Mathematisches Forschungsinstitut Oberwolfach

Report No. 38/2021

DOI: 10.4171/OWR/2021/38

Computational Group Theory (hybrid meeting)

Organized by
Bettina Eick, Braunschweig
Derek Holt, Warwick
Gabriele Nebe, Aachen
Eamonn O'Brien, Auckland

15 August – 21 August 2021

Abstract. This was the eighth Oberwolfach Workshop on Computational Group Theory. It demonstrated how an increasing number and variety of deep theoretical results are being used to devise powerful and practical algorithms in Computational Group Theory. The talks also presented connections with and applications to Number Theory, Combinatorics, Geometry, and Geometric Group Theory.

Mathematics Subject Classification (2010): 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 eighth with this title held at Oberwolfach. It had 55 participants, 26 of whom were able to attend in person. The remaining 29 virtual participants were in different time zones. We scheduled the talks in the usual Oberwolfach style, in the morning between 9.30 and 12.30 and in the afternoon between 16.00 and 18.30. To enable discussions by all participants, including those who missed some of the talks due to time-zone related issues, we organised some additional review sessions: Zoom questions and discussions in the lecture hall; software presentations; and individual meetings using the video conference tool "GatherTown". While these additional efforts did not equal the benefits of all participants meeting in person, they did create a workshop atmosphere that engaged the virtual participants.

The program consisted of four 50-minute survey talks, eighteen 20-minute research talks, and some 5-minute short talks. The latter included talks by the five Oberwolfach Leibniz Graduate Students, and so allowed these young researchers to present their research to an international audience.

The four survey talks were invited by the organisers. The first was by Gunter Malle on *Some open problems in finite group representation theory.* He gave an overview of various famous problems and their conjectured solutions, with particular emphasis on problems where Gerhard Hiss, who retired in July 2021, has made important contributions. Many of the problems discussed can be approached by computational means, and their proofs reduce to verification for finite (nearly) simple groups of Lie type. The second survey was by Claus Fieker and Tommy Hofmann on *What can computational group theory do for number theory?* They gave an overview of the state of the art of the number theory part of the OSCAR open source computer algebra repository, with a view towards group theoretical challenges, for instance in the computation of Galois groups of number fields. The third survey was by Tobias Rossmann on *Towards a symbolic enumeration of orbits.* Its focus was symbolically counting parameterised orbit lengths for an important family of finite p-groups. He showed how this topic connects to other areas of mathematics including algebra, combinatorics and geometry. The final survey was by Rebecca Waldecker on *Refine, Rip, Repeat – Search in permutation groups.* She outlined the important work by Jeff Leon on backtracking using partitions, and reported on recent improvements by her and colleagues aimed at computing rapidly intersections of subgroups and stabilisers of subsets in permutation groups.

The 18 contributed research talks, each 20 minutes long, covered a broad range of topics. They illustrated how the existing techniques of Computational Group Theory can be applied in various mathematical areas, and also how powerful algorithms can be developed by applying deep theoretical results.

One prominent theme among these talks was the isomorphism problem for groups and graphs, and related classification problems. László Babai identified an obstacle to improving on his outstanding result giving a quasi-polynomial bound for the cost of graph isomorphism. Other related talks were given by Heiko Dietrich, Joshua Maglione and Pascal Schweitzer covering practical and theoretical aspects of this topic, and by the young researchers Tobias Moede and Eileen Pan reporting on their classification of various classes of groups of "small" order.

Algorithmic problems in combinatorial and geometric group theory also featured prominently. Martin Bridson presented various computational challenges involving subdirect products of finitely presented groups. Michael Vaughan-Lee reported on his construction by machine of p-groups which are the first known counterexamples of odd order to a long-standing conjecture attributed to Schur that the exponent of the Schur multiplier of a finite group divides its exponent. Other related talks were given by Matthew Conder, Laura Ciobanu, Murray Elder, Alexander Hulpke, Alan Reid, and Katrin Tent covering both new algorithms and theoretical challenges and new results in the area.

The development of high-quality algorithms for permutation groups is one of the long-standing research topics in Computational Group Theory. Young researcher Mun See Chang reported on progress in addressing one of the significant challenges: constructing the normaliser of a subgroup of a permutation group. Colva Roney-Dougal presented important new results on base size and complexity. Other related talks were given by Leonard Soicher and young researchers Dominik Bernhardt and Melissa Lee.

The development of algorithms for linear groups and the associated representation theory is currently one of the most active areas of computational group theory. Emmanuel Breuillard discussed new approaches towards a quantitative form of the Tits alternative and ideas towards the determination of explicit generators of a free subgroup in a linear group. Markus Lohrey presented an algorithm to decide in polynomial time the subgroup membership problem for $\mathrm{GL}(2,\mathbb{Z})$ when certain encodings of its elements are used. Other related talks were given by Alla Detinko, Willem de Graaf, Gerhard Hiss, and Derek Holt (the last presenting on behalf of John Cannon).

The conference also illustrated well the knowledge transfer between different mathematical disciplines. In his talk, Ulrich Thiel presented a question motivated by applications in algebraic geometry; some of the computational group theory experts readily answered it using GAP. Christopher Voll used Hessian matrices and the number of torsion points on elliptic curves to explain puzzling observations about the orders of automorphism groups of a much studied family of finite p-groups.

The two scheduled sessions of 5-minute talks both allowed the young researchers to present their work and gave more experienced researchers the opportunity to draw attention to important new results. Frank Lübeck presented his alternative to Conway polynomials, so allowing consistent computations in significantly larger fields than previously. John Cannon announced a fast algorithm, available in MAGMA, to construct all absolutely irreducible modules for "moderately large" finite groups in characteristic 0.

The talks, reviews, software and problem sessions were well received by the participants. Our schedule left plenty of time for discussions. This was used by many participants to initiate new projects, develop new research ideas and discuss new collaborations. The interactions and exchanges of ideas were a major highlight of the workshop and will no doubt lead to new and interesting projects in computational group theory.

Acknowledgement: The MFO and the workshop organizers would like to thank the Simons Foundation for supporting James B. Wilson in the "Simons Visiting Professors" program at the MFO.

Workshop (hybrid meeting): Computational Group Theory

Table of Contents

Abstracts

Some open problems in the representation theory of finite groups

Gunter Malle

In our talk we gave an overview on some open problems in the representation theory of finite groups, and more concretely, the representation theory of finite quasi-simple groups, with an emphasis on exceptional groups of Lie type. We started out with Alperin's conjecture that the number of p'-classes of a finite group G is always at least as large as that of the normaliser of a Sylow p-subgroup of G. This has recently been proved by Navarro–Tiep in the case $p = 2$ by reformulating it into the corresponding question on the number of irreducible Brauer characters. We then stated Alperin's weight conjecture and reported on recent progress by An–Hiss–Lübeck for groups of type F_4. An important open problem here is the determination of the radical subgroups of exceptional groups of Lie type in bad characteristic. We shortly talked about the problem of completing the determination of the p-blocks of these groups.

We went on to discuss various questions about p-modular decomposition matrices for finite groups of Lie type, ranging from the existence of basic sets, over uni-triangularity and up to the question of a complete determination, at least for the series of exceptional groups. We defined the modular Harish-Chandra series of finite groups with a split BN-pair and reported on the still open problem of their complete determination for groups of Lie type.

The final problem we mentioned is the proof of gap results for the smallest dimensions of non-trivial irreducible representations of the finite simple groups; here the main open case concerns the various series of orthogonal groups, either in small defining characteristic or for small characteristic of the representation.

Generalizing Polycyclic Presentations

Alexander Hulpke
(joint work with Heiko Dietrich)

Polycyclic presentations (PC presentations) and the associated PCGroups are one of the success stories of Computational Group Theory. This is because they not only provide arithmetic for finite solvable groups, but tools – extensions and quotient algorithms –that naturally produce groups in such a representation.

For a generalization to be successful, it similarly needs to provide such constructions, since it otherwise often is easiest to remain in the initial representation a group was given.

We generalize PC presentations through confluent rewriting system, combining extensions with a wreath product ordering. That is, if $G = N.Q$ and we have confluent rewriting systems for N and Q, we take the union of the generating sets and ensure the following:

- Keep the rules for N.
- For each generator pair n, q add a rule $nq \to q \cdot n^q$ that reflects the action of Q-representatives on N.
- Modify Q-rules $l \to r$ by an N-"tail": $l \to r \cdot n$ that describe the cofactors of the extension structure.

In the practical implementation, we take the solvable radical, represented as a PCGroup in place of N. We call such a group a "hybrid group".

This approach yields a natural way to calculate 2-cohomology and extensions: Given a group Q and a Q-module N (the module structure describes the action rules), consider the tail values as variables, the confluence condition of overlaps then yields linear equations in these variables, whose solutions describe the 2-cocycles, each solution corresponds to the associated extension as hybrid group.

Our first application is a generalization of the p-Quotient algorithm to arbitrary finite groups. Given a homomorphism $\varphi\colon F \to H$ from a finitely presented group (of rank k) onto a finite group, we choose an irreducible $\mathbb{F}_pH$-module M. Building on work of Gaschütz [4], we define a universal cover $C = \mathcal{M}_k.H$ so that *every* k-generator extension $N.H$, with N an M-homogeneous module, must be a quotient of C. As in the p-quotient algorithm, the maximal lift of φ to a larger quotient of F then is obtained by evaluating relators for F in this cover.

The second application is an enumeration of perfect groups of orders up to $2 \cdot 10^6$ [6], extending, over 30 years later, the list of [5]. This calculation follows the method used for constructing solvable groups [1]. The required isomorphism tests become feasible due to improvements of the implementation of [2] in GAP.

The author's work has been supported in part by the National Science Foundation (DMS-1720146 to A. Hulpke), 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(5):623–644, 2002.
[2] John Cannon and Derek Holt. Automorphism group computation and isomorphism testing in finite groups. *J. Symbolic Comput.*, 35(3):241–267, 2003.
[3] H. Dietrich and A. Hulpke. Universal covers of finite groups. J. Algebra **569** (2021), 681–712.
[4] W. Gaschütz. Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden. Math. Zeitschr. **60** (1954) 274–286.
[5] Derek F. Holt and W. Plesken. *Perfect groups*. Oxford University Press, 1989.
[6] A. Hulpke. The perfect groups of order up to two million Math.Comp., accepted.

Some comments on group isomorphism

Heiko Dietrich
(joint work with James Wilson)

In this talk we present some new results related to isomorphism testing of groups; this abstract focuses on the first topic (Cayley table model), and only briefly states the main results of the other three topics.

1. Cayley table model (with James Wilson, Colorado State University)

Let n be a positive integer. We consider an $n \times n$ table with entries in $\{1, \ldots, n\}$ as the multiplication table of a binary product where the rows and columns are both labelled by $1, 2, \ldots, n$. For a group multiplication we require that the identity element is denoted "1", that is, the first row and first column must both be $1, 2, \ldots, n$; if this is not the case, then we reject the input. For a subset $\mathcal{S}$ of positive integers we are interested in the decision problem $\mathcal{S}$-GroupIso which takes as input a pair of $n \times n$ tables ($n \in \mathcal{S}$) with entries in $\{1, \ldots, n\}$ and decides whether these tables define binary operations of isomorphic groups of order $n \in \mathcal{S}$.

Booth [11, p. 132] observed that the complexity of $\mathbb{N}$-GroupIso is polynomial-time equivalent to the complexity of graph isomorphism. At the time, that complexity was subexponential, but it has since been shown by Babai [1] to be in quasi-polynomial time with a highly inventive algorithm. Meanwhile Miller [10, 11] credited Tarjan for observing that $\mathbb{N}$-GroupIso can be decided in quasi-polynomial time $n^{O(\log n)}$ through a brute-force algorithm. Surprisingly, this brute-force complexity has been resilient, and group isomorphism testing seems to be a leading bottleneck to improving the complexity of graph isomorphism, see Babai [1, Section 13.2]. Progress on group isomorphism has since then fragmented into work on numerous subclasses: For example, work of Kavitha [9] and Babai-Codenotti-Qiao [2] shows that the difficult instances are groups that admit nontrivial proper abelian normal subgroups; we refer to [5, Section 1] for more details and references. In [5], we have proved the following results, Theorems A, B, and C, showing that group isomorphism testing is "easy" for almost all group orders.

Theorem A. *There is a deterministic multi-tape Turing machine that decides in time $O(n^2(\log n)^d)$ for some constant d whether an $n \times n$ table with entries in $\{1, \ldots, n\}$ describes a group and, if so, returns an injective group homomorphism $\{1, \ldots, n\} \to \mathrm{Sym}_n$ into the group Sym_n of permutations on $\{1, \ldots, n\}$.*

We note that Rajagopalan-Schulman [12, Theorem 5.2] provide an $O(n^2 \log n)$ algorithm for this task, but they cost the binary operation as $O(1)$, which gives an upper bound of $O(n^4(\log n)^2)$ on a Turing machine model.

Theorem A allows us to prove the following; recall that $\mathcal{S} \subset \mathbb{N}$ is dense if $|\mathcal{S} \cap \{1, \ldots, n\}|/n \to 1$ for $n \to \infty$.

Theorem B. *There is a dense subset $\Upsilon \subset \mathbb{N}$ and a deterministic multi-tape Turing machine that decides Υ-GroupIso for $n \in \Upsilon$ in time $O(n^2(\log n)^c)$ for some constant c.*

We stress that Theorem B should not be misunderstood as saying that group isomorphism is efficient on most groups, just on most orders. Our set Υ excludes an important but difficult class of group orders, specifically orders that have a large power of a prime as a divisor. Theorem B therefore goes some way towards confirming the expectation that groups of prime power order are the essential bottleneck to group isomorphism testing.

For the sake of completeness, we provide a description of our set Υ. A prime $p \mid n$ is *isolated* if $k = 0$ for every prime power q^k with $q^k \mid n$ and $p \mid (q^k - 1)$. If, in

addition, $p \not| |T|$ for every non-abelian simple group T of order dividing n, then p is *strongly isolated*. We are now in the situation to give the formal definition of Υ; the proof is based on the Hardy-Ramanujan Theorem and results of Erdős-Pálfy [8].

Theorem C. *The set $\Upsilon \subseteq \mathbb{N}$ of all $n \in \mathbb{N}$ that factor as $n = ab$ and satisfying (1)–(4) is dense:*

(1) *if $p \mid a$ is a prime divisor, then $p \leq \log\log n$ and, if $p^e \mid a$, then $p^e \leq \log n$;*
(2) *if $p \mid b$ is a prime divisor, then $p > \log\log n$ and $p \mid n$ is isolated;*
(3) *the factor b is square-free;*
(4) *the factor b has at most $2\log\log n$ prime divisors.*

Importantly, we prove in [5, Theorem 2.5] that every group G of order $n \in \Upsilon$ has a unique Hall $\pi^{\mathrm{lsi}}(n)$-subgroup B, which is cyclic, and a complement of size $(\log n)^{O((\log\log n)^c)}$ for some c; here $\pi^{\mathrm{lsi}}(n)$ is the set of strongly isolated prime divisors of n that are larger than $\log\log n$. This decomposition is the backbone of our proof of Theorem B. Generalisations of Theorem B to other input models are considered in [7].

2. Cubefree groups (with James Wilson, Colorado State University)

In [6] we consider group isomorphism for groups of cubefree order in the permutation group input model: here groups of order n are given by a set of $O(\log n)$ generating permutations. Our proof of Theorem D relies on the known structure theory of groups of cubefree order; we refer to [6] for details and references.

Theorem D. *There is a polynomial time algorithm that given finite permutation groups G and H, decides whether they are cubefree, and if so, decides that $G \ncong H$, or determines an isomorphism $G \to H$.*

Our algorithm is implemented in GAP. Together with Theorem A, this yields a polynomial time isomorphism test for cubefree groups in the Cayley table input model.

3. C-groups (with Darren Low, Monash University)

Motivated by Theorem B we looked at the class of metacyclic groups, specifically, C-groups: these are groups whose Sylow subgroups are all cyclic. By the classification of Hölder-Burnside-Zassenhaus, every C-group is coprime metacyclic, that is, isomorphic to a semidirect product of coprime cyclic groups. In particular, every group of squarefree order is a C-group. Inspired by Slattery's work [13] on squarefree groups, we devolved practical algorithms for C-groups in [4]: we describe algorithms for CGroup-by-ID-Construction and ID-of-CGroup functionality. This provides a practical isomorphism test for C-groups because two C-groups are isomorphic if and only if they have the same "CGroup-ID". Our algorithms are implemented in GAP.

4. Groups of small order type (with Bettina Eick, TU Braunschweig, and Eileen Pan, Monash University)

In [3] we describe a new explicit determination of the groups of order n where n factors into at most four primes: we present tables with explicit group presentations, an enumeration formula, and we describe algorithms for Group-by-ID-Construction and ID-of-Group functionality. Our algorithms are implemented in GAP; the implementation also covers groups of order p^4q where p and q are distinct primes. For more details we refer to the abstract of Eileen Pan.

References

[1] L. Babai. Graph isomorphism in quasipolynomial time. https://arxiv.org/abs/1512.03547.

[2] L. Babai, P. Codenotti, Y. Qiao. Polynomial-time isomorphism test for groups with no abelian normal subgroups. LNCS - Automata, Languages, and Programming - Proceedings, ICALP, Springer, Warwick, UK, (2012) 51–62.

[3] H. Dietrich, B. Eick, X. Pan Groups whose orders factorise into at most 4 primes. J. Symb. Comp. 108 (2022) 23–40.

[4] H. Dietrich, D. Low. Generation of finite groups with cyclic Sylow subgroups. J. Group Theory 24 (2021) 161–175.

[5] H. Dietrich, J. B. Wilson. Group isomorphism is nearly-linear time for most orders. 62nd Annual IEEE Symposium on Foundations of Computer Science-FOCS 2021 (accepted).

[6] H. Dietrich, J. B. Wilson. Isomorphism testing of groups of cube-free order. J. Algebra 545 (2020) 174–197.

[7] H. Dietrich, J. B. Wilson. Glass-box Algebra: Algebraic computation with verifiable axioms. (in preparation)

[8] P. Erdős, P. Pálfy. On the orders of directly indecomposable groups. Discrete Math. 200 (1999) 165–179.

[9] T. Kavitha. Linear time algorithms for abelian group isomorphism and related problems. J. Comput. System Sci. 73 (2007) 986–996.

[10] G. L. Miller On the $n^{\log n}$ isomorphism technique: A preliminary report. In: Proceedings of the Tenth Annual ACM symposium on Theory of computing, pp. 51–58. ACM (1978).

[11] G. L. Miller. Graph isomorphism, general remarks. J. Comp. Sys. Sci. 18 (2) (1979) 128 - 142.

[12] S. Rajagopalan, L. J. Schulman. Verification of identities. SIAM J. Comput. 29 (2000) 1155-1163.

[13] M. C. Slattery. Generation of groups of square-free order. J. Symb. Comp. 42 (2007) 668–677.

Residual finiteness and computing with infinite linear groups

Alla Detinko

(joint work with Dane Flannery, Alexander Hulpke)

We report on recent progress in our continuing project aimed at practical computation with finitely generated linear groups [1]. Special consideration is given to methods and algorithms exploring the interplay between finitely generated linear groups and linear algebraic groups, as well as applications of our methodology to solution of problems via computer-aided experimentation.

1. Deciding Zariski density. We designed and implemented a number of deterministic and randomized algorithms testing (Zariski) density of a finitely generated linear group in an ambient algebraic group. This includes algorithms based on methods developed by I. Rivin. The practicality and efficiency of each algorithm varies depending on the input. Further details and experimental outcomes are available in [2].

