Mathematisches Forschungsinstitut Oberwolfach

Report No. 27/2025

DOI: 10.4171/OWR/2025/27

Computational Group Theory

Organized by
Heiko Dietrich, Melbourne,
Bettina Eick, Braunschweig
Gabriele Nebe, Aachen
Colva Roney-Dougal, St. Andrews

1 June – 6 June 2025

Abstract. This was the ninth Oberwolfach Workshop on Computational Group Theory. It demonstrated the deep and interesting interactions between theoretical results and powerful practical algorithms in Computational Group Theory. It featured the introduction of the new computer algebra system *OSCAR*, which is expected to lead to a new generation of practical algorithms.

Mathematics Subject Classification (2020): 20-XX, 03-XX, 68-XX, 05-XX, 11-XX, 12-XX, 13-XX, 14-XX, 57-XX.

Introduction by the Organizers

This workshop on *Computational Group Theory* was the ninth Oberwolfach workshop with this title. It had 47 participants, including 12 women. There were four Oberwolfach Leibniz Graduate Students and several further young participants.

The program consisted of four 50-minute survey talks, a total of twenty 20-minute research talks, and some 10-minute short talks. The short talks included talks by all Oberwolfach Leibniz Graduate Students, allowing these young students to present their current research to an international audience. To maximise exposure and early engagement, the short talks were all on the first day of the workshop.

The invited survey talks were designed to cover many of the most important topics in computational group theory. The contributed talks showed how the existing techniques of Computational Group Theory can be applied in various

mathematical areas, and also how powerful algorithms can be developed by the application of an increasing number of profound theoretical results.

The first survey was by Max Horn on *The OSCAR computer algebra system*. This new system has the potential to significantly reshape the way in which computational algebra (and other fields) develop. Horn gave an overview, including descriptions of its many new features and an invitation to the computational group theory community to both contribute and to request features. The power of combining computational group theory with number theory, computational algebraic and elementary geometry was demonstrated in Thomas Breuer's talk, answering a recent question of Serre.

The second survey was by Melissa Lee on *Computation and the sporadic simple groups*. It reported on the longstanding project to determine all maximal subgroups of the sporadic simple groups. This has involved many researchers over many years, and the final open cases were only recently completed by Dietrich, Lee, and Popiel with the massive help of computational group theory. Relatedly, Mikko Korhonen described his recent work on the classification of maximal solvable subgroups of finite classical groups. The two short talks by Eileen Pan and by Linda Hoyer were related to this general area of research.

The third survey was by Youming Qiao *On the complexity of isomorphism problems for tensors, groups, polynomials, and algebras*. Isomorphism problems are central to many algorithms in computational group theory (and in theoretical computer science), forming a significant complexity bottleneck for a range of other problems, as well as being hard to solve in practice. This talk gave an impressive overview of the recent achievements in this area by Qiao and others. Related this this this general area, Pascal Schweitzer surveyed modern practical graph-theoretic algorithms for computing the automorphism group of finite combinatorial objects. Some thought-provoking categorical approaches to the isomorphism problem were presented in James Wilson's talk. Peter Brooksbank gave a talk on methods to determine a change of basis matrix demonstrating that data stored as a tensor is sparse. The family of finite groups for which the isomorphism problem seems hardest are the p-groups. Mima Stanojkovski reported on very recent work introducing new geometric invariants which can often prove that groups are non-isomorphic. The modular isomorphism problem for finite p-groups is a famously difficult problem: Leo Margolis presented a survey of known results, open problems, and new algorithmic methods. Joshua Maglione described the construction of a unipotent group scheme from an elliptic curve, and discussed the isomorphism problem for these schemes. Further, the two early career short talks by Chris Liu and Óscar Fernández Ayala were related to this area.

The final survey was by Eamonn O'Brien on *Algorithms for linear groups: where to?*. He reported on the matrix group recognition project, which was started at the 1993 Oberwolfach computational group theory workshop. The project has now reached many of its original aims, and the talk pointed to the remaining open problems, while inviting young participants to join the programme. Steven Glasby presented significant recent progress on algorithms for recognising classical groups

using so-called *stingray elements*. Charles Leedham-Green spoke on applications of the matrix group recognition project to the computation of intersections. Alla Detinko described important generalisations of matrix group algorithms to infinite domains. Willem de Graaf reported on methods to compute Galois cohomology sets of linear algebraic groups.

Groups can be represented in various different ways and these have a significant impact on algorithmic problems. This was reflected in the talk by Derek Holt who presented a randomised algorithm to compute a smallest sized generating set of a finite permutation group, based on work by Lucchini and Thakkar. Alexander Hulpke spoke on his impressive new machinery for working with *hybrid groups*, a generalisation of polycyclic presentations which he has used to remarkable effect, successfully computing the character table of one of the maximal subgroups of the Monster. Laurent Bartholdi reported on automatic actions of groups, where the associated language is a set of infinite paths read in a graph. The short talks by Peiran Wu and Saul Freedman were related to this area.

Finally, some participants spoke on problems originally inspired by computational group theory. Sean Eberhard presented recent work relating to Babai's famous 1992 diameter conjecture: it was shown that every transitive solvable subgroup of S_n has polynomial diameter. Tommy Hofmann spoke on Wall's D2 problem, describing a new family of presentations of quaternion groups and explaining how computer algebra software can be used to investigate these presentations with respect to homotopy equivalence. Tobias Rossmann surveyed the symbolic enumeration of orbits related to a group scheme acting on a scheme. Daniele Dona discussed for which n one can cover the alternating group A_n by a product of three conjugacy classes. Gunter Malle reported on new properties of subnormalisers of p-elements, which play a central role in a recent new character-theoretic conjecture by Moretó and Rizo. Christopher Voll's talk described a class of multivariate generating functions that can solve enumerative problems in algebra, geometry, and number theory.

Recognising the central role of practical computation, the organisers dedicated a two-hour slot for presentating new computational tools. These included demonstrations of Alexander Hulpke's hybrid group framework and Chris Liu's matrix system solver, and a practical OSCAR presentation by Max Horn. Further, the workshop featured a problem session which identified a variety of new challenges for the computational group theory community.

Our schedule left plenty of discussion time, which was used by participants to initiate new projects, develop new research ideas and discuss new collaborations. This aspect of the workshop was a major highlight and will lead to many interesting future projects in computational group theory. The Oberwolfach workshops on Computational Group Theory have traditionally played a pivotal role in enabling extensive research projects that have significantly shaped the field.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-2230648, "US Junior Oberwolfach Fellows".

Workshop: Computational Group Theory

Table of Contents

Abstracts

The OSCAR computer algebra system

Max Horn

In this talk I present OSCAR [1], an **O**pen **S**ource **C**omputer **A**lgebra **R**esearch system. It is an international project which was founded with generous support by the German research foundation (DFG) through the Collaborative Research Center TRR 195.

OSCAR is a tool for interdisciplinary research and computations in algebra, geometry, and number theory. Its intended audience includes both experts in computer algebra as well as users of it.

OSCAR is "new" but based on several existing systems, the four cornerstones:

- ANTIC (Nemo, Hecke) [2] for number theory,
- GAP [3] for group theory,
- polymake [4] for polyhedral & tropical geometry,
- Singular [5] for commutative algebra & algebraic geometry,

which are tied together and extended by code written in the Julia programming language. The cornerstones are an integral part of OSCAR and many of their creators or custodians are also OSCAR developers; development of OSCAR also benefits the cornerstones.

OSCAR supports all functionality of its cornerstones and much beyond that. For example, a full package for computing invariants of finite and linear reductive groups is included; a library of generic character tables; capabilities in Galois cohomology and group cohomology over "generic" modules; matrix groups over number fields; and more.

Everyone is cordially invited to try our system, provide feedback on it or even join our efforts in developing it further!

A good starting point for getting to know OSCAR is to work through [6], which in 19 chapters discusses topics ranging from basics to advanced research problems with worked out examples leveraging OSCAR.

References

[1] The OSCAR Team, *OSCAR – Open Source Computer Algebra Research system, Version 1.4.0* `https://www.oscar-system.org` (2025).

[2] C. Fieker, W. Hart, T. Hofmann and F. Johansson, *Nemo/Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language*. In: Proceedings of ISSAC '17, pages 157–164, ACM, New York, `https://doi.org/10.1145/3087604.3087611` (2017).

[3] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.14.0*, `https://www.gap-system.org` (2024).

[4] E. Gawrilow, M. Joswig, *polymake: a framework for analyzing convex polytopes*. Polytopes–combinatorics and computation (Oberwolfach, 1997), 43–73, DMV Sem., 29, Birkhäuser, Basel (2000).

[5] W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann, Singular 4-4-0 — A computer algebra system for polynomial computations, `https://www.singular.uni-kl.de` (2024).

[6] W. Decker, C. Eder, C. Fieker, M. Horn, M. Joswig, eds. *The Computer Algebra System OSCAR: Algorithms and Examples*. Algorithms and Computation in Mathematics **32**, Springer, https://doi.org/10.1007/978-3-031-62127-7 (2025).

Computing Galois cohomology sets of real linear algebraic groups

Willem de Graaf
(joint work with Mikhail Borovoi)

Let $G \subset \mathrm{GL}(n, \mathbb{C})$ be a linear algebraic group defined over $\mathbb{R}$. We let $\sigma : G \to G$ be a conjugation (for example complex conjugation on the matrix entries of an element). An element $c \in G$ is called a *cocycle* if $g\sigma(g) = 1$. Two cocycles $c_1, c_2 \in G$ are equivalent if there is an $h \in G$ with $h^{-1}c_1\sigma(h) = c_2$. The set of equivalence classes of cocycles is called the first Galois cohomology set of G and denoted $H^1(G, \sigma)$.

One of the applications of these Galois cohomology sets is the classification of the orbits of the group $G(\mathbb{R}) = \{g \in G \mid \sigma(g) = g\}$. Here we suppose that G acts on a complex vector space V and that there is a conjugation $\sigma : V \to V$ that is compatible with the action of G, that is, $\sigma(g \cdot v) = \sigma(g) \cdot \sigma(v)$ for all $g \in G$ and $v \in V$. Then $G(\mathbb{R})$ acts on $V^\sigma = \{v \in V \mid \sigma(v) = v\}$. Furthermore, if $v \in V^\sigma$ then the set $H^1(Z_G(v), \sigma)$ can be used to classify the $G(\mathbb{R})$-orbits contained in the G-orbit $G \cdot v$.

In joint work ([1]) with Mikhail Borovoi we have developed algorithms for computing $H^1(G, \sigma)$. The input to the algorithm is a basis of the Lie algebra of G along with one element of each component of G. For connected reductive groups we use a theorem of Borovoi relating $H^1(G, \sigma)$ to the orbits of a subgroup of the Weyl group relative to a maximally compact torus T on the set $H^1(T, \sigma)$. For nonconnected reductive groups we use the exact sequence

$$1 \to G^\circ \to G \xrightarrow{\pi} C = G/G^\circ \to 1$$

which yields a natural map $\pi_* : H^1(G, \sigma) \to H^1(C, \sigma)$. Then by lifiting cocycles from C to G we can compute the inverse image $\pi_*^{-1}([c])$ for each element $[c] \in H^1(C, \sigma)$. The lifiting procedure is based on a procedure for neutralizing a 2-cocycle in the second Galois cohomology set.

The algorithms have been implemented in the computer algebra system GAP4. It is a future project to implement them in the computer algebra system Oscar.

References

[1] Mikhail Borovoi and Willem A. de Graaf. *Computing Galois cohomology of a real linear algebraic group* J. Lond. Math. Soc. (2) **109** (2024), no. 5, Paper No. e12906, 53 pp.

Geometric invariants for p-groups

Mima Stanojkovski
(joint work with Eamonn O'Brien)

Finite p-groups remain the principal obstacle to a polynomial time algorithm for finite groups. Groups of exponent p and nilpotency class 2 form a clear bottleneck. An easier task is to establish that two groups are non-isomorphic by exhibiting distinguishing invariants. In my lecture I reported on recent work [1] which introduces geometric invariants for these groups. The following example illustrates related questions.

Example. Let p be an odd prime number and let $\alpha \in \{0, 1, \dots, p-1\}$. Let G_α be the class 2 group of exponent p that is generated by elements a, b, c, d satisfying

$$[a, b] = [c, d], \quad [b, d] = [a, c]^\alpha, \quad [b, c] = 1.$$

Then $|G'_\alpha| = p^3$ and $|G_\alpha| = p^{3+4} = p^7$, and the commutator matrix of G_α is

$$\mathrm{B}_\alpha = \mathrm{B}_\alpha(y_1, y_2, y_3) = \begin{pmatrix} 0 & y_1 & y_2 & y_3 \\ -y_1 & 0 & 0 & \alpha y_2 \\ -y_2 & 0 & 0 & y_1 \\ -y_3 & -\alpha y_2 & -y_1 & 0 \end{pmatrix} \in \mathrm{Mat}_4(\mathbb{F}_p[y_1, y_2, y_3]).$$

The Pfaffian of B_α is $f_\alpha = y_1^2 - \alpha y_2^2 \in \mathbb{F}_p[y_1, y_2, y_3]$ and the zero locus of f_α defines a variety $\mathcal{V}_\alpha$ in $\mathbb{F}_p^3$ whose number of points is an invariant of the isomorphism class of G_α. This number $\#\mathcal{V}_\alpha(\mathbb{F}_p)$ takes the following values:

$$\#\mathcal{V}_\alpha(\mathbb{F}_p) = \begin{cases} p^2 & \text{if } \alpha = 0, \\ 2p^2 - p & \text{if } \left(\frac{\alpha}{p}\right) = 1, \\ p & \text{if } \left(\frac{\alpha}{p}\right) = -1. \end{cases}$$

From the list of the six isomorphism classes of 4-generated groups of order p^7, class 2, and exponent p provided in [2, Sec. 7.4], the number of points of the associated variety – constructed analogously – is the following:

Isomorphism class	7.4.1	7.4.2	7.4.3	7.4.4	7.4.5	7.4.6
$\#\mathcal{V}(\mathbb{F}_p)$	p^3	p^3	$2p^2 - p$	p^2	p^2	p

Imposing $\#\mathcal{V}_\alpha(\mathbb{F}_p) = \#\mathcal{V}(\mathbb{F}_p)$ yields, when $\alpha \neq 0$, that the isomorphism class of G_α is 7.4.3, when α is a quadratic residue modulo p, or 7.4.6, otherwise. The invariant $\#\mathcal{V}_\alpha(\mathbb{F}_p)$ does not distinguish the isomorphism class of G_0 between 7.4.4 and 7.4.5, but the addition of a single similar invariant does, as shown in [1, Tab. 1].

Generalizing this example, we listed some geometric invariants defined from the determinantal ideals attached to the commutator matrix of a class 2 group of exponent p. We then discussed their effectiveness in distinguishing among 5-generator p-groups of exponent p and class 2.

References

[1] E. A. O'Brien and M. Stanojkovski. Geometric invariants for p-groups of class 2 and exponent p, 2024. https://arxiv.org/abs/2411.19555.
[2] M. Vaughan-Lee. The automorphisms of class two groups of prime exponent, 2015. https://arxiv.org/abs/1501.00678.

Hybrid Groups – Generalizing Polycyclic Groups

Alexander Hulpke

PcGroups [4], which are groups given by a polycyclic presentation with elements represented as words in generators in normal form, have been one of the success stories of Computational Group Theory.

The reasons for this success are multiple:

(1) Group elements can be represented effectively, and there is good arithmetic.
(2) Transition to factor groups is easily possible and provides the basis of powerful algorithms in which calculations are reduced to linear algebra and orbit/stabilizer calculations.
(3) Quotient algorithms (such as the p-Quotient [5]) and constructions [1] provide groups in this format.

This success explains the wish to generalize this concept to nonsolvable finite groups. For algorithms, the solvable radical paradigm [2] is already such a generalization, for quotient algorithms; a generalization of quotients is provided by the hybrid quotient algorithm [3]. In particular, the latter raises the wish to have a good arithmetic in formal extensions.

Our process follows [3, Section 7]: We assume a factor group A, given as a permutation group and with a confluent rewriting system; as well as a normal subgroup B, given as a Pc group. To describe the extension structure, we extend rules for A by "tails" in B, and write down, for each generator of A, the induced automorphism of B. Formally this yields a confluent rewriting system for an extension $G \cong B.A$. We denote the natural homomorphism $\nu\colon G \to A$ by ν.

Arithmetic then represents elements in a normal form $a \cdot b$ with a being a normal form word in the generators of A and $b \in B$. Multiplication moves a-elements to the left, as far as needed, and applies the rewriting rules with tail. Whenever B-elements are adjacent, we immediately apply B-arithmetic.

We represent subgroups $S \leq G$, given by generators, by words in these generators that yield an IGS for $S \cap B$. This is done by computing kernel generators for the restriction of ν to S. Subgroup membership then first tests membership in the factor ($\nu(x) \in \nu(S)$?) and then expresses $\nu(x)$ as a word in the generators of $\nu(S)$. Dividing off this word reduces the problem to a membership test of whether $w^{-1}x \in B$ is an element in $S \cap B$. This also provides a method to apply homomorphisms, given on arbitrary generating sets.

This setup has been implemented in GAP; many solvable radical style algorithms immediately become applicable. Performace is easily competitive with that of the earlier approach in [7]. The code is available on `github`.

We applied this representation to construct, from scratch, all the groups that could be possible candiates for the maximal subgroup $2^{10+16}.O_{10}(2)$ of the sporadic Monster group, whose character table had hitherto not been known. Conjugacy class information resulted in two candidate groups, both of which we conjecture have minimal permutation degree about $1.2 \cdot 10^7$, and which thus cannot be handled easily in such a representation.

We computed character tables for both candidates, using the implementation of hybrid groups as described, and classical character theoretic tools (induction from subgroups, lattice reduction). It turned out that one of the candidate groups actually could not embed into M, and the other group had a unique embedding, up to table automorphisms.

Independently, recently Pisani [6] used this same implementation to compute the character table of the maximal subgroup $2^{5+10+20}.(S_3 \times L_5(2))$ of the Monster.

With this result, the (ordinary) character tables of all maximal subgroups of the Monster are known.

The author's work has been supported in part by Simons Foundation Grant 852063, which is gratefully acknowledged.

References

[1] Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. **12** (2002), no. 5, 623–644.

[2] John Cannon, Bruce Cox, and Derek Holt, *Computing the subgroup lattice of a permutation group*, J. Symbolic Comput. **31** (2001), no. 1/2, 149–161.

[3] Heiko Dietrich and Alexander Hulpke, *Universal covers of finite groups*, J. Algebra **569** (2021), 681–712.

[4] Reinhard Laue, Joachim Neubüser, and Ulrich Schoenwaelder, *Algorithms for finite soluble groups and the SOGOS system*, Computational group theory (Durham, 1982) (Michael D. Atkinson, ed.), Academic Press, 1984, pp. 105–135.

[5] M. F. Newman and E. A. O'Brien, *Application of computers to questions like those of Burnside. II*, Internat. J. Algebra Comput. **6** (1996), no. 5, 593–605.

[6] Anthony Pisani, *Computing the character table of a 2-local maximal subgroup of the monster*, https://arxiv.org/abs/2503.15857, 2025.

[7] S. K. Sinanan and D. F. Holt, *Algorithms for polycyclic-by-finite groups*, J. Symbolic Comput. **79** (2017), no. part 2, 269–284.

