Imperial College London

Bases of Primitive Permutation Groups

How to store lots of symmetry in a small amount of space

Melissa Lee and Martin W. Liebeck

EPSRC Engineering and Physical Sciences Research Council

Motivation

Groups form an integral part of many areas of science. For example,

- In **chemistry**, group theory provides a method for determining whether two molecules are isomeric.
- In **quantum physics**, groups and their representations are used to describe the quantum states of elementary particles.

When the objects of study are large, it often becomes difficult to store the relevant permutation groups efficiently on a computer.

Bases were first formally defined by Sims [5] in the early 1970s as a method for storing enormous permutation groups in a small amount of computer memory.

Definitions

A **base** for a permutation group G acting on a set Ω is a subset $B \subseteq \Omega$ such that the pointwise stabiliser G_B is trivial.

Bases are useful because **the action of every permutation is determined by how it acts on the elements of a base.**

So we can characterise the action of each $g \in G$ on Ω by how it acts on B, rather than the whole of Ω. This can save a lot of computer memory, especially if $|B|$ is much smaller than $|\Omega|$.

Therefore, we are interested in determining the size of the **smallest base** of G acting on Ω.

We call this the **base size** and denote it by $b(G)$.

Lemma

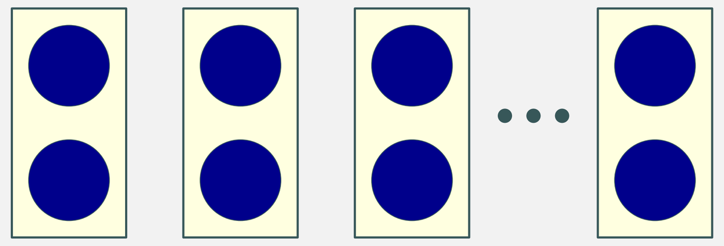
The base size $b(G)$ of the action of a permutation group G on a set Ω of size n satisfies

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

Example 1: "Wild" base size

Not all groups have small bases.

Let $G = C_2^k \wr C_k$ acting on k sets of size 2.



Then $b(G) = \frac{n}{2} = k$, while

$$\frac{\log|G|}{\log n} = \frac{\log(2^k k)}{\log(2k)} = \frac{k + \log_2 k}{\log_2 k + 1}.$$

Here the base size is half of the size of Ω, so we haven't made much improvement to the amount of information needed to describe the action.

Example 2: Primitive groups

We restrict our focus to **primitive groups** because they usually have "small" bases compared to the size of Ω.

Let $G = S_k$ ($k \geq 4$), and let Ω be the set of pairs from $\{1, \ldots, n\}$.

Then

$$\frac{\log|G|}{\log n} = \frac{\log(k!)}{\log(k^2)} > \frac{k}{4}$$

and

$$b(G) = \lceil \frac{2k-2}{3} \rceil < \frac{2k}{3} < \frac{8\log|G|}{3\log n}.$$

So we can find an upper bound for $b(G)$ of the form $c\frac{\log|G|}{\log n}$ for some scalar c.

Conjecture (Pyber (1993))

Let G be a primitive permutation group acting on Ω, with $|\Omega| = n$. Then there exists an absolute constant c such that

$$b(G) \leq c\frac{\log|G|}{\log n}.$$

Pyber's conjecture proved

After contributions from many authors, the conjecture was settled in the affirmative in 2016.

Theorem (Duyan, Halasi & Maróti (2016))

There is a universal constant $c > 0$ such that $b(G)$ of a primitive permutation group G of degree n satisfies

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

The proof uses the classification of primitive groups given in the **O'Nan–Scott Theorem**.

Our work over the past year has been to improve the bound in this conjecture.

Our theorem

A major case in improving the bound is where G is a group whose layer $E(G)$ is **quasisimple**. That is, $E(G)/Z(E(G))$ is a **finite simple group**. The following theorem gives an improvement in this case.

Theorem (L., Liebeck, (2017))

Let $V = V_d(q)$ ($q = p^e$, p prime) and $G \leq GL(V)$, and suppose that $E(G)$ is quasisimple and absolutely irreducible on V. Then one of the following holds:

a) $E(G) = \mathrm{A}_m$ and V is the natural A_m-module over $\mathbb{F}_q$, of dimension $d = m - \delta(p, m)$;

b) $E(G) = Cl_d(q_0)$, a classical group with natural module of dimension d over a subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$;

c) $b(G) \leq 6$.

Our result is key in the following major improvement of the bound in the proof of Pyber's conjecture.

Theorem (Halasi, Liebeck & Maróti (2017))

The base size $b(G)$ of a primitive permutation group G of degree n satisfies

$$b(G) < 2\frac{\log|G|}{\log n} + 27.$$

The authors note that the multiplicative constant of 2 is optimal, but the additive constant may be improved.

Future work and open questions

We are currently working to determine explicit base sizes for the irreducible representations of classical groups described in our main theorem.

So far we have shown that most of the irreducible representations of groups G with layer $E(G) = \mathrm{SL}(n, q)$ have $b(G) = 1$.

We hope to completely classify the base sizes of irreducible representations of linear groups in future, and then extend these results in future to other types of classical groups.

References

[1] H. Duyan, Z. Halasi, and A. Maróti.
A proof of Pyber's base size conjecture.
ArXiv e-prints, November 2016.

[2] Z. Halasi, M. W. Liebeck, and A. Maroti.
Base sizes of primitive groups: bounds with explicit constants.
ArXiv e-prints, February 2018.

[3] M. Lee and M. W. Liebeck.
Bases of quasisimple linear groups.
ArXiv e-prints, February 2018.

[4] László Pyber.
Asymptotic results for permutation groups.
In *Groups and computation (New Brunswick, NJ, 1991)*, volume 11 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 197–219. Amer. Math. Soc., Providence, RI, 1993.

[5] Charles C. Sims.
Computation with permutation groups.
In *Proceedings of the Second ACM Symposium on Symbolic and Algebraic Manipulation*, SYMSAC '71, pages 23–28, New York, NY, USA, 1971. ACM.