2. Strong approximation algorithms. Finitely generated linear groups are residually finite, and approximated by linear groups of the same degree over finite fields. This property enables us to solve a number of fundamental algorithmic problems based on computing in congruence quotients. If, additionally, the strong approximation property occurs, then we can avail of our ability to compute the set $\mathcal{L}_{max}(H)$ of congruence quotients modulo all maximal ideals of the ground domain. Using different characterizations of maximal subgroups of $\mathrm{SL}(n,p)$, this problem was solved for finitely generated dense subgroups of $\mathrm{SL}(n,\mathbb{Q})$ [2, 3]. Similar results are available for finitely generated dense subgroups of $\mathrm{Sp}(n,\mathbb{Q})$. Particular consideration was given to the case of special linear groups of prime degree. Here, efficient techniques based on a step-by-step exclusion of each 'Aschbacher class' were obtained [4].

3. The congruence subgroup property and computing. In the class of groups which satisfy the congruence subgroup property, we developed algorithms to compute the set $\mathcal{L}(H)$ of all congruence quotients of a finitely generated dense group H. That enables us to efficiently construct the arithmetic closure $cl(H)$ (in other terms, the extended congruence subgroup) of H [2]. Additionally, $cl(H)$ provides a tool for solution of further computational problems [2, 4].

4. Applications and computer experimentation. Our algorithms have been implemented in GAP. Using this implementation, we performed a series of experiments with low dimensional representations of finitely presented groups which arose in topology, motivated by long-standing open problems in group theory [2, 3, 4].

Another application is at the interface between differential Galois theory and theoretical physics. We obtained new experimental results for symplectic monodromy groups of hypergeometric differential equations [5]. These are 2-generator dense subgroups of $\mathrm{Sp}(n,\mathbb{Q})$ containing a transvection. For all 916 symplectic hypergeometric monodromy groups in degree $n = 6$, we calculated the arithmetic closure and described related properties of the groups, thus demonstrating the efficiency of our algorithms.

References

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

[2] A. S. Detinko, D. L. Flannery, and A. Hulpke, *Zariski density and computing in arithmetic groups*, Math. Comp. **87** (2018), no. 310, 967–986.

[3] A. S. Detinko, D. L. Flannery, and A. Hulpke, *The strong approximation theorem and algorithms for computing with dense subgroups*, J. Algebra **529** (2019), 536–549.

[4] A. S. Detinko, D. L. Flannery, and A. Hulpke, *Algorithms for experimenting with Zariski dense subgroups*, Exp. Math. **29** (2020), no. 3, 296–305.
[5] A. S. Detinko, D. L. Flannery, A. Hulpke, *Experimenting with symplectic hypergeometric monodromy groups*, Exp. Math. (2020); DOI: 10.1080/10586458.2020.1780516.

Schur's exponent conjecture

Michael Vaughan-Lee

There is a longstanding conjecture attributed to I. Schur that if G is a finite group then the exponent of the Schur multiplier $M(G)$ divides the exponent of G. It is easy enough to show that the conjecture holds true for groups of exponent 2 and 3, but the conjecture was shown to fail for groups of exponent 4 as long ago as 1973. Bayes, Kautsky and Wamsley [1] give an example of a group G of order 2^{68} with exponent 4, where $M(G)$ has exponent 8. However the truth or otherwise of this conjecture has remained open up till now for groups of odd exponent, and in particular it has remained open for groups of exponent 5 and exponent 9.

In my paper [3] I give an example of a four generator group G of order 5^{4122} with exponent 5, where the Schur multiplier $M(G)$ has exponent 25, and an example of a four generator group A of order 3^{11983} and exponent 9, where the Schur multiplier $M(A)$ has exponent 27. Very likely the reason that similar examples have not been found up till now is that computing the Schur multipliers of groups of this size is right on the edge of what is possible with today's computers.

For a survey of the history of this problem see [2].

It is easy to compute the Schur multiplier of the largest finite two generator group of exponent 5, $R(2,5)$. It is elementary abelian of order 5^{31}. Analysis of the details of the calculation shows that any exponent 5 counterexample to Schur's conjecture must have class at least 9. The analysis also shows that if G is an exponent 5 counterexample to Schur's conjecture, and if we write $G = F/R$ where F is free, then there must be an element $r \in R \cap F'$ which is not a product of fifth powers and which is a product of at least two commutators. This led me to consider the following group

$$G = \langle a, b, c, d \,|\, [b,a] = [d,c],\ \text{exponent } 5,\ \text{class } 9 \rangle.$$

which has order 5^{4122} and Schur multiplier

$$M(G) = C_{25} \times C_5^{9170}.$$

I also found a similar example of exponent 9.

$$A = \langle a, b, c, d \,|\, a^3,\ b^3,\ c^3,\ d^3,\ [b,a] = [d,c],\ \text{exponent } 9,\ \text{class } 9 \rangle.$$

This group has order 3^{11983} and Schur multiplier

$$M(A) = C_{27} \times C_3^{25184}.$$

Clearly this basic construction can be "tweaked" in various ways. Let

$$H(q,c) = \langle a, b, c, d \,|\, [b,a] = [d,c],\ \text{exponent } q,\ \text{class } c \rangle.$$

Then the Schur multipliers of $H(8,5)$, $H(16,6)$, $H(32,7)$, $H(64,8)$ have exponents 16, 32, 64, 128 (respectively).

I conjecture that the Schur multiplier of $H(8,12)$ has exponent 32, and that the Schur multiplier of $H(7,13)$ has exponent 49. But these groups are too big for me to compute.

Finally, we make the following observation which shows that the exponent of the Schur multiplier of a finite group of prime power exponent q can be bounded in terms of the exponent of the Schur multiplier of $R(2,q)$. (For any positive integer d we let $R(d,q)$ be the largest finite d generator of exponent q.) If $M(R(2,q))$ has exponent e then $M(R(d,q))$ has exponent e for all $d \geq 2$, and if G is any finite group with exponent q then the exponent of $M(G)$ divides qe.

References

[1] A.J. Bayes, J. Kautsky, and J.W. Wamsley, *Computation in nilpotent groups (application)*, Proceedings of the second international conference on the theory of groups (Australian National Uuniversity, Canberra,1973), Springer, Berlin, 1974, pp. 82–89.

[2] V. Thomas, *On Schur's exponent conjecture and its relation to Noether's rationality problem*, `https://arxiv.org/abs/2007.03476`, 2020.

[3] Michael Vaughan-Lee, *Schur's exponent conjecture — counterexamples of exponent* 5 *and exponent* 9, Int. J. Group Theory **10** (2021), 167–173.

Global symmetry from local information: The core of the Coset Intersection problem

László Babai

The Coset Intersection problem takes two subcosets of the symmetric group and asks if their intersection is non-empty. It is polynomial-time equivalent to other problems of computational group theory (Luks 1980). We review the core idea, summarized in the title, of relatively recent progress on the *asymptotic worst-case complexity* of this problem.

Normalizers of matrix Lie algebras and applications to group isomorphism

Joshua Maglione

(joint work with Peter A. Brooksbank, James B. Wilson)

At the heart of testing isomorphism between groups and algebras is the problem of testing whether two bilinear maps, or more generally tensors, are the same under change of bases of their coordinates. This is known as the tensor isomorphism problem, and it generalizes equivalence of matrices by row and column operations. For example, if G_1 and G_2 are p-groups of class 2 and exponent p, then their commutator determines an alternating $\mathbb{F}_p$-bilinear map $G_i/Z(G_i) \times G_i/Z(G_i) \to G_i'$, and isomorphisms between G_1 and G_2 determine isomorphisms between their commutator tensors.

The strategy we employ to speed up isomorphism testing of groups is to exploit linear operators of tensors $t_i : U \times V \to W$ determined by the commutator. Each t_i factors through the tensor product $U \otimes V$, which uniquely determines a linear map $f_i : U \otimes V \to W$. A brute-force approach essentially exhausts $\mathrm{GL}(U) \times \mathrm{GL}(V)$, searching for an element mapping $\ker(f_1)$ to $\ker(f_2)$. Our approach builds off of work in [2], where the fundamental idea was to use the associative ring of adjoints of t_i, denoted by A_i, to construct the smaller dimensional vector space $U \otimes_{A_i} V$, yielding a polynomial-time isomorphism test for groups whose Lie algebras have genus 2.

We introduce an algorithm to aid in the testing of group isomorphism by reducing to the problem of constructing normalizers of matrix Lie algebras. We do this by constructing the derivation algebras and densor subspaces associated to the tensors. These play a similar role to A_i and $U \otimes_{A_i} V$ above. The main advantage to this approach is that all of the associative algebra operators of tensors, like A_i, embed into the derivation algebra [1], and the densor subspace is, moreover, the smallest generalized tensor product space [4]. Therefore, we view the derivation algebra and the densor subspace to be optimal for isomorphism testing. However, new challenges arise from the representation theory of Lie algebras, which opens further directions of research.

We prove that there exists a polynomial-time algorithm that, given fully nondegenerate K-tensors t_1 and t_2 with $K = 6K$, derivation algebras of Chevalley type, and 1-dimension densor subspaces, decides whether t_1 and t_2 are isomorphic [3]. While computing the normalizer of a matrix Lie algebra is at least as hard as graph isomorphism [5], we give a family of semisimple algebras for which we can construct their normalizers in polynomial time.

We believe the hypotheses of our theorem are not the best possible. Even going through the database of p-groups of order p^7, we find commutator tensors whose derivation algebras have nonabelian simple factors that are not Chevalley Lie algebras (e.g. Witt Lie algebras). These tensors, therefore, do not satisfy our hypotheses, but their densor subspace is 1-dimensional, so we would like to take advantage of such a small subspace. Can we efficiently construct normalizers of the non-Chevalley simple Lie algebras that arise as derivation algebras? Furthermore, what kinds of solvable Lie algebras arise in this context? If these can be sensibly described, can we efficiently construct their normalizers?

References

[1] Peter A. Brooksbank, Joshua Maglione, and James B. Wilson, *Exact sequences of inner automorphisms of tensors*, J. Algebra **545** (2020), 43–63.

[2] Peter A. Brooksbank, Joshua Maglione, and James B. Wilson, *A fast isomorphism test for groups whose Lie algebra has genus 2*, J. Algebra **473** (2017), 545–590.

[3] Peter A. Brooksbank, Joshua Maglione, and James B. Wilson, *Tensor Isomorphism by derivations and densors*, preprint (2020), `arXiv:2005.04046`.

[4] Uriya First, Joshua Maglione, and James B. Wilson, *A spectral theory for transverse tensor operators*, preprint (2020), `arXiv:1911.02518`.

[5] Joshua A. Grochow, *Symmetry and equivalence relations in classical and geometric complexity theory*, Ph.D. Thesis, University of Chicago, 2012.

Geometry and representation theory associated to symplectic reflection groups

Ulrich Thiel
(joint work with Gwyn Bellamy, Johannes Schmitt)

The goal of my talk was to raise awareness of the rich world around symplectic reflection groups and to give an impression of how (computational) group and representation theory can be used to make progress on a seemingly purely geometric question. For the latter I focused on joint work [2] with Bellamy and Schmitt.

Let V be a symplectic finite-dimensional complex vector space. A *symplectic reflection group* is a finite subgroup Γ of symplectic automorphisms of V which is generated by *symplectic reflections*, i.e. by elements $s \in \Gamma$ whose fixed space is of codimension 2 in V.

What does the class of symplectic reflection groups look like? Recall that an (ordinary) complex reflection group is a finite group W of automorphisms of a finite-dimensional complex vector space $\mathfrak{h}$ which is generated by its (ordinary) reflections, i.e. by elements whose fixed space is of codimension 1 in $\mathfrak{h}$. Such groups were classified up to conjugacy by Shephard and Todd [7], and each naturally defines a symplectic reflection group: the vector space $\mathfrak{h} \oplus \mathfrak{h}^*$ carries a natural symplectic form, and with the induced action on this space the group W becomes a symplectic reflection group. Such symplectic reflection groups are called *improper*.

The *proper* (i.e. not improper) ones were classified up to conjugacy by Cohen [5]. They are direct products of *symplectically indecomposable* groups, and these split into two classes: the *symplectically imprimitive* and the *symplectically primitive* ones; the latter class splits further into the groups which are imprimitive or primitive in the usual sense. The class of groups which are both symplectically primitive and complex primitive consists of just 13 groups—they can thus be considered as the *exceptional* ones in the classification—all other classes are infinite.

Note that the class of complex reflection groups contains the class of finite Coxeter groups (the real reflection groups), and thus the class of Weyl groups (the rational reflection groups). The idea behind the "spetses" program initiated by Broué, Malle, and Michel [4] is that it seems there are "fake" algebraic groups associated not just to Weyl groups but to complex reflection groups in general. Given that the class of symplectic reflection groups contains the class of complex reflection groups I find the following question intriguing: do some parts of the "spetses" program make it to the larger class of symplectic reflection groups? Surely not everything, maybe nothing—but maybe something!?

Whereas the invariant theory of complex reflection groups is well understood (the invariant ring is polynomial, the cardinality of a system of fundamental invariants and their degrees are known, etc.) this seems to be unexplored territory for symplectic reflection groups. Even for the improper ones I mostly do not know much about the invariant theory—I have collected some computational data in [9].

I think it would be very interesting and helpful to find algorithms tailored to this special setting to gather more data.

There are not just algebraic questions about the invariant ring $\mathbb{C}[V]^\Gamma$ but geometric ones as well. This comes from the fact that the invariant ring is the coordinate ring of the orbit space V/Γ, which naturally has the structure of an algebraic variety. If $\Gamma \neq 1$, the variety V/Γ always has singularities: it is a classical fact that if Γ is any finite group of linear automorphisms of a finite-dimensional complex vector space V then the quotient V/Γ is smooth (i.e. has no singularities) if and only if Γ is generated by (ordinary) reflections; and a symplectic reflection group contains no (ordinary) reflections since $\mathrm{Sp}(V) \subseteq \mathrm{SL}(V)$. Now, a natural thing to do is to find a *resolution* of V/Γ, i.e. a proper birational map $\pi\colon \tilde{X} \to V/\Gamma$ from a variety $\tilde{X}$ without singularities (the *birational* means that $\tilde{X}$ is "not too far" from V/Γ and the *proper* excludes "useless trivialities" like the inclusion of the smooth locus). A resolution always exists due to a classical theorem by Hironaka. But since V carries a symplectic form, it would be better to look for *symplectic* resolutions: there should be a symplectic form on $\widetilde{X}$ as well and π should be an isomorphism of symplectic varieties over the smooth locus of V/Γ. Such kind of resolutions were introduced by Beauville [1], but in this case they are the same as so-called *crepant* resolutions which algebraic geometers have been studying intensively in general—especially in light of the minimal model program.

The central problem that I mentioned in my talk is: classify all the symplectic reflection groups $\Gamma \subset \mathrm{Sp}(V)$ for which V/Γ admits a (projective) symplectic resolution. Combined research effort over the past 20 years shows that a symplectic resolution only rarely exists, see [2] for a complete overview including references. Before [2], the only remaining cases in the classification were the symplectically primitive but complex imprimitive groups (an infinite class), and 10 among the exceptional ones. In [2] we proved:

Theorem. If Γ is symplectically primitive but complex imprimitive then for all but possibly 39 cases the variety V/Γ does not admit a symplectic resolution.

We have thereby finally reduced the classification problem to *finitely* many open cases. The proof of this result—like many of the previous results by others—relies on the combination of the following facts:

(1) The existence of a symplectic resolution of V/Γ is equivalent to the existence of a *smooth* Poisson deformation of V/Γ.
(2) *All* Poisson deformations arise as the centers of certain deformations of the (non-commutative) skew-group ring $\mathbb{C}[V] \rtimes \Gamma$, namely the *symplectic reflection algebras* $H_{\mathbf{c}}(\Gamma)$ by Etingof and Ginzburg [6]. Here, $\mathbf{c}$ is a parameter from a complex vector space of dimension equal to the number of conjugacy classes of symplectic reflections in Γ.
(3) The Poisson deformation defined by the center of $H_{\mathbf{c}}(\Gamma)$ is smooth if and only if the dimension of all simple $H_{\mathbf{c}}(\Gamma)$-modules is equal to the order of Γ.

This gives us a representation-theoretic tool to attack our seemingly purely geometric problem: if for *any* parameter $\mathbf{c}$ there is a simple $H_{\mathbf{c}}(\Gamma)$-module of dimension $< |\Gamma|$, then V/Γ does *not* admit a symplectic resolution. In [2] we constructed such a module for Γ being symplectically primitive but complex imprimitive. The key idea is as follows. One can find an (ordinary) complex reflection group G_0 whose "doubling" is a subgroup of Γ. The group G_0 turns out to be an exceptional group of rank-2 different from the group G_4 in the Shephard–Todd classification, and for the associated symplectic reflection algebras $H_{\mathbf{c}}(G_0)$ one knew already that simple modules are of dimension $< |G_0|$. We then induced from $H_{\mathbf{c}}(G_0)$ to $H_{\mathbf{c}}(\Gamma)$ to obtain our module. However, some technical details need to be satisfied for our construction to work. By theoretical arguments we could show that this works for all but possibly 73 cases of Γ.

To make the step from 73 down to 39 one needs more precisely knowledge about the representation theory of $H_{\mathbf{c}}(G_0)$. This knowledge came from data that I computed using my software package Champ [8]. The basic idea behind these computations is that for (ordinary) complex reflection groups $W \subset \mathrm{GL}(\mathfrak{h})$ the decomposition $\mathfrak{h} \oplus \mathfrak{h}^*$ of the space for the associated symplectic reflection group gives rise to a triangular decomposition of $H_{\mathbf{c}}(W)$, which then leads to a theory of standard modules. With some computational techniques that I developed (a way to lift a submodule found by the MeatAxe in positive characteristic back to characteristic zero) I was able to decompose the standard modules for many exceptional W.

I currently have no idea how to get from 39 down to 0. More data about the simple modules of the symplectic reflection algebras for the exceptional complex reflection groups G_{11}, G_{17}, G_{18}, G_{19}, and G_{21} may help but I doubt that this is computationally accessible. Another possibility may be to try to computationally construct a module for $H_{\mathbf{c}}(\Gamma)$, and to this end it may be helpful to find central elements in $H_{\mathbf{c}}(\Gamma)$.

I finished my talk by mentioning that we were also able to prove non-existence of a symplectic resolution for one exceptional symplectic reflection group, namely the group S_2 in Cohen's notation. We did this by finding a maximal parabolic subgroup (i.e. the stabilizer of a vector) which was known to not admit a symplectic resolution—a neat trick that was previously used by others, e.g. [3], as well. I added that for the other exceptional groups (of rank > 4) we were not able to test this because we had problems dealing with them computationally. Shortly after my talk Alexander Hulpke and Eamonn O'Brien pointed out to me that one can actually handle them. This made us revisit the exceptional groups and we were eventually able to solve some further cases. The details will be published in an upcoming paper.

References

[1] A. Bauville. *Symplectic singularities*, Invent. Math. **139**(3) (2000), 541–549.
[2] G. Bellamy, J. Schmitt, and U. Thiel. *Towards the classification of symplectic linear quotient singularities admitting a symplectic resolution*, Math. Z. (2021), to appear.

