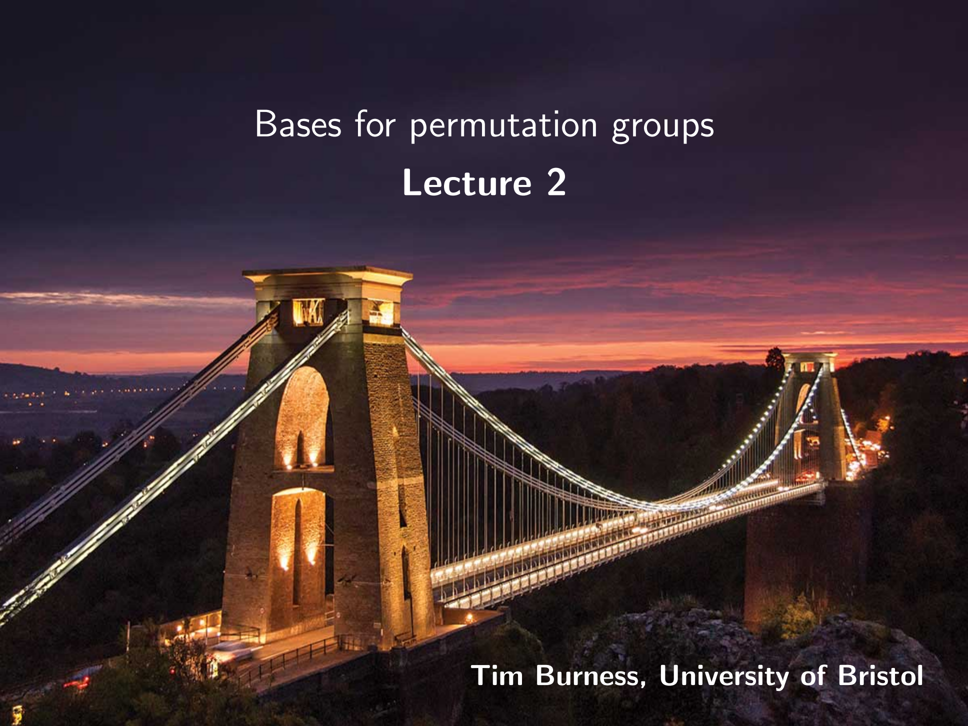
Bases for permutation groups

Lecture 2



Tim Burness, University of Bristol

Today

- **Pyber's base size conjecture:**
  - Main results and key steps in the proof
  - Almost simple groups: standard vs non-standard
  - Base sizes for almost simple primitive groups
- **Cameron's base size conjecture:**
  - Main results
  - Probabilistic methods

t.burness@bristol.ac.uk

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

Link

Pyber's conjecture

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

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

Pyber's conjecture 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.

Main results

Various people worked on Pyber's conjecture over a 25-year period; the final step was completed by Duyan, Halasi and Maróti:

Theorem (Duyan, Halasi & Maróti, 2018)

There exists an absolute constant $c > 0$ such that

$$b(G) \leqslant 45\frac{\log|G|}{\log n} + c$$

for every primitive group G of degree n.

Theorem (Halasi, Liebeck & Maróti, 2019)

If G is a finite primitive group of degree n, then

$$b(G) \leqslant 2\frac{\log|G|}{\log n} + 24$$

The constants

The multiplicative constant in the HLM bound is best possible.

Example

Let $G = VH \leqslant \mathrm{AGL}(V)$, where $H = \mathrm{Sp}_d(p)$ and $V = (\mathbb{F}_p)^d$.

Claim. $b(G) = d + 1$, which equals $\lfloor 2 \log_n |G| \rfloor - 2$ for $p \gg 0$.

The bound $b(G) \leqslant d + 1$ is clear (any basis of V is a base for H).

It remains to show that if $U \subseteq V$ is any subspace with $\dim U = d - 1$, then there exists $1 \neq h \in H$ acting trivially on U.

Write $V = U \oplus \langle y \rangle$ and $U^{\perp} = \langle x \rangle$ (w.r.t. the symplectic form on V).

Then

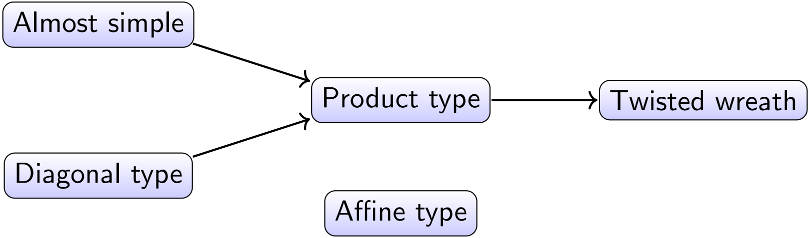
$$h : u + \lambda y \mapsto u + \lambda(x + y)$$

has the desired property.