Some (primitive) coset actions in finite groups of Lie type

X. Eileen Pan

The study of primitive group actions is a central topic in group theory with significant implications across several areas of mathematics, including algebraic geometry, graph theory, and combinatorics. Primitive actions reveal crucial structural information about both the group and the set it acts upon, often serving as a key tool in the classification and understanding of these objects. For example,

primitive actions are fundamental in the classification of finite simple groups. The study of primitive actions is also useful to analyse automorphism groups of mathematical objects, such as graphs and algebraic varieties. In particular, there has been an extensive investigation of finite primitive distance-transitive graphs that requires profound knowledge of primitive actions of certain families of groups; we refer to [2] for a comprehensive survey on this topic. Distance-transitive graphs are examples of coherent configurations introduced by Higman [6]. Related concepts that stem from transitive actions have been studied by many other authors under different terminology, such as association scheme and centraliser algebra (also known as cellular algebra). We refer to Chapter 3 in the classic textbook by Cameron [5] for the background and further discussion on coherent configurations and their relations to transitive actions.

Informed by the Orbit-Stabiliser Theorem, the goal of finding suborbits and subdegrees can be achieved by the computation of subgroup intersections, which in general gives insights to the study of subgroup structure and group invariants. In [4] the authors have determined the base size of the finite simple group $G_2(q)$ by showing that the primitive action on the cosets of its maximal subgroup of type $A_1\tilde{A}_1$ (here our notation indicates that the second A_1 factor is generated by the short root subgroups) has a trivial two-point stabiliser.

The knowledge of a complete list of the suborbits and corresponding subdegrees has direct applications in calculating the permutation characters, for which many authors have been drawn to the coset actions of finite groups of Lie type. For instance, Lawther and Saxl [9] determined the suborbits of $B_2(q)$ on the cosets of ${}^2B_2(q)$, and of $B_2(q^2)$ on $B_2(q)$ (the latter only occurs when q is even). With similar methods, Lawther [7] determined the suborbits of $G_2(q)$ on the cosets of ${}^2G_2(q)$ (with q a power of 3) and that of $G_2(q^2)$ on $G_2(q)$. We note that these actions are not primitive but the methods employed in their papers still shed lights on our project. In [8], Lawther also determined explicitly the suborbit representatives and the subdegrees of the primitive action of $F_4(q)$ on the cosets of $B_4(q)$, which is a maximal-rank subgroup in $F_4(q)$. At the time of writing, the general problem of finite exceptional groups of Lie type acting on cosets of their maximal subgroups remains partially open; our goal is to contribute to this discussion. Motivated and guided by the treatments of the coset actions of finite groups of Lie type in the aforementioned works [7, 8, 9], our work determines the suborbits and corresponding subdegrees of the primitive $G_2(q)$-actions on the cosets of the subgroups of maximal rank.

We note that the subdegrees of the action of $G_2(q)$ on the cosets of maximal subgroups $\mathrm{SL}_3(q).2$ and $\mathrm{SU}_3(q).2$ are given in [1, 10], using geometrical methods that are different from ours. Moreover, since the authors considered the action in the 2-closure of $G_2(q)$ whose point-stabiliser coincides with the maximal subgroups of type $A_2.2$ in $G_2(q)$, their results do not consider explicit suborbit representatives in $G_2(q)$.

By the nature of our approach to the problem, some of the proofs are heavily computational and we use MAGMA [3] and its existing constructions of finite

groups of Lie type to assist these calculations. We aim to generalise the approach to calculate some (primitive) actions of other finite groups of exceptional Lie type, typically on the cosets of maximal-rank subsystem subgroups or involution centralisers. For example, we aim to investigate the groups E_6, E_7, E_8 of adjoint types and some of their involution centralisers. Our calculation of the subdegrees given explicit representatives written in its Bruhat normal form involves theoretic proofs and brute force computation using computer algebra systems such as MAGMA. We report on a preliminary implementation and its current bottlenecks.

References

[1] E. Bannai, S.-Y. Song and H. Yamada, Character tables of the association schemes coming from the action of $G_2(q)$ on hyperplanes of type $\mathrm{O}_6^\epsilon(q)$, J. Appl. Math. Comput. **26** (2008), no. 1-2, 125–131.

[2] J. van Bon, Finite primitive distance-transitive graphs, European J. Combin. **28** (2007), no. 2, 517–532.

[3] W. Bosma, J. J. Cannon and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[4] T. C. Burness, M. Garonzi and A. Lucchini, On the minimal dimension of a finite simple group, J. Combin. Theory Ser. A **171** (2020), 105175, 32 pp.

[5] P. J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, 45, Cambridge Univ. Press, Cambridge, 1999.

[6] D. G. Higman, Intersection matrices for finite permutation groups, J. Algebra **6** (1967), 22–42.

[7] R. Lawther, Some coset actions in $G_2(q)$, Proc. London Math. Soc. (3) **61** (1990), no. 1, 1–17.

[8] R. Lawther, The action of $F_4(q)$ on cosets of $B_4(q)$, J. Algebra **212** (1999), no. 1, 79–118.

[9] R. Lawther and J. Saxl, On the actions of finite groups of Lie type on the cosets of subfield subgroups and their twisted analogues, Bull. London Math. Soc. **21** (1989), no. 5, 449–455.

[10] M. W. Liebeck, C. E. Praeger and J. Saxl, On the 2-closures of finite permutation groups, J. London Math. Soc. (2) **37** (1988), no. 2, 241–252.

Orthogonal determinants of finite groups of Lie type

Linda Hoyer

Let G be a finite group and $K \subseteq \mathbb{R}$ be a field. Let n be a positive integer. An *orthogonal* representation is a homomorphism $\rho : G \to \mathrm{GL}_n(K)$. An averaging argument shows that there is a (in general non-unique) factoring

$$\rho : G \to \mathrm{O}(K^n, \beta) \hookrightarrow \mathrm{GL}_n(K)$$

for β a non-degenerate, symmetric bilinear form. In [1], the authors introduce the notion of *orthogonal stability*: The representation ρ is called *orthogonally stable* if and only if there is an element $d \in K^\times$ such that $\det(\beta) = d \cdot (K^\times)^2$ for any such factoring. In that case, we say that $\det(\rho) := d \cdot (K^\times)^2$ is the *orthogonal determinant* of ρ.

The orthogonally stable representations are exactly the orthogonal representations that decompose over $\mathbb{R}$ as a direct sum of irreducible $\mathbb{R}$-representations of even dimension.

The notion of orthogonally stable representations naturally generalises to orthogonally stable characters: A character χ of G is called orthogonally stable if and only if it is afforded by an orthogonally stable representation. It is further shown in [1] that orthogonal determinants $\det(\chi) \in (\mathbb{Q}(\chi)^\times)^2$ can be defined as an invariant of orthogonally stable characters.

An important class of orthogonally stable characters is given by the set

$$\mathrm{Irr}^+(G) := \{\chi \in \mathrm{Irr}(G) \mid \chi \text{ orthogonal of even dimension}\}.$$

Indeed, the character table together with the orthogonal determinants of the $\mathrm{Irr}^+(G)$-characters allows for a calculation of the orthogonal determinants of all orthogonally stable characters of G.

Let $\chi \in \mathrm{Irr}^+(G)$ and let $\rho : G \to \mathrm{GL}_n(K)$ be a representation affording χ. Let $\iota : KG \to KG$ be the involution induced by $\iota(g) := g^{-1}$. By [2], there exists an element $h \in \mathbb{Q}G$ with $\iota(h) = -h$. For any such element, it holds that $\det(\chi) = \det(\rho(h))$. This generalizes to *monomial* algebras, i.e., algebras with involutions that have a well-defined notion of orthogonal determinants, see [4]. Examples of monomial algebras include group algebras and Iwahori–Hecke algebras.

Let now $G = G(q)$ be a finite group of Lie type with q a power of an odd prime. Let $B \subseteq G$ be a Borel subgroup and $T \subseteq B$ be a maximal torus. We fix a character $\chi \in \mathrm{Irr}^+(G)$. One of the two following occurs:

(1) $\mathrm{Res}^G_B(\chi)$ is an orthogonally stable character of B. Since B is solvable, $\det(\chi)$ is easy to calculate, see [4].
(2) There is a character $\theta \in \mathrm{Irr}(T)$ such that χ appears in $\mathrm{Ind}^G_B(\theta)$.

We will from now on assume we are in case (2); let $\theta \in \mathrm{Irr}(T)$ be the corresponding character. Let $\mathcal{H} := \mathrm{End}(\mathrm{Ind}^G_B(\theta))$ be the *relative* Hecke algebra. A condensation argument now lets us reduce the calculation of $\det(\chi)$ to $\det(\chi')$, where $\chi' \in \mathrm{Irr}^+(\mathcal{H})$. The structure of such relative Hecke algebras is completely known (see [3]), so a further reduction to Iwahori–Hecke algebras is possible.

The orthogonal determinants of Iwahori–Hecke algebras of types A_n and B_n have been fully determined, see [5] and [6]. Type D_n is an easy corollary of type B_n. This leaves us with the exceptional types. The representation matrices of the exceptional Iwahori–Hecke algebras are explicitely given in CHEVIE [7]; the calculation of the determinants of the matrices of skew-symmetric elements is done in OSCAR [8]. Currently, the only case left for calculations is for type E_8, which proves a computational challenge due to the sheer size (> 1000 dimensions) of the matrices involved.

References

[1] G. Nebe and R. Parker, *Orthogonal stability*, J. Algebra **614** (2023), 362–391.
[2] G. Nebe, *Orthogonal determinants of characters*, Arch. Math. **119**, No. 1 (2022), 19–26.
[3] R. Howlett, R. Kilmoyer, *Principal series representations of finite groups with split BN pairs*, Commun. Algebra **8** (1980), 543–583.
[4] L. Hoyer, *Orthogonal Determinants of* $\mathrm{GL}_n(q)$, Preprint arXiv:2412.10797, 2024.
[5] R. Dipper, G. James, *Blocks and idempotents of Hecke algebras of general linear groups*, Proc. London Math. Soc. (3), **54**(1) (1987), 57–82.

[6] R. Dipper, G. James, E. Murphy, *Gram determinants of type B_n*, J. Algebra **189**(2) (1997), 481–505.
[7] J. Michel, *The development version of the CHEVIE package of GAP3*, J. Algebra **435** (2015), 308–336.
[8] W. Decker, C. Eder, C. Fieker, M. Horn, M. Joswig, *The computer algebra system OSCAR. Algorithms and examples*, Algorithms and Computation in Mathematics **32**. Cham: Springer (2025).

The maximum irredundant base size: found and formalised

Peiran Wu
(joint work with Colva M. Roney-Dougal)

In this talk, I present a formula for the maximum irredundant base size of certain wreath products in product action and report on my formalisation of the formula in Lean.

An irredundant base of a finite permutation group G on Δ is a sequence of points in Δ that produces a strictly descending chain of pointwise stabiliser subgroups in G, terminating at the trivial subgroup. The maximum size of irredundant bases is denoted by $\mathrm{I}(G, \Delta)$. Kelsey and Roney-Dougal [4] showed that if G is primitive on Δ, then either $\mathrm{I}(G, \Delta) < 5 \log_2 |\Delta|$ or the action is large-base. A large-base action is, up to permutation isomorphism, the product action of degree $\binom{m}{k}^n$ by a subgroup of $\mathrm{S}_m \wr \mathrm{S}_n$ containing $(\mathrm{A}_m)^n$, for some m, n, and k. This motivated us to study the maximum irredundant base size of wreath products in product action. One of our main results is the following.

Theorem. *Let H and K be finite permutation groups on Σ and Γ, respectively, with $n \coloneqq |\Gamma| \geqslant 2$. If every point stabiliser in G has exactly one fixed point, then*

$$\mathrm{I}(H \wr K, \Sigma^n) = n\,\mathrm{I}(H, \Sigma) - (n-1).$$

Combined with the maximum irredundant base size of the subset actions of S_m and A_m, found by Gill and Lodà [3], this theorem yields tight lower and upper bounds on the maximum irredundant base size of primitive large-base groups.

The theorem above is formalised in Lean [1], using the functional programming language's large mathematical library, mathlib [5]. Lean has seen very active use in the formalisation of mathematics in the last few years. One high-profile project featuring Lean is the formalisation of the proof of the polynomial Freiman-Ruzsa conjecture [2].

In the talk, I describe the difficulties I was faced with when formalising the theorem above and the definitions and known results that it relies on. These difficulties include (a) dealing with the differences between set theory, which mathematicians are familiar with, and dependent type theory, which Lean is based on and derives its power and flexibility from; (b) stating and providing explicit proofs of facts that are too obvious to mention in research article; and (c) identifying and correcting errors in the natural-language proof being formalised.

References

[1] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in Automated deduction – CADE 28 (2021), 625–635.
[2] Y. Dillies, B. Mehta, and T. Tao, *The polynomial Freiman–Ruzsa conjecture*, (2023), available at `https://github.com/teorth/pfr`.
[3] N. Gill and B. Lodà, *Statistics for* S_n *acting on k-sets*, J. Algebra, **607** (2022), 286–299.
[4] V. Kelsey and C. M. Roney-Dougal, *On relational complexity and base size of finite primitive groups*, Pac. J. Math., **318** (2022), no. 1, 89–108.
[5] The mathlib community, *The Lean mathematical library*, in Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (2020), 367–381.

Bases for primitive sporadic almost simple permutation groups

Saul D. Freedman
(joint work with Hong Yi Huang, Melissa Lee, Kamilla Rekvényi)

Let G be a permutation group on a finite set Ω. A *base* for G is a subset of Ω whose pointwise stabiliser in G is trivial, and the *base size* of G, denoted $b(G)$, is the smallest size of a base. In order to study groups of base size two, Burness and Giudici [3] introduced the *Saxl graph* of G, whose vertices are the points of Ω, and whose edges are the bases of size two. They conjectured that if G is primitive with $b(G) = 2$, then any two vertices in this graph have a common neighbour. While this conjecture is open in general, they proved it in certain cases, including many where G is a sporadic almost simple group. Additional work towards proving the conjecture has been carried out in [4, 9, 11].

To facilitate a similar study of groups of arbitrary base size at least two, we define in [6] the *generalised Saxl graph* $\Sigma(G)$ of G: the vertex set is again Ω, and a 2-subset $\{\alpha, \beta\}$ of Ω is an edge if and only if $\{\alpha, \beta\}$ is a subset of a base for G of size $b(G)$. (The *Saxl hypergraph*, an alternative generalisation where the edges are the bases of size $b(G) \geq 2$, was recently introduced and studied in [10].) We extend the above conjecture in the obvious way, as follows.

Conjecture 1. *If G is primitive with $b(G) \geq 2$, then any two vertices of $\Sigma(G)$ have a common neighbour.*

Moreover, we prove the conjecture for various families of groups.

Theorem 2. *Suppose that G is primitive with $b(G) \geq 2$. Then G satisfies Conjecture 1 if one of the following holds:*

(1) *G is a sporadic almost simple group with $b(G) \geq 3$;*
(2) *G is almost simple with soluble point stabiliser;*
(3) *G has socle $G_0 := \mathrm{PSL}_2(q)$ for a prime power q, and if $|G : G_0|$ is even, then the point stabiliser is not of type $\mathrm{GL}_2(q^{1/2})$; or*
(4) *G lies in one of several families of groups of diagonal type.*

In fact, when G is primitive with socle $\mathrm{PSL}_2(q)$, we determine precisely when $\Sigma(G)$ is complete. To do so, we complete the evaluation of $b(G)$ for every such G.

The proof of Case (1) of Theorem 2, where G is sporadic with $b(G) \geq 3$, relies on computations in Magma [1] and GAP [7], as well as the results in [5, 13] that specify $b(G)$ for each G. When the degree of G is sufficiently small, it is straightforward to construct G in Magma using the database of Atlas groups, and to show that G satisfies Conjecture 1 by checking sufficient conditions on the suborbits of G. However, no permutation representations for $G \in \{\mathrm{Ly}, \mathrm{Th}\}$ (here, the degrees are between 8.8 million and 280 million) are provided in any publicly available Magma databases. To construct these permutation groups, we employ the following method described in [8].

(1) Using Magma's database of Atlas groups, construct an irreducible matrix group $M \leq \mathrm{GL}_d(q)$ (with d and q relatively small), such that $M \cong G$ and such that the maximal subgroup H of M corresponding to a point stabiliser in G stabilises a (low-dimensional) proper nonzero subspace U of $\mathbb{F}_q^d$.
(2) Construct H, using generators from [14], and then U.
(3) Construct G as the permutation group induced by the action of M on the orbit U^M of subspaces of $\mathbb{F}_q^d$.

We note that this requires significant computational resources, e.g. 171 GB of RAM, and a runtime in the order of a few days, for the group of degree 280 million.

Of course, the above methods are not feasible when the degree of G is significantly larger. In the case where $G = \mathrm{Fi}_{23}$ with degree 1.3 billion or $G = \mathrm{Fi}_{24}$ with degree 4.9 billion, we show that G satisfies Conjecture 1 via Magma computations, carried out in the permutation representation for G of minimal degree, involving double cosets $G_\alpha x G_\alpha$ for $x \in G$ and a fixed $\alpha \in \Omega$. For each of the remaining large degree groups, we verify the conjecture via a probabilistic calculation performed using the GAP Character Table Library [2]. This generalises a technique used in [3] for sporadic groups of base size two, and relies on theory introduced in [12].

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24** (1997), 235–265.
[2] T. Breuer, *The GAP Character Table Library, Version 1.3.4*, 2022.
[3] T.C. Burness and M. Giudici, *On the Saxl graph of a permutation group*, Math. Proc. Cambridge Philos. Soc., **168** (2020), 219–248.
[4] T.C. Burness and H.Y. Huang, *On the Saxl graphs of primitive groups with soluble stabilisers*, Algebr. Comb., **5** (2022), 1053–1087.
[5] T.C. Burness, E.A. O'Brien and R.A. Wilson, *Base sizes for sporadic simple groups*, Israel J. Math., **177** (2010), 307–333.
[6] S.D. Freedman, H.Y. Huang, M. Lee and K. Rekvényi, *On the generalised Saxl graphs of permutation groups*, preprint, 2025. arXiv: 2410.22613.
[7] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.12.2*, 2022.
[8] D. Holt and D. Pasechnik, *Explicit permutation representation of the Thompson sporadic simple group?* MathOverflow, `https://mathoverflow.net/q/203180`, April 17, 2015.
[9] H. Y. Huang, *Bases for permutation groups and related problems*, PhD thesis, University of Bristol, 2025.
[10] M. Lee and A. Pisani, *The Saxl hypergraph of a permutation group*, preprint, 2025. arXiv: 2505.13849.

[11] M. Lee and T. Popiel, *Saxl graphs of primitive affine groups with sporadic point stabilisers*, Internat. J. Algebra Comput., **33** (2023), 369–389.
[12] M.W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc., **12** (1999), 497–520.
[13] M. Neunhöffer, F. Noeske, E.A. O'Brien and R.A. Wilson, *Orbit invariants and an application to the Baby Monster*, J. Algebra, **341** (2011), 297–305.
[14] R.A. Wilson, P. Walsh, J. Tripp, I. Suleiman, R.A. Parker, S. Norton, S. Nickerson, S. Linton, J.N. Bray and R. Abbott, *ATLAS of Finite Group Representations – Version 3*, `http://atlas.math.rwth-aachen.de/Atlas/v3/`, accessed April 15, 2024.

Simultaneous Sylvester Systems and some applications

Chris Liu
(joint work with Joshua Maglione, James B. Wilson)

For a bilinear map $u * v := \langle t|u, v\rangle$ described by a tensor t, its adjoint algebra, $\mathrm{Adj}(t)$, consisting of operators α satisfying

$$\alpha u * v = u * \alpha v,$$

encode substantial qualities of the tensor while remaining theoretically computable [1]. However, computation is often out of practical reach. (At least $O(n^6)$ for cubic tensors.)