[3] G. Bellamy and T. Shedler, *On the (non)existence of symplectic resolutions of linear quotients*, Math. Res. Lett. **23**(6) (2016), 1537–1564.
[4] M. Broué, G. Malle, J. Michel. *Towards spetses. I*, Transform. Groups **4**(2–3) (1999), 157–218.
[5] A.M. Cohen. *Finite quaternionic reflection groups*, J. Algebra **64** (1980), 293–324.
[6] P. Etingof and V. Ginzburg. *Symplectic reflection algebras, Calogero-Moser space, and deformed Harish-Chandra homomorphism*, Invent. Math. **147**(2) (2002), 243–348.
[7] G.C. Shephard and J.A. Todd. *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.
[8] U. Thiel. *Champ: a Cherednik algebra Magma package*, LMS J. Comput. Math. **18**(1) (2015), 266–307. Software available at `https://github.com/ulthiel/Champ`.
[9] U. Thiel. *Fundamental invariants of improper symplectic reflection groups*, `https://ulthiel.com/math/research/data/fundamental-invariants-of-improper-symplectic-reflection-groups/`.

A possible alternative for Conway polynomials

Frank Lübeck

For any fixed prime p, the Conway polynomials $C_{p,n}(X) \in \mathbb{F}_p[X]$, $n \in \mathbb{Z}_{>0}$, give an explicit construction of an algebraic closure of the prime field $\mathbb{F}_p$ with p elements. The polynomial $C_{p,n}$ describes the finite field with p^n elements as algebraic extension, and the corresponding generator of this field is a primitive root, that is of multiplicative order $p^n - 1$.

Conway polynomials are used in various computer algebra packages (GAP, Magma, Flint, ...) for standardized notations of finite field elements.

These polynomials define a lift homomorphism

$$\bar{\mathbb{F}}_p^\times \hookrightarrow \mathbb{C}^\times,$$

which is used in (the computation of) mathematical data on modular representations of finite groups, e.g. for computing values of Brauer characters or for reductions of ordinary characters modulo p (Modular ATLAS, ATLAS of group representations, ...).

Unfortunately, Conway polynomials are very difficult to compute. The known ones needed enormous computational resources and some needed for current applications are impossible to compute in practice.

In my short talk I advertised a new two-step approach to address this (so allowing far larger finite fields to be handled):

(A) First, an easy to describe and implement construction of the algebraic closure of finite prime fields (that is, a construction of each finite subfield together with efficiently computable embeddings).

(B) Second, for each positive integer m, prime to p, a practical construction of a standardized element of multiplicative order m (in the description from (A)). The definition also provides a practically computable lift homomorphism.

References

[1] F. Lübeck, *Standard Generators of Finite Fields and their Cyclic Subgroups*, preliminary version, `https://arxiv.org/abs/2107.02257` (2021).

[2] F. Lübeck, StandardFF, *a GAP package for finite fields*, reference implementation, `https://github.com/frankluebeck/StandardFF` (2021).

Discrete and free groups acting on locally finite trees

Matthew Conder

Let T be a locally finite simplicial tree. Its isometry group $\mathrm{Isom}(T)$ is a topological group with respect to the topology of pointwise convergence.

In [1], we present an algorithm to decide whether or not a pair of isometries g_1, g_2 generate a subgroup G of $\mathrm{Isom}(T)$ which is both discrete and free of rank two. The algorithm proceeds by replacing either g_1 or g_2 by g_1g_2 or $g_1g_2^{-1}$ until the sum of translation lengths $l(g_1)+l(g_2)$ is minimised. Such a 'minimal' pair also generates G and either contains an elliptic isometry (and hence G is either not free or not discrete) or satisfies the hypotheses of the Ping Pong Lemma (and hence G is both discrete and free). This method of systematically minimising translation length was motivated by a 'trace minimising' procedure used in [2, Algorithm 2] to decide if two-generated subgroups of $\mathrm{SL}_2(\mathbb{R})$ are both discrete and free.

A natural generalisation of this work is to decide whether or not an n-tuple $X = (g_1, \ldots, g_n)$ of isometries of T generates a subgroup G of $\mathrm{Isom}(T)$ which is both discrete and free of rank n. Minimising the sum of translation lengths $l(g_1)+\cdots+l(g_n)$ is not always successful in producing an n-tuple either containing an elliptic element or satisfying the hypotheses of the Ping Pong Lemma. We instead aim to minimise the following quantity:

$$L(X) = \sum_{1\leq i\leq n} l(g_i) + \sum_{1\leq i<j\leq n} l(g_ig_j) + l(g_ig_j^{-1}).$$

We consider performing multiple product replacements simultaneously to reduce $L(X)$. For $j \in \{1, \ldots, n\}$ and $S_1, S_2 \subseteq \{1, \ldots, n\}\backslash\{j\}$, we denote by $X^j_{S_1,S_2}$ the n-tuple obtained from X by replacing $g_i \mapsto g_jg_i$ if $i \in S_1$ and $g_i \mapsto g_ig_j^{-1}$ if $i \in S_2$. Note that X and $X^j_{S_1,S_2}$ generate the same subgroup G of $\mathrm{Isom}(T)$.

Definition. An n-tuple $X = (g_1, \ldots, g_n)$ of isometries of T is *minimal* if $L(X) \leq L(X^j_{S_1,S_2})$ for all $j \in \{1, \ldots, n\}$ and $S_1, S_2 \subseteq \{1, \ldots, n\}\backslash\{j\}$.

Conjecture. A minimal n-tuple $X = (g_1, \ldots, g_n)$ of isometries of T either contains an elliptic element or satisfies the hypotheses of the Ping Pong Lemma.

We have proved the conjecture for $n = 2, 3$ and have computational evidence that it holds for $n > 3$. Subject to the conjecture, there is an algorithm to decide whether or not a finitely generated subgroup of $\mathrm{Isom}(T)$ is both discrete and free.

We have implemented this algorithm in Magma for n-generated subgroups of $\mathrm{PSL}_2(\mathbb{Q})$ (viewed as subgroups of $\mathrm{PSL}_2(\mathbb{Q}_p)$, and hence of the isometry group of the corresponding Bruhat-Tits tree). It runs efficiently when n, p and the translation

lengths of the input are all small. For instance, if $n = 6$, $p = 7$ and each input element has translation length at most 20, then the algorithm has a runtime of approximately 1 minute.

References

[1] M. J. Conder, Discrete and free two-generated subgroups of SL_2 over non-archimedean local fields, *Journal of Algebra* **553** (2020), 248–267.

[2] B. Eick, M. Kirschmer and C. Leedham-Green, The constructive membership problem for discrete free subgroups of rank 2 of $\mathrm{SL}_2(\mathbb{R})$, *LMS J. Comput. Math.* **17**:1 (2014), 345-359.

Saxl graphs of sporadic groups

Melissa Lee

(joint work with Tomasz Popiel)

A *base* for a permutation group $G \leq \mathrm{Sym}(\Omega)$ is a subset of Ω whose pointwise stabiliser is trivial. The *base size* of G is the minimal cardinality of a base. If G has base size 2, then the corresponding *Saxl graph* $\Sigma(G)$ has vertex set Ω and two vertices are adjacent if they form a base for G. A recent conjecture of Burness and Giudici [1] states that if G is a finite primitive permutation group with base size 2, then every two vertices in $\Sigma(G)$ have a common neighbour. We discuss recent work on this conjecture in [2], where G is an affine group with an almost quasisimple point stabiliser H such that $\mathrm{soc}(H/Z(H))$ is a sporadic simple group.

References

[1] T. C. Burness and M. Giudici, "On the Saxl graph of a permutation group", *Math. Proc. Cambridge Phil. Soc.* **168** (2020) 219–248.

[2] M. Lee and T. Popiel, "Saxl graphs of primitive affine groups with sporadic point stabilisers", preprint (2021); `https://arxiv.org/abs/2108.02470`

Groups of small order type

Xueyu Eileen Pan

It is a central theme in group theory to classify (finite) groups up to isomorphism. Of particular interest is the classification of all groups of a given order n; this has started with the work of Cayley and the introduction of axiomatically defined groups. Since then a vast amount of literature has emerged, dealing with groups of special orders or order types (that is, orders that factorise into a particular form, such as $n = pq$ for distinct primes p and q). This MPhil project aims to investigate groups whose orders factorise into at most four primes. Theoretical classifications exist in the literature, but most expositions are lengthy and it is difficult to extract results. This project elaborates a new self-contained and independent determination of the isomorphism class representatives for these groups, presented in a unified and modern language. Importantly, this project leads to efficient construction algorithms for these groups, which we have implemented as

a software package SOTGrps for the computer algebra system GAP. The SOTGrps package extends the SmallGroups library of GAP and provides an identification functionality as well as a "construction-by-ID" method; this leads to a dynamic database of groups (where groups can be efficiently constructed on demand) and a practical isomorphism test (by comparing group-IDs). The approach used in this project can be extended to other order types. As an example, new algorithms for the construction and identification of groups of order p^4q are also implemented in SOTGrps. Some results of this project appear in [1].

References

[1] H. Dietrich, B. Eick, X. Pan, *Groups whose orders factorise into at most four primes*, Journal of Symbolic Computation **108** (2022), 23–40.

Rewriting systems and what kinds of groups they present

Murray Elder
(joint work with Adam Piggott)

I explain some recent joint work with Adam Piggott about classifying groups presented by (inverse-closed) finite convergent length-reducing rewriting systems.

Madlener and Otto [1] conjectured that a group is presented by a finite convergent length-reducing rewriting system if and only if it is plain (the free product of finite and infinite cyclic groups).

We prove that the problem of deciding if an inverse-closed finite convergent length-reducing rewriting system does not present a plain group is in NP. Our proof relies on new geometric and algebraic characterisations of groups presented by such rewriting systems. The related preprint is at https://arxiv.org/abs/2106.03445

References

[1] K. Madlener and F. Otto, "Groups presented by certain classes of finite length-reducing string-rewriting systems," in *Rewriting techniques and applications (Bordeaux, 1987)*, vol. 256 of *Lecture Notes in Comput. Sci.*, pp. 133–144, Springer, Berlin, 1987.

What can computational group theory do for number theory

Claus Fieker, Tommy Hofmann

In the talk we presented classical as well as more recent applications of computational group theory to number theory, with a view towards challenges in practice.

Galois groups. One of the classical applications of algorithms for permutation groups is the computation of Galois groups of rational polynomials using the algorithm of Stauduhar [1] and its generalizations due to Fieker and Jürgen Klüners [2]. For a transitive permutation group G of degree n with subgroup U, the following problems have to be solved:

(1) Find the maximal transitive subgroups of G.
(2) Find a polynomial $f \in \mathbf{Z}[x_1, \ldots, x_n]$ such that $\mathrm{Stab}_G(f) = U$. The polynomial f needs to be a form such that evaluating f at points of $\mathbf{C}^n$ is fast.
(3) Find coset representatives for G/U.
(4) Given an element $\sigma \in G$, find coset representatives τ of G/U such that $\sigma \in U^\tau$.
(5) Compute and intersect wreath products.

While all current implementations for permutation groups work quite well for small degrees, computations become challenging for large degrees, with the threshold depending on the chosen computer algebra system.

Inverse Galois problem for solvable groups. Constructing normal number fields with solvable Galois group G can be done by translating a normal series of G with abelian quotients to a corresponding tower of abelian extensions of $\mathbf{Q}$. When moving up the tower on the number field side, so-called embedding problems have to be solved, which are intimately connected with exact sequences of the form

$$(*) \qquad 1 \longrightarrow A \longrightarrow X \longrightarrow G \longrightarrow 1,$$

where X, G are finite groups and A is abelian.

(6) Given X and G, find all possible abelian groups A and actions of G on A such that the sequence $(*)$ is exact.

When enumerating possible congruence subgroups for abelian extensions of a fixed normal number field, the following problem needs to be solved:

(7) Given a finite abelian group A and a finite group G acting on A, determine all G-invariant subgroups B of A with A/B a p-group of specific isomorphism class.

If the quotient A/B is an elementary abelian p-group, the classical MeatAxe can be used to solve this problem. The general case requires an extensions of this method.

Norm relations and subfields. Recent work [3] of Jean-François Biasse, Aurel Page and the authors has shown how to systematically exploit the subfield structure when solving various computational problems for number fields. In case the number field is normal with Galois group G, it was shown that this is possible if there exists a *norm relation* of the form

$$d = \sum_{1 \lneq H \leq G} a_H \, \mathrm{N}_H \, b_H$$

in $\mathbf{Z}[G]$, where H is running over the non-trivial subgroups of G, $d \in \mathbf{Z}$, $a_H, b_H \in \mathbf{Z}[H]$ and $\mathrm{N}_H = \sum_{g \in H} g$. Given information on the subgroups of G, the existence, respectively non-existence, of such a relation can easily be established. A more challenging problem is the determination of an explicit norm relation or a norm relation with specific properties:

(8) Given a finite group G find an explicit norm relation. In addition make d as small as possible or ensure that only normal subgroups, or subgroups of small index, are involved.

References

[1] R. P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996.

[2] C. Fieker and J. Klüners, *Computation of Galois groups of rational polynomials*, LMS J. Comput. Math. **17**, (2014), no. 1, 141–158.

[3] J.-F. Biasse, C. Fieker, T. Hofmann and A. Page, *Norm relations and computational problems in number fields*, arXiv:2002.12332.

Magma's role in identifying all principal congruence link complements

Alan W. Reid

(joint work with Mark D. Baker, Matthias Goerner)

Let d be a square-free positive integer, let O_d denote the ring of integers in $\mathbb{Q}(\sqrt{-d})$, and h_d denote the class number of $\mathbb{Q}(\sqrt{-d})$.

Setting $Q_d = \mathbb{H}^3/\mathrm{PSL}(2, \mathrm{O_d})$ to be the Bianchi orbifold, it is well-known that Q_d is a finite volume hyperbolic orbifold with h_d cusps (see [5, Chapters 8 & 9] for example). A non-compact finite volume hyperbolic 3-manifold X is called *arithmetic* if X and Q_d are commensurable, that is to say they share a common finite sheeted cover (see [5, Chapter 8] for more on this).

An important class of arithmetic 3-manifolds consists of the *congruence* manifolds. Recall that a subgroup $\Gamma < \mathrm{PSL}(2, \mathrm{O_d})$ is called a *congruence subgroup* if there exists an ideal $I \subset O_d$ so that Γ contains the *principal congruence group*:

$$\Gamma(I) = \ker\{\mathrm{PSL}(2, \mathrm{O_d}) \to \mathrm{PSL}(2, \mathrm{O_d/I})\}.$$

The largest ideal I for which $\Gamma(I) < \Gamma$ is called the *level* of Γ. A manifold M is called *congruence* (resp. *principal congruence*) if M is isometric to a manifold $\mathbb{H}^3/\Gamma$ where $\Gamma(I) < \Gamma < \mathrm{PSL}(2, \mathrm{O_d})$ (resp. $\Gamma = \Gamma(I)$) for some ideal I.

In an email to the first and third authors in 2009, W. Thurston asked the following question about principal congruence link complements:

"Although there are infinitely many arithmetic link complements, there are only finitely many that come from principal congruence subgroups. Some of the examples known seem to be among the most general (given their volume) for producing lots of exceptional manifolds by Dehn filling, so I'm curious about the complete list."

In this talk, we described some of the computational group theoretic aspects of our work (particularly the use of MAGMA [4]) with Baker and Goerner [1], [2], and [3] that led to the complete enumeration all the principal congruence link complements in S^3, together with their levels. This is summarized in the following result:

Theorem. *The following list of* 48 *pairs* (d, I) *describes all principal congruence subgroups* $\Gamma(I) < \mathrm{PSL}(2, \mathrm{O_d})$ *such that* $\mathbb{H}^3/\Gamma(I)$ *is a link complement in* S^3*:*

(1) $d = 1$**:** $I = \langle\ 2\ \rangle, \langle\ 2 \pm i\ \rangle, \langle\ (1 \pm i)^3\ \rangle, \langle\ 3\ \rangle, \langle\ 3 \pm i\ \rangle, \langle\ 3 \pm 2i\ \rangle, \langle\ 4 \pm i\ \rangle$.
(2) $d = 2$**:** $I = \langle\ 1 \pm \sqrt{-2}\ \rangle, \langle\ 2\ \rangle, \langle\ 2 \pm \sqrt{-2}\ \rangle, \langle\ 1 \pm 2\sqrt{-2}\ \rangle, \langle\ 3 \pm \sqrt{-2}\ \rangle$.
(3) $d = 3$**:** $I = \langle\ 2\ \rangle, \langle\ 3\ \rangle, \langle\ (5 \pm \sqrt{-3})/2\ \rangle, \langle\ 3 \pm \sqrt{-3}\ \rangle, \langle\ (7 \pm \sqrt{-3})/2\ \rangle, \langle\ 4 \pm \sqrt{-3}\ \rangle, \langle\ (9 \pm \sqrt{-3})/2\ \rangle$.
(4) $d = 5$**:** $I = \langle\ 3, (1 \pm \sqrt{-5})\ \rangle$.
(5) $d = 7$**:** $I = \langle\ (1 \pm \sqrt{-7})/2\ \rangle, \langle\ 2\ \rangle, \langle\ (3 \pm \sqrt{-7})/2\ \rangle, \langle\ \pm\sqrt{-7}\ \rangle, \langle\ 1 \pm \sqrt{-7}\ \rangle, \langle\ (5 \pm \sqrt{-7})/2\ \rangle, \langle\ 2 \pm \sqrt{-7}\ \rangle, \langle\ (7 \pm \sqrt{-7})/2\ \rangle, \langle\ (1 \pm 3\sqrt{-7})/2\ \rangle$.
(6) $d = 11$**:** $I = \langle\ (1 \pm \sqrt{-11})/2\ \rangle, \langle\ (3 \pm \sqrt{-11})/2\ \rangle, \langle\ (5 \pm \sqrt{-11})/2\ \rangle$.
(7) $d = 15$**:** $I = \langle\ 2, (1 \pm \sqrt{-15})/2\ \rangle, \langle\ 3, (3 \pm \sqrt{-15})/2\ \rangle, \langle\ (1 \pm \sqrt{-15})/2\ \rangle, \langle\ 5, (5 \pm \sqrt{-15})/2\ \rangle, \langle\ (3 \pm \sqrt{-15})/2\ \rangle$.
(8) $d = 19$**:** $I = \langle\ (1 \pm \sqrt{-19})/2\ \rangle$.
(9) $d = 23$**:** $I = \langle\ 2, (1 \pm \sqrt{-23})/2\ \rangle, \langle\ 3, (1 \pm \sqrt{-23})/2\ \rangle, \langle\ 4, (3 \pm \sqrt{-23})/2\ \rangle$.
(10) $d = 31$**:** $I = \langle\ 2, (1 \pm \sqrt{-31})/2\ \rangle, \langle\ 4, (1 \pm \sqrt{-31})/2\ \rangle, \langle\ 5, (3 \pm \sqrt{-31})/2\ \rangle$.
(11) $d = 47$**:** $I = \langle\ 2, (1 \pm \sqrt{-47})/2\ \rangle, \langle\ 3, (1 \pm \sqrt{-47})/2\ \rangle, \langle\ 4, (1 \pm \sqrt{-47})/2\ \rangle$.
(12) $d = 71$**:** $I = \langle\ 2, (1 \pm \sqrt{-71})/2\ \rangle$.

REFERENCES

[1] M. D. Baker, M. Goerner and A. W. Reid, *All principal congruence link complements*, J. Algebra **528** (2019), 497–504.

[2] M. D. Baker, M. Goerner and A. W. Reid, *Technical Report: All Principal Congruence Link Groups*, `arXiv:1902.04722`.

[3] M. D. Baker, M. Goerner and A. W. Reid, *All Known Principal Congruence Links*, `arXiv:1902.04426`.

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

[5] C. Maclachlan and A. W. Reid, *The Arithmetic of Hyperbolic 3-Manifolds*, Graduate Texts in Math. **219**, Springer-Verlag, Berlin, 2003.