Strategy for the proof

Recall that the **O'Nan-Scott Theorem** partitions the finite primitive groups into five families.

The proof of Pyber's conjecture proceeds by considering each family of primitive groups in turn, none of which are straightforward.



The final step, handled by DHM, concerned the affine groups $G = VH$ with $H \leqslant \mathrm{GL}(V)$ imprimitive.

Diagonal type

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive **diagonal type** group of degree n, so

$$T^k \trianglelefteqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$$

where $k \geqslant 2$, T is a nonabelian simple group, $P \leqslant S_k$ and $n = |T|^{k-1}$.

We may identify Ω with T^k/D, where $D = \{(t, \ldots, t) \,:\, t \in T\} < T^k$.

Here $P \leqslant S_k$ is the group induced by the conjugation action of G on the k factors of $\mathrm{soc}(G) = T^k$.

Fact. G primitive $\implies$ either P is primitive, or $k = 2$ and $P = 1$.

Theorem (Fawcett, 2013)

We have

$$\left\lceil \frac{\log |G|}{\log n} \right\rceil \leqslant b(G) \leqslant \left\lceil \frac{\log |G|}{\log n} \right\rceil + 2.$$

In fact, $b(G) = 2$ if $P \neq A_k, S_k$.

An example

Suppose $G = T \times T$ and $\Omega = G/D$, where $D = \{(t,t) \,:\, t \in T\}$.

Here $\log|G|/\log n = 2$ and we claim that $b(G) = 3$.

First observe that $b(G) \geqslant 3$ since

$$\{(t,t) \,:\, t \in C_T(b^{-1}a)\} \neq 1$$

is the stabilizer in D of the coset $D(a,b) \in \Omega$.

Recall that $T = \langle x, y \rangle$ is 2-generated (via CFSG) and note that

$$\{(t,t) \,:\, t \in C_T(x) \cap C_T(y)\} = 1$$

is the pointwise stabilizer of $\{D, D(x,1), D(y,1)\}$, so $b(G) \leqslant 3$.

Another example

Let $G = T^k.(\mathrm{Out}(T) \times P)$ where $k \geqslant 33$ and $P \neq A_k, S_k$.

Seress (1997): There exists $\Gamma \subseteq \{1, \ldots, k\}$ such that $P_\Gamma = 1$.

(This is false for $P = \mathrm{AGL}_5(2)$ with $k = 2^5 = 32$.)

Write $T = \langle x, y \rangle$ and $\{1, \ldots, k\} = \Delta_1 \cup \Delta_2 \cup \Gamma$ (disjoint) with $|\Delta_i| \neq |\Gamma|$.

Define $D(t_1, \ldots, t_k) \in \Omega$, where $t_i = 1$ if $i \in \Delta_1$, $t_i = x$ if $i \in \Delta_2$ and $t_i = y$ if $i \in \Gamma$.

Claim. $\{D, D(t_1, \ldots, t_k)\}$ is a base.

Suppose $g = (\varphi, \ldots, \varphi)\pi \in G$ fixes $D(t_1, \ldots, t_k)$, where $\varphi \in \mathrm{Aut}(T)$. Then there exists $s \in T$ such that $(t_{i^{\pi^{-1}}})^\varphi = st_i$ for all i.

This implies that $\pi \in P_\Gamma = 1$ and $x^\varphi = x$, $y^\varphi = y$, so $g = 1$.

Product type

These groups arise as "blow-ups" of almost simple or diagonal type primitive groups.

We have $T^k \trianglelefteqslant G \leqslant L \wr P$, where

- $L \leqslant \mathrm{Sym}(\Gamma)$ is primitive with socle T (almost simple or diagonal);
- $P \leqslant S_k$ is induced by the conjugation action of G on the $k \geqslant 2$ factors of $\mathrm{soc}(G) = T^k$; and
- G acts on $\Omega = \Gamma \times \cdots \times \Gamma = \Gamma^k$ with its **product action**.

Fact. G primitive $\implies$ P is transitive.

Theorem (B & Seress, 2015)

Pyber's conjecture holds for primitive groups of product type.