The equations defining $\mathrm{Adj}(t)$ are closely related to equations defining module homomorphisms, the centralizer/center of a matrix algebra, and the centroid of a tensor. Succinctly, each reduces to solving a system of matrix equations of the form

$$(\forall i)\ XA_i + B_iY = C_i$$

for appropriately constructed A_i, B_i, C_i in the unknowns X, Y. This we call *Simultaneous Sylvester Systems*.

For the center of a matrix algebra, methods of Eberly and Giesbrecht computes generators within a logarithmic factor of the cost of solving $n \times n$ systems of linear equations [2]. For module homomorphisms, the Meataxe [3] and condensation based methods [4] break down the single large system of matrix equations to many smaller pieces.

Yet there are bottleneck examples with Loewy length 3 where computing module homomorphisms bottoms out to the brute-force solving of a Simultaneous Sylvester System as a system of linear equations. In my talk, I described an algorithm that compute solutions to these systems efficiently. It uses a solve and lift paradigm that is agnostic of the underlying data interpretation. We observe both practical and complexity improvements in our Magma implementation.

References

[1] Peter A. Brooksbank, James B. Wilson, *Computing isometry groups of Hermitian maps*, Trans. Amer. Math. Soc. 364 (2012), no. 4, 1975–1996.

[2] W. Eberly and M. Giesbrecht. 1996. *Efficient decomposition of associative algebras.* In Proceedings of the 1996 international symposium on Symbolic and algebraic computation (ISSAC '96). Association for Computing Machinery, New York, NY, USA, 170–178. https://doi.org/10.1145/236869.236931
[3] R. A. Parker, *The computer calculation of modular characters (the Meat-Axe)*, in: Computational Group Theory, Academic Press, London, 1984, pp. 267–274
[4] A. J. E. Ryba. *Computer condensation of modular representations.* J. Symbolic Comput., 9(5–6):591–600, 1990. Computational group theory, Part 1.

Computing the breadths of algebras and $\mathcal{T}$-groups

Óscar Fernández Ayala
(joint work with Bettina Eick)

In the talk, we reviewed the definitions of the breadth $\mathrm{br}(G)$ of a p-group G and the class-breadth conjecture. For a p-group, the breadth of $g \in G$ is defined as the size of its conjugacy class;

$$p^{\mathrm{br}(g)} = |g^G| = [G : C_G(g)].$$

Then the class-breadth conjecture can be stated as follows:

$$\mathrm{cl}(G) \leq \mathrm{br}(G) + 1,$$

where $\mathrm{cl}(G)$ is the nilpotency class of G. Leedham-Green, Neumann, and Wiegold [1] proved the following:

Theorem 1. *Let G be a p-group, then*

$$\mathrm{cl}(G) \leq \frac{p}{p-1}\,\mathrm{br}(G).$$

They also proved that the conjecture holds when $\mathrm{br}(G) < p$. In 1987, Felsch, Neubüser, and Plesken [3] found a family of 2-groups that break the conjecture, but it remains open for odd primes. The breadth of an algebra L is the maximum of $\dim(L) - \dim(C_L(x))$ for $x \in L$ and the class-breadth conjecture can be stated as $\mathrm{cl}(L) \leq \mathrm{br}(L)+1$. In [1] it was proven that the conjecture holds for nilpotent Lie algebras over infinite fields and for associative algebras over any field. It was also given a nilpotent Lie algebra over $\mathbb{F}_2$ that refuted the conjecture; later, in 2006, Eick, Newman, and O'Brien [2] proved that there are nilpotent Lie algebras over any finite field that serve as counterexamples to the conjecture. In our work, we describe an algorithm to compute the breadth of an algebra L given by structure constants. Until now, computing the breadth for infinite algebraic objects has not been possible. The algorithm exploits the fact that for given basis B of L the left multiplication endomorphism $\mathcal{L}_x : L \to L$ defined as $\mathcal{L}_x(y) = y \cdot x$ can be represented as a matrix $M_B(x)$. Then

$$\mathrm{br}(x) = \mathrm{rank}\, M_B(x).$$

If $B = \{b_1, \ldots, b_n\}$, then we can represent any element of L as the linear combination $X = X_1 b_1 + \cdots + X_n b_n$ with indeterminates X_i over the field where L

is defined. We say that a polynomial $f(X_1, \ldots, X_n)$ vanishes over a field K if $f(k_1, \ldots, k_n) = 0$ for all $k_1, \ldots, k_n \in K$. Then the following holds:

Theorem 2. *Let L be an algebra over the field K with basis B. Then $\mathrm{br}(L) = m$ if and only if for each $l > m$ all $l \times l$ minors of $M_B(X)$ vanish over K and there is an $m \times m$ minor that does not vanish over K.*

For nilpotent algebras, we could prove the following

Theorem 3. *Let L be a nilpotent algebra over a field K of class $c > 1$ and dimension n with basis B. Then $M_B(X)$ has a $(c-1)\times(c-1)$ minor $f(X_1, \ldots, X_n)$ which is non-zero and,*

(a) *If K is infinite, then the class-breadth conjecture holds for L.*
(b) *If K is finite and there exists a $(c-1) \times (c-1)$ matrix minor f with $|K| > \mathrm{md}(f)$, then the class-breadth conjecture holds for L.*

Finally, we give an application for finitely generated nilpotent groups, $\mathcal{T}$-group, in short. The breadth of a polycyclic group G is the maximum of $h(G) - h(C_G(x))$ for $x \in G$, where $h(G)$ is the Hirsch length of G. Mann and Segal [4] proved that the class-breadth conjecture holds for $\mathcal{T}$-groups. We could prove the following:

Theorem 4. *Let G be a $\mathcal{T}$-group and let $\Lambda(G)$ be the rational nilpotent Lie algebra associated to G via the Mal'tsev correspondence, then*

$$\mathrm{br}(G) = \mathrm{br}(\Lambda(G)).$$

Combining Theorem 3 and Theorem 4 leads to a proof of the fact that the class-breadth conjecture holds for $\mathcal{T}$-groups.

References

[1] C.R. Leedham-Green, P.M. Neumann, and J. Wiegold, *The breadth and the class of a finite p-group.* J. London Math. Soc. **2** (1969), 409–420.
[2] B. Eick, M.F. Newman, and E.A. O'Brien, *The class-breadth conjecture revisited.* J. Algebra. **300.1** (2006), 384–393.
[3] W. Felsch, J. Neubüser, and W. Plesken *Space groups and groups of prime-power order. IV. Counterexamples to the class-breadth conjecture.* J. London Math. Soc. **2** (1981) , 113–122.
[4] A. Mann, and D. Segal *Breadth in polycyclic groups.* Internat. J. Algebra Comput. **17** (2007), 1073–1083. pp. 1073–1083.

Hall–Littlewood polynomials, affine Schubert series, and lattice enumeration

Christopher Voll
(joint work with Joshua Maglione)

In [1], Joshua Maglione and I introduced *Hall-Littlewood-Schubert series*, a new class of multivariate generating functions. Their definition features semistandard Young tableaux and polynomials related with the classical Hall-Littlewood polynomials. Via judicious substitutions of their exponentionally many variabes, Hall-Littlewood-Schubert series solve various enumerative problems in algebra, geometry, and number theory. These include Hecke series associated with groups of symplectic similitudes over local fields. In my talk, however, I put the spotlight on the specialization of Hall–Littlewood–Schubert series to *Hermite–Smith series*. These generating functions enumerate lattices in $\mathbb{Z}^n$ simultaneously by two invariants: their Smith normal form and the diagonal entries of the matrices representing them in Hermite normal form with respect to a fixed ordered $\mathbb{Z}$-basis of the ambient lattice.

References

[1] J. Maglione, C. Voll, *Hall–Littlewood polynomials, affine Schubert series, and lattice enumeration*, `https://arxiv.org/pdf/2203.10287`

Computation and the sporadic simple groups

Melissa Lee

This talk explores the pivotal role of computation in the construction and analysis of the sporadic simple groups, beginning with Gagen and Ward's 1965 proof of the existence of Janko's first group [7]. Indeed, the existence of nine of the sporadic simple groups involved the use of a computer (see [5, Section 2.5] for an overview and techniques), and even today, there is no known computer-free construction of the O'Nan sporadic simple group.

Conversely, the desire to explicitly construct the sporadic simple groups motivated the development of several crucial techniques in computational group theory, including bases [14], fundamental to algorithms for permutation groups, and Richard Parker's MeatAxe [10], used to determine irreducible modules.

The first publicly available database of representations of the sporadic simple groups and related groups was produced by Wilson [15] and dubbed "Volume 3 of the ATLAS", after [2] and [8]. This database grew from the 600 representations mentioned in [15], to today include over 5700 representations on over 700 groups [1]. In particular, there are representations of all sporadic simple groups except the Monster group, along with many related groups.

The Monster group $\mathbb{M}$, the largest sporadic group, has proved to be the most challenging to construct computationally due to the absence of a feasibly small degree permutation or matrix representation. The first construction of generators

of the Monster on computer was produced by Linton, Parker, Walsh and Wilson in 1998 [9], based on the 196,883-dimensional matrix representation of the Monster over $\mathbb{F}_2$. This, along with a construction over $\mathbb{F}_3$ developed by Holmes and Wilson [6] led to the discovery of several more maximal subgroups of the Monster (see [16, Section 3.6]), and eventually reduced the list of remaining possibilities for maximal subgroups to almost simple groups with socle one of $\mathrm{PSL}_2(8)$, $\mathrm{PSL}_2(13)$, $\mathrm{PSL}_2(16)$, or $\mathrm{PSU}_3(4)$.

These cases were explored by [4], who discovered the final two classes of maximal subgroups, $\mathrm{PGL}_2(13)$ and $\mathrm{PSU}_3(4).4$. This work was done using `mmgroup`, a Python package implementing the Monster written by Martin Seysen [13]. This package represents a large breakthrough in our ability to compute with $\mathbb{M}$, as it is the first publicly available implementation, it is open-source, and it is able to multiply elements of $\mathbb{M}$ together (including a *word reduction* algorithm) in approximately 35 milliseconds, around 100,000 faster than was possible in earlier implementations. Further developments using `mmgroup` include explicit constructions of the maximal subgroups of $\mathbb{M}$ [3], the construction of the last unknown character table of a maximal subgroup of $\mathbb{M}$ [11], and the determination of class fusions from maximal subgroups to $\mathbb{M}$ [12].

References

[1] R. Abbott, J. Bray, S. Linton, S. Nickerson, S. Norton, R. Parker, S. Rogers, I. Suleiman, J. Tripp, P. Walsh, and R. Wilson. ATLAS of Finite Group Representations – Version 3. `http://atlas.math.rwth-aachen.de/Atlas/v3/`. Accessed: 18/6/2025.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. ATLAS *of finite groups*. Oxford University Press, Eynsham, 1985.

[3] H. Dietrich, M. Lee, A. Pisani, and T. Popiel. Explicit construction of the maximal subgroups of the monster. *arXiv preprint arXiv:2411.12230*, 2024.

[4] H. Dietrich, M. Lee, and T. Popiel. The maximal subgroups of the monster. *Advances in Mathematics*, 469:110214, 2025.

[5] D. Gorenstein. *Finite simple groups: an introduction to their classification*. Springer Science & Business Media, 2013.

[6] P. E. Holmes and R. A. Wilson. A new computer construction of the Monster using 2-local subgroups. *J. London Math. Soc. (2)*, 67(2):349–364, 2003.

[7] Z. Janko. A new finite simple group with abelian sylow 2-subgroups and its characterization. *Journal of Algebra*, 3(2):147–186, 1966.

[8] C. Jansen, K. Lux, R. Parker, and R. Wilson. *An atlas of Brauer characters*, volume 11 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1995.

[9] S. Linton, R. Parker, P. Walsh, and R. Wilson. Computer construction of the Monster. *J. Group Theory*, 1(4):307–337, 1998.

[10] R. A. Parker. The computer calculation of modular characters (the meat-axe). *Computational group theory*, pages 267–274, 1984.

[11] A. Pisani. Computing the character table of a 2-local maximal subgroup of the monster. *arXiv preprint arXiv:2503.15857*, 2025.

[12] A. Pisani and T. Popiel. Conjugacy class fusion from four maximal subgroups of the monster. *Journal of Computational Algebra*, 11:100021, 2024.

[13] M. Seysen. A fast implementation of the Monster group: The Monster has been tamed. *Journal of Computational Algebra*, 9:100012, 2024.

[14] C. C. Sims. Computation with permutation groups. In *Proceedings of the second ACM symposium on Symbolic and algebraic manipulation*, pages 23–28, 1971.
[15] R. A. Wilson. An atlas of sporadic group representations. In *The atlas of finite groups: ten years on (Birmingham, 1995)*, volume 249 of *London Math. Soc. Lecture Note Ser.*, pages 261–273. Cambridge Univ. Press, Cambridge, 1998.
[16] R. A. Wilson. Maximal subgroups of sporadic groups. In *Finite simple groups: thirty years of the atlas and beyond*, volume 694 of *Contemp. Math.*, pages 57–72. Amer. Math. Soc., Providence, RI, 2017.

Finding exotic presentations of quaternion groups

Tommy Hofmann
(joint work with John Nicholson)

We report on an ongoing investigation of Wall's D2 problem and the interactions with computational group theory (and computer algebra in general). Given a finitely presented group G, can we classify its collection of finite presentations? To make this precise, we must first specify an equivalence relation on the class of finite presentations. Examples of such equivalence relations can be obtained by specifying transformations or moves on relations. Obtaining classification results for such equivalence relations appears to be hard, as is witnessed by the open Andrew–Curtis conjecture.

We instead consider the following equivalence relation, which is coming from topological considerations. A finite presentation $\mathcal{P}$ for a group G has an associated finite 2-complex $X_{\mathcal{P}}$ with fundamental group G. We say that two finite presentations are *homotopy equivalent* if their associated 2-complexes are. Our goal is a classification of presentations up to homotopy equivalence, which is inextricably linked to Wall's D2 problem [1]. For a finitely presented group G, the question is whether certain algebraic 2-complexes of $\mathbf{Z}[G]$-modules are geometrically realizable. In this case, we say that G satisfies the *D2 property*.

Our focus is on the quaternion groups Q_{4n}, which for small orders have been investigated with respect to the D2 property. In particular, the group Q_{32} was independently proposed as a counterexample to the D2 problem by Cohen [2] and Dyer [3].

A pair of finite presentations for a group G are said to be *exotic* if they have the same deficiency but are not homotopy equivalent. For $n \geq 6$, the existence of exotic presentations is necessary for Q_{4n} to have the D2 property. Except for Q_{28}, where the existence of exotic presentations has been established by the work of Mannan–Popiel [4], no exotic presentations for larger quaternion groups have been known.

In this talk, we describe a new family of presentations of quaternion groups and explain how computer algebra software like Magma and Oscar can be used to investigate these presentations with respect to homotopy equivalence, allowing us to prove that Q_{32} is not a counterexample to the D2 problem. In fact, we show the following.

Theorem.

(1) *If* $6 \leq n \leq 8$*, then* Q_{4n} *has the* D2 *property.*
(2) *If* $n = mk$ *where* $6 \leq m \leq 12$ *and* $k \geq 1$ *is odd, then* Q_{4n} *has an exotic presentation.*

The case Q_{28} was established previously in [5] using the exotic presentations of Mannan–Popiel.

References

[1] C. T. C. Wall, *Finiteness conditions for* CW*-complexes*, Ann. of Math. (2) **81** (1965), 56–69.
[2] Joel M. Cohen, *Complexes dominated by a* 2*-complex*, Topology **16** (1977), no. 4, 409–415.
[3] Micheal N. Dyer, *On the essential height of homotopy trees with finite fundamental group*, Compositio Math. **36** (1978), no. 2, 209–224.
[4] Wajid H. Mannan and Tomasz Popiel, *An exotic presentation of* Q_{28}, Algebr. Geom. Topol. **21** (2021), no. 4, 2065–2084.
[5] John Nicholson, *On CW-complexes over groups with periodic cohomology*, Trans. Amer. Math. Soc. **374** (2021), no. 9, 6531–6557.

Diameter bounds for soluble transitive permutation groups

Sean Eberhard

(joint work with Elena Maini, Luca Sabatini, Gareth Tracey)

If G is a finite group generated by a set X, we write ℓ_X for the length function with respect to X, i.e., if $g \in G$ then $\ell_X(g)$ is the length of the minimal representation of g as a product of elements of $X \cup X^{-1}$. For a subset $S \subseteq G$ we write $\ell_X(S) = \max_{g \in S} \ell_X(g)$. The *diameter* of G with respect to X is $\mathrm{diam}(G, X) = \ell_X(G)$, and we define

$$\mathrm{diam}(G) \;=\; \max_{\langle X \rangle = G} \mathrm{diam}(G, X).$$

There are at least two fundamental open conjectures about diameters of finite groups.

(1) (Babai's conjecture, 1992 [1]) If G is a finite simple group then $\mathrm{diam}(G) \leq C_1(\log |G|)^{C_2}$ for some absolute constants C_1, C_2.
(2) (folklore) If G is a transitive permutation group of degree n then $\mathrm{diam}(G) \leq C_1 n^{C_2}$ for some absolute constants C_1, C_2.

More aggressively, one might conjecture that $C_2 = 2$. The best known bound for the diameter of transitive permutation groups $G \leq S_n$ is a quasipolynomial bound of the form

$$\mathrm{diam}(G) \leq \exp((\log n)^{4+o(1)})$$

due to Helfgott–Seress [3].

The inception of the present project (which is work in progress) was the question of whether the folklore conjecture 2 above is really plausible for other transitive permutation groups, particularly say soluble permutation groups, which may yet be exponentially large and so could potentially have large diameter. Indeed we did not seem to have a polynomial bound even for transitive p-subgroups such as

$C_p \wr \cdots \wr C_p$ (the Sylow p-subgroup of S_{p^h}). This is a question that seems to have been overlooked.

Our first main result is a general bound for the diameter of a finite soluble group. Recall that the *exponent* $\exp(G)$ of a group G is the smallest integer e such that $g^e = 1$ for all $g \in G$. The *derived length* L of G is the least integer L such that $G^{(L)} = 1$. We prove that if G is a finite soluble group of derived length L and

$$e = \max\{\exp(G^{(i)}/G^{(i+1)}) : 0 \le i < L\} \le \exp(G)$$

then

$$\operatorname{diam}(G) \le 4^{L-1}\, e\, (\log_2 |G|)^2.$$

It follows that we have a good bound for the diameter of a soluble group whenever its derived length and exponent are controlled. There are several notable corollaries.

First, if G is a finite soluble group of exponent $\exp(G)$ then

$$\operatorname{diam}(G) \;\le\; \exp(G)(4 \log_2 |G|)^8.$$

This follows from a result of Glasby [2] that $L < 3 \log_2 \log_2 |G| + 9$.

Next, if $G \le S_n$ is transitive and soluble then

$$\operatorname{diam}(G) \;\le\; n^{6.16},$$

and furthermore if G is nilpotent then

$$\operatorname{diam}(G) \;\le\; n^5.$$

In the case of primitive soluble groups, we prove a nearly linear bound, which is optimal up to the logarithmic factors:

$$\operatorname{diam}(G) \;\le\; n(\log n)^{O(1)}.$$

It would be fascinating to know the optimal exponents in these bounds. It is not known whether any transitive subgroup of S_n has more than quadratic diameter. On the other hand, congruence quotients of the Grigorchuk group G give examples of transitive 2-subgroups $G_h = \langle X \rangle \le S_n$ (where $X = \{a, b, c, d\}$ is the standard generating set) $n = 2^h$, with

$$n^{1.3} \ll \operatorname{diam}(G_h, X) \ll n^{1.94}.$$

(Conjecturally, the lower bound is close to correct in this case.)