Weisfeiler-Leman and Group Isomorphism

Pascal Schweitzer
(joint work with Jendrik Brachter)

The complexity of the Group Isomorphism Problem and the computation of normal forms for finite groups remain unsettled. While numerous practical and sophisticated algorithms have been developed over the years, developing algorithms with polynomial worst case upper bounds remains a challenge. This is true even for comparatively benign types of groups, such as nilpotent groups of class 2.

The Weisfeiler-Leman (WL) algorithm is a powerful, efficient combinatorial algorithm that has been successfully analyzed and applied in the context of the Graph Isomorphism Problem. There is a fairly natural way to apply it to groups which is widely unexplored.

I will give an introduction to the WL algorithm and discuss for it various recent results related to the complexity of the Group Isomorphism Problem. This includes a systematic study of classic isomorphism invariants, many of which turn out to be captured by WL. It also includes examples of pairs of non-isomorphic groups that have the same $\log(n)$-subgroup-profiles distinguished in polynomial time [1].

References

[1] Jendrik Brachter and Pascal Schweitzer. On the Weisfeiler-Leman dimension of finite groups. In Holger Hermanns, Lijun Zhang, Naoki Kobayashi, and Dale Miller, editors, *LICS '20: 35th Annual ACM/IEEE Symposium on Logic in Computer Science, Saarbrücken, Germany, July 8-11, 2020*, pages 287–300. ACM, 2020.

Classifying the non-synchronizing primitive permutation groups

Leonard H. Soicher

A permutation group G on a finite set Ω is *non-synchronizing* if there is a non-null non-complete graph Γ with vertex-set Ω, such that the clique number and chromatic number of Γ are equal and $G \leq \mathrm{Aut}(\Gamma)$.

The study of non-synchronizing permutation groups arose from a problem in the theory of automata, and turns out to have strong connections to certain problems in combinatorics, finite geometry, and computation (see [1]). It it easy to see that, if $|\Omega| > 2$, then an intransitive or imprimitive permutation group on Ω is non-synchronizing. Hence, the interest is in the non-synchronizing primitive permutation groups.

I have classified the non-synchronizing primitive permutation groups of degree up to 464. It turns out that, amongst the 3667 primitive permutation groups having degree in $\{2, \ldots, 464\}$, exactly 1093 are non-synchronizing. The main tools used in the classification were:

- the GAP system [3], in particular its library of primitive permutation groups;
- the GAP package GRAPE [5], in particular its clique and proper vertex-colouring functionality;
- a list maintained of certain known or discovered graphs having primitive automorphism group and clique number equal to chromatic number;
- an approach due to Peter Cameron for primitive groups of affine type of prime-squared or prime-cubed degree;
- Theorem 1.4 of [2];
- a new hybrid GAP/GRAPE/C program of the author for computing the cliques with given vertex-weight sum in a graph whose vertices are weighted with non-zero d-vectors of non-negative integers, which was used for two cases, employing parallel computation on the Queen Mary Apocrita HPC facility [4], supported by QMUL Research-IT.

Details of the computations and classification are available from the author.

References

[1] J. Araújo, P.J. Cameron, and B. Steinberg, Between primitive and 2-transitive: Synchronization and its friends, EMS Surveys in Mathematical Sciences **4** (2017), 101–184.
[2] J.N. Bray, Q. Cai, P.J. Cameron, P. Spiga, and H. Zhang, The Hall-Paige conjecture, and synchronization for affine and diagonal groups, *Journal of Algebra* **545** (2020), 27–42.
[3] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.11.1, 2021. `www.gap-system.org`
[4] T. King, S. Butcher, and L. Zalewski, Apocrita - High performance computing cluster for Queen Mary University of London, 2017. `http://doi.org/10.5281/zenodo.438045`
[5] L.H. Soicher, The GRAPE package for GAP, Version 4.8.3, 2019. `https://gap-packages.github.io/grape`

Effective estimate for the joint spectral radius

Emmanuel Breuillard

The joint spectral radius $R(S)$ of a finite set of matrices $S \subset M_{d\times d}(\mathbb{R})$ is a quantity describing the maximal rate of growth of the product set S^n as n grows. If $\|\cdot\|$ is a norm on $\mathbb{R}^d$, inducing an operator norm on $M_{d\times d}(\mathbb{R})$ then

$$R(S) := \lim_{n\to+\infty} \|S^n\|^{\frac{1}{n}}.$$

This quantity, which is a conjugation invariant and does not depend on the choice of norm, was introduced by Rota and Strang [8] in the 60's and appears naturally in many contexts, often in applied maths (wavelets, symbolic dynamics, ergodic optimization, control theory, etc.) where the question of estimating $R(S)$ for a concrete set S arises [7, 9, 6]. To this end an inequality due to J. Bochi [1] relates the joint spectral radius to the maximal eigenvalue of short words in S:

$$R(S) \le \max_{k\le k(d)} \left[|\lambda|, \lambda \text{ eigenvalue of some } g \in S^k\right]^{\frac{1}{k}} \le C(d)\cdot R(S) \tag{1}$$

where $k(d)$ and $C(d)$ are constants independent of S. Bochi's proof was not effective. We provide a different argument, which gives explicit constants:

Theorem 1. [2, Theorem 5] *In* (1) *one can take* $C(d) = 1 + \epsilon$, *and* $k(d) \ll_\epsilon d^{3+\epsilon}$ *for any* $\epsilon > 0$ *(with explicit constants). If* $\mathbb{R}$ *is replaced by an ultrametric complete valued field, then we have equality, i.e.* $C(d) = 1$, *and* $k(d) \ll_\epsilon d^{1+\epsilon}$.

Part of the motivation comes from the study of quantitative forms of the Tits alternative, see [5, 3, 4], and the wish to elaborate an algorithm to produce explicit generators of a free subgroup in the subgroup generated by S. Theorem 1 allows to produce short words with letters in S admitting a large eigenvalue, which is a basic step in the proof of the Tits alternative. It also yields an effective (although still too large) value for the constant $N(d)$ in the following theorem:

Theorem 2 ([4], Corollary 3.6)**.** *There is* $N(d) \in \mathbb{N}$ *such that if* $S \subset GL_d(\mathbb{C})$ *is a finite symmetric set generating an infinite subgroup, then there is an element of infinite order in* S^k, *for some* $k \leq N(d)$.

References

[1] Jairo Bochi. Inequalities for numerical invariants of sets of matrices. *Linear Algebra Appl.*, 368:71–81, 2003.

[2] Emmanuel Breuillard, *On the joint spectral radius*, preprint 2021, arXiv 2103.09089.

[3] Emmanuel Breuillard. Heights on $GL(2)$ and free subgroups. *Chicago Univ. Press*, Geometry, Rigidity and Group Actions, Zimmer's Festschrift, 2011.

[4] Emmanuel Breuillard. A height gap theorem for finite subsets of $\mathrm{GL}_d(\overline{\mathbb{Q}})$ and nonamenable subgroups. *Ann. of Math. (2)*, 174(2):1057–1110, 2011.

[5] Emmanuel Breuillard and Tsachik Gelander. Uniform independence in linear groups, Invent. Math. 173 (2008), 225–263.

[6] Jeffrey C. Lagarias and Yang Wang. The finiteness conjecture for the generalized spectral radius of a set of matrices. *Linear Algebra Appl.*, 214:17–42, 1995.

[7] Raphaël Jungers. *The joint spectral radius*, volume 385 of *Lecture Notes in Control and Information Sciences*. Springer-Verlag, Berlin, 2009. Theory and applications.

[8] Gian-Carlo Rota and Gilbert Strang. A note on the joint spectral radius. *Nederl. Akad. Wetensch. Proc. Ser. A 63 = Indag. Math.*, 22:379–381, 1960.

[9] Fabian Wirth. The generalized spectral radius and extremal norms. *Linear Algebra Appl.*, 342:17–40, 2002.

Subgroup Membership in GL(2, $\mathbb{Z}$)

Markus Lohrey

The subgroup membership problem (also known as the generalized word problem) for a group G asks whether for given group elements $g_0, g_1, \ldots, g_k \in G$, g_0 belongs to the subgroup $\langle g_1, \ldots, g_k \rangle$ generated by $g_1, \ldots, g_k$. To make this a well-defined computational problem, one has to fix an input representation for elements of G. Here, a popular choice is to restrict to finitely generated groups. In this case, group elements can be encoded by finite words over a finite set of generators. The subgroup membership problem is one of the best studied problems in computational group theory.

For a finitely generated free group the subgroup membership problem can be solved in polynomial time. This can be shown using Stallings's folding procedure [4]. Moreover, Grunschlag [1] showed that if G is a finite extension of a group H (with G and H both finitely generated), then there is a polynomial time reduction from the subgroup membership problem of G to the subgroup membership problem for H. As a consequence, the subgroup membership problem for every finitely generated virtually free group can be solved in polynomial time. One of the best known examples of a finitely generated virtually free group is the group $\mathsf{GL}(2,\mathbb{Z})$. We therefore obtain a polynomial time algorithm for the subgroup membership problem of $\mathsf{GL}(2,\mathbb{Z})$. But this result assumes that elements of $\mathsf{GL}(2,\mathbb{Z})$ are represented by finite words over some fixed set of generators for $\mathsf{GL}(2,\mathbb{Z})$. The more natural representation of elements of $\mathsf{GL}(2,\mathbb{Z})$ are 4-tuples of binary encoded integers that represent (2×2)-matrices. From the above discussion, it is not clear whether for this input representation the subgroup membership problem for $\mathsf{GL}(2,\mathbb{Z})$ is still solvable in polynomial time. When writing the matrix

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

as a word over some fixed set of generators, the resulting word must have length $\Omega(n)$, which is exponential in the bit length of n. Hence, one cannot switch in polynomial time from the representation by matrices with binary encoded integers to the representation by words over generators. Nevertheless we can prove the following result:

Theorem 1. *The subgroup membership problem for* $\mathsf{GL}(2,\mathbb{Z})$ *can be solved in polynomial time when group elements are represented by matrices with binary encoded integers.*

In order to prove this result, we apply a variant of Stallings' folding procedure for compressed words that is motivated by work of Gurevich and Schupp [2]. They present a polynomial time algorithm for the subgroup membership problem in a free group $F(\Sigma)$, where elements of the free group are represented by words of the form $a_1^{z_1} a_2^{z_2} \cdots a_k^{z_k}$. Here, the a_i are from $\Sigma \cup \Sigma^{-1}$, i.e., they are single generators, and the z_i are binary encoded integers. Gurevich and Schupp proceed in [2] by showing that a similar approach also works for the free product $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$, which is isomorphic to the modular group $\mathsf{PSL}(2,\mathbb{Z})$. As a corollary, they deduce that the subgroup membership problem for $\mathsf{PSL}(2,\mathbb{Z})$ is decidable in polynomial time when all matrix entries are encoded in binary notation.

In order to apply the approach of Gurevich and Schupp to related groups such as $\mathsf{GL}(2,\mathbb{Z})$, it turns out to be useful to generalize their folding procedure for compressed words. In our variant of Stalling's folding we allow edges that are labelled with powers of the form w^z for w a word and z a binary encoded integer. This leads us to a polynomial time algorithm for the subgroup membership problem in a free group $F(\Sigma)$, where elements of $F(\Sigma)$ are represented by words of the form $w_1^{z_1} w_2^{z_2} \cdots w_k^{z_k}$. Here, the z_i are (as in [2]) binary encoded integers, but the w_i are arbitrary words over the generating set $\Sigma \cup \Sigma^{-1}$ instead of only single generators.

We call this problem the power-compressed subgroup membership problem for the free group $F(\Sigma)$. We then proceed to show that the power-compressed subgroup membership problem can be also solved in polynomial time for every virtually free group, by extending the polynomial time reduction from Grunschlag's work [1] to the power-compressed setting. As a corollary of this we finally obtain Theorem 1.

We also present another application of our power-compressed folding procedure. In the finite index problem for a group G the goal is to compute the index (an element of $\mathbb{N} \cup \{\infty\}$) of a given finitely generated subgroup of G.

Theorem 2. *The finite index problem for finitely generated subgroups of* $\mathsf{GL}(2,\mathbb{Z})$ *can be decided in polynomial time, when elements of* $\mathsf{GL}(2,\mathbb{Z})$ *are represented by matrices with binary encoded integers.*

An extended abstract of this work appeared in [3].

References

[1] Zeph Grunschlag, *Algorithms in Geometric Group Theory*, PhD thesis, University of California at Berkley, 1999.

[2] Yuri Gurevich and Paul E. Schupp, *Membership problem for the modular group*, SIAM Journal on Computing **37(2)** (2007), 425–459.

[3] Markus Lohrey, *Subgroup membership in GL*$(2,\mathbb{Z})$, Proceedings of the 38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021, volume 187 of LIPIcs (2021), Schloss Dagstuhl - Leibniz-Zentrum für Informatik.

[4] John R. Stallings, *Topology of finite graphs*, Inventiones Mathematicae **71(3)** (1983), 551–565.

Base sizes and complexity

Colva M. Roney-Dougal

(joint work with Veronica Kelsey, Mariapia Mosciatiello)

A *base* for a permutation group $G \leq \mathrm{Sym}(\Omega)$ is a sequence $\underline{\beta} = (\alpha_1, \ldots, \alpha_k)$ of points from Ω such that the pointwise stabiliser

$$G_{\alpha_1,\ldots,\alpha_k} = 1.$$

We write $b(G)$ for the size of the smallest base for G. The base $\underline{\beta}$ is *irredundant* if for all i, the stabiliser $G_{\alpha_1,\ldots,\alpha_i}$ properly contains $G_{\alpha_1,\ldots,\alpha_{i+1}}$. We write $I(G)$ for the size of the largest irredundant base for G. It is easy to use the orbit-stabiliser theorem to show that

$$b(G) \leq I(G) \leq b(G) \log n.$$

There are many examples of groups (for instance, S_n itself) for which $b(G) = I(G)$. Similarly, Blaha in [1] proved that for infinitely many n, there exists a subgroup G of S_n with $I(G) \geq \frac{1}{3} b(G) \log n$, so up to constants this upper bound is best possible.

Bases are crucial data structures when working with permutation groups on a computer, and so bounds on base size can be used to prove various complexity bounds within computational group theory. Sims proved (see for example [6])

that given generators for a permutation group G, an irredundant base for G can be computed in polynomial time.

A primitive group $G \leq \mathrm{Sym}(\Omega)$ is *large base* if there exist integers $\ell \geq 1$, $k \geq 5$ and $1 \leq m \leq k/2$ such that up to permutation isomorphism

$$\mathrm{A}_k^\ell \trianglelefteq G \leq \mathrm{S}_k \wr \mathrm{S}_\ell,$$

where Ω is all ℓ-tuples of m-subsets of $\{1, \ldots, k\}$. If $\ell = 1$ then these groups are almost simple, otherwise they are of product action type. As the name suggests, large base groups can have very large bases, but Liebeck proved in [4] that if $G \leq \mathrm{S}_n$ is primitive and not large base, then $b(G) \leq 9 \log n$. Moscatiello and the author [5] have improved this bound, and shown that if G is not the Mathieu group M_{24} in its natural action on 24 points, then $b(G) \leq \lceil \log n \rceil + 1$. Furthermore, they classified the groups for which $b(G) > \log n + 1$: there is one infinite family, plus some of the other Mathieu groups.

It follows from this, together with the bound $I(G) \leq b(G) \log n$, that if G is primitive and not large base then $I(G) \leq 2(\log n)^2$, but recently Gill, Lodà and Spiga conjectured [2] that for such groups there should exist a constant c such that $I(G) \leq c \log n$. In a very recent preprint [3] Kelsey and the author have proved this conjecture, with $c = 5$. This bound is correct up to constants, and close to best possible.

We conclude with an application of this second result. Blaha showed in [1] that given generators for a subgroup G of S_n, computing a base of size $b(G)$ is NP-hard, but that in polynomial time the obvious greedy algorithm computes a base of size $O(b(G) \log \log n)$. This implies with Liebeck's result that if G is primitive and not large base then a base of size $O(\log n \log \log n)$ can be computed in polynomial time. We now deduce that in polynomial time we can compute a base of size less than $5 \log n$.

References

[1] K.D. Blaha, *Minimum bases for permutation groups: the greedy approximation*, J. Algorithms **13** (1992), no. 2, 297–306.

[2] N. Gill, B. Lodà and P. Spiga, *On the height and relational complexity of a finite permutation group*, Nagoya Math. J, to appear.

[3] V. Kelsey and C.M. Roney-Dougal, *On relational complexity and base size of finite primitive groups*, arXiv preprint 2107.14208.

[4] M.W. Liebeck, *On minimal degrees and base sizes of primitive permutation groups*, Arch. Math. (Basel) **43** (1984), no. 1, 11–15.

[5] M. Moscatiello and C.M. Roney-Dougal, *Base size of primitive permutation groups*, Monatsh. Math. to appear.

[6] C.C. Sims, Computational methods in the study of permutation groups. In: Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967) pp. 169–183 Pergamon, Oxford.

Classification of real trivectors in dimension nine

Willem de Graaf
(joint work with Mikhail Borovoi, Hông Vân Lê)

Let F be a field and $V = F^n$. The elements of $\bigwedge^3 V$ are called trivectors of an n-dimensional space. The group $\mathrm{GL}(n, \mathbb{C})$ naturally acts on $\bigwedge^3 V$. The question is what its orbits are.

In 1978 Vinberg and Elashvili [1] published a classification of the orbits of $\mathrm{SL}(9, \mathbb{C})$ on $\bigwedge^3 \mathbb{C}^9$. Here we report on our recent classification of the $\mathrm{SL}(9, \mathbb{R})$ orbits on $\bigwedge^3 \mathbb{R}^9$. The results are contained in the preprints [2] (long version with full details) and [3] (shorter version intended for publication).

We first say a few words on the set up in [1]. Using Vinberg's theory of θ-groups there is a $\mathbb{Z}/3\mathbb{Z}$-grading of the simple complex Lie algebra of type E_8 by which we can realize the action of $\mathrm{SL}(9, \mathbb{C})$ on $\bigwedge^3 \mathbb{C}^9$. This provides a Jordan decomposition of the elements of $\mathfrak{g}_1$. Accordingly the orbits are divided into three groups: nilpotent, semisimple and mixed orbits.

In order to classify the real orbits we use Galois cohomology. Let $\mathcal{O}$ be an orbit with a real point y. Then the $\mathrm{SL}(9, \mathbb{R})$-orbits contained in $\mathcal{O} \cap \bigwedge^3 \mathbb{R}^9$ correspond bijectively to the elements of the set $H^1 C_y$, where C_y is the stabilizer of y in $\mathrm{SL}(9, \mathbb{C})$.

We use this to classify the real orbits. Each nilpotent orbit has a real representative. But the semisimple and mixed orbits may not have real points. In both cases we have developed a method to decide whether a given orbit has a real point and to find one in the affirmative case. The method for semisimple orbits uses the $H^1\Gamma$ where Γ is a finite group. The method for the mixed orbits uses the $H^2 C_u$, where u is an element of mixed type.

We encountered some computational problems. The stabilizer C_y is given by polynomial equations, but we need its structure (for example, its component group). For this we often used Gröbner bases, using the computer algebra system Singular. We computed the sets $H^1 C_y$ by hand, but we are working at an algorithm for that. We used the computer algebra system GAP for working with the Lie algebra of type E_8 and its elements.

References

[1] È. B. Vinberg and A. G. Elashvili. *A classification of the three-vectors of nine-dimensional space*, Trudy Sem. Vektor. Tenzor. Anal. **18** (1978), 197–233. English translation: Selecta Math. Sov., 7, 63-98, (1988).