Key tool: The distinguishing number

Definition

Let $P \leqslant \mathrm{Sym}(\Delta)$ be a transitive permutation group of degree $k \geqslant 2$.

The **distinguishing number** of P, denoted $d(P)$, is the minimal number of colours needed to colour the elements of Δ so that the stabilizer in P of this colouring is trivial.

For example, $d(S_k) = k$ and $d(A_k) = k - 1$. Note that $|P| < d(P)^k$.

Theorem

- **Seress (1996)**: P solvable $\implies d(P) \leqslant 5$
- **Seress (1997), Dolfi (2000)**: If $P \neq A_k, S_k$ is primitive then $d(P) \leqslant 4$, with $d(P) = 2$ if $k \geqslant 33$
- **Duyan, Halasi & Maróti (2018)**: $\sqrt[k]{|P|} < d(P) \leqslant 48 \sqrt[k]{|P|}$

A special case

Recall that $T^k \trianglelefteqslant G \leqslant L \wr P$, $L \leqslant \mathrm{Sym}(\Gamma)$, $\Omega = \Gamma^k$ and $|\Delta| = k$.

Let $\{\gamma_1, \ldots, \gamma_b\}$ be a base for L, $b = b(L)$, and set $\alpha_i = (\gamma_i, \ldots, \gamma_i) \in \Omega$.

If $g = (x_1, \ldots, x_k)\pi \in G$ fixes each α_i, then $\gamma_i^{x_j} = \gamma_i$ for all i, j and thus $g = (1, \ldots, 1)\pi$. Set $m = \lceil \log_{|\Gamma|} d(P) \rceil$.

Fact. There is a set of partitions $X_1, \ldots, X_m$ of Δ, each with at most $|\Gamma|$ parts, such that their pointwise stabilizer in P is trivial.

There is a set of partitions $X_1, \ldots, X_m$ of Δ, each with at most $|\Gamma|$ parts, such that their pointwise stabilizer in P is trivial.

Example. $\Delta = \{0, \ldots, 9\}$, $P = S_{10}$, $|\Gamma| = 5$, $m = \lceil \log_5 10 \rceil = 2$

For $\ell \in \Delta$, write $\ell = a_1(\ell) + 5a_2(\ell)$ with $a_i(\ell) \in \{0, 1, 2, 3, 4\}$.

For $i \in \{1, 2\}$ and $j \in \{0, 1, 2, 3, 4\}$, set

$$X_{i,j} = \{\ell \in \{0, \ldots, 9\} \,:\, a_i(\ell) = j\}$$

and define

$$\begin{aligned} X_1 &= X_{1,0} \cup X_{1,1} \cup \cdots \cup X_{1,4} = \{0, 5\} \cup \{1, 6\} \cup \{2, 7\} \cup \{3, 8\} \cup \{4, 9\} \\ X_2 &= X_{2,0} \cup X_{2,1} = \{0, 1, 2, 3, 4\} \cup \{5, 6, 7, 8, 9\} \end{aligned}$$

Then the pointwise stabilizer in P of X_1 and X_2 is trivial.

A special case

Let $\{\gamma_1, \ldots, \gamma_b\}$ be a base for L, $b = b(L)$, and set $\alpha_i = (\gamma_i, \ldots, \gamma_i) \in \Omega$.

If $g = (x_1, \ldots, x_k)\pi \in G$ fixes each α_i, then $\gamma_i^{x_j} = \gamma_i$ for all i, j and thus $g = (1, \ldots, 1)\pi$. Set $m = \lceil \log_{|\Gamma|} d(P) \rceil$.

Fact. There is a set of partitions $X_1, \ldots, X_m$ of Δ, each with at most $|\Gamma|$ parts, such that their pointwise stabilizer in P is trivial.

This allows us to define a collection of points $\beta_1, \ldots, \beta_m$ in Ω such that $(1, \ldots, 1)\pi \in \bigcap_i G_{\beta_i}$ iff $\pi = 1$. Therefore

$$b(G) \leqslant m + b(L) \leqslant \log_{|\Gamma|} d(P) + b(L) + 1 < \log_n |P| + b(L) + 4$$

since $d(P) \leqslant 48\sqrt[k]{|P|}$ and $|\Gamma| \geqslant 5$.

If L is **almost simple** and $b(L) \leqslant c\frac{\log |L|}{\log |\Gamma|}$, then $b(G) \leqslant c\frac{\log |G|}{\log n} + c + 4$ since $|L| \leqslant |T||\Gamma|$ and $|G| \geqslant |T|^k|P|$.