References

[1] L. Babai and Á. Seress, On the diameter of permutation groups, *European J. Combin.*, 13(4):231–243, 1992. 10.1016/S0195-6698(05)80029-0.

[2] S. P. Glasby, The derived length of finite soluble groups, *Bull. Austral. Math. Soc.*, 48(3):471–476, 1993. 10.1017/S0004972700016136.

[3] H. A. Helfgott and Á. Seress, On the diameter of permutation groups, *Ann. of Math. (2)*, 179(2):611–658, 2014. 10.4007/annals.2014.179.2.3.

On the Modular Isomorphism Problem

Leo Margolis
(joint work with Taro Sakurai)

The Isomorphism Problem for group rings asks, whether an isomorphism of RG, the group ring of a finite group G over a commutative ring R, to another group ring RH, implies the isomorphism of the base groups G and H. While this has clearly negative answers in general, e.g. any two abelian groups of the same order have isomorphic group algebras over the complex numbers, some specific formulations are much less obvious and received a lot of attention over decades. After summarizing the main historic results, especially for the case that R is the ring of integers, we concentrate on the so-called Modular Isomorphism Problem (MIP): it asks if the isomorphism $FG \cong FH$ implies the isomorphism $G \cong H$ in case G is a finite p-group and F a field of characteristic p. The question goes back at least to a survey of R. Brauer [1].

If the coefficient field in the (MIP) is finite, so is the algebra FG and it becomes accessible to computer algebraic methods. Moreover, the augmentation ideal of FG coincides with its Jacobsen radical and studying quotients by powers of the Jacobsen radical allows to reduce the problem to the study of nilpotent algebras of smaller dimensions. This gave rise to the development and implementation of two algorithms [8, 3] which we recall along with other early applications of computers to the study of the problem. We then summarize also the theoretical knowledge on (MIP) which includes positive results, but also the recent negative solutions in the class of 2-groups [4] and their slight generalization [5, 2]. From the positive results we would like to highlight that though for the class of p-groups of exponent p and nilpotency class 2, featuring prominently in other talks of this wokrshop, the problem found a positive solution over the prime field already in the 1970's [7] it remains open over general fields.

Several open questions are then presented. This includes the most natural question, if the (MIP) holds for odd primes, and also the question if it is possible that the group algebras of two finite p-groups are non-isomorphism over $\mathbb{F}_p$ but become isomorphic over a bigger field of characteristic p. We mention a new result that the 2-groups which provide the negative solutions for the (MIP) have non-isomorphic group rings over the ring $\mathbb{Z}/4\mathbb{Z}$ [6]. This investigation led to a new idea to study the (MIP) which in particular might allow a computer algebraic study independent of the ground field. This involves a question in algebraic geometry and ultimately asks to decide if a certain polynomial lies in the ideal generated in a polynomial ring whose generators depend on the relations of the groups which are compared. It still remains to see if this idea can lead to new results, in particular using the tools available in `singular` or `magma`.

References

[1] R. Brauer, *Representations of finite groups*, Lectures in Modern Mathematics **1**(11), Wiley, New York (1963), 133–175.

[2] C. Bagiński, K. Zabielski *The Modular Isomorphism Problem – the alternative perspective on counterexamples*, J. Pure Appl. Algebra **229**(1) 107826 (2025).
[3] B. Eick, *Computing automorphism groups and testing isomorphisms for modular group algebras*, J. Algebra **320**(11) (2008), 3895–3910.
[4] D. García-Lucas, L. Margolis, Á. del Río, *Non-isomorphic 2-groups with isomorphic modular group algebras*, J. Reine Angew. Math. **783** (2022), 269–274.
[5] L. Margolis, T. Sakurai, *Identification of non-isomorphic 2-groups with dihedral central quotient and isomorphic modular group algebras*, Rev. Math. Iberoam. to appear, DOI 10.4171/RMI/1531 (2025).
[6] L. Margolis, T. Sakurai, *Group algerbas and their coefficient rings*, in preparation (2025+).
[7] I.B.S. Passi, S.K. Sehgal, *Isomorphism of modular group algebras*, Math. Z. **129** (1972), 65–73.
[8] M. Wursthorn, *Isomorphisms of modular group algebras: an algorithm and its application to groups of order* 2^6, J. Symbol. Comput. **15**(2) (1993), 211–227.

Automatic actions

Laurent Bartholdi

Automatic actions are actions of a group G on an ω-regular language $L \subseteq A^\omega$ in such a way that, for every $g \in G$, the graph of the action $\{(\xi, g(\xi)) : \xi \in L\}$ is an ω-regular subset of $L \times L \subseteq (A \times A)^\omega$.

(Recall that an ω-regular language $\leq A^\omega$ is given by a finite graph (called *automaton*) with certain vertices called *initial*, certain edges called *recurrent*, and labels $\in A$ on every edge. The associated language is the set of infinite paths read in the graph, starting at an initial vertex, and traversing infinitely often a recurrent edge.)

More generally, a relation (say n-ary) on L is ω-regular if it is a regular language on the alphabet A^n. For example, the equivalence relation E_0, relating all sequences that eventually coincide, is ω-regular: it has two vertices, one initial with $A \times A$ loops and $A \times A$ edges to the other vertex; and $\{(a, a) : a \in A\}$ recurrent loops at that other vertex.

Note that if G is finitely generated then it suffices to give an automaton per generator, to describe fully the automatic action. Thus an automatic actions of finitely generated groups are given by a finite amount of data.

This notion generalizes numerous examples: the *automatic actions* of [1], the *automata actions* on rooted trees that lead to the first examples of groups of intermediate growth [3], and the substitutional subshifts [2]. In my talk, I paid particular attention to decidability questions related to these actions.

In particular, an automatic action is an example of an *ω-automatic structure*: recall that a structure $(X, \rho_1, \rho_2, \dots)$, consisting of a set X and operations/relations ρ_i, is ω-automatic if there exists an ω-regular language L, an ω-regular equivalence relation E with $L/E \cong X$, and operations relations R_i on L that lift the operations ρ_i. A fundamental, if easy result is:

Theorem 1 (Khoussainov-Nerode [4]; Kuske-Lohrey [5])**.** *If $(X, \rho_1, \dots)$ is ω-automatic, then its first-order theory is decidable.*

Thus for example the word problem for automatic actions of finitely generated groups ("does $g \in G$, given as a product of generators, act trivially?") is decidable.

More can be said in certain cases. An ω-regular relation $R \subset L \times L$ is *bounded* if $R \setminus E_0$ is finite, and an automatic action is bounded if its acts by bounded relations; namely, for every $g \in G$ there are finitely many $\xi \in L$ such that ξ and $g(\xi)$ do not eventually agree. I can prove:

Theorem 2. *If G has a bounded action on L, then its orbit relation $\{(\xi, g(\xi)) : g \in G, \xi \in L\}$ is ω-regular.*

All substitional subshifts can be described by bounded automatic actions; and most examples of automata groups fall is this class too. It follows that a large number of dynamically-relevant notions are decidable: minimality, topological transitivity, etc.

In the case of *Pisot* substitutional subshifts, namely those for which the growth rate of the substitution is an algebraic number all of whose Galois conjugates are inside the unit disk, even more can be said:

Theorem 3 (joint with I. Mitrofanov)**.** *If $\mathbb{Z} \curvearrowright X$ is a Pisot substitutional subshift, then the action map itself is automatic: there is an automatic structure*

$$(\mathbb{Z} \sqcup X, 0, 1, \xi_0, +, \cdot, d)$$

where ξ_0 is a fixed point of the substitution, $'+' \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is addition, $'\cdot' \colon \mathbb{Z} \times X \to X$ is the group action, and $d \colon X \times X \to \mathbb{Z}$ is the logarithm of the distance function.

It follows, for example, that the proximality relation, equicontinuity relation etc. are all decidable.

References

[1] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston. *Word processing in groups.* Jones and Bartlett Publishers, Boston, MA, 1992.

[2] Durand, F., Host, B., Skau, C.: Substitutional dynamical systems, Bratteli diagrams and dimension groups. Ergodic Theory Dynam. Systems **19**(4), 953–993 (1999)

[3] R. I. Grigorchuk. On the Milnor problem of group growth. *Dokl. Akad. Nauk SSSR*, 271(1):30–33, 1983.

[4] Khoussainov, B., Nerode, A.: Automatic presentations of structures. Logic and computational complexity (Indianapolis, IN, 1994), Lecture Notes in Comput. Sci. 960, 367–392.

[5] Kuske, D., Lohrey, M.: Logical aspects of Cayley-graphs: the group case. Annals of Pure and Applied Logic **131**(1–3), 263–286 (2005)

On the Complexity of Isomorphism Problems for Tensors, Groups, Polynomials, and Algebras

Youming Qiao

(joint work with Josh Grochow, Gábor Ivanyos, James B. Wilson, Peter A. Brooksbank, Markus Bläser, Alexander Rogovskyy, Xiaorui Sun, Kate Stange, Yinan Li, Chuanqi Zhang, Antoine Joux, Anand Narayanan, Zhengfeng Ji, Fang Song, Aaram Yun...)

Two matrices are called equivalent if one can be transformed into the other by multiplying with invertible matrices on the left and right. Extending this idea to 3-tensors, it is natural to define two 3-tensors as isomorphic if they can be transformed into each other by multiplication with three invertible matrices along the three directions.

In the past few years, Tensor Isomorphism has been studied from the perspectives of complexity, algorithms, and cryptography. We briefly report some main messages from these works.

Complexity. In [1], it is shown that Tensor Isomorphism captures the complexity of testing isomorphism for several algebraic structures, including polynomials, certain families of groups, and associative or Lie algebras. Here "captures" can refer to either polynomial-time equivalence or the containment relation between orbit structures.

This prompts the introduction of a complexity class called Tensor Isomorphism. By varying the underlying fields/rings and group types and actions, Tensor Isomorphism has connections to cryptography (Goldreich–Micali–Wigderson zero-knowledge protocol for isomorphism problems) [2], quantum information [3], number theory (Bhargava's approach to Gauss composition law), and geometry (classification of Calabi–Yau threefolds) [4].

Algorithms. Algorithms for Tensor Isomorphism have been studied intensively in the past few years. The following algorithms are for $n \times n \times n$ tensors over $\mathbb{F}_q$.

- **Algorithms with worst-case analyses:** In [5], Xiaorui Sun presented the first $n^{o(\log n)}$-time algorithm for testing isomorphism of p-groups of class 2 and exponent p. This was subsequently improved and simplified in [6]. The key of [6] is to develop a $q^{O(n^{1.5}\cdot\log(n))}$-time algorithm for Tensor Isomorphism.
- **Algorithms with average-case analyses:** By [7], Tensor Isomorphism can be solved in time $q^{O(n)}$ in the average-case sense.
- **Heuristic algorithms:** In [8], a heuristic algorithm for Tensor Isomorphism in time $q^{n/2} \cdot \mathrm{poly}(n, \log q)$ was presented.

Cryptography. Tensor Isomorphism is a candidate of the so-called pseudorandom group action, which can support several cryptographic functionalities [2]. A digital signature scheme, called MEDS, was implemented and submitted to the

NIST's call for post-quantum digital signature schemes [9]. The heuristic algorithm for Tensor Isomorphism in [8] was motivated by evaluating the security of MEDS.

A desirable feature of digital signature schemes is the quantum random oracle model (QROM) security [10]. For MEDS to have the QROM security, it is enough to show that a random $n \times n \times n$ tensor over $\mathbf{F}_q$ has the trivial stabiliser group. This was shown to be the case in [11]. The techniques were then used to answer some open questions on enumerating p-groups of class 2 and exponent p in [12].

References

[1] Joshua A. Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials I: Tensor Isomorphism-completeness. *SIAM J. Comput.*, 52:568–617, 2023.

[2] Z. Ji, Y. Qiao, F. Song, and A. Yun, *General linear group action on tensors: A candidate for post-quantum cryptography*, in Theory of Cryptography - 17th International Conference, TCC 2019, vol. 11891 of Lecture Notes in Computer Science, Springer, 2019, pp. 251–281,

[3] Zhili Chen, Joshua A. Grochow, Youming Qiao, Gang Tang, and Chuanqi Zhang. On the complexity of isomorphism problems for tensors, groups, and polynomials III: actions by classical groups. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference, ITCS 2024, January 30 to February 2, 2024, Berkeley, CA, USA*, volume 287 of *LIPIcs*, pages 31:1–31:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[4] Joshua A. Grochow, Youming Qiao, Katherine E. Stange, and Xiaorui Sun. On the complexity of isomorphism problems for tensors, groups, and polynomials V: Over commutative rings. STOC'25, to appear.

[5] Xiaorui Sun. Faster isomorphism for p-groups of class 2 and exponent p. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 433–440. ACM, 2023.

[6] Gábor Ivanyos, Euan Jacob Mendoza, Youming Qiao, Xiaorui Sun, and Chuanqi Zhang. Faster isomorphism testing of p-groups of frattini class-2. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024*, pages 1408–1424. IEEE, 2024.

[7] Peter A. Brooksbank, Yinan Li, Youming Qiao, and James B. Wilson. Improved algorithms for alternating matrix space isometry: From theory to practice. In Fabrizio Grandoni, Grzegorz Herman, and Peter Sanders, editors, *28th Annual European Symposium on Algorithms, ESA 2020, September 7-9, 2020, Pisa, Italy (Virtual Conference)*, volume 173 of *LIPIcs*, pages 26:1–26:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[8] Anand Kumar Narayanan, Youming Qiao, and Gang Tang. Algorithms for matrix code and alternating trilinear form equivalences via new isomorphism invariants. In *43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Eurocrypt 2024*, 2024.

[9] Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Lars Ran, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. MEDS matrix equivalence digital signature (2023). *Submission to the NIST Digital Signature Scheme standardization process*, 2023.

[10] Markus Bläser, Zhili Chen, Dung Hoang Duong, Antoine Joux, Tuong Ngoc Nguyen, Thomas Plantard, Youming Qiao, Willy Susilo, and Gang Tang. On digital signatures based on group actions: QROM security and ring signatures. In *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceedings, Part I*, volume 14771 of *Lecture Notes in Computer Science*, pages 227–261. Springer, 2024.

[11] Markus Bläser, Yinan Li, Youming Qiao, Alexander Rogovskyy. On average orders of automorphism groups of bilinear maps over finite fields. Preprint as arXiv:2503.07299.
[12] Simon R. Blackburn, Peter M. Neumann, and Geetha Venkataraman. *Enumeration of finite groups*. Cambridge University Press, 2007.

Some groups coming from elliptic curves

Joshua Maglione
(joint work with Mima Stanojkovski)

We define a unipotent group scheme $G_{E,P}$ coming from an elliptic curve E given by a short Weierstrass formula and a point P on E different from $(0:1:0)$. We characterize when two such (abstract) groups are isomorphic over finite fields, and we determine the cardinalities of their automorphism groups. We use this to constructively recognize such groups and return the possibly empty coset of isomorphisms to such a group $G_{E,P}$. Additional results, details, and examples can be found in [4]

Let K be the finite field with $q = p^e$ elements for a prime $p \geqslant 5$ and $e \in \mathbb{N}$. Let $a, b \in K$ such that $4a^3 + 27b^2 \neq 0$, so that $y^2z = x^3 + axz^2 + bz^3$ defines an elliptic curve E in variables x, y, z. Let $P = (\lambda : \mu : 1)$ be a projective point on E, written $P \in E(K)$. We set $\mathcal{O} = (0:1:0) \in E(K)$. To define $G_{E,P}$ we use the Baer correspondence [1]. Let y_1, y_2, y_3 be variables and set

$$C_{E,P} = \begin{pmatrix} y_1 - \lambda y_3 & y_2 - \mu y_3 & 0 \\ y_2 + \mu y_3 & \lambda y_1 + (a + \lambda^2)y_3 & y_1 \\ 0 & y_1 & -y_3 \end{pmatrix} \in \mathrm{Mat}_3(K[y_1, y_2, y_3]).$$

Let $B_{E,P} = \left(\begin{smallmatrix} 0 & C_{E,P} \\ -C_{E,P}^{\mathrm{t}} & 0 \end{smallmatrix}\right)$, so $B_{E,P}$ defines an alternating K-bilinear map. Thus, let $G_{E,P}$ be the associated Baer group scheme over K; see [4, Sec. 1.5 & 2.4]. The following theorem characterizes when two such abstract groups are isomorphic.

Theorem 1. *Let E and E' be elliptic curves over K with $P \in E(K) \setminus \{\mathcal{O}\}$ and $P' \in E'(K) \setminus \{\mathcal{O}'\}$. The following are equivalent.*

(1) $G_{E,P}(K) \cong G_{E',P'}(K)$.
(2) *There exists $\sigma \in \mathrm{Gal}(K/\mathbb{F}_p)$ and an isomorphism of elliptic curves $\varphi : E' \to \sigma(E)$ such that $P' \mapsto \sigma(P)$.*

Theorem 1 provides a way to enumerate the isomorphism classes within the set

$$\mathcal{G}_q = \left\{ G_{E,P}(\mathbb{F}_q) \;\middle|\; \begin{array}{c} a, b \in \mathbb{F}_q,\ E : y^2 = x^3 + ax + b, \\ P \in E(\mathbb{F}_q) \end{array} \right\}.$$

See the author's problem presentation and [4, Conj. 6.9] for a conjecture concerning $|\mathcal{G}_q/{\cong}|$.

The ingredients to prove Theorem 1 are also used to count the cardinalities of the automorphism groups of the $G_{E,P}(K)$. For $m \in \mathbb{N}$, we denote by $E[m](K)$ the m-torsion subgroup of the abelian group $E(K)$.

Theorem 2. *There exists a subgroup $S \leqslant \mathrm{Gal}(K/\mathbb{F}_p)$ such that*

$$\frac{|\mathrm{Aut}(G_{E,P}(K))|}{p^{18e^2}} = |S| \cdot |E[3](K)| \cdot \frac{|\mathrm{Aut}_{\mathcal{O}}(E)|}{|\mathrm{Aut}_{\mathcal{O}}(E) \cdot P|} \cdot \begin{cases} |\mathrm{GL}_2(K)| & \text{if } P \in E[2](K) \setminus \{\mathcal{O}\}, \\ 2(p-1) & \text{otherwise.} \end{cases}$$

As a consequence of Theorem 2, the function $p \mapsto |\mathrm{Aut}(G_{E,P}(\mathbb{F}_p))|$ is almost never a polynomial on residue classes. See [4, Cor. 1.5] for details. Therefore, the phenomenon observed in [2] is very common.

The next theorem states that we can both constructively recognize the groups $G_{E,P}(K)$ and construct the coset of isomorphisms. We significantly improve upon the running time of deciding isomorphism between such groups.

Theorem 3. *There are algorithms that, given a group G of order p^{9m},*

1. *decide if there exists an elliptic curve E over $\mathbb{F}_{p^m}$ and $P \in E(\mathbb{F}_{p^m}) \setminus \{\mathcal{O}\}$ such that $G \cong G_{E,P}(\mathbb{F}_{p^m})$, and if so,*
2. *return the coset of isomorphisms $G \to G_{E,P}(\mathbb{F}_{p^m})$.*

The first algorithm is Las Vegas and runs in time polynomial in $\log |G|$. The second algorithm runs in time $O(|G|^{1/9})$.

The bottleneck for the second algorithm is that it runs through all the points on the elliptic curve E. We have implemented the algorithms from Theorem 3 in Magma which is publicly available [3].

References

[1] R. Baer, *Groups with abelian central quotient*, Trans. Amer. Math. Soc. **44** (1938), No. 3, 357–386.