[2] M. Borovoi, W. A. de Graaf, and H. V. Lê. *Real graded Lie algebras, Galois cohomology and classification of trivectors in* $\mathbb{R}^9$, `arXiv:2106.00246 [math.RT]`, (2021).

[3] M. Borovoi, W. A. de Graaf, and H. V. Lê. *Classification of real trivectors in dimension nine*, `arXiv:2108.00790 [math.RT]`, (2021).

Construction of quasiprimitive permutation groups

Dominik Bernhardt
(joint work with Alice C. Niemeyer, Cheryl E. Praeger)

Finite quasiprimitive permutation groups are transitive permutation groups acting on a finite set Ω such that each non-trivial, normal subgroup acts transitively on Ω. Every finite primitive permutation group is a finite quasiprimitive permutation group, but there are many imprimitive, quasiprimitive permutation groups. In 1993, Cheryl Praeger described in [2] a structure theorem for finite quasiprimitive permutation groups by analogy to the O'Nan-Scott-Theorem for finite primitive permutation groups. Coutts, Quick and Roney-Dougal extended various databases of certain types of primitive permutation groups of small degree to a complete database of all primitive groups of degree at most 4095, see [1, 3] and references therein.

In this talk, we present methods to construct finite quasiprimitive, imprimitive permutation groups, called *quimp groups*, and as an application present a database of the quimp groups of degree at most 4095. This extends the database of primitive groups to a database of all quasiprimitive permutation groups of degree at most 4095.

The classification of quasiprimitive permutation by Cheryl Praeger splits such groups into 8 distinct classes, 3 of which are always primitive. The remaining 5 cases are almost simple groups (AS type), product action type groups (PA type), twisted wreath type groups (TW type), simple diagonal type groups (SD type) and compound diagonal type groups (CD type). Quimp groups of SD and CD type have degrees larger than 4095 and we only briefly mention methods to construct them. For the remaining three types, we describe our methods used to construct these groups.

References

[1] Hannah J. Coutts, Martyn Quick, Colva M. Roney-Dougal, The primitive permutation groups of degree less than 4096, Comm. Algebra **39**, (2011) 3526–3546.
[2] Cheryl E. Praeger, An O'Nan-Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs, J. London Math. Soc. (2) **47** (1993), 227–239.
[3] Colva M. Roney-Dougal, The primitive permutation groups of degree less than 2500, J. Algebra **292** (2005), 154–183.

The normaliser problem

Mun See Chang
(joint work with Christopher Jefferson, Colva M. Roney-Dougal)

The normaliser problem (Norm) asks for a generating set for $N_G(H)$, given generating sets for subgroups G and H of S_n. Wiebking proved in [8] that, in general, Norm can be solved in simply exponential time $2^{O(n)}$, but better bounds exist by restricting the classes of the input groups G and/or H (see for example [4, 6]). In particular, if H is primitive, then Norm can be solved in quasipolynomial

$2^{O(\log^3 n)}$ [5]. We show that, given subgroups H and G of S_n, in quasipolynomial time $2^{O(\log^3 n)}$, we can decide if $N_{\mathrm{S}_n}(H)$ is primitive, and if so output $N_G(H)$.

Let Norm-Sym be the problem of computing $N_{\mathrm{S}_n}(H)$, given a subgroup H of S_n. Luks in [3] gives a complexity hierarchy consisting of various combinatorial and permutation group problems, but we do not yet know where exactly Norm-Sym sits in the hierarchy. We show that, for a fixed prime p, solving Norm-Sym for a subgroup H of S_{pk} whose transitive constituents are permutation isomorphic to C_p is polynomial-time equivalent to computing the monomial automorphism group of a linear code $C \leq \mathbb{F}_p^k$. As a corollary, Norm-Sym is at least as hard as computing the permutation automorphism group of a linear code over $\mathbb{F}_2$.

In practice, Norm and Norm-Sym are solved using backtrack search, based on methods by Leon [2]. Theißen in [7] uses orbital graphs to reduce the search space. However, we observe that if H acts on each orbit as C_p, orbitals do not provide useful refinements, and we design a much faster algorithm to compute normalisers using linear codes. For future work, we are interested in improving other cases where the normaliser computation is slow, and we aim to implement these techniques in the graph backtrack framework [1].

References

[1] C. Jefferson, M. Pfeiffer, W.A Wilson, R. Waldecker. Permutation group algorithms based on directed graphs. *J. Algebra*, 585:723–758, 2021.

[2] J.S. Leon. Permutation group algorithms based on partitions, I: Theory and algorithms. *J. Symbolic Comput.*, 12:533–583, 1991.

[3] E.M. Luks. Permutation groups and polynomial-time computation. In *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, 11:139–175. Amer. Math. Soc., 1993.

[4] E.M. Luks, T. Miyazaki. Polynomial-time normalizers for permutation groups with restricted composition factors. In *Proc. ISSAC*, pp176–183. ACM, 2002.

[5] C.M. Roney-Dougal, S. Siccha. Normalisers of primitive permutation groups in quasipolynomial time. *Bull. Lond. Math. Soc.*, 52(2):358–366, 2020.

[6] S. Siccha. Towards Efficient Normalizers of Primitive Groups. In *Mathematical Software – ICMS 2020*, pp105–114. Springer, 2020.

[7] H. Theißen. Eine Methode zur Normalisatorberechnung in Permutationsgruppen mit Anwendungen in der Konstruktion primitiver Gruppen. *PhD thesis*, RWTH Aachen, 1997.

[8] D. Wiebking. Normalizers and permutational isomorphisms in simply-exponential time. In *Proc. 31st ACM-SIAM SODA*, pp230–238. SIAM, 2020.

The enumeration of groups of order $p^n q$ for $n \leq 5$

Tobias Moede

(joint work with Bettina Eick)

Let $n \leq 5$. We determine functions $\mathcal{N}_n(p, q)$ that, evaluated at arbitrary different primes p and q, yield the number of isomorphism types of groups of order $p^n q$. The determined functions $\mathcal{N}_n(p, q)$ are (generalized) polynomials on residue classes in p and q.

Our results can be found in [1]. For $n \leq 3$ our results agree with [2, 3, 5] up to some previously known misprints. For $n = 4$ our results agree with the results

of [4] with the exception of the number of non-nilpotent groups of order p^4q with normal Sylow q-subgroup. The functions describing groups of order p^5q were not previously known.

References

[1] B. Eick and Tobias Moede, *The enumeration of groups of order p^nq for $n \leq 5$*, J. Algebra **507** (2018), 571–591.

[2] O. Hölder, *Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4*, Math. Ann. **43** (1893), 301–412.

[3] O. Hölder, *Die Gruppen mit quadratfreier Ordnungszahl*, Nachr. Ges. Wiss. zu Göttingen (1895), 211–229.

[4] R. Laue, *Zur Konstruktion und Klassifikation endlicher auflösbarer Gruppen*, Bayreuth. Math. Schr. **9** (1982).

[5] A. E. Western, *Groups of Order p^3q*, Proc. Lond. Math. Soc. **30** (1899), 209–263.

Burnside groups of relatively small odd exponent

Katrin Tent

(joint work with Agatha Atkarskaya, Eliyahu Rips)

In 1902 Burnside asked whether every finitely generated group of finite exponent is necessarily finite. This question was first answered in the negative in 1964 by Golod and Shafarevich who constructed an infinite finitely generated torsion group. However, their example has unbounded exponent raising the question whether the so-called free Burnside group

$$B(m,n) = F_m/\langle w^n : w \in F_m\rangle$$

of exponent n is finite where F_m is the free group in m generators. For exponent $n = 2, 3, 4$ and 6 it is known by work of Burnside, Sanov, and M. Hall that the free Burnside group is indeed finite for every finite number m of generators. On the other hand, in 1968 Adian and Novikov gave the first proof that the free Burnside group $B(m,n)$ is infinite for odd $n > 4381$. Adian later improved the bound to odd $n > 665$ (and fairly recently even announced a proof for odd $n > 101$). Together with work of Ivanov in 1992 on the case of even exponent one now knows that the group $B(m,n)$ is infinite for all $m > 1$ and all $n > 2^{48}$. The proofs of Adian and Novikov use a very involved induction process with a long list of assumptions. Ol'shanski's more geometric proof in 1982 was important as it provided a much simplified path, however it applies only for $n > 10^{10}$. While arguably the Burnside question has thus long been settled, we believe that it is indeed important to provide readable and accessible proofs which give useful lower bounds for the infiniteness of $B(m,n)$, particularly. Not only will it be useful to have relatively short proofs, but in many cases it is less the result itself which is needed in applications, but rather the methods that were developed in the process of proving them. This seems particularly true in the questions surrounding the Burnside problem. Our proof is based on Rips' idea to choose a canonical representative for every coset in $B(m,n)$. This is done inductively using the rank of a word $w \in F_m$ for the induction. Here, we define the rank $rk(w)$ to be at least

$k+1$ if the word w (cyclically) contains a subword of the form v^7 for some word $v \in F_m$ with $rk(v) \geq k$ and we define

$$N_k = \langle w^n : rk(w) \leq k \rangle.$$

The canonical form $can_k(w)$ for a word w is a canonical representative for wN_k. In particular, if $w, w_0 \in F_m$ are such that $wN_k = w_0N_k$, then $can_k(w) = cank(w_0)$. Furthermore, for any $w \in F_m$, the canonical form stabilizes, i.e. for any $w \in F_m$ there is some k such that $can_k(w) = can_l(w)$ for all $l > k$. We define an algorithm that inductively produces $can_k(w)$ for any k. We choose $can_k(w)$ to be a relatively short coset representative. However, we cannot just define $can_k(w)$ as the shortest representative because, intuitively, the canonical form of a relator w^n has to be chosen in such a way that a small change in the word w should result only in a small change of the canonical form in terms of periodic subwords. This means that we are looking for a very stable choice of coset representatives. It then follows easily from the description of the canonical form that every cube-free element of F_m is already in canonical form. The infiniteness of the Burnside group now follows immediately from the fact that there are infinitely many cube-free words in two generators.

For our method to give a relatively short and accessible proof, we currently need the exponent n to be greater than 297. However, we expect that this can be much improved. The proof also yields (the previously known result) that the infinite free Burnside groups are not finitely presented.

References

[1] A. Atkarskaya, A. Kanel-Belov, E. Plotkin, E. Rips. Small cancellation rings, 2020, https: `https://arxiv.org/abs/2010.03992`

[2] A. Atkarskaya, A. Kanel-Belov, E. Plotkin, E. Rips. Group-like small cancellation theory for rings, 2020, `https://arxiv.org/abs/2010.02836`

[3] A. Atkarskaya, A. Kanel-Belov, E. Plotkin, E. Rips. Construction of a quotient ring of Z_2F in which a binomial $1 + w$ is invertible using small cancellation methods, Contemporary Mathematics, IMCP, Volume 726, 2019, `https://arxiv.org/abs/1807.10070`

[4] E. Rips, Y. Segev, K. Tent, A sharply 2-transitive group without a non-trivial abelian normal subgroup. J. Eur. Math. Soc. (JEMS) 19 (2017), no. 10, 2895–2910.

[5] E. Rips, K. Tent, Sharply 2-transitive groups of characteristic 0. J. Reine Angew. Math. 750 (2019), 227–238.

[6] K. Tent, Sharply 3-transitive groups. Adv. Math. 286 (2016), 722–728.

Constructing the absolutely irreducible modules for a finite group

John Cannon

We have developed algorithms that can construct all absolutely irreducible modules (AIMs) over either a finite field or the complex field for a wide range of groups. Let G be a finite group and K a field. It is assumed that there are very efficient methods for splitting a KG-module into irreducibles, testing a KG-module for irreducibility and determining whether two KG-modules are isomorphic. The first step is to construct the table of complex characters for G using the method

described by Bill Unger [3]. The general approach is to use character theory to identify KG-modules that contain new irreducibles before actually constructing any modules. These modules are constructed from known KG-modules by operations such as tensor product, induction, or extension (only in the complex case).

In the modular case it is not assumed that the Brauer characters of G are known in advance, but as soon as a new irreducible KG-module is found, its Brauer character is computed. So modules containing new irreducibles are found by applying the above operations to Brauer characters. The basic AIM algorithm, where K is a finite field and G is a permutation group, uses the given permutation representation to construct a faithful KG-module M and then proceeds by splitting and tensoring M and selected descendants until all the irreducible modules have been found. This is guaranteed to find all irreducibles by the Burnside-Steinberg-Brauer theorem. Recent development of fast algorithms for constructing a faithful permutation representation of a finite matrix group extends the application of this permutation group algorithm to finite matrix groups over any ring. The algorithm can cope with very large groups, of order up to 10^9 at least, and large numbers of AIMs. See [1] for details.

An algorithm for complex AIMs developed by Allan Steel is based on techniques originally developed in his PhD thesis [2]. First, the absolutely irreducible KG-modules of moderate dimension (typically under 500 over $\mathbb{Q}$ or under 50 over a non-trivial number field) are constructed using a Meataxe-type algorithm using condensation to split suitable permutation or induced KG-modules. Next, for each missing KG-module for which its restriction to some maximal subgroup H is known (by character theory) to be also absolutely irreducible, the appropriate KH-module is constructed recursively and then extended to the desired KG-module. Finally, a hybrid method is used to construct any missing KG-modules: in each case a theoretically defined KG-module is conjugated by modular techniques to construct an actual KG-module whose restriction to a maximal subgroup H equals a *compact* KH-module which has been recursively constructed; this makes possible the practical computation of large-dimension KG-modules over non-trivial number fields such that the resulting matrices have small entries. For example, the 72 absolutely irreducible KG-modules for $\mathrm{PSL}(3,8)$ are computed in two hours, including dimension-511 modules written over a number field of degree 18.

The correctness of the KG-modules obtained by either method can be tested by checking that they satisfy the relations of a (strong) presentation for G. Their characters can also be compared with those in the character table of G.

References

[1] J. J. Cannon, A. K. Steel & W. R. Unger. Construction of the irreducible modular representations of a finite group. *J. Algebra*, **545**, 2020, 64–87.

[2] A.K. Steel. Construction of Ordinary Irreducible Representations of Finite Groups. PhD thesis, University of Sydney, 2012.

[3] William R. Unger. Computing the character table of a finite group. *J. Symbolic Comp.* 41(8), 2006, 847-8626.

Towards a symbolic enumeration of orbits

Tobias Rossmann

Let U_n be the group scheme of upper unitriangular $n \times n$ matrices. Let $\mathbf{G} \leqslant \mathrm{U}_n$ be a unipotent group scheme. Let $\mathfrak{O}$ be a compact discrete valuation ring with maximal ideal $\mathfrak{P}$. This talk was devoted to the enumeration of the orbits of $\mathbf{G}(\mathfrak{O}/\mathfrak{P}^m)$ on its natural module and to the enumeration of the conjugacy classes of $\mathbf{G}(\mathfrak{O}/\mathfrak{P}^m)$.

Restricting attention to unipotent groups provides us with a rich structure. Suppose that $\mathbf{G}$ is fixed and that the residue characteristic of $\mathfrak{O}$ is sufficiently large. For the enumeration of linear orbits, we can then assume that $\mathbf{G}$ is an abelian group scheme attached to a module of matrices. For the enumeration of conjugacy classes, we can assume that $\mathbf{G}$ is obtained from an alternating bilinear map by a variant of the classical Baer correspondence. In either case, our counting problem is naturally related to the study of rank loci within modules of matrices; apart from classical constructions, this builds upon work of O'Brien and Voll [6].

Enumerating matrices of given rank is known to be a geometrically "wild" problem [1]. This has interesting consequences for the enumeration of orbits. For example, one can construct explicit examples of $\mathbf{G} \leqslant \mathrm{U}_n$ such that the total number of orbits of $\mathbf{G}(\mathbf{F}_q)$ on $\mathbf{F}_q^n$ is a polynomial in q, but such that the number of orbits of $\mathbf{G}(\mathbf{F}_q)$ of size q^i (for a suitable fixed i) is not PORC as q ranges over primes. (For an example, combine [3, §1.7] and [8, §4].) Beyond explicit constructions, by combining [1] and [9], one can show that there exist examples of this type in which the non-PORC behaviour is arbitrarily wild in a precise sense.

The main part of the talk revolved around the enumeration of conjugacy classes by means of generating functions. Drawing upon work of du Sautoy [4], the *class-counting zeta function* of a group scheme $\mathbf{G}$ over a ring R is the Dirichlet series

$$\zeta^{\mathrm{cc}}_{\mathbf{G}}(s) = \sum_{I \lhd R} \mathrm{k}(\mathbf{G}(R/I))\,|R/I|^{-s},$$

where the sum extends over ideals of finite index of R and $\mathrm{k}(G)$ denotes the number of conjugacy classes of a group G. Given $\mathbf{G} \leqslant \mathrm{GL}_n$, the study of $\zeta^{\mathrm{cc}}_{\mathbf{G}\otimes\mathfrak{O}}(s)$ as $\mathfrak{O}$ ranges over compact discrete valuation rings is of particular interest. Henceforth, q denotes the residue field size of $\mathfrak{O}$. In many cases of interest, there are "geometric formulae" for $\zeta^{\mathrm{cc}}_{\mathbf{G}\otimes\mathfrak{O}}(s)$ that combine finitely many rational functions in q and q^{-s} and the numbers of $(\mathfrak{O}/\mathfrak{P})$-rational points of schemes derived from $\mathbf{G}$. Excluding small residue characteristics, such formulae have been obtained for Chevalley groups [2] and for unipotent groups [7] in characteristic zero.

As a tentative definition, by a symbolic computation of $\mathrm{k}(\mathbf{G}(\mathfrak{O}/\mathfrak{P}^m))$ for fixed $\mathbf{G} \leqslant \mathrm{U}_n$ and varying $\mathfrak{O}$ (of large residue characteristic) and m, we mean the explicit construction of a geometric formula of the aforementioned type for $\zeta^{\mathrm{cc}}_{\mathbf{G}\otimes\mathfrak{O}}(s)$. While possible in principle, this definition leads to theoretical and practical issues. For example, it seems to be unknown whether equality of two such formulae is even decidable. In practice, many examples of class-counting (and other) zeta functions

of interest turn out to be *uniform* in the sense that given $\mathbf{G}$, there exists a single rational function $W(X,T) \in \mathbf{Q}(X,T)$ such that for all $\mathfrak{O}$ (subject perhaps to restrictions on its characteristic or residue characteristic), $\zeta^{\mathrm{cc}}_{\mathbf{G}\otimes\mathfrak{O}}(s) = W(q,q^{-s})$. In that case, our problem of symbolically enumerating conjugacy classes is tantamount to computing $W(X,T)$.

Zeta functions enumerating linear orbits and conjugacy classes of unipotent groups can be usefully regarded as special cases of *ask zeta functions* [7]. The latter functions are obtained by averaging over sizes of kernels within suitable parameterisations of modules of matrices. This averaging operation is related to the enumeration of orbits via a Lie-theoretic linearisation of the orbit-counting lemma. The study of ask zeta functions combines established results from p-adic integration and algebraic duality operations ("Knuth duality") [8].

