of a finite permutation group*, arXiv:2005.03942
- **Gill, Loda:** *Statistics for S_n acting on k-sets*, arXiv:2101.08644

Some further reading

- Bailey, Cameron: *Base size, metric dimension and other invariants of groups and graphs*, Bull. Lond. Math. Soc. 43 (2011), 209–242.
- Burness: Chapter 5 in *Simple groups, fixed point ratios and applications*, in Local representation theory and simple groups, 267–322, EMS Ser. Lect. Math., Eur. Math. Soc., 2018.
- Cameron: Chapter 4 in *Permutation groups*, LMS Student Texts, 45, CUP, 1999.
- Liebeck, Shalev: *Bases of primitive permutation groups*, Groups, combinatorics & geometry (Durham, 2001), 147–154, WSP, 2003.
- Seress: Chapter 4 in *Permutation group algorithms*, Cambridge Tracts in Mathematics, 152, CUP, 2003.

Calculating $b(G)$

In general, calculating the **exact** base size of a finite permutation group is a difficult problem.

- There is no known efficient algorithm for calculating $b(G)$, or for constructing a base of minimal size.
- **Blaha (1992):** Determining if $b(G) \leqslant c$ for a given constant c is an **NP-complete** problem.

A small base can be constructed using a **greedy algorithm** – choose $\alpha_k \in \Omega$ from an orbit of $\bigcap_{i=1}^{k-1} G_{\alpha_i}$ of largest possible size.

Blaha (1992) shows that this yields a base of size $O(b(G) \log\log |\Omega|)$.

Typically, we are interested in obtaining "good" bounds on $b(G)$.

First bounds

Let G be a finite permutation group of degree n. If $\{\alpha_1, \ldots, \alpha_b\}$ is a base of minimal size then each inclusion in the stabilizer chain

$$G > G^{(1)} > G^{(2)} > \cdots > G^{(b-1)} > 1$$

is proper (where $G^{(k)} = \bigcap_{i=1}^{k} G_{\alpha_i}$) and we deduce that

$$2^b \leqslant |G| \leqslant \prod_{i=0}^{b-1}(n-i) \leqslant n^b.$$

This gives the following elementary result:

Proposition

If G is a permutation group of degree n, then

$$\frac{\log |G|}{\log n} \leqslant b(G) \leqslant \log_2 |G|.$$

$$\frac{\log |G|}{\log n} \leqslant b(G) \leqslant \log_2 |G|$$

It is easy to find transitive groups at both ends of this range:

- If $G = S_n$ and $\Omega = \{1, \ldots, n\}$, then

$$b(G) = n - 1 < 2\frac{\log |G|}{\log n}$$

- If $G = C_2 \wr C_{n/2}$ and $\Omega = \{1, \ldots, n\}$, then

$$b(G) = n/2 = \log_2 |G| - \log_2(n/2) > \frac{1}{2} \log_2 |G|$$

Note. The first example is **primitive**, while the latter is **imprimitive**.

Primitivity

Recall that a transitive group $G \leqslant \mathrm{Sym}(\Omega)$ is **primitive** if Ω has no nontrivial G-invariant partitions.

Equivalently: G_α is a maximal subgroup of G.

The finite primitive groups are described by the **O'Nan-Scott Theorem**, which partitions the groups into five families, according to the structure and action of the **socle**:

(1) Diagonal type (2) Product type (3) Twisted wreath type

(4) Affine (5) Almost simple

Combined with **CFSG**, this gives a powerful approach for studying bases of finite primitive groups.

But first let us recall some results obtained using "classical" methods.

Theorem (Bochert, 1889)

Let $G \neq A_n, S_n$ be a primitive group of degree n. Then $b(G) \leqslant n/2$.