[2] M. du Sautoy, M. Vaughan-Lee, *Non-PORC behaviour of a class of descendant p-groups*, J. of Algebra, **361** (2012), 287–312.

[3] J. Maglione, *EGroups*, Magma implementation, (2022), `github.com/joshmaglione/egroups`.

[4] J. Maglione, M. Stanojkovski, *Smooth cuboids in group theory*, Algebra Number Theory, **19** (2025), No. 5, 967–1006.

Isomorphism Strategies via Categories

James B. Wilson

(joint work with Peter A. Brooksbank, Heiko Dietrich, Joshua Maglione, Eamonn A. O'Brien)

A central tool in isomorphism testing of groups is to locate an isomorphism invariant such as a characteristic structure [3]. However, examples for Rotländer [4] and others shows that some groups have characteristic structures that are indistinguishable from those of other subgroups and thus as a tool for reducing isomorphism testing this inserts a new problem of first solving the matching problem of characteristic structures, which can be as hard as isomorphism testing directly. The problem is in the definition of characteristic structures as a property of individual groups.

We introduce a category-wide characterization of characteristic structures. With this definition the matching problem becomes more tractable. Furthermore, this

characterization allows for a study of the source of characteristic subgroups through a categorical lens. Examples include adjoint functors pairs and more generally relies on the introduction of a representation theory for categories. The implementation of such a representation theory is made possible by reducing categories to ordinary algebras by dropping the objects and treating them as essentially algebraic structures similar to monoids.

Reports on joint work [1, 2] with P.A. Brooksbank, H. Dietrich, J. Maglione, and E.A. O'Brien.

References

[1] Peter A. Brooksbank, Heiko Dietrich, Joshua Maglione, E. A. O'Brien, James B. Wilson *Categorification of characteristic structures*, arXiv:2502.01138.

[2] Peter A. Brooksbank, Joshua Maglione, E. A. O'Brien, James B. Wilson *Isomorphism invariant metrics*, arXiv:2304.00465

[3] Bettina Eick, C. R. Leedham-Green, and E. A. O'Brien, *Constructing automorphism groups of p-groups*, Comm. Algebra 30 (2002), no. 5, 2271–2295.

[4] Ada Rottländer *Nachweis der Existenz nicht-isomorpher Gruppen von gleicher Situation der Untergruppen.* Mathematische Zeitschrift, 28(1):641–653, 1928.

Detecting structure in tensors using algebraic invariants

Peter Brooksbank

(joint work with Martin Kassabov, James Wilson)

An ℓ-tensor is a multilinear function $t : U_1 \times \cdots \times U_\ell \to \mathbb{K}$, where each U_a is a $\mathbb{K}$-space called an *axis* of t. Fixing for each $a \in \{1, \ldots, \ell\}$ a basis $e_{a,1}, \ldots, e_{a,d_a}$ for U_a, one can represent t as an ℓ-way array Γ, where $\Gamma(i_1, \ldots, i_\ell) = t(e_{1,i_1}, \ldots, e_{\ell,i_\ell})$. Applying a tuple $\mathrm{X} = (X_1, \ldots, X_\ell)$ of invertible matrices, one can change t for an equivalent tensor t^{X}, where $t^{\mathrm{X}}(u_1, \ldots, u_\ell) = t(X_1 u_1, \ldots, X_\ell u_\ell)$. This operation transforms the array Γ representing t to a new array Γ^{X} that records t evaluated at the new axis bases determined by X.

Broadly speaking, the computational problem addressed in this talk is whether, given a tensor recorded as an array Γ relative to some arbitrary basis, one can compute a basis change X such that the resulting array Γ^{X} is "sparse". More precisely, we ask whether the existence of certain *null patterns* can be detected within the given array Γ and revealed by the array Γ^{X}. In the case of a matrix (2-tensor) Γ, for example, it is easy to find a pair (X, Y) of invertible matrices so that $\Gamma^{(X,Y)} = X\Gamma Y^\top$ is the diagonal matrix $\mathbf{1}_r \oplus \mathbf{0}_{n-r}$, where r is the rank of Γ. Variants that capture additional symmetries—such as Jordan normal form—are also easy to compute for matrices.

The problem is much harder—not to mention less clearly defined—for tensors of higher valence, but a great many applications benefit from the discovery of null patterns in tensor data. For instance, block diagonal structures are sought in blind source separation [5], where higher-order statistics such as moments or cumulants of independent events occur as distinct clusters on the diagonal. Another common type of decomposition focuses on a pair of axes and seeks decompositions

along their common face. Applications of face block decompositions include polynomial and algebra factorization [7, 9], outlier detection [1], simultaneous block diagonalization of matrices [4, 8], and low-rank approximation problems [6].

Based on work in [2], this talk outlines a new strategy to detect and reveal null patterns in tensors. First, a computable family of null patterns is defined using a matrix parameter $\mathcal{C}$ called a "chisel". This family includes the diagonal and face block decompositions of the previous paragraph, and a whole lot more. For instance, there is a chisel that parametrizes patterns where data in a 3-tensor congregates around a surface, a curve, or a tube. Secondly, an algorithm is presented that, given an array Γ representing a tensor t and a chisel matrix $\mathcal{C}$, finds a change of basis that reveals a null pattern parameterized by $\mathcal{C}$ (or determines that no such pattern exists). The methods we present are to a great extent field agnostic, and in preliminary testing are tolerant of a certain amount of noise.

The talk also includes demonstrations of the algorithm in action using an implementation in the Julia system that is publicly available on GitHub [3].

References

[1] Evrim Acar, Seyit A. Çamtepe, M.S. Krishnamoorthy, and Bülent Yener. Modeling and multiway analysis of chatroom tensors. In *Intelligence and Security Informatics. ISI 2005. Lecture Notes in Computer Science*, volume 3495. Springer, Berlin, Heidelberg, 2005.

[2] Peter Brooksbank, Martin Kassabov, James Wilson. Detecting cluster patterns in tensor data. https://arxiv.org/abs/2408.17425

[3] Peter Brooksbank, Martin Kassabov, James Wilson. *OpenDleto*: Julia software for detecting null patterns in tensor data. https://github.com/thetensor-space/OpenDleto

[4] Yunfeng Cai and Ren-Cang Li. Perturbation analysis for matrix joint block diagonalization. *Linear Algebra Appl.*, 581:163–197, 2019.

[5] J.-F. Cardoso. Super-symmetric decomposition of the fourth-order cumulant tensor. blind identification of more sources than sensors. , 5(5):3109–3112, 1991. ISBN: 0-7803-0003-3.

[6] Lieven De Lathauwer. Decompositions of a higher-order tensor in block terms—part ii: Definitions and uniqueness. *SIAM Journal on Matrix Analysis and Applications*, 30(3):1033–1066, 2008.

[7] W. Eberly and M. Giesbrecht. Efficient decomposition of associative algebras over finite fields. *J. Symbolic Comput.*, 29(3):441–458, 2000.

[8] James B. Wilson. Decomposing p-groups via Jordan algebras. *J. Algebra*, 322(8):2642–2679, 2009.

[9] James B. Wilson. Existence, algorithms, and asymptotics of direct product decompositions, I. *Groups Complex. Cryptol.*, 4(1):33–72, 2012.

IR-Algorithms for graph isomorphisms and automorphisms

Pascal Schweitzer

(joint work with Markus Anders)

In the talk, I surveyed techniques used by modern practical algorithms for the automorphism group computation of graphs. These tools can also be used to compute automorphisms of any other explicitly given finite combinatorial object. Indeed,

I highlighted that there is a polynomial time reduction from automorphism problems of general, explicitly described combinatorial objects to graph isomorphism. This justifies a focus on graphs.

This algorithmic problem is known to be in the complexity class NP, but neither known to be NP-complete nor known to be in the complexity class P. With the appearance of Babai's quasipolynomial time algorithm for the graph isomorphism problem, focus has shifted to group isomorphism as a special case. Specifically, the group isomorphism problem for groups, given by multiplication table, reduces in polynomial time to the graph isomorphism problem. In turn, the graph isomorphism problem reduces to the permutational group isomorphism problem.

A problem related to the graph isomorphism problem is that of canonization. In the talk, I also surveyed what is currently known about the relationship between isomorphism problems and canonization problems. For example, a polynomial time reduction from the graph isomorphism problem to the canonization problem is immediate, but no polynomial-time reduction in the other direction is known.

The main part of the talk focused on modern practical techniques. The foremost technique, pioneered by Brendan McKay in his tool nauty, is the individualization-refinement framework (IR). The framework is widely used by almost all existing tools for symmetry computation. I presented theoretical and practical developments of recent years in this area [1]. They show that randomized search traversal techniques are provably superior to deterministic techniques. This is corroborated by a new practical software tool DEJAVU freely available at `automorphisms.org`.

Finally, I emphasized that despite recent breakthroughs, it is still an open problem whether there is an algorithm for the group isomorphism problem that runs in time polynomial in the orders of the given groups. It is generally believed that the question is both a major bottleneck to find a better graph isomorphism algorithm, and also to find faster group isomorphism algorithms, even when considered in encoding models other than multiplication tables.

References

[1] M. Anders and P. Schweitzer. Search problems in trees with symmetries: Near optimal traversal strategies for individualization-refinement algorithms. In *48th International Colloquium on Automata, Languages, and Programming, ICALP 2021, July 12-16, 2021, Glasgow, Scotland (Virtual Conference)*, volume 198 of *LIPIcs*, pages 16:1–16:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

Maximal solvable subgroups

Mikko Korhonen

A subgroup of a group G is said to be *maximal solvable* if it is maximal among the solvable subgroups of G, with respect to inclusion. One basic motivation for considering maximal solvable subgroups comes from the fact that for various classes of groups, the following property holds: *if $H \leq G$ is solvable, then $H \leq M$ for some maximal solvable subgroup M of G.* (This property is obviously true for finite groups, and more generally for linear groups by a classical result of Zassenhaus

[15].) For such a group G, one can thus try to understand the solvable subgroup structure of G by first examining the maximal solvable subgroups of G.

Although in general classifying all solvable subgroups of a given group G is a hopeless problem, for some families of groups one can get very precise information about their maximal solvable subgroups, and in some cases even a complete classification is feasible. This then provides at least some partial information about the solvable subgroup structure of G. This sort of approach has been used for various problems related to solvable subgroups, see for example [10], [8], [4], [9], [1].

In his 1870 *Traité* [5], Jordan gave a classification of the maximal solvable subgroups of symmetric groups. The classification reduces to the primitive case, which is equivalent to the problem of classifying maximal irreducible solvable subgroups of $\mathrm{GL}_d(p)$, where p is a prime. In $\mathrm{GL}_d(p)$, the problem is reduced to the case of primitive irreducible solvable subgroups. These subgroups are then constructed in terms of maximal irreducible solvable subgroups of general symplectic groups $\mathrm{GSp}_{2k}(r)$ (r prime) and orthogonal groups $\mathrm{O}^{\pm}_{2k}(2)$.

Jordan's results on maximal solvable subgroups seem to have received little attention compared to some of his other results. Later, properties of maximal solvable subgroups have been studied by many authors, perhaps most notably by Suprunenko in the 1950s and 1960s [12], [13]. In [13, Section 18 – Section 20], Suprunenko describes the general structure and construction of maximal solvable subgroups of $\mathrm{GL}_n(\mathbb{F})$ over an arbitrary field $\mathbb{F}$, thus generalizing some of the results of Jordan. For the most part, Suprunenko does not attempt to study when the subgroups given by the construction are maximal solvable in $\mathrm{GL}_n(\mathbb{F})$, although he does illustrate the construction by giving a complete classification of maximal irreducible solvable subgroups of $\mathrm{GL}_r(q)$ for r prime [13, 21.3]. Further analysis of the prime degree case for classical groups was done by Detinko, see for example [2]. For other previous work related to maximal solvable subgroups, see for example [3], [14], [11].

In our talk, we reported on our recent work [6] that considers the classification of maximal solvable subgroups of finite classical groups. In [6] we provide the first modern exposition of the classical results of Jordan, and more generally, we provide a complete classification of the maximal irreducible solvable subgroups of the following groups:

- $\mathrm{GL}_n(q)$ (general linear groups)
- $\mathrm{GSp}_n(q)$, $\mathrm{Sp}_n(q)$ (symplectic groups)
- $\mathrm{GO}_n(q)$, $\mathrm{O}_n(q)$ (orthogonal groups)
- $\Omega_n(q)$ (n even, q even)

In the orthogonal and symplectic case, we also classify more generally the *metrically completely reducible* maximal solvable subgroups, where metrically completely reducible means that the group has no nonzero invariant subspaces which are totally isotropic.

In all cases, the classification provides an explicit recursive construction that allows one to write down generators for the maximal solvable subgroups. This can then be implemented on a CAS such as Magma or GAP. In a Magma package

(MIRS on Github [7]), we have implemented the generators for maximal irreducible solvable subgroups of $\mathrm{GL}_n(q)$ for certain degrees n and arbitrary q. Here "certain degrees" means that the exponents in the prime factorization of n are not too big — in particular the implementation works for all $1 \leq n \leq 127$, and also for arbitrary squarefree n. Using the results from [6], with further work this implementation could be extended to arbitrary n, and for the other classical groups considered in our work.

References

[1] A. A. Baykalov, *Base sizes for finite linear groups with solvable stabilisers*, J. Group Theory, to appear.

[2] A. S. Detinko. Maximal solvable subgroups of the special linear group over an arbitrary field. *Sibirsk. Mat. Zh.*, 33(6):39–46, 229, 1992.

[3] J. D. Dixon. *The structure of linear groups*. Van Nostrand-Reinhold, London, 1971.

[4] S. Dolfi, *Large orbits in coprime actions of solvable groups*, Trans. Amer. Math. Soc. **360** (2008), no. 1, 135–152.

[5] C. Jordan. *Traité des substitutions et des équations algébriques*. Gauthier-Villars, Paris, 1870.

[6] M. Korhonen, *Maximal solvable subgroups of finite classical groups*, Lecture Notes in Mathematics, vol. 2346, Springer, 2024.

[7] M. Korhonen, *MIRS*, GitHub repository (2024), `https://github.com/korhonenmikko/MIRS`

[8] A. Mann, *Soluble subgroups of symmetric and linear groups*, Israel J. Math. **55** (1986), no. 2, 162–172.

[9] E. A. O'Brien, I. Ponomarenko, A. V. Vasil'ev, and E. Vdovin, *The 3-closure of a solvable permutation group is solvable*, J. Algebra **607** (2022), 618–637.

[10] P. P. Pálfy, *A polynomial bound for the orders of primitive solvable groups*, J. Algebra **77** (1982), no. 1, 127–137.

[11] M. W. Short. *The primitive soluble permutation groups of degree less than* 256, volume 1519 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1992.

[12] D. A. Suprunenko. *Soluble and nilpotent linear groups*. American Mathematical Society, Providence, R.I., 1963.

[13] D. A. Suprunenko. *Matrix groups*. American Mathematical Society, Providence, R.I., 1976. Translated from Russian, Translation edited by K. A. Hirsch, Translations of Mathematical Monographs, Vol. 45.

[14] A. E. Zalesskiĭ and V. S. Konjuh. Sylow π-subgroups of the classical groups. *Mat. Sb. (N.S.)*, 101(143)(2):231–251, 1976.

[15] H. Zassenhaus. Beweis eines satzes über diskrete gruppen. *Abh. Math. Sem. Univ. Hamburg*, 12(1):289–312, 1937.

Zeros of S-characters

Thomas Breuer

(joint work with Michael Joswig, GunterMalle)

In [6], Zhmud' defines an *S-character* of a finite group G to be an integral linear combination of the irreducible complex characters of G that takes only nonnegative real values and that contains the trivial character 1_G exactly once. For example, every transitive permutation character of G is an S-character. Each non-trivial S-character vanishes on some group element. By [3], each non-trivial transitive

permutation character vanishes even on some element of prime power order. J-P. Serre asks in [5] whether this holds more generally for S-characters.

We show that this is not the case, by constructing counterexamples. In order to compute the set of S-characters of a group G, we proceed as follows. Take the real matrix of orbit sums of the complex irreducible characters of G under complex conjugation, and omit duplicate columns, call the resulting $n \times n$ matrix A, and consider the polytope $\{v \in \mathbb{R}^n; vA \in \mathbb{R}^n_{\geq 0}, v_1 = 1\}$. The coordinates of the S-characters of G are exactly the lattice points of this polytope. The computer algebra system OSCAR [4] provides the necessary functionality for the enumeration of these lattice points. In particular, it supports polytopes defined by inequalities over a number field embedded into the field of real numbers, and it supports the conversion of real character values to elements of such number fields.

Since we are interested only in those S-characters which are nonzero on all elements of prime power order, we can a priori consider the in general smaller polytope obtained by replacing the inequality $(vA)_i \geq 0$ by $(vA)_i \geq 1$ whenever the i-th column of A has only rational values and corresponds to elements of prime power order.

The alternating group on eight points is the group with the smallest number of conjugacy classes which has a non-trivial S-character that is nonzero on all elements of prime power order. This group is also the group of smallest order with this property whose character table is in the ATLAS of Finite Groups [2].

Many more examples occur for larger ATLAS groups, they are listed in the paper [1]. The OSCAR code for reproducing these results can be found at `https://github.com/oscar-system/S_characters.jl`.

References

[1] Thomas Breuer, Michael Joswig, Gunter Malle, *Zeros of S-characters*, Journal of Computational Algebra **13–14** (2025), 100031.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[3] B. Fein, W. M. Kantor, M. Schacher, *Relative Brauer groups. II.*, J. reine angew. Math. **328** (1981), 39–57.

[4] The OSCAR Team, *OSCAR – Open Source Computer Algebra Research system, version 1.3.1*, 2025, `https://www.oscar-system.org`.

[5] J-P. Serre, *Zéros de caractères*, ArXiv 2312.17551v2, 2024.

[6] É. M. Zhmud', *On a variety of nonnegative generalized characters of a finite group*, Ukraïn. Mat. Zh. **47** (1995), 1338–1349; translation in Ukrainian Math. J. **47** (1995), 1526–1540.

Towards an algorithm for recognizing classical groups

Stephen Glasby

(joint work with Alice C. Niemeyer and Cheryl E. Praeger)

A paradigm for analyzing subgroups of a finite matrix group $\mathrm{GL}_d(\mathbb{F})$ involves first constructing a composition tree whose leaves are quasisimple groups. The most common quasisimple groups that arise in practice are the finite classical groups, so

there is much interest in fast constructive recognition algorithms of such groups. Ideas for previous algorithms for this task are due to Brooksbank, Kantor, Seress, Neunhöffer, Leedham-Green, O'Brien, ... We build on their ideas.

In joint work with Alice Niemeyer and Cheryl Praeger, we sought to design and analyze algorithms to recognize classical groups acting on their natural module. We call an element $g \in \mathrm{GL}(V)$ a *stingray element* if g acts irreducibly on $U = V(1-g)$, and hence fixes pointwise a complement to U in V. We proved in [5] that two random non-degenerate subspaces of a classical group, of complementary dimensions, span the natural module with high probability. In [3] with Ihringer and Mattheus, we improved these bounds to $1 - 3/(2|\mathbb{F}|)$ where $|\mathbb{F}|$ is the size of the underlying field. This allowed us to prove in [4] that a random pair (g, g') of stingray elements in a classical group on V with high probability has $U = V(1-g)$ disjoint from $U' = V(1-g')$ and $\langle g, g' \rangle$ is a nondegenerate classical group.