The problem of computing class-counting zeta functions has a particularly satisfactory solution for *graphical group schemes*. Given a graph Γ with distinct vertices $v_1,\dots,v_n$, the associated graphical group scheme $\mathbf{G}_\Gamma$ generalises a number of constructions in the literature. In particular, for an odd prime p, the group $\mathbf{G}_\Gamma(\mathbf{F}_p)$ is the maximal quotient of class at most 2 and exponent dividing p of the right-angled Artin group $\langle x_1,\dots,x_n \mid [x_i,x_j]=1 \text{ whenever } v_i \not\sim v_j\rangle$. Class-counting zeta functions associated with graphical group schemes turn out to be uniform in a very strong sense: given Γ, there exists $W_\Gamma(X,T) \in \mathbf{Q}(X,T)$ such that for each compact discrete valuation ring $\mathfrak{O}$ as above, $\zeta^{\mathrm{cc}}_{\mathbf{G}_\Gamma\otimes\mathfrak{O}}(s) = W_\Gamma(q,q^{-s})$; see [9, Cor. B]. Thanks to a constructive proof, these rational functions can be explicitly computed, at least for small graphs. They also exhibit a rich combinatorial structure, in particular for *cographs* [9, Thms C–D].

The final part of the talk contained a brief overview of some further developments. Topics discussed included Lins's work [5] on bivariate conjugacy class and representation zeta functions, steps [3, Thm E] towards understanding class-counting zeta functions of group schemes derived from free nilpotent Lie algebras, and the enumeration of conjugacy classes of graphical groups over finite fields [10].

References

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

[2] M. N. Berman, J. Derakhshan, U. Onn, and P. Paajanen, *Uniform cell decomposition with applications to Chevalley groups*, J. Lond. Math. Soc. (2) 87 (2013), no. 2, 586–606.

[3] A. Carnevale and T. Rossmann, *Linear relations with disjoint supports and average sizes of kernels* (preprint), arXiv:2009.00937.

[4] M. du Sautoy, *Counting conjugacy classes*, Bull. London Math. Soc. 37 (2005), no. 1, 37–44.

[5] P. M. Lins de Araujo, *Bivariate representation and conjugacy class zeta functions associated to unipotent group schemes, I: Arithmetic properties*, J. Group Theory 22 (2019), no. 4, 741–774.

[6] E. A. O'Brien and C. Voll, *Enumerating classes and characters of p-groups*, Trans. Amer. Math. Soc. 367 (2015), no. 11, 7775–7796.

[7] 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.

[8] T. Rossmann, *The average size of the kernel of a matrix and orbits of linear groups, II: duality*, J. Pure Appl. Algebra 224 (2020), no. 4, 106203.

[9] T. Rossmann and C. Voll, *Groups, graphs, and hypergraphs: average sizes of kernels of generic matrices with support constraints.* To appear in Mem. Amer. Math. Soc., arXiv:1908.09589.
[10] T. Rossmann, *Enumerating conjugacy classes of graphical groups over finite fields* (preprint), arXiv:2107.05564.

Refine, Rip, Repeat - Search in permutation groups

Rebecca Waldecker

Improving backtrack search methods for permutation groups. Let G be a permutation group on a finite set Ω. There are some problems that frequently occur and that, currently, cannot be solved in polynomial time. For example: computing the intersection of two subgroups of G, computing the centraliser or normaliser of a subgroup, or computing the stabiliser of some combinatorial structure (e.g. a graph or a partition).

The state of the art is to perform a so-called backtrack search, which is based on a sophisticated strategy to search for the subgroup in question. This happens in a systematic way and with pruning techniques that keep the search tree as small as possible. This method was first described by Sims [12] and was used to calculate element centralisers and conjugacy classes based on a search method that uses a base and strong generating set. Then it was extended by Leon [7], inspired by and building on work by McKay [9] on graphs. The infrastructure of the search changed from group elements to pairs of ordered partitions, with techniques to refine the partitions, to split the search and to prune the search tree. Leon describes how to solve problems like the computation of subgroup intersections, set stabilisers or subgroup normalisers within his framework. His methods show bad worst case behaviour, but the existing implementations (in GAP [1] and Magma [2]) often perform very well in practice. There is not much hope that problems like subgroup intersection or set stabiliser will ever be solved in polynomial time, given that these problems are at least as difficult as graph isomorphism ([11]), which is why we focus on improving backtrack methods and effective pruning. Theißen demonstrated in his thesis [13] how the performance of normaliser computation can be improved by using orbital graphs. This inspired us to systematically use orbital graphs for refinement during a backtrack search with ordered partitions (joint work with Chris Jefferson and Markus Pfeiffer). Our new refiners in [4] proved to be very effective for several typical search problems – in fact our experiments show that performance can be improved by several orders of magnitude for a range of typical problems. Our results lead to several questions:

(1) Could the search be sped up even more by changing the infrastructure of the search tree, away from ordered partitions?
(2) As orbital graphs are not always effective for refinement, we might investigate other types of graphs. But which ones will be most useful and what are the costs of computing them?
(3) Where are the bottlenecks?

It came as a surprise that, with the new refinement methods, the search involves almost no branching anymore and therefore the algorithms spend most of their time computing stabiliser chains. More substantial progress will therefore depend on faster calculations for stabiliser chains or on ideas that reduce the number of stabiliser chains that need to be computed.

Next we worked on changing the search infrastructure from ordered partitions to stacks of labelled digraphs (joint work with Chris Jefferson, Markus Pfeiffer, and Wilf Wilson, see [6] and [10]). Instead of a search tree where the nodes are pairs of ordered partitions of Ω, we now use pairs of stacks of labelled digraphs with vertex set Ω. One of the advantages is that more information can be used for refinement simultaneously, and hence the existing, very fast algorithms for the computation of graph isomorphisms become even more useful. As in [4], the work in [6] is also accompanied by extensive experiments.

Ongoing and future work. We aim at improving calculations for stabiliser chains (Chris Jefferson, Ruth Hoffmann and others) because there is now substantial evidence that this is a new bottleneck. Also, we want to develop a more conceptual approach to refiners (Chris Jefferson and Wilf Wilson). Therefore, if a new search infrastructure is designed and if it uses a refining technique, then our results about the quality of refiners will likely be applicable in this new context. Indeed, we plan to explore more variety in our backtrack search infrastructure. Among other things, this is relevant for the calculation of normalisers (Chris Jefferson, Mun See Chang, Wilf Wilson). While the computation of normalisers is often possible in Magma with impressive speed, there is still room for improvement in GAP, and we believe that our methods from [6] can be successfully extended in the direction of faster normaliser calculation. Quite a few examples suggest that the addition of extra vertices to the graphs that we use, and an appropriate adaptation of our methods, will lead to substantial improvements. There is also a direct connection between stabiliser problems and conjugacy problems, another class of typical problems with many applications. This ties into our work on minimal and canonical images ([5]), and there is yet unpublished related work that will contribute to the new GAP package `vole` (see [10]).

Finally, I would like to encourage the community to inform me (or Chris Jefferson or Ruth Hoffmann) of examples of hard problems, so that we can challenge the strength of our methods and begin to create a library of examples (for example on the website `GrpLib`, see [10]) against which future developments can be tested.

References

[1] The GAP Group. *GAP – Groups, Algorithms, and Programming,* Version 4.11.1, 2021.
[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.* **24** (1997) 235–265.
[3] Christopher Jefferson and Eliza Jonauskyte. *Images – GAP package,* 2016.
[4] Christopher Jefferson, Markus Pfeiffer, and Rebecca Waldecker. New refiners for permutation group search, *J. Symbolic Comput.* **92** (2019) 70–92.
[5] Christopher Jefferson, Eliza Jonauskyte, Markus Pfeiffer, and Rebecca Waldecker. Minimal and canonical images, *Journal of Algebra* **521** (2019) 481–506.

[6] Christopher Jefferson, Markus Pfeiffer, Rebecca Waldecker, and Wilf A. Wilson. Permutation group algorithms based on directed graphs, *Journal of Algebra* **585** (2021) 723–758. Extended Version: `https://arxiv.org/abs/1911.04783`
[7] Jeffrey S. Leon. Permutation group algorithms based on partitions. I. Theory and algorithms, *J. Symbolic Comput.* **12** (1991) 533–583.
[8] Steve Linton. Finding the smallest image of a set. In *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation,* ISSAC '04, 229-234, New York, NY, USA, 2004. ACM.
[9] Brendan D. McKay. Practical graph isomorphism, *Congr. Numer.* **30** (1980) 45–87.
[10] The PEAL website: PErmutation groups and ALgorithms. `https://peal.github.io/`
[11] Akos Seress. *Permutation Group Algorithms.* Cambridge University Press, 2003.
[12] Charles Sims. Determining the Conjugacy Classes of a Permutation Group. In: *Computers in Algebra and Number Theory,* SIAM-AMS Proc. Vol. IV, Am. Math. Soc., 1971.
[13] Heiko Theißen. *Eine Methode zur Normalisatorberechnung in Permutationsgruppen mit Anwendungen in der Konstruktion primitiver Gruppen*, Ph.D. thesis, RWTH Aachen, 1997.

Hessian matrices, automorphisms of p-groups, and torsion points of elliptic curves

Christopher Voll
(joint work with Mima Stanojkovski)

In my talk I reported on [6]. In this paper, we compute the orders of the automorphism groups of finite p-groups arising naturally via Hessian determinantal representations of certain elliptic curves defined over number fields. We interpret these orders in terms of the numbers of 3-torsion points (or flex points) of the relevant curves over finite fields. Our work greatly generalizes and conceptualizes previous examples given by du Sautoy and Vaughan-Lee [2]. It explains, in particular, why the orders arising in these examples vary with the primes in a "wild", viz. nonquasipolynomial, manner.

The following is a condensed summary of our main results. Given an elliptic curve E and $n \in \mathbb{N}$, we denote by $E[n]$ the n-torsion points of E and write $\mathrm{Aut}_O(E)$ for the automorphism group of E.

Theorem 1. *Let E be an elliptic curve over $\mathbb{Q}$ and let F be a finite field of odd characteristic p over which E has good reduction. Assume that $|E[2](F)| = 4$. Then there exist p-groups $\mathbf{G}_1(F)$, $\mathbf{G}_2(F)$, and $\mathbf{G}_3(F)$ such that the following hold:*

(1) *each $\mathbf{G}_i(F)$ is a group of order $|F|^9$, exponent p, and nilpotency class 2;*
(2) *for each $i = 1, 2, 3$, there exists $T_i \leq E \rtimes \mathrm{Aut}_O(E)$ such that*

$$|\operatorname{Aut}(\mathbf{G}_i(F))| = |F|^{18} \cdot |\operatorname{GL}_2(F)| \cdot |T_i(F)| \cdot |\operatorname{Gal}(F/\mathbb{F}_p)|.$$

Moreover, if $\delta \in F \setminus \{0\}$ is such that $E = E_\delta$ is given by $y^2 = x^3 - \delta x$ over F, then

$$|T_i(F)| = |E_\delta[3](F)| \cdot \gcd(|F| - 1, [\lceil 4/i \rceil])$$

and, for $i \neq j$, the groups $\mathbf{G}_i(F)$ and $\mathbf{G}_j(F)$ are isomorphic if and only if $\{i, j\} = \{2, 3\}$ and $p \equiv 1 \bmod 4$. Any two groups associated with distinct values of δ are non-isomorphic.

We remark that, at least apart from characteristic 3, Theorem 1 covers all elliptic curves over $\mathbb{Q}$ with j-invariant 1728.

We record an arithmetic implication pertaining to groups of the form $\mathbf{G}_i(\mathbb{F}_p)$ as p varies over the set of rational primes Π. Recall, e.g. from [1] or [3], that a set of primes is a *Frobenius set* if it is a finite Boolean combination of sets of primes defined by the solvability of polynomial congruences. A function $f : \Pi \to \mathbb{Z}$ is *Polynomial On Frobenius Sets* (*POFS*) if there exist a positive integer N, Frobenius sets $\Pi_1, \ldots, \Pi_N$ partitioning Π, and polynomials $f_1, \ldots, f_N \in \mathbb{Z}[T]$ such that the following holds: $p \in \Pi_j \iff f(p) = f_j(p)$.

Corollary 1. *Let $\delta \in \mathbb{Z}$ and consider $E = E_\delta$ as in Theorem 1. Let $i \in \{1, 2, 3\}$ and assume that $\delta \in \mathbb{Z}$ is the square of an integer if $i \neq 1$. Then the function $p \mapsto |\operatorname{Aut}(\mathbf{G}_i(\mathbb{F}_p))|$ is POFS.*

Special groups of the form discussed in Theorem 1 (viz. for $E = E_1$, $F = \mathbb{F}_p$ and $i = 1$) were studied in [2], mainly with a view towards their immediate descendants, viz. specific groups of order p^{10} arising from these groups via the p-group generation algorithm [4]. The relevant special case of Corollary 1 was known to the authors of [2]; see (the remarks following) [6, Theorem 1.2]. They also established that, in the special case they studied, the function in Corollary 1 is not *Polynomial On Residue Classes* (*PORC*) (or quasi- or pseudo-polynomial, in combinatorialists' parlance). One of the main contributions of [6] is to connect the variation of the orders of the relevant automorphism groups with the structure of the group of 3-torsion points $E[3]$ of the elliptic curve E, affording an arithmetic interpretation.

We obtain the groups $\mathbf{G}_i(F)$ in Theorem 1 from the elliptic curve E in two steps. First we construct three Hessian linear determinantal representations of E, viz. Hessian 3×3-matrices $\mathrm{B}_i(y_1, y_2, y_3)$ of linear forms in variables y_1, y_2, y_3 whose determinants each define E. More precisely, if f is a homogeneous cubic polynomial defining E as projective curve, it is well-known—essentially by work of Hesse from 1844—that the *Hessian equation*

$$\alpha f = \operatorname{Hes}(\beta f + \operatorname{Hes}(f))$$

has exactly three solutions $(\alpha, \beta) \in \mathbb{C}^2$, yielding pairwise inequivalent linear symmetric determinantal representations of f over the complex numbers $\mathbb{C}$. Here, the *Hessian* (*polynomial*) $\operatorname{Hes}(g)$ of a cubic polynomial g is the determinant $\det(\mathrm{H}(g))$ of the *Hessian matrix* $\mathrm{H}(g) = \left(\frac{\partial^2 g}{\partial y_i \partial y_j}\right)_{ij}$ associated with g. Each of these three solutions gives rise to a Hessian matrix B_i.

Second we associate, in case E is defined over $\mathbb{Q}$, with each of the matrices B_i a 9-dimensional unipotent group scheme $\mathbf{G}_i = \mathbf{G}_{\mathrm{B}_i}$, each defined over a suitable finite extension of $\mathbb{Q}$. Informally speaking, the matrices B_i encode the commutator structures of the resulting groups of rational points. These groups may also be interpreted as Heisenberg groups over commutative algebras whose structure constants are encoded in the matrices B_i.

To prove Theorem 1 we determine which automorphisms of the elliptic curve E are induced by automorphisms of the p-groups $\mathbf{G}_i(F)$. For $E = E_\delta$, we study the

realisability of translations by 3-torsion points of E_δ by elements of $\mathrm{PGL}_3(F)$, viz. $(\mathrm{Aut}\ \mathbb{P}^2)(F)$. We first show that the only translations of E_δ that lift to $\mathrm{PGL}_3(F)$ are those coming from 3-torsion points and then see to the actual realisability of these as linear transformations. A similar phenomenon is discussed in [5, Rem. B]: under suitable assumptions, translations by n-torsion points of genus one curves embedded into $\mathbb{P}^{n-1}$ are induced by linear automorphisms of $\mathbb{P}^{n-1}$.

References

[1] M. Bardestani, K. Mallahi-Karai, and J. Salmasian, *Kirillov's orbit method and polynomiality of the faithful dimension of p-groups*, Compos. Math. **155** (2019), no. 8, 1618–1654.

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

[3] J. C. Lagarias, *Sets of primes determined by systems of polynomial congruences*, Illinois J. Math. **27** (1983), no. 2, 224–239.

[4] E. A. O'Brien, *The p-group generation algorithm*, J. Symbolic Comput. **9** (1990), no. 5-7, 677–698.

[5] C. O'Neil, *Jacobians of genus one curves*, Math. Res. Lett. **8** (2001), no. 1-2, 125–140.

[6] M. Stanojkovski, C. Voll, *Hessian matrices, automorphisms of p-groups, and torsion points of elliptic curves*, Math. Ann. **236** (2021).

Free group homomorphisms and the Post Correspondence Problem

Laura Ciobanu

(joint work with Alan Logan)

The Post Correspondence Problem (PCP) is a classical problem in computer science that can be stated as: is it decidable whether, given two morphisms g and h between two free monoids A and B, there is any nontrivial $x \in A$ such that $g(x) = h(x)$? This question can be phrased in terms of equalisers, asked in the context of free groups F_1 and F_2, and expanded: if the *equaliser* $\mathrm{Eq}(g, h)$ of g and h is defined to be the subgroup consisting of all x where $g(x) = h(x)$, that is,

$$\mathrm{Eq}(g, h) = \{x \in F_1 \mid g(x) = h(x)\},$$

it is natural to wonder not only whether the equaliser is trivial, but what its rank or basis might be.

While the PCP for monoids is famously insoluble [5] and acts as a source of undecidability in many areas of computer science and mathematics, the PCP for free groups is open, as are the related questions about rank, basis, or further generalisations. However, in our work we show that there are links and surprising equivalences between these problems in free groups, and classes of maps for which we can give complete answers.

1. Marked morphisms

Suppose Σ, Δ are finite sets. A set of words $\mathbf{s} \subseteq \Delta^*$ is *marked* if any two distinct $u, v \in \mathbf{s}$ start with a different letter of Δ, which implies $|\mathbf{s}| \leq |\Delta|$. A free monoid morphism $f : \Sigma^* \to \Delta^*$ is *marked* if the set $f(\Sigma)$ is marked. An *immersion of free groups* is a morphism $f : F(\Sigma) \to F(\Delta)$ where the set $f(\Sigma \cup \Sigma^{-1})$ is marked.

Halava, Hirvensalo and de Wolf [3] showed that PCP (for free monoids) is decidable for marked morphisms. In [1], inspired by their methods, we were able to obtain stronger results (Theorem 1) for this kind of map, as well as expand to the world of free groups (Theorem 2), where we employ 'finite state automata'-like objects called *Stallings graphs*.

Theorem 1. *If S is a set of marked morphisms from Σ^* to Δ^*, then there exists a finite alphabet Σ_S and a marked morphism $\psi_S : \Sigma_S^* \to \Sigma^*$ such that* $\mathrm{Image}(\psi_S) = \mathrm{Eq}(S)$. *Moreover, for S finite, there exists an algorithm with input S and output the marked morphism ψ_S.*

Corollary 1. *The simultaneous (for a set of morphisms, rather than just a pair) PCP is decidable for marked morphisms of free monoids.*

Theorem 2. *If S is a set of immersions from $F(\Sigma)$ to $F(\Delta)$, then there exists a finite alphabet Σ_S and an immersion $\psi_S : F(\Sigma_S) \to F(\Sigma)$ such that* $\mathrm{Image}(\psi_S) = \mathrm{Eq}(S)$. *Moreover, when S is finite, there exists an algorithm with input S and output the immersion ψ_S.*

Corollary 2. *The simultaneous (for a set of morphisms, rather than just a pair) PCP is decidable for immersions of free groups.*

2. Variations on the PCP

We write PCPI for the PCP with at least one map injective, in which case the subgroup $\mathrm{Eq}(g, h)$ is finitely generated and a finite description relates to bases: The *Basis Problem* (BP) takes as input a tuple (Σ, Δ, g, h), where $g, h : F(\Sigma) \to F(\Delta)$, and outputs a basis for $\mathrm{Eq}(g, h)$. In [2] we show that the BP is equivalent to the *Rank Problem* (RP), which seeks the number of elements in a basis, and was asked by Stallings in 1984. Recent results settle the BP for certain classes of free group maps [1], but despite this progress its solubility remains open in general. The analogous problem for free monoids, which we call the *Algorithmic Equaliser Problem* (AEP) because it aims to describe the equaliser in terms of automata rather than bases, is insoluble by work of Saarela.