Proof. Suppose B is a base with $|B| = b(G) > n/2$. Then $C = \Omega \setminus B$ is not a base, so there exists $1 \neq x \in \bigcap_{\alpha \in C} G_\alpha$ and $\mathrm{supp}(x) \subseteq B$ where

$$\mathrm{supp}(x) = \{\alpha \in \Omega \,:\, \alpha^x \neq \alpha\}.$$

Fix $\alpha \in \mathrm{supp}(x)$. By minimality, $B \setminus \{\alpha\}$ is not a base, so there exists $1 \neq y \in \bigcap_{\beta \in B \setminus \{\alpha\}} G_\beta$. Note that

$$\mathrm{supp}(y) \subseteq \Omega \setminus (B \setminus \{\alpha\}) = C \cup \{\alpha\}.$$

Now $\mathrm{supp}(y) \cap B \neq \emptyset$ since B is a base, so α is the only point in Ω moved by both x and y.

This implies that $[x, y] \in G$ is a 3-cycle and thus G contains A_n by a theorem of Jordan. Contradiction. ∎

Babai's bound

Theorem (Babai, 1981/2)

Let $G \neq A_n, S_n$ be a primitive group of degree n.

- If G is not 2-transitive, then $b(G) < 4\sqrt{n}\log_e n$.
- If G is 2-transitive, then $b(G) < c^{\sqrt{\log n}}$ for some absolute constant c.

- Babai's ingenious proof does **not** use CFSG: in the simply primitive case, there is a translation into a more general, purely combinatorial, problem concerning coherent configurations.
- **Pyber (1993)** improved the bound for 2-transitive groups (also without CFSG): $b(G) < c(\log n)^2$ for some absolute constant c.
- There is a nice discussion of these results in **Dixon & Mortimer** (see Sections 5.3 and 5.6).

The simply primitive case

For $\alpha, \beta \in \Omega$, let $\Psi_{\alpha\beta} = \{\gamma \in \Omega : \alpha, \beta$ are in different G_γ-orbits$\}$.

Easy check. $S \subseteq \Omega$ is a base if $S \cap \Psi_{\alpha\beta} \neq \emptyset$ for all distinct $\alpha, \beta \in \Omega$.

Set $n = |\Omega|$, $b(G) = k + 1$ and $d = \min\{|\Psi_{\alpha\beta}| : \alpha, \beta \in \Omega, \alpha \neq \beta\}$.

Let Δ be the set of k-element subsets of Ω.

For $S \in \Delta$, let $\chi_{\alpha\beta}(S) = 1$ if $S \cap \Psi_{\alpha\beta} = \emptyset$, o.w. $\chi_{\alpha\beta}(S) = 0$.

Define $m = \sum \chi_{\alpha\beta}(S)$, summing over all $S \in \Delta$ and $\alpha, \beta \in \Omega$, $\alpha \neq \beta$.

Easy check. By estimating m in two different ways, we get

$$2\binom{n}{k} \leqslant m \leqslant n(n-1)\binom{n-d}{k}$$

and thus $k < n(2\log_e n - \log_e 2)/d$.

Final step. $d > \sqrt{n}/2$, which gives $b(G) < 4\sqrt{n}\log_e n$. ■

Liebeck's bound

Stronger bounds can be proved using CFSG:

Theorem (Liebeck, 1984)

Let $G \neq A_n, S_n$ be a primitive group of degree n. Then either

- $b(G) < 9\log_2 n$; or
- $(A_m)^r \trianglelefteq G \leqslant S_m \wr S_r$, where $r \geqslant 1$ and the action of S_m is on k-sets and the wreath product has the product action of degree $\binom{m}{k}^r$.

In particular, $b(G) < c\sqrt{n}$ for some absolute constant c.

This is best possible (up to constants):

- e.g. $G = \mathrm{AGL}_d(2)$, $\Omega = (\mathbb{F}_2)^d$: $b(G) = d + 1 = \log_2 n + 1$
- e.g. $G = S_m$, $\Omega = \{\text{2-sets}\}$: $b(G) = \lceil 2(m-1)/3 \rceil$ and $n = \binom{m}{2}$

Comments on the proof

Step 1. Use **O'Nan-Scott** to reduce to almost simple groups.