Twisted wreath type

Here $G = T^k{:}P \leqslant \mathrm{Sym}(\Omega)$, where $\mathrm{soc}(G) = T^k$ with T simple and $P \leqslant S_k$ is transitive. Since T^k is regular, we have $n = |\Omega| = |T|^k$.

Then $G \leqslant L \leqslant \mathrm{Sym}(\Omega)$, where $L = T^2 \wr P = (T^2)^k{:}P$ is primitive of product type, so

$$b(G) \leqslant b(L) \leqslant c\frac{\log|L|}{\log n} < 2c\frac{\log|G|}{\log n}$$

by the result for product type groups.

Theorem (Fawcett, 2013/21)

We have

$$\left\lceil \frac{\log|G|}{\log n} \right\rceil \leqslant b(G) \leqslant \left\lceil \frac{\log|G|}{\log n} \right\rceil + 2.$$

Moreover, $b(G) = 2$ if P is (quasi)primitive.

Affine groups

Here $G = VH \leqslant \mathrm{AGL}(V)$, where $V = (\mathbb{F}_p)^d$ with p prime and $H \leqslant \mathrm{GL}(V)$ is the stabilizer of the zero vector.

Fact. G primitive $\implies$ H acts irreducibly on V

Recall that $b(G) = b(H) + 1$.

Some special cases:

- H solvable: $b(G) \leqslant 4$ by **Seress (1996)**
- $(p, |H|) = 1$: $b(G) \leqslant 95$ by **Gluck & Magaard (1998)**

  In fact, $b(G) \leqslant 3$ by **Halasi & Podoski (2016)**

So we may assume H is nonsolvable and p divides $|H|$.

Recall that H is **primitive** if it does not preserve a nontrivial direct sum decomposition of V.

Affine groups: primitive vs imprimitive

Theorem

Let $G = VH \leqslant \mathrm{AGL}(V)$ be a primitive affine group of degree n with point stabilizer $H \leqslant \mathrm{GL}(V)$.

- H primitive: $b(H) \leqslant 18 \log_n |H| + c$ (Liebeck & Shalev, 2002/14)
- H imprim: $b(H) \leqslant 45 \log_n |H| + c$ (Duyan, Halasi & Maróti, 2018)

In fact, $b(G) \leqslant 2 \log_n |G| + 16$ (Halasi, Liebeck & Maróti, 2019).

Note that if H preserves the decomposition $V = V_1 \oplus \cdots \oplus V_k$, then H acts transitively on the summands (by irreducibility).

So the induced group $P \leqslant S_k$ is transitive and the bound $d(P) \leqslant 48 \sqrt[k]{|P|}$ is a key tool for bounding $b(H)$.

Almost simple groups

To complete our discussion of Pyber's base size conjecture, let us assume $G \leqslant \mathrm{Sym}(\Omega)$ is **almost simple**.

Here $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for some nonabelian simple group G_0 (the **socle** of G) and $H = G_\alpha$ is a maximal subgroup of G with $G = HG_0$.

By the **Classification of Finite Simple Groups**, one of the following holds:

- $G_0 = A_m$ is an alternating group with $m \geqslant 5$
- G_0 is one of 26 sporadic simple groups: $\mathrm{M}_{11}, \mathrm{M}_{12}, \ldots, \mathbb{B}, \mathbb{M}$
- G_0 is a classical group: $\mathrm{L}_m(q)$, $\mathrm{U}_m(q)$, $\mathrm{PSp}_m(q)$, $\mathrm{P\Omega}^{\epsilon}_m(q)$
- G_0 is an exceptional group: ${}^2B_2(q), {}^2G_2(q), \ldots, E_7(q), E_8(q)$

In studying bases for almost simple primitive groups, it is natural to make a distinction between **standard** and **non-standard** groups.

Intuitively, if G is standard then $|H|$ is "big" and typically $b(G)$ can be arbitrarily large.

Example. If $G = \mathrm{PGL}_m(q)$ and Ω is the set of 1-dimensional subspaces of $(\mathbb{F}_q)^m$, then $|G| \sim q^{m^2-1}$ and $|\Omega| \sim q^{m-1}$, so

$$b(G) \geqslant \log_{|\Omega|} |G| \sim m+1$$

can be arbitrarily large (in fact, $b(G) = m+1$).

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 is classical and Ω is an orbit of subspaces (or pairs of subspaces) of the natural module V.