The above probability has the form $1 - c/|\mathbb{F}|$. To bound c, we need an upper bound for the probability of non-generation. This leads us to consider various Aschbacher classes. Non-generation (for type $\mathbf{X} = \mathbf{L}$) is dominated by the reducible case: in [2] we prove that $\langle g, g' \rangle$ is reducible with probability less than $q^{-1} + q^{-2}$. (This required graph-theoretic ideas involving the q-Kneser graph.) Bounding the probability that $\langle g, g' \rangle$ is a $\mathcal{C}_9$-group requires intricate representation theory, and was done with Alex Zalesski in [1]. The remaining Aschbacher classes $\mathcal{C}_2, \ldots, \mathcal{C}_8$ are handled in [6]. Nongeneration occurs with a very low probability, in many cases $c/q^{ee'}$ where $e = \dim(V(1-g))$, $e' = \dim(V(1-g'))$ and c is 'small'.

References

[1] S.P. Glasby, Alice C. Niemeyer, Cheryl E. Praeger and A. E. Zalesski, Absolutely irreducible quasisimple linear groups containing elements of order a specified Zsigmondy prime. Submitted 13 November 2024. https://arxiv.org/abs/2411.08270

[2] S.P. Glasby, Alice C. Niemeyer and Cheryl E. Praeger, Bipartite q-Kneser graphs and two-generated irreducible linear groups, *Linear Algebra Appl.* 710 (2025), 203–229.

[3] S.P. Glasby, Ferdinand Ihringer and Sam Mattheus, The proportion of non-degenerate complementary subspaces in classical spaces, *Des. Codes, Cryptogr.* 91(9) (2023), 2879–2891.

[4] S.P. Glasby, Alice C. Niemeyer and Cheryl E. Praeger, Random generation of direct sums of finite non-degenerate subspaces, *Linear Algebra Appl.* 649 (2022), 408–432.

[5] S.P. Glasby, Alice C. Niemeyer and Cheryl E. Praeger, The probability of spanning a classical space by two non-degenerate subspaces of complementary dimension, *Finite Fields Their Appl.* 82 (2022), paper no. 102055.

[6] S. P. Glasby and Alice C. Niemeyer and Cheryl E. Praeger, The probability that two elements with large 1-eigenspaces generate a classical group, in preparation.

Orbits: tame and wild

Tobias Rossmann

This talk was devoted to recent developments in the symbolic enumeration of orbits. Let $\mathbf{G}$ be a group scheme acting on a scheme $\mathbf{X}$. (Schemes are assumed to be separated and of finite type in the following.) For example, $\mathbf{G} \leqslant \mathrm{GL}_n$ could be a linear group scheme acting naturally on affine n-space or on itself by conjugation.

Our goal is to determine the number of orbits $h(\mathbf{G} \curvearrowright \mathbf{X}; q) := |\mathbf{X}(\mathbf{F}_q)/\mathbf{G}(\mathbf{F}_q)|$ as a "symbolic function" of the prime power q. Let $\mathbf{Y}$ be the scheme representing the functor $R \rightsquigarrow \{(x, g) \in \mathbf{X}(R) \times \mathbf{G}(R) : xg = x\}$. Burnside's lemma shows that $|\mathbf{X}(\mathbf{F}_q)/\mathbf{G}(\mathbf{F}_q)| = |\mathbf{Y}(\mathbf{F}_q)|/|\mathbf{G}(\mathbf{F}_q)|$. Hence, $h(\mathbf{G} \curvearrowright \mathbf{X}; q)$ is expressible in terms of the numbers of $\mathbf{F}_q$-rational points of schemes—this is an archetypal example of a function which depends geometrically on q. We regard such functions as *tame* when they are (close to being) polynomial in q; otherwise, they are *wild*.

It is natural to ask just how wild the functions $q \mapsto h(\mathbf{G} \curvearrowright \mathbf{X}; q)$ can be if $\mathbf{G}$ and $\mathbf{X}$ are themselves restricted to be geometrically tame. By [8, Thm A], we can approximate (in a suitable sense) the number of $\mathbf{F}_q$-rational points on an arbitrary scheme by means of (a) numbers of linear orbits of commutative unipotent groups or (b) by means of class numbers of Baer group schemes, all uniformly in q. This combines a deep result due to Belkale and Brosnan [1] and recent techniques surrounding so-called *ask zeta functions* (introduced in [5]). We conclude that symbolically enumerating linear orbits and conjugacy classes of unipotent groups is a fundamentally hopeless task in the sense that it is as hard as enumerating solutions to arbitrary $\mathbf{Z}$-defined systems of polynomial equations over $\mathbf{F}_q$.

On the other hand, for many specific families of groups of interest, we can of course do much better. Let $\mathrm{k}(H)$ denote the number of conjugacy classes ("class number") of a group H. Let $\mathfrak{O}$ be a compact discrete valuation ring with maximal ideal $\mathfrak{P}$, e.g. the p-adic integers $\mathbf{Z}_p$ or a power series ring $\mathbf{F}_q[\![z]\!]$. The *class-counting zeta function* of a group scheme $\mathbf{G}$ over $\mathfrak{O}$ is the generating function

$$\mathsf{Z}^{\mathrm{cc}}_{\mathbf{G},\mathfrak{O}}(T) := \sum_{k=0}^{\infty} \mathrm{k}(\mathbf{G}(\mathfrak{O}/\mathfrak{P}^k))T^k.$$

The second half of the talk focused on recent developments surrounding class-counting zeta functions of *graphical groups*. Given a graph Γ and (commutative) ring R, the graphical group $\mathbf{G}_\Gamma(R)$ is a certain nilpotent group of class at most 2 whose commutator structure encodes adjacency in Γ. For precise definitions, see [7, Section 3.4] or [6, Section 1.1]. For example, the graphical group scheme associated with a complete graph K_n is a group scheme version of the free class-2-nilpotent group on n generators. By [7, Thm A], given any Γ, there exists an explicitly computable rational function $W_\Gamma(X, T) \in \mathbf{Q}(X, T)$ (denoted $W^{-}_{\Gamma}(X, T)$ in [7]) such that for each compact discrete valuation ring $\mathfrak{O}$ with residue field size q, we have $\mathsf{Z}^{\mathrm{cc}}_{\mathbf{G}_\Gamma,\mathfrak{O}}(T) = W_\Gamma(q, q^m T)$; here, m denotes the number of edges of Γ. We conclude that the class numbers $\mathrm{k}(\mathbf{G}_\Gamma(\mathfrak{O}/\mathfrak{P}^k))$ depend tamely on $\mathfrak{O}$ and also on the congruence level k.

In the talk, I reported on two further recent results that both establish forms of tameness with respect to natural graph-theoretic operations:

- The *join* $\Gamma_1 \vee \Gamma_2$ of graphs Γ_1 and Γ_2 is obtained from their disjoint union $\Gamma_1 \oplus \Gamma_2$ by adding an edge connecting each vertex of Γ_1 to each vertex of Γ_2. By [9, Thm A], the rational function $W_{\Gamma_1 \vee \Gamma_2}(X, T)$ is expressible as an explicit "distorted sum" of translates of $W_{\Gamma_1}(X, T)$ and $W_{\Gamma_2}(X, T)$. This result relies on a description of $W_\Gamma(X, T)$ in terms of p-adic integrals

involving what we call animations. By an *animation* of a graph $\Gamma = (V, E)$, we mean a partial function from V to V which, whenever defined, sends a vertex to one of its neighbours.

- It is easy to see that $W_{\Gamma_1 \oplus \Gamma_2}(X, T)$ is the *Hadamard product* of $W_{\Gamma_1}(X, T)$ and $W_{\Gamma_2}(X, T)$. In general, predicting properties of Hadamard products of rational generating functions from properties of the factors seems to be very difficult. Building upon and extending work of Gessel and Zhuang [4], in [3] (see also [2]), we obtained explicit formulae for Hadamard products of certain rational generating functions. As an application, in [3, Section 5.3], we recorded several instances of explicit formulae for zeta functions enumerating linear orbits and conjugacy classes. In particular, our findings show that, given n, there exists an explicit rational function $W_n(X, Y_1, \ldots, Y_n, T)$ such that, up to an explicit translation, the rational function $W_{\mathrm{K}_{d_1} \oplus \cdots \oplus \mathrm{K}_{d_n}}(X, T)$ coincides with $W_n(X, X^{d_1}, \ldots, X^{d_n}, T)$.

Both results have direct applications to explicitly computing $W_\Gamma(X, T)$ and hence to symbolically enumerating conjugacy classes of graphical groups.

References

[1] P. Belkale and P. Brosnan, *Matroids, motives, and a conjecture of Kontsevich*, Duke Math. J. 116 (2003), no. 1, 147–188.

[2] A. Carnevale, V. D. Moustakas, and T. Rossmann, *From coloured permutations to Hadamard products and zeta functions*. Proceedings of the 36th Conference on Formal Power Series and Algebraic Combinatorics (Bochum). Sém. Lothar. Combin. 91B (2024), Article #56, 12 pp.

[3] A. Carnevale, V. D. Moustakas, and T. Rossmann, *Coloured shuffle compatibility, Hadamard products, and ask zeta functions*. Bull. Lond. Math. Soc. (2025), 23 pages. DOI:10.1112/blms.70081

[4] I. M. Gessel and Y. Zhuang, *Shuffle-compatible permutation statistics*. Adv. Math. 332 (2018), 85–141.

[5] T. Rossmann, *The average size of the kernel of a matrix and orbits of linear groups*. Proc. Lond. Math. Soc. (3) 117 (2018), no. 3, 574–616.

[6] T. Rossmann, *Enumerating conjugacy classes of graphical groups over finite fields*. Bull. Lond. Math. Soc. 54 (2022), no. 5, 1923–1943

[7] T. Rossmann and C. Voll, *Groups, graphs, and hypergraphs: average sizes of kernels of generic matrices with support constraints*. Mem. Amer. Math. Soc. 294 (2024), no. 1465, vi+120 pp.

[8] T. Rossmann, *On the enumeration of orbits of unipotent groups over finite fields*. Proc. Amer. Math. Soc. 153 (2025), no. 2, 479–495.

[9] T. Rossmann and C. Voll, *Ask zeta functions of joins of graphs* (preprint). arXiv:2505.10263

Alternating groups as products of three conjugacy classes

Daniele Dona

In 2021, Garonzi and Maróti [5] proved a result about normal subsets of $\mathrm{Alt}(n)$ that in particular implies the following.

Theorem 1 ([5], Thm. 1.1)**.** *For any $\varepsilon > 0$, any $n \gg_\varepsilon 1$, and any four conjugacy classes C_1, C_2, C_3, C_4 of $G = \mathrm{Alt}(n)$ with $|C_i| \geq |G|^{\frac{1}{2}+\varepsilon}$, we have $C_1C_2C_3C_4 = G$.*

In particular, since every element of a given class in $\mathrm{Alt}(n)$ has the same cycle structure, for any $g \in \mathrm{Alt}(n)$ and any four such cycle structures there is a way to write $g = \alpha_1\alpha_2\alpha_3\alpha_4$ with α_i having those structures.

It is easy to show that, for any $\delta > 0$ and n large enough, there are classes C_1, C_2 of size $\geq |\mathrm{Alt}(n)|^{1-\delta}$ such that C_1C_2 does not cover $\mathrm{Alt}(n)$, or even $\mathrm{Alt}(n) \setminus \{e\}$. In light of [5], the next question is: can we cover $\mathrm{Alt}(n)$ with *three* such classes? This is Problem 20.23 in the Kourovka Notebook [6], and the answer is "yes".

Theorem 2 ([2], Thm. 1.2)**.** *There is $\delta > 0$ such that, for any $n \gg 1$ and any three classes C_1, C_2, C_3 of $G = \mathrm{Alt}(n)$ with $|C_i| \geq |G|^{1-\delta}$, we have $C_1C_2C_3 = G$.*

A few facts from the literature:

- the same statement is trivial for G abelian or sporadic and δ small enough, and was already known for all finite simple groups of Lie type [8];
- stronger statements, asking for approximately the same number of solutions to $g = \alpha_1\alpha_2\alpha_3$ for every $g \in G$, are known to be true for G of Lie type [4] but false for $G = \mathrm{Alt}(n)$ [9];
- explicit counterexamples [1] show that we must have $\delta \leq \frac{1}{2}$.

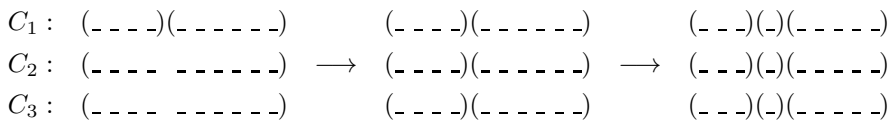
Theorem 2 allows every g to be written as $g = \alpha_1\alpha_2\alpha_3$ for α_i having a fixed cycle structure yielding a large enough class: in practice, the condition $|C| \geq |\mathrm{Alt}(n)|^{1-\delta}$ corresponds approximately to having at most δn cycles. However, having a solution to $g = \alpha_1\alpha_2\alpha_3$ does not necessarily mean that we have a constructive way to build the appropriate α_i. As a matter of fact, many papers dealing with products of conjugacy classes are not constructive: at least since the paper by Liebeck and Shalev on diameters of finite simple groups [7], character theory has been used as a powerful but non-constructive tool to prove similar statements. Character-theoretic techniques might be necessary to deal with problems on groups of Lie type, but problems on alternating groups should be within the reach of elementary and constructive arguments.

The proof of Theorem 2 is one such case. It relies on the following intermediate result, entirely self-contained in the paper.

Theorem 3 ([2], Thm. 1.4)**.** *There is $\delta > 0$ such that, for any $n \gg 1$ and any three classes C_1, C_2, C_3 of $G = \mathrm{Alt}(n)$ with $|C_i| \geq |G|^{1-\delta}$, we have $C_1C_2 \supseteq C_3$.*

To give a little taste of the arguments involved, let us see a baby example. Suppose we want to build elements $\alpha_i \in C_i \subseteq \mathrm{Sym}(10)$ such that $\alpha_1\alpha_2 = \alpha_3$, where C_1 is the class of elements made of a 4-cycle and a 6-cycle, and $C_2 = C_3$ is the class of 10-cycles.

First, we might try and manipulate the cycles in order to simplify the problem, subdividing it into more manageable pieces. We confide for now in our ability to walk back our simplifications in the future. For instance, we might take:



Solutions for the simplified problem on the right are immediate, by putting together $(1\,2\,3)^2 = (1\,3\,2)$, $(4)^2 = (4)$, and so on.

Now we need to go backwards. After a few attempts, we can figure out that, using only the elements $3, 4, 9, 10$, we may perform the following:

$$\begin{array}{rl} \gamma_1: & (1\,2\,\mathbf{3})(\mathbf{4})(5\,6\,7\,8\,\mathbf{9})(\mathbf{10}) \\ \gamma_2: & (1\,2\,\mathbf{3})(\mathbf{4})(5\,6\,7\,8\,\mathbf{9})(\mathbf{10}) \\ \gamma_1\gamma_2: & (2\,1\,\mathbf{3})(\mathbf{4})(6\,8\,5\,7\,\mathbf{9})(\mathbf{10}) \end{array} \quad \longrightarrow \quad \begin{array}{rl} \gamma_1(3\,4)(9\,10): & (1\,2\,\mathbf{4}\,\mathbf{3})(5\,6\,7\,8\,\mathbf{10}\,\mathbf{9}) \\ (3\,9\,4)\gamma_2(3\,10\,4): & (1\,2\,\mathbf{10}\,\mathbf{4})(5\,6\,7\,8\,\mathbf{9}\,\mathbf{3}) \\ \gamma_1(4\,9\,10)\gamma_2(3\,10\,4): & (2\,1\,\mathbf{10}\,\mathbf{3})(6\,8\,\mathbf{4}\,5\,7\,\mathbf{9}) \end{array}$$

One important thing to notice is that it does not really matter what the rest of the strings of elements in the γ_i look like: for any triple of $\gamma_i = (\vec{\gamma}_{i1}\,3)(4)(\vec{\gamma}_{i2}\,9)(10)$, the manipulation above would work just as well. Moreover, since by hypothesis the classes are large, the cycles are on average quite long, so there are many elements to play with. In our example, even if the elements $3, 4, 9, 10$ have been moved around, making some of them unusable, we might still use $2, 8$ to do the following:

$$\begin{array}{rl} \beta_1: & (4\,3\,1\,\mathbf{2})(\mathbf{8}\,10\,9\,5\,6\,7) \\ \beta_2: & (10\,4\,1\,\mathbf{2})(\mathbf{8}\,9\,3\,5\,6\,7) \\ \beta_1\beta_2: & (1\,10\,3\,\mathbf{2})(\mathbf{8}\,4\,5\,7\,9\,6) \end{array} \quad \longrightarrow \quad \begin{array}{rl} \beta_1: & (4\,3\,1\,\mathbf{2})(\mathbf{8}\,10\,9\,5\,6\,7) \\ \beta_2(2\,8): & (10\,4\,1\,\mathbf{8}\,9\,3\,5\,6\,7\,\mathbf{2}) \\ \beta_1\beta_2(2\,8): & (1\,10\,3\,\mathbf{8}\,4\,5\,7\,9\,6\,\mathbf{2}) \end{array}$$

and solve at last the original problem.

The proof of Theorem 3 is simply a much more laborious version of the straightforward strategy above. In particular, it produces an explicit algorithm solving the problem of finding triples of α_i of given cycle structure satisfying $\alpha_1\alpha_2 = \alpha_3$. Then, using also results of Dvir [3], there is an algorithm to find $\alpha_1\alpha_2\alpha_3 = g$ for any given g, yielding an elementary proof of Theorem 2. It is quite surprising that a proof of these theorems was not found in the 1980s: the technology involved is essentially the same.

The constant δ and the lower bound on n for which Theorems 2–3 hold are not explicitly stated in the paper, but they can be recovered easily. They are likely to be outside the realm of practical applications, but also likely to be improvable to that point, modulo a reasonable amount of effective work.

Most importantly, the proof suggests that problems of this sort on $G = \mathrm{Alt}(n)$ can be solved by elementary means, and they can be turned into explicit algorithms. The dream goal would be to determine whether $C_1C_2 \supseteq C_3$ (or equivalently whether $\alpha_1\alpha_2 = \alpha_3$ has solutions with $\alpha_i \in C_i$) for any three given classes. It might prove problematic to reach an exact answer in some extreme cases, for instance when $|C_3|$ is very close to $|C_1||C_2|$, but Theorem 3 is still quite modest in comparison to what may reasonably be hoped for.

For instance, can we constructively prove that $C_1C_2 \supseteq C_3$ whenever $|C_1|, |C_2| \geq |G|^{1-\delta}$ and $|C_3| \geq |G|^{10\delta}$, say? Or even more, can we do it for $|C_i| = |G|^{\eta_i}$ with $|\eta_1 - \eta_2| + \delta \leq \eta_3 \leq \eta_1 + \eta_2 - \delta$? Can we settle the case $G = \mathrm{Alt}(n)$ of Problem 19.12 of the Kourovka Notebook, namely, for every normal subset $S \subseteq G$ and every class $C \subseteq G$ the product SC contains at least as many classes as S? Or can we disprove any of the above by families of explicit counterexamples?

References

[1] J. L. Brenner, *Covering theorems for FINASIGS VIII – Almost all conjugacy classes in A_n have exponent ≤ 4*, J. Aust. Math. Soc. **25**:210–214, 1978.

[2] D. Dona, *Products of three conjugacy classes in the alternating group*, `arXiv:2505.06012v1`, 2025.

[3] Y. Dvir, *Covering properties of permutation groups*, in Z. Arad and M. Herzog (editors), *Products of Conjugacy Classes in Groups*, pages 197–221. Springer-Verlag, Berlin (Germany), 1985.

[4] F. Fumagalli and A. Maróti, *On the Gowers trick for classical simple groups*, J. Pure Appl. Algebra **229**(1), 2025. Article no. 107833.