Step 2. Combine **CFSG** and results on the subgroup structure of simple groups to show that either $|G_\alpha| < |G|^{8/9}$ (so $|G| < n^9$), or G is a **standard** group (e.g. $G = S_m$ acting on k-sets).

Step 3. If $|G| < n^9$ then $b(G) \leqslant \log_2 |G| < 9 \log_2 n$. Otherwise G is standard and appropriate bases can be constructed explicitly.

By applying more recent results on bases, the constant in Liebeck's main bound can be improved:

Theorem (Moscatiello & Roney-Dougal, 2020)

If G is primitive of degree n, and not "large base", then

$$b(G) \leqslant \max\{\lceil \log_2 n \rceil + 1, 7\}.$$

Pyber's conjecture

Recall that if G is a permutation group of degree n, then

$$\frac{\log|G|}{\log n} \leqslant b(G) \leqslant \log_2|G|$$

A highly influential conjecture of Pyber asserts that every finite **primitive** group has a small base in the following sense:

Conjecture (Pyber, 1993)

There is an absolute constant c such that

$$b(G) \leqslant c\,\frac{\log|G|}{\log n}$$

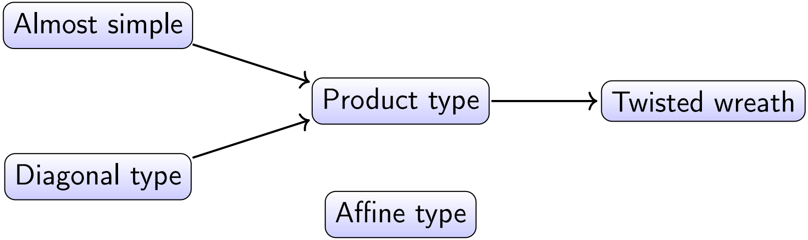
for every primitive group G of degree n.

Comments on the proof

The proof of Pyber's conjecture was finally completed by **Duyan, Halasi and Maróti (2018)**, building on earlier work by Benbenishty, Fawcett, Liebeck, Seress, Shalev and others.

The basic strategy: apply the **O'Nan-Scott Theorem** and handle each family of primitive groups in turn.

None are straightforward and there is certainly no easy reduction to almost simple groups. The final case involved a certain class of affine groups.



Solvable groups

A special case of Pyber's conjecture was settled by Seress in a much stronger form:

Theorem (Seress, 1996)

If G is a finite solvable primitive group, then $b(G) \leqslant 4$.

- If G is solvable and primitive, then $\mathrm{soc}(G)$ is elementary abelian and it is straightforward to show that $G = VH \leqslant \mathrm{AGL}(V)$ is **affine**, where $V = (\mathbb{F}_p)^d$ and $H \leqslant \mathrm{GL}(V)$ is irreducible.
- If H is a finite solvable group and V is a faithful irreducible $\mathbb{F}_p H$-module, then there exist $v_1, v_2, v_3 \in V$ such that $\bigcap_i C_H(v_i) = 1$.
- The bound is best possible: by work of **Pálfy** and **Wolf**, there are infinitely many solvable primitive groups G of degree n with $|G| > n^3$.

Comments on the proof

It suffices to show that $b(H) \leqslant 3$ w.r.t the action of H on V. There are two cases to consider: H is **primitive** or **imprimitive** as a linear group.

- Notice that $b(H) = 1$ iff $\bigcup_{1 \neq x \in H} C_V(x) \neq V$.
- *H* **primitive:** Seress extends earlier work of **Gluck & Manz (1987)** on $|C_V(x)|$ to show that $b(H) = 1$ in "most" cases.
- *H* **imprimitive:** Here $H \leqslant L \wr T \leqslant \mathrm{GL}(V)$, where $L \leqslant \mathrm{GL}(V_1)$ is primitive and $T \leqslant S_k$ is transitive (both L and T are solvable).