Moreover, in [2] we consider the *generalised* PCP (GPCP), which is an important generalisation of the PCP for both free groups and monoids. For group homomorphisms $g, h : F(\Sigma) \to F(\Delta)$ and fixed elements u_1, u_2, v_1, v_2 of $F(\Delta)$, the GPCP asks if, given an 8-tuple $(\Sigma, \Delta, g, h, u_1, u_2, v_1, v_2)$, there is an $x \in F(\Sigma) \setminus \{1\}$ such that $u_1 g(x) u_2 = v_1 h(x) v_2$. For free monoids, the PCP is equivalent to the GPCP. The corresponding connection for free groups is more complicated, and explaining this connection is the main motivation of our work in [2]. In particular, the GPCP for free groups is known to be undecidable [4, Corollary 4.2] but this proof does not imply that the PCP for free groups is undecidable (because of injectivity issues). In [2] we connect the PCP with the GPCP in free groups via a sequence of implications, and require at least one map to be injective.

3. Open questions

As mentioned in my lecture, the PCP remains open for free groups, even in the rank 2 case. The GPCP is also open if we require at least one map to be injective. There are numerous other problems related to PCP where the decidability status is not known.

However, in the case where decidability was established, such as for marked morphisms (in free monoids) and immersions (in free groups), the next step is to implement the algorithms that solve PCP. At the moment the complexity appears to be exponential, but there are standard tools, like Stallings foldings, that need to be widely available and usable in a range of contexts, including PCP. We hope that we will make progress in this directions in terms of concrete computations.

References

[1] L. Ciobanu and A. Logan, *The Post correspondence problem and equalisers for certain free group and monoid morphisms*, In: 47th International Colloquium on Automata, Languages, and Programming (ICALP 2020), **120**, 1–16.
[2] L. Ciobanu and A. Logan, *Variations on the Post Correspondence Problem for free groups*, 25th International Conference on Developments in Language Theory (DLT 2021), to appear.
[3] Vesa Halava, Mika Hirvensalo, and Ronald de Wolf. *Marked PCP is decidable*, Theoret. Comput. Sci., **255**(1-2), (2001), 193–204.
[4] A. Myasnikov, A. Nikolaev, and A. Ushakov, *The Post correspondence problem in groups*. J. Group Theory **17**(6), (2014), 991–1008.
[5] Emil L. Post, *A variant of a recursively unsolvable problem*, Bull. Amer. Math. Soc., **52**, (1946), 264–268.

Concise presentations and subdirect products of groups

Martin Bridson

It is easy to see that certain groups are finitely presented, for example finite groups, finitely generated abelian groups, and polycyclic groups. In more geometric settings, finite presentations arise from proper co-compact actions on simply connected manifolds or cell complexes. But in situations where one does not have an obvious way of constructing a presentation or a proper co-compact action on a suitable space, determining finite presentation can be a delicate question; $\mathrm{SL}(d,\mathbb{Z})$, mapping class groups of surfaces, and finitely generated metabelian groups provide instructive examples of how non-obvious presentations might be identified in such circumstances, while the difficulty of the challenge is illustrated by the fact that there is no algorithm that can determine which finite subsets of a direct product of two free groups generate finitely presented subgroups.

The train of ideas that begins with the 1-2-3 Theorem of [1] and culminates in the VSP Theorem of [3] (recalled below) provides new criteria for recognising finitely presented groups and constructing finite presentations. The *Binary Subgroup* construction described below is an outgrowth of this train of ideas. It relies on insights that were developed in the quest to understand groups that embed in direct products of free groups, surface groups and, more generally, residually

free groups. In a series of papers leading to [2, 3], the structure of such groups was shown to be determined to a large extent by the finiteness properties of the group. For the purposes of this talk, the most relevant finiteness property, beyond finite presentation, is the following: a finitely generated group G is *weakly of type* $\mathrm{FP}_k(\mathbb{Z})$ (abbreviated wFP_k) if $H_i(G_0, \mathbb{Z})$ is finitely generated for all $i \leq k$ and all $G_0 < G$ of finite index.

Binary Subgroups: I will concentrate on two particular instances of a general construction. The construction can be varied, for example, by replacing the binary expansions of $1, \ldots, m$ with other sets of m distinct binary expansions. The finiteness of the resulting group and its co-nilpotency class (the least c such that $\gamma_c(F^m) < B$) will vary with the sets chosen.

Let $F = F(a_1, \ldots, a_r)$ be a free group of rank r and let F^m be its m-th direct power. We consider two subgroups $B_0(m) < B_1(m) < F^m$. The subgroup $B_0(m)$ is generated by the $r\lfloor 1+\log_2 m \rfloor$ elements $a_{i,j}$ defined as follows: consider the array with m columns and $\lfloor 1 + \log_2 m \rfloor$ rows where column k is the binary expansion of k, with units at the top; for $j = 0, \ldots, \lfloor \log_2 m \rfloor$ let $\varepsilon_j(m)$ be the word in the alphabet $\{0, 1\}$ that is the j-th row; we treat $\varepsilon_j(m)$ as a multi-index and, for each a_i, define $a_{i,j} \in F^m$ to be the element obtained by raising a_i to this index, with the convention $a_i^1 = a_i$ and $a_i^0 = 1$ (the identity). For example, when $m = 18$, the array gives $5r$ words, including, from row ε_1,

$$a_{i,1} = (1, a_i, a_i, 1, 1, a_i, a_i, 1, 1, a_i, a_i, 1, 1, a_i, a_i, 1, 1, a_i).$$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ε_0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
ε_1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1
ε_2	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0
ε_3	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
ε_4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1

Let $B_1(m) = \langle B_0, \delta_1, \ldots, \delta_r \rangle < F^m$, where $\delta_i := (a_i, \ldots, a_i)$. We use the standard notation for the lower central series, $\gamma_1(G) = G$ and $\gamma_{c+1}(G) = [G, \gamma_c(G)]$.

Theorem 1. *For the direct power F_r^m, with $r \geq 2, m \geq 3$,*

(1) *the rank of $B_0(m)$ is $r(\lfloor 1 + \log_2 m \rfloor)$;*
(2) *the rank of $B_1(m)$ is $r(\lfloor 2 + \log_2 m \rfloor)$;*
(3) *$B_0(m)$ contains $\gamma_{m-1}(F^m)$;*
(4) *$B_1(m)$ contains $\gamma_c(F^m)$, where $c = \lfloor 1 + (m-1)/2 \rfloor$;*
(5) *$B_0(m)$ is finitely presented but not of type wFP_3;*
(6) *if $m \leq 4$ then $B_1(m) = F^m$;*
(7) *if $m \geq 5$ then $B_1(m)$ is finitely presented, type FP_3 but not wFP_4;*
(8) *$\forall c \; \exists$ polynomial $p_c(m)$ s.t. $m > p_c(\log_2 m) \implies \gamma_c(F^m) \not\subseteq B_1(m)$.*

Concise Presentations: $\mathbb{Z}^m$ requires m generators and $n(n-1)/2 = \mathrm{rk}H_2(\mathbb{Z}^n, \mathbb{Z})$ relators. But when one removes the homological obstructions to requiring fewer generators and relators, the improvements are dramatic. Philip Hall initiated the study of economical generating sets for direct powers of finite perfect groups and the theory was subsequently developed by Jim Wiegold and others to cover infinite groups. The statement about the growth of generating sets in the following theorem is proved in this literature, the statement about relators is new [4]. Here, $d(K)$ is the minimal number of generators that a group K requires and $\rho(K)$ is the least number of relators in any presentation.

Theorem 2. *Let G be a finitely presented group. If $H_1G = H_2G = 0$, then $d(G^m) = O(\log m)$ and $\rho(G^m) = O(\log m)^3$.*

Theorem 1 allows us to extend the statement about $d(G^m)$ to cover direct products of distinct groups. The group $\overline{B}$ in the following theorem is the image of $B_0(m) < F_r^m$ under the obvious epimorphism.

Theorem 3. *For all $G_1, \ldots, G_m$ with $d(G_i) \leq r$, let $D := G_1 \times \cdots \times G_m$. Then*

$$\exists \overline{B} < D \quad \text{with} \quad d(\overline{B}) \leq r\lfloor 1 + \log_2 m \rfloor \quad \text{and} \quad \gamma_{m-1}(D) < \overline{B}.$$

If the G_i are finitely presented, then so is $\overline{B}$.

Corollary 1. *For G_i perfect, if $d(G_i) \leq r$ then $d(G_1 \times \cdots \times G_m) \leq r\lfloor 1 + \log_2 m \rfloor$.*

Background: The proof of Theorem 1 relies on the following results. Recall that a *limit group* is a finitely generated group Λ that is fully residually free: for every finite $X \subset \Lambda$ there exists a homomorphism $\phi : \Lambda \to F_2$ that is injective on X. Fundamental groups of compact orientable surfaces are limit groups. Recall too that a subgroup of a direct product is termed a *subdirect product* if it projects onto each of the direct factors, and is *full* if it intersects each factor non-trivially.

Theorem 4 ([2])**.** *Let $D = \Lambda_1, \ldots, \Lambda_m$ be product of non-abelian limit groups and $S < D$ a finitely presented, full sub-direct product. Then*

1. *$p_{ij}(S) < \Lambda_i \times \Lambda_j$ has finite index for $1 \leq i < j \leq m$;*
2. *for some $D_0 < D$ of finite index, $\gamma_{m-1}(D_0) < S$;*
3. *$[D : S] = \infty \implies S$ is not of type wFP_k, some $k \leq m$.*

Point (3) was improved by Kochloukova [5] and Kuckuck [6]:

Theorem 5. *For $2 \leq k \leq m$, a full subdirect product of non-abelian limit groups $S < \Lambda_1 \times \cdots \times \Lambda_m$ virtually surjects each k-tuple of factors iff it is wFP_k.*

The converse to (1) holds in great generality.

Theorem 6 (VSP Theorem [3])**.** *Let $S < D := G_1 \times \cdots \times G_m$ be a subdirect product of finitely presented groups. If S satisfies* **VSP***, that is $p_{ij}(S) < G_i \times G_j$ has finite index for $1 \leq i < j \leq m$, then*

1. *S is finitely presented;*
2. *$\gamma_{m-1}(D_0) < S$, some $D_0 < D$ of finite index;*
3. *S is closed in the profinite topology.*

Moreover, $\exists$ **algorithm** *that given finite presentations of* G_i *and a finite set* $\Sigma \subset G_1 \times \cdots \times G_n$ *will construct finite presentation of* $S = \langle \Sigma \rangle$ *if* S *has VSP.*

The algorithm alluded to here is explicit and I would be interested in having a practical implementation of it that covers at least the case where the G_i are free and surface groups and the projections to pairs are surjective.

References

[1] G. Baumslag, M. R. Bridson, C. F. Miller III and H. Short, *Fibre products, non-positive curvature, and decision problems*, Comment. Math. Helv. **75** (2000), 457–477.

[2] M. R. Bridson, J. Howie, C. F. Miller III and H. Short, *Subgroups of direct products of limit groups*, Ann. of Math. **170** (2009), 1447–1467.

[3] M. R. Bridson, J. Howie, C. F. Miller III and H. Short, *On the finite presentation of subdirect products and the nature of residually free groups.* Amer. J. Math., **135** (2013), 891–933.

[4] M. R. Bridson, *Concise presentations of direct products*, Proc. Amer. Math. Soc., DOI: `https://doi.org/10.1090/proc/13991`.

[5] D. H. Kochloukova, *On subdirect products of type* FP_m *of limit groups*, J. Group Theory **13** (2010), 1–19.

[6] B. Kuckuck, *Subdirect products of groups and the* $n - (n+1) - (n+2)$ *conjecture*, Q. J. Math. **65** (2014), 1293–1318.

Condensing the Steinberg module

Gerhard Hiss

(joint work with Thomas Breuer, Frank Lübeck and Klaus Lux)

This work is part of the *Modular Atlas* project, whose aim is the computation of the Brauer character tables associated to the finite simple groups included in the Atlas [1], henceforth called the Atlas groups. By an associated Brauer character table of a simple group G we understand a Brauer character table of the universal covering group of G (which includes the Brauer character table of G), or of the automorphism group of G.

A first portion of these tables, comprising all groups up to the sporadic simple group of McLaughlin, is contained in [4]. Since the publication of this volume, new tables have been computed, which are available online at

`http://www.math.rwth-aachen.de/homes/MOC/`.

Currently, there are 13 simple Atlas groups, of which 7 are sporadic groups, for which not all of the associated Brauer character tables are known.

The work presented here began in 2018. At that time, the smallest non-sporadic simple Atlas group with an unknown Brauer character table was $F_4(2)$, the automorphism group of a simple Lie algebra of type F_4 over the field with 2 elements. This group has a universal covering group $2.F_4(2)$ and an automorphism group $F_4(2).2$. There are also bicyclic extensions of shape $2.F_4(2).2$.

Using Steinberg's tensor product theorem, Veldkamp in [10] determined the Brauer character table of $F_4(2)$ in characteristic 2. In [11], White computed the

Brauer character tables for blocks of $2.F_4(2)$ with cyclic defect groups. The remaining Brauer character tables for $2.F_4(2)$ were established in [3], up to some unknown parameters in characteristic 3.

This talk reports on the resolution of this open case by condensing the Steinberg module of $F_4(2)$. In [9] Steinberg constructed, for any finite group G with a split BN-pair of characteristic p and any integral domain Θ, a ΘG-module St, now called the Steinberg module of G over Θ. This is free as a Θ-module, and its Θ-rank equals the order of a Sylow p-subgroup of G. An explicit basis of St is given in [9], as well as formulae for the entries of the matrix which represents, with respect to this basis, the action of an element of G on St.

Let now $G := F_4(2)$ and $\Theta := \mathbb{F}_3$. We could conclude from our results in [3] that the knowledge of the composition multiplicities in the Steinberg module St of $\mathbb{F}_3 G$ would be enough to complete the Brauer character table of the principal 3-block of G. (The Brauer character tables for the non-principal 3-blocks of $2.G$ could be determined by more elementary means.) Now St has dimension $2^{24} = 16\,777\,216$, which is too large for a direct attack with Richard Parker's MeatAxe64 [7].

To overcome this difficulty, we used condensation methods. As a condensation subgroup we took $K = Z(U_P)$, where U_P is the unipotent radical of a parabolic subgroup P of $F_4(2)$ of type C_3. Now K has order 2^7, and condensing St with the trace idempotent $\iota := 1/|K| \sum_{x \in K} x$ corresponding to K yields the $\iota\, \mathbb{F}_3 G\, \iota$-module $\iota\,\mathrm{St}$ of dimension $2^{17} = 131\,072$, which is feasible for the MeatAxe64. (It is perhaps worthwhile to remark that an analogous condensation subgroup does not exist for the groups $F_4(q)$ for odd q. If P denotes a parabolic subgroup of $F_4(q)$ of type C_3 and U_P its unipotent radical, then $|Z(U_P)| = q^7$ if q is even, and $|Z(U_P)| = q$, if q is odd.)

Let $X \subseteq G$ be such that X contains a set of representatives for the P-P double cosets in $F_4(2)$ as well as a generating set of P modulo K. Then, according to Noeske's criterion [6], the condensation algebra $\iota\, \mathbb{F}_3 G\, \iota$ is generated, as an $\mathbb{F}_3$-algebra, by the elements $\iota x \iota$, $x \in X$. A set X with these properties, containing eleven non-trivial elements, is easily found using the Chevie system [2], largely employing Jean Michel's extensions of Chevie [5]. These are also used to compute the condensed matrices for these eleven elements, i.e. matrices for the action of $\iota x \iota$, $x \in X$ on $\iota\,\mathrm{St}$. One such condensed matrix requires approximately 2.5 GB of memory.

Richard Parker chopped the condensed module $\iota\,\mathrm{St}$ into smaller modules of dimensions around 40 000. These remaining modules were chopped using the C-MeatAxe written by Michael Ringe [8]. This gives a composition series of $\iota\,\mathrm{St}$ as a $\iota\, \mathbb{F}_3 G\, \iota$-module. From the bounds on the parameters given in [3] we can easily check that $\iota\, S \neq 0$ for every composition factor S of St. Thus the composition multiplicities in St and in $\iota\,\mathrm{St}$ agree, yielding our result.

As to the Brauer character tables for the groups $F_4(2).2$ and $2.F_4(2).2$, there are some open problems which we hope to resolve in the near future.

References

[1] 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.

[2] M. Geck, G. Hiss, F. Lübeck, G. Malle, and G. Pfeiffer. CHEVIE — A system for computing and processing generic character tables. *AAECC* **7** (1996), 175–210.

[3] G. Hiss, Decomposition matrices of the Chevalley group $F_4(2)$ and its covering group, *Comm. Algebra* **25** (1997), 2539–2555.

[4] C. Jansen, K. Lux, R. A. Parker and R. A. Wilson, Atlas of Brauer Characters, Oxford Science Publications, 1995.

[5] J. Michel, The development version of the `CHEVIE` package of `GAP3`, *J. Algebra* **435** (2015), 308–336.

[6] F. Noeske, Tackling the generation problem in condensation, *J. Algebra* **309** (2007), 711–722.

[7] R. A. Parker, meataxe64, Matrices over finite fields, `https://meataxe64.wordpress.com/`.

[8] Michael Ringe, The MeatAxe – Computing with Modular Representations, `http://www.math.rwth-aachen.de/~MTX/`.

[9] R. Steinberg, Prime power representations of finite linear groups II, *Canad. J. Math.* **9** (1957), 347–351.

[10] F. D. Veldkamp, Representations of algebraic groups of type F_4 in characteristic 2, *J. Algebra* **16** (1970), 326–339.

[11] D. L. White, Brauer trees of $2.F_4(2)$, *Comm. Algebra* **20** (1992), 3353–3368.

Summary of the Problem Session

Laura Ciobanu.

As already mentioned, the PCP remains open for free groups, even in the rank 2 case. The GPCP is also open if we require at least one map to be injective. There are numerous other problems related to PCP where the decidability status is not known. However, in the case where decidability was established, such as for marked morphisms (in free monoids) and immersions (in free groups), the next step is to implement the algorithms that solve PCP. At the moment the complexity appears to be exponential, but there are standard tools, like Stallings foldings, that need to be widely available and usable in a range of contexts, including PCP. We hope that we will make progress in this directions in terms of concrete computations.

We now list some questions about commutators in linear groups. Suppose G is an infinite linear group, such as $SL(n,\mathbb{Z})$ or $GL(n,\mathbb{Z})$, $n \geq 2$.

Question 1. Is it possible to decide whether given a matrix M in the group G, M can be written as the commutator of two other matrices in G, that is, $M = [A, B]$, where $A, B \in G$?

Question 2. If the answer to Question 1 is positive, what it the complexity of the algorithm and can this be implemented for small n?

The context for Questions 1 and 2 is that there is a nice algorithm for free groups due to Wicks: an element w over the generators X of a free group $F(X)$ is the commutator of two other elements in $F(X)$ if and only if the reduced word

representing w has the form (up to cyclic permutations)

$$\alpha \circ \beta \circ \gamma \circ \alpha^{-1} \circ \beta^{-1} \circ \gamma^{-1},$$

where α, β, γ are reduced words over X and $\circ$ denotes the fact that no cancellation is possible between neighbouring words.

Thus being able to decide whether a matrix M in a linear group G belongs to a free subgroup (with known generators) is enough to answer the questions above. A computational version of the Tits alternative would help with this part, and this leads to the following.