Otherwise, G is **non-standard**.

Standard actions of alternating and symmetric groups

Suppose $G \leqslant \mathrm{Sym}(\Omega)$ is a **standard** group with socle $G_0 = A_m$ and point stabilizer H. Then either

- H is of type $S_k \times S_{m-k}$ with $1 \leqslant k < m/2$; or
- H is of type $S_b \wr S_a$ with $m = ab$ and $a, b \geqslant 2$.

Here Ω is the set of k-element subsets of $\{1, \ldots, m\}$ in the first case, and the set of partitions of $\{1, \ldots, m\}$ into a parts of size b in the second.

Typically, bounds on $b(G)$ in these cases are obtained by constructing explicit bases.

Theorem (Benbenishty, 2005)

Pyber's conjecture holds when G is standard and $G_0 = A_m$.

Action on k-sets

Suppose $G_0 = A_m$ and Ω is the set of k-element subsets of $\{1, \ldots, m\}$, where $1 \leqslant k < m/2$.

The exact base size is **not** known in all cases. The best result is:

Theorem (Halasi, 2012)

Suppose $G = S_m$ and $\Omega = \{k\text{-sets}\}$ with $1 \leqslant k < m/2$. Then

$$\left\lceil \frac{2m-2}{k+1} \right\rceil \leqslant b(G) \leqslant \lceil \log_{\lceil m/k \rceil} m \rceil \cdot (\lceil m/k \rceil - 1)$$

and the lower bound is equality if $k \leqslant \sqrt{m}$.

In particular, **[HLM, 2019]** show that $b(G) \leqslant 2 \log_{|\Omega|} |G| + 16$.

Action on partitions

Theorem (Benbenishty, Cohen & Niemeyer, 2007)

Suppose $G = S_m$ and Ω is the set of partitions of $\{1, \ldots, m\}$ into a parts of size b, where $a, b \geqslant 2$.

- If $a \geqslant b > 2$ then $b(G) \leqslant 6$.
- If $a < b$ then $\lceil \log_a b \rceil \leqslant b(G) \leqslant \lceil \log_a b \rceil + 3$.

Example. If $G = S_8$ and $H = S_4 \wr S_2$, then $b(G) = 5 = \lceil \log_a b \rceil + 3$.

In recent work, the **exact** base size has been computed in **all** cases.

Action on partitions

Theorem

Suppose $G = S_m$ and Ω is the set of partitions of $\{1, \dots, m\}$ into a parts of size b, where $a, b \geqslant 2$.

- **B, Garonzi & Lucchini (2020), James (2006):** If $a \geqslant b$ and $(a, b) \neq (2, 2)$, then

$$b(G) = \begin{cases} 4 & \text{if } (a,b) = (3,2) \\ 2 & \text{if } b \geqslant 3 \text{ and } a \geqslant \max\{b+3, 8\} \\ 3 & \text{otherwise} \end{cases}$$

- **Morris & Spiga (2021):** If $a < b$ then

$$b(G) = \begin{cases} \lceil \log_a(b+3) \rceil + 1 & \text{if } a = 2,\ b \neq 4 \\ \lceil \log_a(b+2) \rceil + 1 & \text{if } a \geqslant 3,\ (a,b) \neq (3,7) \\ 5 & \text{if } (a,b) = (2,4) \\ 4 & \text{if } (a,b) = (3,7) \end{cases}$$

Standard actions of classical groups

Suppose $G \leqslant \mathrm{Sym}(\Omega)$ is a **standard** group with classical socle $G_0 = \mathrm{Cl}(V)$ and point stabilizer H. Then either

- H is the stabilizer in G of an appropriate subspace of V;
- $G_0 = \mathrm{L}_m(q)$, $G \not\leqslant \mathrm{P\Gamma L}_m(q)$ and H is the stabilizer in G of an appropriate pair of subspaces of V; or
- $G_0 = \mathrm{Sp}_m(q)$, q is even and $H \cap G_0 = \mathrm{O}^{\pm}_m(q)$.

Once again, bounds on $b(G)$ are usually obtained by explicit constructions.

Theorem

- **Benbenishty (2005):** Pyber's conjecture holds when G is a standard classical group.
- **Halasi, Liebeck & Maróti (2019):** $b(G) \leqslant 2\log_{|\Omega|}|G| + 16$.

Non-standard groups

Now assume $G \leqslant \mathrm{Sym}(\Omega)$ is a **non-standard** group with socle G_0 and point stabilizer H.