  Seress proves that $d(T) \leqslant 5$, where $d(T)$ is the **distinguishing number** of T: there is a partition of $\{1, \ldots, k\}$ into at most 5 parts such that no $1 \neq x \in T$ preserves each part of the partition.

  By combining this with the fact that $b(L) \leqslant 3$ (for the action of L on V_1), he shows that $b(L \wr T) \leqslant 3$ and thus $b(H) \leqslant 3$.

An example

Suppose H preserves a decomposition $V = V_1 \oplus \cdots \oplus V_k$, where $\dim V_i = \ell$ and $H \leqslant L \wr T \leqslant \mathrm{GL}(V)$ with $L \leqslant \mathrm{GL}(V_1)$ primitive.

Let $\{1, \ldots, k\} = P_1 \cup \cdots \cup P_5$ be a distinguishing partition for $T \leqslant S_k$.

The case $b(L) = 1$. Let $w_1 \in V_1$ be in a regular L-orbit and let $w_i \in V_i$ be an image of w_1 under T. Define $v_1, v_2, v_3 \in V$ as follows:

$$v_1 = \sum_{i \in P_1 \cup P_2 \cup P_3} w_i, \;\; v_2 = \sum_{i \in P_1 \cup P_4} w_i, \;\; v_3 = \sum_{i \in P_2 \cup P_5} w_i$$

Suppose $g \in L \wr T$ fixes v_1, v_2 and v_3. Let $i \in P_1$ and write $V_i^g = V_j$.

Since g fixes v_1 and v_2, we have $j \in (P_1 \cup P_2 \cup P_3) \cap (P_1 \cup P_4) = P_1$, so g preserves P_1.

Similarly, g preserves $P_2, \ldots, P_5$, which forces $g \in L^k$ and thus $g = 1$.

Almost simple groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be an **almost simple** primitive group of degree n with socle G_0 and point stabilizer H.

Definition

We say that G is **standard** if one of the following holds:

- $G_0 = A_m$ and Ω is an orbit of subsets or partitions of $\{1, \ldots, m\}$;
- $G_0 = \mathrm{Cl}(V)$ is classical and Ω is an orbit of subspaces (or pairs of subspaces) of V.

The proof of Liebeck's $b(G) < 9 \log_2 n$ bound uses the fact that $|G| < n^9$ if G is **non-standard**: Is $b(G)$ bounded by an absolute constant?

Conjecture (Cameron, 1990s)

There is an absolute constant c such that $b(G) \leqslant c$ for every non-standard group G. Moreover, $c = 7$ is best possible.

Next week

- **Pyber's conjecture:**
  - Main results
  - Overview of the proof
  - Bases for almost simple primitive groups: standard vs non-standard
- **Cameron's conjecture:**
  - Main results
  - Probabilistic methods

Some references

- Babai: *On the order of uniprimitive permutation groups*, Annals of Math. **113** (1981), 553–568.
- Babai: *On the order of doubly transitive permutation groups*, Invent. Math. **65** (1982), 473–484.
- Blaha: *Minimum bases for permutation groups: the greedy approximation*, J. Algorithms **13** (1992), 297–306.
- Bochert: *Über die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann*, Math. Ann. **33** (1889), 584–590.
- Liebeck: *On minimal degrees and base sizes of primitive permutation groups*, Arch. Math. **43** (1984), 11–15.
- Pyber: *Asymptotic results for permutation groups*, in Groups and Computation (eds. L. Finkelstein and W. Kantor), DIMACS Series, vol. 11, pp.197–219, 1993.
- Seress: *The minimal base size of primitive solvable permutation groups*, J. London Math. Soc. **53** (1996), 243–255.