Question 3. Given a linear group G and matrix $M \in G$, is it possible to determine whether M belongs to a (non-trivial) free subgroup of G, and if the answer is positive, find the basis of this free subgroup.

For $n = 2$ the matrix groups will be virtually free, that is, they contain a free subgroup of finite index, and the questions here are known to be decidable. However, using matrices directly instead of generators for $SL(2, \mathbb{Z})$ or $GL(2, \mathbb{Z})$ presents an interesting additional challenge. For $n \geq 3$ nothing appears to be known regarding any of the questions.

Finally, Question 1 is known to be undecidable in (examples of) nilpotent groups of class 2 by work of Roman'kov, so this is a difficult question for arbitrary groups.

Bettina Eick.

The classification of p-groups of maximal class is a long standing problem in group theory. It was initiated by Blackburn who obtained a full classification for $p \in \{2, 3\}$. For primes $p \geq 5$ this classification has been investigated in many publications and it is still widely open.

Leedham-Green & McKay introduced the *constructible groups*. These form an large and important subset of the groups of maximal class. Their construction translates the isomorphism problem for these groups to an interesting problem in algebraic number theory.

To describe the algebraic number theory setting in detail, write $\mathbb{Q}_p$ and $\mathbb{Z}_p$ for the p-adic rational and integral numbers, respectively, let θ be a primitive p-th root of unity over $\mathbb{Q}_p$ and let $K = \mathbb{Q}_p(\theta)$. Let U denote the unit group of the maximal order of K and let G be the split extension of U by the Galois group of K. Then there is a full $\mathbb{Z}_p$-lattice Γ in the vector space $K^{(p-3)/2}$ so that the isomorphism problem for constructible groups translates to the problem of determining orbits of the infinite group G on the finite quotients $(\theta - 1)^n\Gamma/(\theta - 1)^{n+e}\Gamma$. Details on the translation can also be found in a recent paper by Dietrich & Eick.

It is an open problem to investigate these orbits by computational methods for varying n and e. For example, it would be useful to have methods to compute with algebraic number fields over $\mathbb{Q}_p$, their unit groups and Galois groups.

Meinolf Geck and Gunter Malle.

The Cambridge ATLAS and/or the libraries of computer algebra systems like GAP and MAGMA contain the character tables of some of the finite Chevalley groups of exceptional type, like $F_4(2)$. Of course, eventually, we would like to construct

the "generic" character table for the underlying infinite family of groups, i.e., in this case $F_4(2^f)$ for any integer $f \geq 1$. The theoretical framework for doing this is provided by Lusztig's geometric character theory, developed in the 1980s; see [3] for a recent survey. Now, certain issues arising in the "generic" context can be resolved using explicitly computed information for individual members of those infinite families; see [1], [2] for examples of this procedure. Thus, while posing an interesting computational challenge in itself, the knowledge of the character tables of individual groups like $F_4(2)$ is also very helpful from a theoretical point of view. As far as yet unknown character tables of Chevalley groups of exceptional type are concerned, we find the following numbers for their sizes:

$$|\mathrm{Irr}(F_4(3))| = 273, \quad |\mathrm{Irr}(E_6(3))| = 1269, \quad |\mathrm{Irr}({}^2E_6(3))| = 1389,$$
$$|\mathrm{Irr}(E_7(2))| = 531, \quad |\mathrm{Irr}(E_7(3)_{\mathrm{sc}})| = 5052,$$
$$|\mathrm{Irr}(E_8(2))| = 1156, \quad |\mathrm{Irr}(E_8(3))| = 12825, \quad |\mathrm{Irr}(E_8(5))| = 519071.$$

(This list appears in [3, App. A.3]; it is compiled using Lübeck's online data [4].) Thus, it might be within reach to determine the individual character tables of $F_4(3)$ and $E_7(2)$ ...

References

[1] M. Geck, *On the values of unipotent characters in bad characteristic*, Rend. Cont. Sem. Mat. Univ. Padova **141** (2019), 37–63.

[2] M. Geck, *Computing Green functions in small characteristic*, J. Algebra **561** (2020), 163–199.

[3] M. Geck and G. Malle, *The character theory of finite groups of Lie type: A guided tour*, Cambridge Studies in Advanced Mathematics **187**, Cambridge University Press, 2020.

[4] F. Lübeck, *Data for finite groups of Lie type and related algebraic groups*, available at `http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/index.html`.

Tommy Hofmann.
The following problem makes an appearance when investigating algorithmic questions related to a theorem of Eichler from number theory. Let $G = \langle g_1, \ldots, g_l \rangle \leq \mathrm{GL}_n(\mathbf{F}_q)$ be a finite matrix group, $v \in \mathbf{F}_q^n$ and $w \in G.v$ an element of the orbit of v under G. Is there an efficient way to find an element $g \in G$, as a word in the generators $g_1, \ldots, g_l$, such that $g.v = w$? If not, is there an affirmative answer in the case $G = \mathrm{GL}_n(\mathbf{F}_q)$? In typical applications n is small and q will be large so that an orbit enumeration or a naive search is infeasible.

Alexander Hulpke.
I hope this is somewhat a minimal formulation of a problem, which of course has obvious extensions.

Let $G = \langle g_1, g_2, \ldots, g_k \rangle \leq \mathrm{SL}_n(\mathbb{Z})$. A useful class of homomorphisms defined on G are congruence homomorphisms. For $n \geq 3$ and $[\mathrm{SL}_n(\mathbb{Z}) : G]$ finite, every homomorphism from G onto a finite group factors through such a congruence homomorphism, but we do not assume that this index is finite. (In fact, the reason for the question is an attempt to use noncongruence homomorphisms to certify infinite index in some cases.)

Now let H be a small finite group – already the case of $|H| = 2$ is interesting. Suppose someone (an unreliable oracle) gave us a map, defined on the generators of G, that maps these generators to a generating set of H. Is there any way to test/verify whether this map extends to a homomorphism? (Of interest is of course the case when it does not factor through a congruence homomorphism.)

Christopher Jefferson, Rebecca Waldecker, and Mun See Chang.

Question. Let $G \leq \mathrm{Sym}(\Omega)$. We say that a vertex and edge coloured graph Γ with vertex set $V \supseteq \Omega$ and edge set E *represents* G if and only if the automorphism group $\mathrm{Aut}(\Gamma)$ satisfies:

- Ω is a union of orbits of $\mathrm{Aut}(\Gamma)$, and
- the restriction of $\mathrm{Aut}(\Gamma)$ to Ω is G.

What is the smallest graph (where size is measured as $|V|+|E|$) which represents a group G?

Example. Consider the group $G = \langle (1,2,3), (1,2), (1,4)(2,5)(3,6) \rangle$. This group can be represented by the graph with vertex set $\{1, 2, \ldots, 8\}$ and edge set

$$\{\{1,7\},\{2,7\},\{3,7\},\{4,8\},\{5,8\},\{6,8\}\}.$$

The automorphism group of this graph is $\langle (1,2,3), (1,2), (1,4)(2,5)(3,6)(7,8) \rangle$.

Background. When solving problems such as group intersection, stabiliser and normaliser, a standard technique which keeps appearing is approximating permutation groups as the automorphism groups of various combinatorial structures – where "approximation" means that these automorphism groups are *supergroups* of the groups we want to consider.

Leon [4] approximated groups by considering the automorphisms of ordered partitions.

This was recently extended by approximating permutation groups on a set Ω with the automorphism group of an edge-labelled directed graph on Ω [3]. Such an approximation works perfectly if G is 2-closed, because then we just use the orbital graphs.

The implementation of [3] allows adding extra vertices – these are currently used in various constructions:

- We can build graphs whose automorphism group is the stabiliser of combinatorial objects such as sets of sets, or sets of tuples – in general any data structure recursively built from sets and tuples.
- The normaliser of a group G stabilises the *set* of orbital graphs of a group G. This cannot, in general, be represented as a graph on Ω, so previous work in this area by Theißen [7] had to find a single orbital graph (or union of small number of orbital graphs) which is stabilised by the normaliser. We can instead build a larger graph whose automorphisms are exactly those permutations which stabilise the set of orbital graphs.

- Some permutation groups are not 2-closed, but are 2-closed with respect to a different action. For example, consider the set S of images of the set $\{1,2,3\}$ under the group `G=TransitiveGroup(20,1024)`. Now $|S| = 40$, and the action of G on S is faithful. Furthermore, G is 2-closed with respect to this action.

We know that for all groups we can built such graphs, but the general construction is $O(|G|)$. We can also produce some lower bounds, for example the alternating group on n points cannot be represented with a number of extra vertices that is polynomial (in n).

We are interested in a variety of sub-questions, including:

(1) Which classes of groups can be represented with graphs where $|V| + |E|$ is $O(|\Omega|)$, $O(|\Omega| \log(|\Omega|))$, or a low-order polynomial in $|\Omega|$?
(2) What methods are used to make such constructions?
(3) How can we quickly find such representations?
(4) Where the group cannot be compactly represented, can low-index supergroups be represented? For example, in practice we often find that subgroups of the alternating group cannot be represented, but index-2 supergroups can be.

References

[1] S. Huczynska, C. Jefferson, and S. Nepšinská, *Strong external difference families in abelian and non-abelian groups*, Cryptogr. Commun. **13** (2021), no. 2, 331–341.
[2] C. Jefferson, E. Jonauskyte, M. Pfeiffer, and R. Waldecker, *Minimal and canonical images*, J. Algebra **521** (2019), 481–506.
[3] C. Jefferson, M. Pfeiffer, W. A. Wilson, and R. Waldecker, *Permutation group algorithms based on directed graphs*, J. Algebra **585** (2021), 723–758.
[4] J. Leon, *Permutation group algorithms based on partitions. I. Theory and algorithms*, J. Symbolic Comput. **12** (1991), no. 4–5, 533–583.
[5] S. Linton, *Finding the smallest image of a set*, Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, 229–234.
[6] B. McKay and A. Piperno, *Practical graph isomorphism, II*, J Symbolic Comput. **60** (2014), 94–112.
[7] H. Theißen, *Eine Methode zur Normalisatorberechnung in Permutationsgruppen mit Anwendungen in der Konstruktion primitiver Gruppen. PhD thesis*, RWTH Aachen, 1997.

Tobias Rossmann.

Let Γ be a (finite, simple) graph with distinct vertices $v_1, \dots, v_n$. Let p be an odd prime. Define a p-group

$$\mathbf{G}_\Gamma(\mathbf{F}_p) := \big\langle x_1, \dots, x_n \mid [x_i, x_j] = 1 \text{ whenever } v_i \not\sim v_j, \\ \text{class} \leq 2, \text{ exponent dividing } p \big\rangle;$$

these groups go by various names in the literature.

What does the ordinary representation theory of $\mathbf{G}_\Gamma(\mathbf{F}_p)$ look like? In particular, given Γ and $i \geq 1$, how does $\#\{\chi \in \mathrm{Irr}(\mathbf{G}_\Gamma(\mathbf{F}_p)) : \chi(1) = p^i\}$ behave as a function of p?

This problem is equivalent to counting matrices of given rank in $M_\Gamma(\mathbf{F}_p) := \{A = [a_{ij}] \in \mathrm{M}_n(\mathbf{F}_p) : A = -A^\top,\ a_{ij} = 0 \text{ whenever } v_i \not\sim v_j\}$ as a function of p. It is known that the number of conjugacy classes of size p^i of $\mathbf{G}_\Gamma(\mathbf{F}_p)$ is given by a polynomial in p (for fixed Γ and i).

James B. Wilson.
Question. Let K be a field and $U_1, \dots, U_\ell$ finite-dimensional K-vector space. Given $t \in U_1 \otimes \cdots \otimes U_\ell$, decide if there is an $n > 4$ and a homomorphism $\rho : \mathrm{Alt}(n) \to \mathrm{GL}(U_1) \times \cdots \times \mathrm{GL}(U_\ell)$ such that for each $x \in \mathrm{Alt}(n)$,

$$t(\omega_1 \otimes \cdots \otimes \omega_\ell) = t, \qquad \rho(x) = (\omega_1, \dots, \omega_\ell).$$

Context. The target of interest is the group

$$\mathrm{Aut}(t) = \{(\omega_1, \dots, \omega_\ell) \in \mathrm{GL}(U_1) \times \cdots \times \mathrm{GL}(U_\ell) \mid t(\omega_1 \otimes \cdots \otimes \omega_\ell) = t\}.$$

There are methods to decide if a (quasi-)simple group of Lie type acts, for example by solving linear equation for the algebra of derivations

$$\mathrm{Der}(t) = \{(\omega_1, \dots, \omega_\ell) \in \mathrm{GL}(U_1) \times \cdots \times \mathrm{GL}(U_\ell) \mid 0 = t(\omega_1 \otimes \cdots \otimes 1) + \cdots + t(1 \otimes \cdots \otimes \omega_\ell)\}.$$

However, there is no apparent tool to distinguish between the action by a solvable $\mathrm{Aut}(t)$ and an alternating action. We would like to know ways to inspect t and determine if it admits the action by an alternating group.
Question. Compute a tighter lower bound for

$$\begin{aligned}\mathrm{Prob}(&T_1, \dots, T_c \in \mathbb{M}_{a \times b}(K) \mid \\ &\text{if } (F, G) \in \mathbb{M}_a(K) \times \mathbb{M}_b(K) \text{ where } (\forall i).(FT_i = T_iG) \\ &\text{then } (\exists \lambda \in K)((F, G) = (\lambda I_a, \lambda I_b)) \\ &)\end{aligned}$$

This bound is used to time various randomized isomorphism tests and also in group enumeration. Its estimates are so far either too small causing for slower algorithms or large enough but only when the scalars map into a large extension of K. Tighter bounds over the base field are desired.

Reporter: Joshua Maglione

Participants

Prof. Dr. Laszlo Babai
Dept. of Mathematics & Computer Science
The University of Chicago
Ryerson Hall
1100 East 58th St.
Chicago, IL 60637
UNITED STATES

Prof. Dr. Laurent Bartholdi
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstrasse 3-5
37073 Göttingen
GERMANY

Dominik Bernhardt
Lehrstuhl für Algebra und Darstellungstheorie
RWTH Aachen
Pontdriesch 10-16
52062 Aachen
GERMANY

Prof. Dr. Emmanuel Breuillard
Department of Pure Mathematics and Mathematical Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Prof. Dr. Martin R. Bridson
Mathematical Institute
Oxford University
Andrew Wiles Building
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

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

Prof. Dr. John J. Cannon
School of Mathematics and Statistics
The University of Sydney
Sydney NSW 2006
AUSTRALIA

Mun See Chang
School of Computer Science
University of St. Andrews
North Haugh
St. Andrews Fife KY16 9SS
UNITED KINGDOM

Dr. Laura Ciobanu-Radomirovic
Department of Mathematics
Heriot-Watt University
Riccarton
Edinburgh EH14 4AS
UNITED KINGDOM

Dr. Matthew Conder
Department of Mathematics
The University of Auckland
Auckland 1010
NEW ZEALAND

Dr. David A. Craven
School of Mathematics
The University of Birmingham
Edgbaston
Birmingham B15 2TT
UNITED KINGDOM

Dr. Willem A. de Graaf
Dipartimento di Matematica
Università di Trento
Via Sommarive 14
38050 Povo (Trento)
ITALY

Dr. Alla Detinko
School of Mathematics and Physical Sciences
University of Hull
Cottingham Road
Hull HU6 7RX
UNITED KINGDOM

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

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

Prof. Dr. Murray Elder
School of Mathematical and Physical Sciences
University of Technology Sydney
P.O. Box 123
Broadway NSW 2007
AUSTRALIA

Prof. Dr. Claus Fieker
Fachbereich Mathematik
Technische Universität Kaiserslautern
Postfach 3049
67653 Kaiserslautern
GERMANY

Prof. Dr. Dane Flannery
Mathematics Department
National University of Ireland, Galway
University Road
Galway H91 TK33
IRELAND

Prof. Dr. Meinolf Geck
Fachbereich Mathematik
Lehrstuhl für Algebra
Universität Stuttgart
Pfaffenwaldring 57
70569 Stuttgart
GERMANY

Prof. Dr. Gerhard Hiß
Lehrstuhl für Algebra und Zahlentheorie
RWTH Aachen
Pontdriesch 14-16
52062 Aachen
GERMANY

Dr. Tommy Hofmann
Fachbereich Mathematik
Technische Universität Kaiserslautern
Postfach 3049
67653 Kaiserslautern
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
Technische Universität Kaiserslautern
Gottlieb-Daimler-Strasse Building 48
67633 Kaiserslautern
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 Computer Science
University of St. Andrews
North Haugh
St. Andrews Fife KY16 9SX
UNITED KINGDOM

Dr. Markus Kirschmer
Institut für Mathematik
Universität Paderborn
Warburger Str. 100
33098 Paderborn
GERMANY

Prof. Dr. Alex Kontorovich
Department of Mathematics
Rutgers University
Hill Center, Busch Campus
110 Frelinghuysen Road
Piscataway NJ 08854-8019
UNITED STATES

Dr. Melissa Lee
Department of Mathematics
The University of Auckland
Auckland 1010
NEW ZEALAND

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. Martin W. Liebeck
Department of Mathematics
Imperial College of Science,
Technology and Medicine
180 Queen's Gate, Huxley Bldg.
London SW7 2BZ
UNITED KINGDOM

Prof. Dr. Markus Lohrey
Department für Elektrotechnik und Informatik
Universität Siegen
Hölderlinstraße 3
57076 Siegen
GERMANY

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
Fakultät für Mathematik
Universität Bielefeld
Postfach 10 01 31
33501 Bielefeld
GERMANY

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

Dr. Tobias Moede
Institut für Analysis und Algebra
Technische Universität Braunschweig
Universitätsplatz 2
38106 Braunschweig
GERMANY

PD Dr. Jürgen Müller
Lehrstuhl für Algebra und Zahlentheorie
RWTH Aachen
Pontdriesch 14/16
52062 Aachen
GERMANY

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
School of Mathematics
Monash University
Wellington Road
3800 Clayton
AUSTRALIA

Richard A. Parker
70 York Street
Cambridge CB1 2PY
UNITED KINGDOM

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

Prof. Dr. Alan W. Reid
Department of Mathematics
Rice University
MS 136
Houston TX 77005-1892
UNITED STATES

Dr. Colva M. 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 Mathematics, Statistics and
Applied Mathematics
National University of Ireland, Galway
University Road
Galway H91 TK33
IRELAND

Dr. Csaba Schneider
Departamento de Matemática - ICEX
Universidade Federal de Minas Gerais
Caixa Postal 702
Av. Antonio Carlos, 6627
Belo Horizonte 31270-901
BRAZIL

Prof. Dr. Pascal Schweitzer
Fachbereich Mathematik
Technische Universität Kaiserslautern
Postfach 3049
67653 Kaiserslautern
GERMANY

Prof. Dr. Michael R. Vaughan-Lee
Scotland
Gaitgil House
Twynholm
Kirkcudbright DG6 4PH
UNITED KINGDOM

Prof. Dr. Leonard H. Soicher
School of Mathematical Sciences
Queen Mary University of London
Mile End Road
London E1 4NS
UNITED KINGDOM

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

Prof. Dr. Dr. Katrin Tent
Institut für Mathematische Logik und
Grundlagenforschung
Universität Münster
Einsteinstrasse 62
48149 Münster
GERMANY

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

Prof. Dr. Ulrich Thiel
Fachbereich Mathematik
T.U. Kaiserslautern
Erwin-Schrödinger-Straße
67653 Kaiserslautern
GERMANY

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