Roughly speaking, this means that one of the following holds:

- G_0 is a sporadic or an exceptional group.
- $G_0 = A_m$ and $H \cap G_0$ acts **primitively** on $\{1, \ldots, m\}$.
- $G_0 = \mathrm{Cl}(V)$ is a classical group and $H \cap G_0$ acts **irreducibly** on V.

Remark. If G is classical then **Aschbacher's theorem** implies that H is contained in one of the subgroup collections labelled $\mathcal{C}_1, \ldots, \mathcal{C}_8, \mathcal{S}$.

Then "non-standard" means that $H \notin \mathcal{C}_1$ (and we also exclude one case in $\mathcal{C}_8$: $G_0 = \mathrm{Sp}_m(q)$, q even, H type $\mathrm{O}^{\pm}_m(q)$).

Recall the following result of **Liebeck** from last week:

Theorem (Liebeck, 1984)

If G is a non-standard group of degree n, then $|G| < n^9$.

We remark that this can be strengthened as follows:

Theorem (Liebeck & Saxl, 1992)

Either $|G| < n^5$ or $(G, n) = (\mathrm{M}_{23}, 23)$, $(\mathrm{M}_{24}, 24)$.

So for Pyber's conjecture, we need to show there exists an absolute constant c such that $b(G) \leqslant c$ for every non-standard group G.

Cameron's conjecture

Let $G \leqslant \mathrm{Sym}(\Omega)$ be non-standard of degree n.

Conjecture

- **Cameron & Kantor (1993):** There exists an absolute constant c such that almost every c-tuple of points in Ω is a base for G.
- **Cameron (1999):** $b(G) \leqslant 7$, with equality iff $(G, n) = (\mathrm{M}_{24}, 24)$.

Theorem

- **Liebeck & Shalev (1999):** The C-K conjecture is true (with an undetermined constant), hence Pyber holds for non-standard groups.
- **B et al. (2007-11):** Cameron's conjecture is true, and almost every 6-tuple is a base.

Next week

- The proof of Cameron's conjecture
- Fixed point ratios for groups of Lie type
- Extensions of Cameron's conjecture
- Bases for primitive groups with solvable stabilizers

Some references

- Benbenishty: *On actions of primitive groups*, PhD thesis, The Hebrew University of Jerusalem, 2005.
- Burness: *On base sizes for actions of finite classical groups*, J. London Math. Soc. **75** (2007), 545–562.
- Burness: *On base sizes for almost simple primitive groups*, J. Algebra **516** (2018), 38–74.
- Burness, Garonzi, Lucchini: *Finite groups, minimal bases and the intersection number*, submitted (arXiv:2009.10137)
- Burness, Guralnick, Saxl: *On base sizes for symmetric groups*, Bull. London Math. Soc. **43** (2011), 386–391.
- Burness, Liebeck, Shalev: *Base sizes for simple groups and a conjecture of Cameron*, Proc. London Math. Soc. **98** (2009), 116–162.

- Burness, O'Brien, Wilson: *Base sizes for sporadic simple groups*, Israel J. Math. **177** (2010), 307–334.
- Burness, Seress: *On Pyber's base size conjecture*, Trans. Amer. Math. Soc. **367** (2015), 5633–5651.
- Cameron, Kantor: *Random permutations: some group-theoretic aspects*, Combin. Probab. Comput. **2** (1993), 257–262.
- Duyan, Halasi, Maróti: *A proof of Pyber's base size conjecture*, Adv. Math. **331** (2018), 720–747.
- Fawcett: *The base size of a primitive diagonal group*, J. Algebra **375** (2013), 302–321.
- Fawcett: *Bases of twisted wreath products*, submitted (arXiv:2102.02190)
- Halasi: *On the base size for the symmetric group acting on subsets*, Studia Sci. Math. Hungar. **49** (2012), 492–500.

- Halasi, Liebeck, Maróti: *Base sizes of primitive groups: Bounds with explicit constants*, J. Algebra **521** (2019), 16–43.
- James: *Partition actions of symmetric groups and regular bipartite graphs*, Bull. London Math. Soc. **38** (2006), 224–232.
- Liebeck, Shalev: *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), 497–520.
- Liebeck, Shalev: *Bases of primitive linear groups II*, J. Algebra **403** (2014), 223–228.
- Morris, Spiga: *On the base size of the symmetric and the alternating group acting on partitions*, preprint (arXiv:2102.10428)