[5] M. Garonzi and A. Maróti, *Alternating groups as products of four conjugacy classes*, Arch. Math. (Basel) **116**(2):121–130, 2021.

[6] E. I. Khukhro and V. D. Mazurov, *Unsolved problems in group theory – The Kourovka Notebook. No. 20*, `https://kourovka-notebook.org` and `arXiv:1401.0300v33`, 2022.

[7] M. W. Liebeck and A. Shalev, *Diameters of finite simple groups: sharp bounds and applications*, Ann. of Math. (2) **154**:383–406, 2001.

[8] A. Maróti and L. Pyber, *A generalization of the diameter bound of Liebeck and Shalev for finite simple groups*, Acta Math. Hungar. **164**(2):350–359, 2021.

[9] Y. Roichman, *Upper bound on the characters of the symmetric groups*, Invent. Math. **125**(3):451–485, 1996.

Algorithms for matrix groups over infinite domains: methods and applications

Alla Detinko

(joint work with Dane Flannery, Alexander Hulpke)

We present recent developments of our ongoing work on algorithms for practical computation with linear groups over infinite domains [1]. Special consideration is given to new techniques for groups over number fields based on the strong approximation property and residual finiteness of the groups. We illustrate applications of our algorithms to the solution of a variety of problems.

1. Strong approximation algorithms. Given a finitely generated group $H \subset \mathrm{SL}(n, \mathbb{P})$, where $\mathbb{P}$ is a number field, our aim is to test whether H is (Zariski) dense in $\mathrm{SL}(n)$, and if so, find the set $\mathcal{L}_{max}(H)$ of congruence quotients of H modulo all maximal ideals I of R; here $R \subset \mathbb{P}$ is the integral domain generated by entries of elements of H. This requires a characterization of subgroups of $\mathrm{SL}(n, p^k)$. In the talk we consider a method based on classification of irreducible subgroups of $\mathrm{SL}(n, p^k)$, $p \geq 2$, $k \geq 1$, generated by transvections. An advantage of the method is its computational efficiency. Applying this approach to a group H containing a transvection t, we design practical algorithms both for testing density of H and computing the set $\mathcal{L}_{max}(H)$. In contrast to the previously studied case of matrix groups over rationals, dense groups over $\mathbb{P} \neq \mathbb{Q}$ may not surject onto $\mathrm{SL}(n, R/I)$ for infinitely many maximal ideals I of R. We provide a criterion of congruence of H and $\mathrm{SL}(n, R)$ modulo all maximal $I \lhd R$. As an application we construct (countably many) free subgroups of $\mathrm{SL}(n, R)$ satisfying this property. A

motivation of the construction is long-standing open problems on the subgroup structure of $\mathrm{SL}(n, R)$ [4].

2. Exploiting the congruence subgroup property. As another application of our methods, we develop an alternative approach to a long standing open problem of (non)-freeness of Möbius groups $G(m) = \left\langle \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix} \right\rangle$, for rational $m = \frac{a}{b} \in (0, 2)$. Our approach is based on the congruence subgroup property of $\mathrm{SL}(2, \mathbb{Z}[\frac{1}{b}])$ [2]. This enables us to obtain a group-theoretical characterization of $G(m)$ in terms of the extended congruence subgroup $\mathrm{cl}(G(m))$ containing $G(m)$. Non-freeness of $G(m)$ can be decided via arithmeticity testing of $G(m)$ in the ambient group $\mathrm{SL}(2, \mathbb{Z}[\frac{1}{b}])$. The latter is based on algorithms constructing a presentation of $\mathrm{SL}(2, \mathbb{Z}[\frac{1}{b}])$ [3]. Our experimental output provides new examples of non-free groups $G(m)$, as well as a justification of arithmeticity of known non-free groups $G(m)$. We are not aware of any examples of thin (i.e. infinite index) groups $G(m)$.

References

[1] A. Detinko, D. Flannery, *Linear groups and computation*, Expo. Math. 37 (2019), no. 4, 454–484.

[2] A. S. Detinko, D. L. Flannery, A. Hulpke, *Zariski density and computing with S-integral groups*, J. of Algebra, **624** (2023), 93–105.

[3] A. S. Detinko, D. L. Flannery, A. Hulpke, *Freeness and arithmeticity of rational Möbius groups*, Contemp. Math., **783** (2023), 47–56.

[4] M. Kapovich, A. Detinko, and A. Kontorovich, *List of problems on discrete subgroups of Lie groups and their computational aspects*, Contemp. Math., **783** (2023), 113–126.

Algorithms for linear groups: where to?

Eamonn A. O'Brien

At the 1988 inaugural MFO meeting on Computational Group Theory, Joachim Neübuser asked for an algorithm to decide whether a group $G = \langle X \rangle \leq \mathrm{GL}(d, q)$ contains $\mathrm{SL}(d, q)$. This prompted the "matrix group recognition" project, a research program which generated much activity, drew on the outputs of many researchers, and led to excellent outcomes. In this lecture, we reviewed the project, identifying both its successes and outstanding theoretical and practical questions.

Neumann and Praeger [7] proposed, as a first step, using the classification by Aschbacher [1] of maximal subgroups of classical groups. Exploiting this classification often offers reductions via homomorphisms onto smaller structures, and provides the basis for a recursive algorithm which ultimately constructs composition factors. We can now decide computationally that a matrix group is in a specific Aschbacher category. Membership of the "tensor product" and "tensor induction" categories are not known to be decidable in polynomial time; Ryba's recent algorithm [8] relies on a solution to the "pure tensor" problem which is not known to be solvable in polynomial time.

The first step yielded CompositionTree [2]. Its central components are:

- Algorithms to realise effectively the Aschbacher classification.
- Constructive recognition of composition factors. This relies on many contributions, including those of Brooksbank, Kantor and Seress. Csaba Schneider and Don Taylor provide the "rewriting" machinery to realise explicitly the isomorphisms between the standard copy and the user-supplied copy of a simple group. An important base case is $\mathrm{SL}(2,q)$: in odd characteristic, we lack a constructive recognition algorithm which does not rely on a discrete log oracle.
- Verification of the construction by using short presentations for the composition factors.

This algorithm provides as output the equivalent of the Schreier-Sims data structure for permutation groups: we learn the order of the input matrix group G, its composition factors, and can solve the constructive membership problem for G.

Holt, Leedham-Green and O'Brien [6] proved the following.

Theorem: *There is a Las Vegas polynomial-time algorithm that takes as input $G = \langle X \rangle \leq \mathrm{GL}(d,q)$ and, subject to the existence of a discrete log oracle for $\mathrm{GF}(q^i)$ and an oracle to factorise integers of the form $q^i - 1$ for $1 \leq i \leq d$, and to the availability of polynomial-time constructive recognition algorithms and short presentations for the non-abelian composition factors of G, it constructs a composition tree for G.*

Polynomial-time constructive recognition algorithms and short presentations are available for most finite simple groups. However, we lack such algorithms for defining characteristic absolutely irreducible representations of the following exceptional groups: ${}^2B_2(2^{2k+1})$, ${}^2G_2(q)$, ${}^3D_4(2^k)$, and ${}^2F_4(2^{2k+1})$.

A finite group G has a characteristic series $\mathcal{C}$ of subgroups:

$$1 \leq O_\infty(G) \leq S^*(G) \leq P(G) \leq G,$$

where $O_\infty(G)$ is the soluble radical of G,

$$S^*(G)/O_\infty(G) = T_1 \times \ldots \times T_k$$

where T_i is non-abelian simple, $\phi : G \longmapsto \mathrm{Sym}(k)$ is the representation of G induced by conjugation on $\{T_1, \ldots, T_k\}$, and $P(G) = \ker \phi$.

The second stage of the project is the development of the infrastructure to apply the *soluble radical model*: a general framework for computation developed by Cannon, Holt and their collaborators (see for example [4]). They refine $\mathcal{C}$ to obtain

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_r = O_\infty(G) \leq S^*(G) \leq P(G) \leq G$$

where N_i/N_{i-1} is elementary abelian. This refinement can be constructed using the output of CompositionTree. The general paradigm to solve a problem in G using this model is the following: solve the problem first in $H := G/N_r$, and then, successively, solve it in G/N_i, for $i = r-1, \ldots, 0$.

We can often reduce the problem for H to its constituent almost simple groups. We considered two cases where some of the requisite information is available. The

maximal subgroups of almost simple classical groups are described in [3]. The conjugacy problem for (quasi)simple groups is solved in [5] and some progress has been made on this problem for finite exceptional groups, but as yet we lack a solution for the almost simple groups.

Finally, we identified some hard problems where this model does not immediately seem applicable. These include constructing the normaliser of a subgroup, the intersection of two subgroups, and the stabiliser of a subspace.

References

[1] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.* **76**, 469–514, 1984.

[2] Henrik Bäärnhielm, Derek Holt, C. R. Leedham-Green, and E. A. O'Brien. A practical model for computation with matrix groups. *J. Symbolic Comput.* **68**, 27–60, 2015.

[3] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal. The maximal subgroups of the low-dimensional finite classical groups. London Math. Soc. Lecture Note Ser., **407** Cambridge University Press, Cambridge, 2013.

[4] John J. Cannon and Derek F. Holt. Automorphism group computation and isomorphism testing in finite groups. *J. Symbolic Comput.* **35**, 241–267, 2003.

[5] Giovanni De Franceschi, Martin W. Liebeck and Eamonn A. O'Brien. Conjugacy in finite classical groups. Springer Monographs in Mathematics, 2025.

[6] C.R. Leedham-Green, Derek Holt and E. A. O'Brien. Constructing composition factors for a linear group in polynomial time. *J. Algebra* **361**, 215–236, 2020.

[7] Peter M. Neumann and Cheryl E. Praeger. A recognition algorithm for special linear groups. *Proc. London Math. Soc.* (3), **65**, 555–603, 1992.

[8] Alex Ryba. Recognition of absolutely irreducible matrix groups that are tensor decomposable or induced. *J. Algebra* **610**, 911–934, 2022.

Subnormalisers and picky elements

Gunter Malle

The *subnormaliser* of an element x of a group G was defined by Casolo in 1990 as $\mathrm{Sub}_G(x) := \langle S_G(x)\rangle$, where $S_G(x) := \{g \in G \mid \langle x\rangle \lhd\rhd \langle x, g\rangle\}$. It plays a central role in a recent new conjecture by Moretó and Rizo on character correspondences in finite groups. In our talk we presented some new basic properties of subnormalisers of p-elements x, where p is a prime, in finite groups, showing that such subnormalisers control the fusion "around the element x" and which also give a good handle to an efficient algorithmic method for their computation.

A special case is that of p-elements lying in a unique Sylow p-subgroup P of G, which are then called *picky*. In this case $\mathrm{Sub}_G(x)$ is the normaliser $N_G(P)$.

We reported on our determination of all picky p-elements in simple groups of Lie type, as well as partial results on subnormalisers in these groups. The latter turn out to be quite a bit more subtle and varied than in the ambient algebraic groups, which we also considered. In all cases that we could consider, the conjecture of Moretó and Rizo turned out to hold.

Computing a smallest sized generating set in a finite group

Derek Holt
(joint work with Gareth Tracey)

For a finitely generated group G we define $d(G)$ to be the size of a smallest generating set of G, that is

$$d(G) := \min\{|X| : X \subseteq G,\ \langle X\rangle = G\}.$$

As well as being of theoretical interest, knowledge of a smallest sized set is useful in many computations involving G, such as searching for homomorphisms from G to another group. But until recently, computing $d(G)$ in finite groups was thought to be very difficult in general. There were, for example, implemented algorithms that performed recursive calculations on members of the set of all subgroups of G.

For non-cyclic groups, we have the easily computed lower bound

$$d(G) \geq \max(2, d(G/[G,G])),$$

and we can attempt to check whether $d(G) = \max(2, d(G/[G,G]))$ by choosing a small sample of random subsets of G of size $\max(2, d(G/[G,G]))$ and testing whether they generate G. This approach works in a substantial proportion of finite groups, including all nilpotent groups, in which the bound is known to be exact. It works, for example, in 108 of the 150 small groups of order 900, but it is not hard to find examples in which it fails:

1. $G = A_5^{20}$. We have $d(G) = 3$, but $\max(2, d(G/[G,G])) = 2$.

2. $G = p^k\colon 2 := \langle x_1, \ldots, x_k, t \mid x_i^p = [x_i, x_j] = t^2 = 1,\ t^{-1}x_i t = x_i^{-1}\rangle$, for an odd prime p and $k \geq 2$. We have $d(p^k\colon 2) = k + 1$ but $\max(2, d(G/[G,G])) = 2$.

Then in 2024, Lucchini and Thakkar [5] proposed a new method for computing $d(G)$ for a finite group G. Its complexity is polynomial in $|G|$ ($O(|G|^{13/5})$ *generating tests*, which are tests whether a given set of elements generates a group), which is not ideal (polynomial in $\log|G|$ would be preferable for large groups), but it is far more effective in practice than all previously proposed general algorithms.

The Lucchini–Thakkar algorithm is deterministic. But there is an alternative randomized version of the algorithm for subgroups of $\mathrm{Sym}(n)$ with expected running time polynomial in n. This is joint work with Gareth Tracey [2].

The first step of the (Lucchini–Thakkar) algorithm is to compute a chief

$$1 = N_0 < N_1 < \cdots < N_u = G$$

of G. This can be done in polynomial time in permutation groups and in solvable groups defined by a PC presentation.

The algorithm proceeds by computing smallest sized generating sets of the quotients G/N_k for each k, starting with $k = u - 1$, and using these to do the same for G/N_{k-1}. More precisely, for $k = u-1, u-2, \ldots, 2, 1$, we find elements $g_1, g_2, \ldots, g_{d_k}$ of G that map onto smallest sized generating sets of G/N_k.

Since the top quotient G/N_{u-1} is simple, it is either cyclic or non-abelian and 2-generated, and we easily find a smallest generating set by choosing random

elements. *The probability that two random elements generate a given finite nonabelian simple group is at least* 53/90*, which is the probability in the simple group* A_6.

For the inductive step of using a smallest generating set of G/N_k to find one of G/N_{k-1}, we simplify notation by redefining $G := G/N_{k-1}$ and $N := N_k/N_{k-1}$. So N is a minimal normal subgroup of G, and we assume that we have already computed $d = d(G/N)$, and that we have found elements $g_1, \ldots, g_d \in G$ such that $G/N = \langle g_1N, \ldots, g_dN\rangle$.

The algorithm makes use of a number of earlier results, including the following crucial result of Gaschütz [1], which is proved by a quick but ingenious counting argument.

Proposition 1. *Let* $N \lhd G$ *with* N *finite. If* $G/N = \langle g_1N, \ldots, g_dN\rangle$ *and* G *can be generated by* d *elements, then there exist* $n_1, \ldots, n_d \in N$ *with* $G = \langle g_1n_1, \ldots, g_dn_d\rangle$.

In our situation, it turns out that either $d(G) = d$, which is the case if and only if $G = \langle g_1n_1, \ldots, g_dn_d\rangle$ for some $n_i \in N$, or $d(G) = d + 1$.

Assume, as above, that N is a minimal normal subgroup of the finite group G with $d(G/N) = d$ and $G = \langle g_1N, \ldots, g_dN\rangle$. Then either N is elementary abelian of order p^ℓ for some prime p and $l > 0$, or N is a direct product of isomorphic nonabelian simple groups. For the elementary abelian case we have the following result of Lucchini and Menegazzo [4].

Proposition 2. *If* $N = \langle e_1, e_2, \ldots, e_\ell\rangle$ *is abelian of order* p^ℓ *for a prime* p *then either*

(1) $d(G) \le d$ *and either* $G = \langle g_1, \ldots, g_d\rangle$*, or there exist* $1 \le i \le d$ *and* $1 \le j \le \ell$ *such that* $G = \langle g_1, \ldots, g_{i-1}, g_ie_j, g_{i+1}, \ldots, g_d\rangle$*; or*
(2) $d(G) = d + 1$ *and* $G = \langle g_1, \ldots, g_d, x\rangle$ *for all* $1 \ne x \in N$.

This result makes the case when N is abelian fast, and of complexity polynomial in n for subgroups of $\mathrm{Sym}(n)$.

The nonabelian case is more difficult but, by the following result of Lucchini [3], $d(G)$ is again equal either to $d(G/N)$ or to $d(G/N) + 1$.

Proposition 3. *If* N *is nonabelian, then either*

C1 *there exist* $n_1, \ldots, n_d \in N$ *with* $G = \langle g_1n_1, \ldots, g_dn_d\rangle$*; or*
C2 *there exist* $n_1, \ldots, n_d, n_{d+1} \in N$ *with* $G = \langle g_1n_1, \ldots, g_dn_d, n_{d+1}\rangle$.

The problem is to determine which of the two cases we are in, but assume for the moment that we know that.

In the deterministic version, we search systematically through all d-tuples or $(d + 1)$-tuples of elements of N until we find a generating set of G.

In our randomized version, we try randomly selected d- or $(d + 1)$-tuples of elements of N until we find a generating set of G. We can prove that the expected number of tuples that we need to test is polynomial in n.

We have been focusing on a single nonabelian chief factor of a group but, as the examples below indicate, it turns out that Case C1 occurs for a large proportion of the nonabelian chief factors of a group, so we proceed by assuming initially that we are in Case C1, but eventually give up and systematically try all d-tuples if we fail

to find a d-element generating set. The low proportion (logarithmically small) of Case C1 chief factors enables to establish expected polynomial-time performance for the whole group.

Here are some timings of our Magma implementation on a selection of examples.

Group	Degree	$d(G)$	Time
A_5^{19}	95	2	0.6
A_5^{20}	100	3	3
A_5^{100}	500	3	252
$L_3(2)^{57}$	399	2	75
$L_3(2)^{58}$	506	3	236
$3^{30} : 2$	90	31	0.51
$3^{50} : 2$	150	51	8
$((2_b^4)^5 : A_5) \times (L_3(2)^{58})$	456	3	259, 77
$(3^{10} : 2) \times (L_3(2)^{58})$	436	11	224, 34

The two timings given for the final two examples are for two different choices of chief series. The first and slower time is for Magma's default choice, which has abelian chief factors as low down in the series as possible. The second faster time is for a series with the nonabelian chief factors as low as possible. We wrote some Magma code that computes such a series, which is slightly slower than the default, but worthwhile in this context.

The reason for this is that the large number of generators that are necessary for G arise from the abelian chief factors, and it is preferable that these are found earlier in the computation (i.e. from the factors near the top of the series), because that results in Case C2 not occurring in the nonabelian chief factors at the bottom of the series.

References

[1] W. Gaschütz, Zu einem von B. H. Neumann und H. Neumann gestellten Problem, *Math. Nachr.* **14** (1955), 249–252.

[2] Derek F. Holt and Gareth Tracey, Minimal sized generating sets of permutation groups, arXiv:404.03952.

[3] A. Lucchini, Generators and minimal normal subgroups, *Arch. Math. (Basel)* **64** (1995), no. 4, 273–276.

[4] A. Lucchini and F. Menegazzo, Computing a set of generators of minimal cardinality in a solvable group, *J. Symbolic Comput.* **17** (1994), no. 5, 409–420.

[5] Andrea Lucchini and Dhara Thakkar, The Minimum Generating Set Problem, *J. Algebra* **640** (2024) 117–128.

Finding G-submodules

Charles Leedham-Green
(joint work with Eamonn O'Brien, with help from Derek Holt)

This work is a contribution to the matrix group recognition program [1], which was started over 30 years ago, and has now given us the same kind of functionality for matrix groups over finite fields that we have for permutation groups. We can, in general, compute with reasonable facility, with matrices of degree up to about 250 over fields of that may be rather large. This work has been the central focus of some of the Oberwolfach workshops in computational group theory, and is well represented at the present meeting. Some of the ongoing work is aimed at improving existing algorithms to enable us to work in bigger matrix groups, but the present paper has a different aim. There are some general problems that arise in computation in finite groups, be they permutation or matrix groups, that are intrinsically hard. That is to say, we see no hope of a polynomial time algorithm, and our ambition is limited to relatively small examples. Two such problems are the intersection problem - given generating sets for subgroup G and H of a universal group U find a generating set for $G \cap H$ - and the normaliser problem - given generating sets for subgroups G and H of U, with $G > H$, find a generating set for $N_G(H)$. Our primary motive with the present paper is with advancing the intersection problem.

It is essential when working on the intersection problem to concentrate on the geometry, and to avoid black box algorithms as far as possible. As a result the algorithm we are developing will be very complex, and we have first to deal with many special cases. One such case, which is already solved, reduces to the following problem. Given a set $\mathcal{S}$ of subspaces of the finite dimensional space V over some finite field, find a generating set for the subgroup G of $\mathrm{GL}(V)$ that preserves all the subspaces in $\mathcal{S}$ [2]. It then seems desirable to solve the following problem. Given a generating set for a subgroup G of $\mathrm{GL}(V)$, find the set of G-submodules of V. However, consideration of the case when G is the trivial group already suggests that this is the wrong problem. Rather we seek to find a set $\mathcal{S}$ of G-submodules of V that is dense in the set of all G-submodules of V, in the sense that the subgroup of $\mathrm{GL}(V)$ consisting of those elements that fix every element of $\mathcal{S}$ fixes every G-submodule of V. Such a set $\mathcal{S}$ is sufficient for our needs, and may be taken to have cardinality at most $\log_2 |G|$, whereas the number of G-submodules of V need not be polynomially bounded.

If V is semi-simple, not withstanding the case when $G = \langle 1 \rangle$, there is a simple solution to the problem. The number of subspaces required is at most twice the composition length of V.

If V has Loewy length 2, so that the Jacobson radical $\mathrm{J}(V)$ of V is semi-simple, matters are not so easy. One reduces at once to the case when $V/\mathrm{J}(V)$ and $\mathrm{J}(V)$ are homogeneous. So let A and B be irreducible G-modules, and suppose that $V/\mathrm{J}(V)$ is $\sum_{i=1}^{m} A_i$ and that $\mathrm{J}(V)$ is $\sum_{j=1}^{n} B_j$, and that G-module isomorphisms from A to each A_i and from B to each B_j are given. It is now easy to see that required set $\mathcal{S}$

of G submodules may be constructed as the union of three sets. One set consists of subspaces that contain $\mathrm{J}(V)$, one of subspaces that are contained in $\mathrm{J}(V)$, and the third consisting of subspaces X satisfying the two conditions $(X+\mathrm{J}(V))/\mathrm{J}(V) \cong A$ and $\mathrm{J}(V)/(X \cap \mathrm{J}(V)) \cong B$. Sets of the first two kinds are constructed as in the semi-simple case. There are exponentially many subspaces of type three, and a polynomially bounded set of such subspaces must be selected. This reduces to finding suitable elements of $\mathrm{Ext}^1_G(A, B)$. The details depend on whether A and B are absolutely irreducible, and on whether A is isomorphic to B. Finding these elements reduces to solving certain simultaneous quadratic equations over $\mathrm{GF}(p)$, where p is the characteristic of the underlying field, in two sets of unknowns, the equations being linear in either set separately.

We see no prospect of finding a reasonable algorithm for bad cases when V has Loewy length 3. The critical case is when each of $V/\mathrm{J}(V)$ and $\mathrm{J}(V)/\mathrm{J}^2(V)$ and $\mathrm{J}^2(V)$ are all reducible and homogeneous. However the modest expectation of our ability to compute intersections suggests that this will not give rise to a bottle-neck.

References

[1] Henrik Bäärnhielm, Derek F. Holt, C.R. Leedham-Green, and Eamonn O'Brien. *A practical model for computation with matrix groups*, J. Symbolic Comput. **68**, 27–60, 2015.

[2] Ruth Schwingel. *Two Matrix Group Algorithms with Applications to Computing the Automorphism Group of a Finite p-Group*. Ph.D. Queen Mary University of London 2000.

Summary of the Problem Session

A problem session was held on 5 June, 2025. The following problems were presented.

Melissa Lee.

Problem 1. Let p be a prime such that $p-2$ is also prime. Does there exist a faithful irreducible representation of A_p over a field in any characteristic $r > 0$ such that all elements of orders p and $p-2$ act fixed-point-freely? It is easy to show this is not the case if $r > p$.

Problem 2. Prove that if $G \leq \mathrm{Sym}(\Omega)$ has exactly two orbits of size $\frac{1}{2}|\Omega| > 1$, then G has a derangement (i.e., a fixed-point-free element). This was first conjectured by Ellis and Harper [1], who prove it when G is simple, nilpotent, has order at most 1000, or acts primitively on an orbit, or if $\frac{1}{2}|\Omega|$ is a prime power. Lee, Popiel and Verret [2] have also verified the conjecture for $|\Omega| \leq 60$ and $\frac{1}{2}|\Omega|$ a product of distinct primes.

References

[1] D. Ellis and S. Harper, *Orbits of permutation groups with no derangements*, arXiv:2408.16064 [math.GR], 2024. Available at `https://arxiv.org/abs/2408.16064`.

[2] M. Lee, T. Popiel and G. Verret, *Derangements in permutation groups with two orbits*, arXiv:2506.11396 [math.GR], 2025. Available at `https://arxiv.org/abs/2506.11396`.

Mima Stanojkovski.
Let p be an odd prime number and let ω be a primitive element of $\mathbb{F}_p$. For the following two groups assume the additional constraints that the exponent is p and the nilpotency class is 2:

$$G_1 = \langle a, b, c, d, e \mid [c, b], [d, b], [e, c], [e, d], [d, c] = [b, a], [e, b] = [c, a], [e, a] = [d, a]^\omega \rangle,$$
$$G_2 = \langle a, b, c, d, e \mid [d, a], [e, a], [c, b], [d, b], [e, c], [d, c] = [b, a], [e, b] = [c, a] \rangle.$$

In [3] these groups are labeled 8.5.14 and 8.5.15, respectively, and their automorphism group sizes are computed and shown to be different. Is there a "simpler invariant" for non-isomorphism testing of these groups? The Magma [1] code for G_1 and G_2 is available at [2].

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[2] E. A. O'Brien and M. Stanojkovski. Geometric invariants for finite p-groups. `https://github.com/eamonnaobrien/Invariants-class2-pgroups`.

[3] M. Vaughan-Lee. The automorphisms of class two groups of prime exponent, 2015. `https://arxiv.org/abs/1501.00678`.

Stephen Glasby.
Let n be a positive integer, and suppose that $k \in \{1, 2, \ldots, n\}$ where $n/\gcd(n, k)$ is odd. Let $\mathbb{F}_{2^n}$ denote the finite field of order 2^n, and $\mathbb{F}_{2^n}^\times = \mathbb{F}_{2^n} \setminus \{0\}$ its multiplicative group. If $x, y \in \mathbb{F}_{2^n}^\times$ satisfy $(y + x)(y^{2^k} + x^{-4^k}) = 1$, then is it true that $y = z^{-1} + z^{2^k}$ for some $z \in \mathbb{F}_{2^n}^\times$?

Joshua Maglione.
We write $G_{E,P}$ for the unipotent group scheme arising from an elliptic curve E and a point P on the curve; see the author's abstract and [2, Sec. 1.5].

$$\mathcal{G}_q = \left\{ G_{E,P}(\mathbb{F}_q) \;\middle|\; \begin{array}{c} a, b \in \mathbb{F}_q,\ E : y^2 = x^3 + ax + b, \\ P \in E(\mathbb{F}_q) \end{array} \right\}.$$

Let $N_q = |\mathcal{G}_q/\cong|$ which counts the number of isomorphism classes of the groups arising from the above construction.

Conjecture 1 ([2, Conj. 6.9])**.** *For all primes $p \geqslant 5$, we have*

$$N_p = p^2 + p - \gcd(p - 2, 3) + \gcd(p - 1, 4).$$

Conjecture 1 has been verified for primes up to 100. It would be of further interest to know which pairs (E, P) yield an *immediate descendant*, namely, for which pairs (E, P) does there exist the following central extension

$$1 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow G \longrightarrow G_{E,P}(\mathbb{F}_p) \longrightarrow 1?$$

Here, G is a group with nilpotency class 3 and cardinality p^{10}. In [1], du Sautoy and Vaughan-Lee show that $G_{E,P}(\mathbb{F}_p)$, for E given by $y^2 = x^3 - x$ and $P = (0, 0)$, has a non-PORC[1] number of immediate descendants. It would be remarkable if the sum of *all* the numbers of immediate descendants of all groups in $\mathcal{G}_p$, up to isomorphism, yielded a PORC function.

References

[1] M. du Sautoy, M. Vaughan-Lee, *Non-PORC behaviour of a class of descendant p-groups*, J. of Algebra, **361** (2012), 287–312.

[2] J. Maglione, M. Stanojkovski, *Smooth cuboids in group theory*, Algebra Number Theory, **19** (2025), No. 5, 967–1006.

Bettina Eick.
Let $A, B \in GL(n, \mathbb{Z})$. Is it decidable if $\langle A, B\rangle$ is free on $\{A, B\}$? If yes, then devise an algorithm for this purpose. Some notes:

- Successively listing words in the generators will eventually determine a relation in the generators if there exists one. This approach will not terminate if the group is free.
- It is not known if this problem is decidable and there is a strong suspicion that it may be undecidable in general. It would still be of interest to consider this problem in special cases.
- Of course, this question would also be of interest for rings and fields other than $\mathbb{Z}$.

Tommy Hofmann.
For $n \geq 3$, there exists a polynomial time algorithm that given q and n determines a presentation of $\mathrm{SL}_n(\mathbf{F}_q)$. This follows from a simplified version of the Steinberg presentation due to Chiaselotti.

Question: Does there exists a polynomial time algorithm, that given q finds a presentation of $\mathrm{SL}_2(\mathbf{F}_q)$?

Note that complexity condition implies that (i) the bit-length of these presentations must be polynomial in $\log(q)$; (ii) the generating set of such a presentation is not allowed to contain elements of the form $\left(\begin{smallmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{smallmatrix}\right)$, where $\langle \omega \rangle = \mathbf{F}_q^\times$. Condition (i) excludes the standard Steinberg presentation and condition (ii) excludes presentations on "standard generators" by O'Brien–Leedham-Green.

[1] A function f from the set of primes to the integers is PORC if there exists an integer N and polynomials $g_0, g_1, \ldots, g_{N-1}$ such that $f(p) = g_k(p)$ where $p \equiv k \pmod N$.

Klaus Lux.
Find a finite group G of minimal order, which is the nonsplit extension of a group Q by a group N with all composition factors of Q and N being nonabelian. See also the discussion in [1].

References

[1] D. Madore, *Examples of extensions of non-solvable groups by one another*, MathOverflow, `https://mathoverflow.net/q/301784`, June 2, 2018.

Leo Margolis.
We say that a finite group G has the *nilpotent decomposition* property, if for every nilpotent element $n \in \mathbb{Z}G$ in the integral group ring of G and every primitive central idempotent $e \in \mathbb{Q}G$ in the rational group algebra of G the product ne lies in $\mathbb{Z}G$. We ask, if this property holds for groups of shape $C_p \rtimes C_{q^k}$ where p and q are primes, k a natural number and the action of C_{q^k} is not faithful. In particular, a group of interest is given by $C_{17} \rtimes C_8$ with the action by inversion. We refer to [1] for the motivation of the problem and background.

References

[1] G. Jansens, L. Margolis *On integral decomposition of unipotent elements in integral group rings*, Mathematical Proceedings of the Cambridge Philosophical Society (to appear) (2025).

Reporter: Saul D. Freedman

Participants

Prof. Dr. Laurent Bartholdi
Dept. de Mathématiques
Université Claude Bernard Lyon I
43, Bd. du 11 Novembre 1918
69622 Villeurbanne Cedex
FRANCE

Dr. Thomas Breuer
Lehrstuhl für Algebra und Zahlentheorie
RWTH Aachen University
52062 Aachen
GERMANY

Prof. Dr. Peter A. Brooksbank
Department of Mathematics
Bucknell University
1 Dent Drive
17837 Lewisburg, PA 17837
UNITED STATES

Prof. Dr. Pierre-Emmanuel Caprace
Institut de Recherche en Mathématiques et Physique (IRMP)
Université Catholique de Louvain
Chemin du Cyclotron, 2
P.O. Box L7.01.02
1348 Louvain-la-Neuve
BELGIUM

Dr. Willem A. de Graaf
Dipartimento di Matematica
Università di Trento
Via Sommarive 14
38123 Povo (Trento)
ITALY

Dr. Alla Detinko
School of Computing & Mathematics
The University of Huddersfield
Queensgate
Huddersfield HD1 3DH
UNITED KINGDOM

Prof. Dr. Heiko Dietrich
School of Mathematics
Monash University
Clayton Victoria, 3800
AUSTRALIA

Dr. Daniele Dona
HUN-REN Alfréd Rényi Institute of Mathematics
Reáltanoda utca 13-15
1053 Budapest
HUNGARY

Dr. Sean Eberhard
Mathematics Institute
Zeeman Building
University of Warwick
Coventry CV4 7AL
UNITED KINGDOM

Prof. Dr. Bettina Eick
Institut für Analysis und Algebra
Fachbereich Mathematik, Fakultät 1
Technische Universität Braunschweig
Universitätsplatz 2
38106 Braunschweig
GERMANY

Oscar Fernandez Ayala
Institut für Analysis und Algebra
Fachbereich Mathematik, Fakultät 1
Technische Universität Braunschweig
Universitätsplatz 2
38106 Braunschweig
GERMANY

Prof. Dr. Claus Fieker
Fachbereich Mathematik
RPTU Kaiserslautern Landau
Postfach 3049
67653 Kaiserslautern
GERMANY

Prof. Dr. Dane Flannery
School of Mathematical and Statistical Sciences
University of Galway, Ireland
University Road
Galway H91 TK33
IRELAND

Dr. Saul Freedman
Department of Mathematics
Colorado State University
Weber Building
Fort Collins, CO 80523-1874
UNITED STATES

Prof. Dr. Stephen P. Glasby
Dept. of Mathematics and Statistics
University of Western Australia
26 Cintra Road, Waratah
2298 Newcastle, WA 6009
AUSTRALIA

Jun.-Prof. Dr. Tommy Hofmann
Department Mathematik
Universität Siegen
57068 Siegen
GERMANY

Prof. Dr. Derek F. Holt
Mathematics Institute
University of Warwick
Gibbet Hill Road
Coventry CV4 7AL
UNITED KINGDOM

Prof. Dr. Max Horn
Department of Mathematics
University of Kaiserslautern-Landau
Gottlieb-Daimler-Straße Building 48
67633 Kaiserslautern
GERMANY

Linda Hoyer
Institut für Mathematik
RWTH Aachen
Templergraben 55
52062 Aachen
GERMANY

Prof. Dr. Alexander Hulpke
Department of Mathematics
Colorado State University
1874 Campus Delivery
Fort Collins, CO 80523-1874
UNITED STATES

Dr. Chris Jefferson
School of Science and EngineeringUniversity of Dundee
23 Perth Road
Dundee DD1 4HN
UNITED KINGDOM

Dr. Mikko Korhonen
Shenzhen International Center for Mathematics
Southern University of Science and Technology
1088 Xueyuan Road
Shenzhen, Guangdong Province 518 055
CHINA

Dr. Melissa Lee
School of Mathematics
Monash University
9 Rainforest Walk
Clayton Victoria, 3800
AUSTRALIA

Prof. Dr. Charles R. Leedham-Green
School of Mathematical Sciences
Queen Mary University of London
Mile End Road
London E1 4NS
UNITED KINGDOM

Prof. Dr. Steve Linton
School of Computer Science
University of St. Andrews
Jack Cole Building
North Haugh
St. Andrews, Fife KY16 9SX
UNITED KINGDOM

Dr. Alastair James Litterick
School of Mathematics, Statistics and Actuarial Science,
University of Essex
Wivenhoe Park
Colchester CO4 3SQ
UNITED KINGDOM

Chris Liu
Department of Mathematics
Colorado State University
Fort Collins, CO 80523-1874
UNITED STATES

Dr. Frank Lübeck
Lehrstuhl für Algebra und Zahlentheorie
RWTH Aachen
Pontdriesch 14/16
52062 Aachen
GERMANY

Prof. Dr. Klaus Lux
Department of Mathematics
University of Arizona
617 N. Santa Rita
Tucson AZ 85721-0089
UNITED STATES

Dr. Joshua Maglione
University of Galway
School of Mathematical and Statistical Science
University Road
Galway H91 TK33
IRELAND

Prof. Dr. Gunter Malle
Fachbereich Mathematik
Technische Universität Kaiserslautern
Postfach 3049
67653 Kaiserslautern
GERMANY

Dr. Leo Margolis
Universidad Autonoma de Madrid
and
ICMAT (Instituto de Ciencias Matematicas)
Campus de Cantoblanco, UAM
28049 Madrid
SPAIN

Prof. Dr. Gabriele Nebe
Lehrstuhl für Algebra und Zahlentheorie
RWTH Aachen
Pontdriesch 14/16
52062 Aachen
GERMANY

Prof. Dr. Alice Niemeyer
Lehrstuhl für Algebra und Darstellungstheorie
RWTH Aachen
Pontdriesch 10-16
52062 Aachen
GERMANY

Prof. Dr. Eamonn A. O'Brien
Department of Mathematics
The University of Auckland
Private Bag 92019
1132 Auckland
NEW ZEALAND

Eileen Xueyu Pan
Mathematics Institute
University of Warwick
School of Mathematics
Monash University
Gibbet Hill Road
Coventry CV4 7AL
UNITED KINGDOM

Prof. em. Dr. Cheryl E. Praeger
School of Physics, Mathematics and ComputingThe University of Western Australia
35 Stirling Highway
Crawley WA 6009
AUSTRALIA

Dr. Youming Qiao
University of Technology Sydney
School of Computer Science
15 Broadway
Sydney 2007
AUSTRALIA

Prof. Dr. Colva Roney-Dougal
School of Mathematics and Statistics
University of St Andrews
North Haugh
St. Andrews Fife KY16 9SS
UNITED KINGDOM

Dr. Tobias Rossmann
School of Mathematical and Statistical Sciences
University of Galway
Galway
University Road
Galway H91 TK33
IRELAND

Marie Roth
Fachbereich Mathematik
T.U. Kaiserslautern
Postfach 3049
67618 Kaiserslautern
GERMANY

Prof. Dr. Pascal Schweitzer
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt
GERMANY

Dr. Mima Stanojkovski
Dipartimento di Matematica
Università di Trento
Via Sommarive 14
38123 Povo (Trento)
ITALY

Prof. Dr. Christopher Voll
Fakultät für Mathematik
Universität Bielefeld
Postfach 10 01 31
33501 Bielefeld
GERMANY

Prof. Dr. Rebecca Waldecker
Institut für Mathematik
Martin-Luther-Universität Halle-Wittenberg
Theodor-Lieser-Straße 5
06120 Halle / Saale
GERMANY

Prof. Dr. James B. Wilson
Department of Mathematics
Colorado State University
Weber Building
Fort Collins, CO 80523-1874
UNITED STATES

Peiran Wu
University of St. Andrews
Mathematical Institute
North Haugh
St. Andrews KY16 9SS
UNITED KINGDOM