Mathematisches Forschungsinstitut Oberwolfach

Report No. 37/2016

DOI: 10.4171/OWR/2016/37

Computational Group Theory

Organised by
Bettina Eick, Braunschweig
Gerhard Hiß, Aachen
Derek Holt, Coventry
Eamonn O'Brien, Auckland

31 July – 6 August 2016

Abstract. This was the seventh workshop on Computational Group Theory. It showed that Computational Group Theory has significantly expanded its range of activities. For example, symbolic computations with groups and their representations and computations with infinite groups play a major role nowadays. The talks also presented connections and applications to cryptography, number theory and the algorithmic theory of algebras.

Mathematics Subject Classification (2010): 20xx,11-04,11Hxx,13-04,13A50,16Zxx,17-04,17Bxx, 18-04,18Gxx, 37F10,68-04,68Nxx,68Wxx.

Introduction by the Organisers

This workshop on *Computational Group Theory* was the seventh of this title held at Oberwolfach. It had 53 participants and, among these, four Oberwolfach Leibniz Graduate Students who visited Oberwolfach for the first time.

The program of this workshop consisted of four long survey talks, a variety of research talks, and some short talks. A highlight was its problem session which exhibited various new possible directions of research. It also featured a session with software demonstrations. The short talks included talks by the Oberwolfach Leibniz Graduate Students and thus allowed these young students to present their current research projects to an international audience.

The four long survey talks were invited by the organisers. The speakers of these talks were selected to give a broad overview on a current theme. The first of these talks was by Alexei Myasnikov *Complexity of the conjugacy problem in groups and cryptography.* It exhibited various interesting applications of the algorithmic theory of non-commutative groups to cryptography and it discussed a selection of open problems in this area. The second survey talk was by Willem de Graaf (*Generators for arithmetic groups*). It gave an overview on the state of the art on the central problem of finding generators for an explicitly given arithmetic group. A practical solution of this problem in the area of infinite matrix groups would have many significant applications. James Wilson (*Group isomorphism is tied up in knots*) gave a survey talk on the isomorphism problem for finite groups. This is particularly interesting due to its connection to the recent developments by Laszlo Babai on the highly interesting graph isomorphism problem. The fourth survey talk was given by Derek Holt (*A new method for verifying hyperbolicity of finitely presented groups*). It reported on a long standing project in the area of computations with finitely presented groups and its recent successful new developments.

The 21 research talks of this workshop were 30 minutes long and covered a broad range of topics. They showed that the research in Computational Group Theory has significantly expanded in recent years. Robert Wilson reported on the classification of maximal subgroups of sporadic groups, in particular considering the only remaining open case: the Monster. The talks by Liebeck, Ryba and Praeger were related to the matrix group recognition project. This major project has been initiated by Joachim Neubüser on the 4th Oberwolfach workshop on computational group theory and it still is of great significance today. Leedham-Green reported on some possible applications of this project. Computational group theory has various connections to representation theory and this has been exhibited by the very interesting talks of Geck, Malle and Magaard. Cannon discussed the powerful algorithm of Unger to construct character tables of finite groups and its applications in the construction of modular representations. A highlight was the talk by Detinko who reported on very significant recent advances in the area of practical algorithms for infinite matrix groups. This talk also showed that there are highly interesting new challenges in the area of infinite matrix groups. Computational aspects of the theory of p-groups were discussed in the talks by Dietrich, Röhrle and Vaughan-Lee. These talks underline that the algorithmic theory for p-groups has expanded in recent years from computations with individual p-groups to different types of symbolic computations. This has led to deep new results in the area, but it also opens up new, deep and interesting challenges for computational group theory. Computations with finitely presented groups is an area in computational group theory that has its roots in the very beginning of the research area and still has many interesting open problems today. New methods in this area were presented in the talk by Nebe. Applications of computational group theory in the computation of zeta functions of groups were discussed in the closely related talks by Rossmann and Voll. Pfeiffer and Kreuzer both considered different aspects of computational methods for Burnside rings of groups. Computational group theory and computations with various types of algebras are adjacent areas and the talks by Niemeyer and Shpectorov presented two completely different aspects of this. Finally, the connection between computational group theory and algorithmic number theory was underlined in the talk by Fieker.

The talks as well as the problem session and the software session were very well received by the participants. Our schedule left plenty of time for discussions. This time was used by many participants to initiate new projects, develop new research ideas and discuss new collaborations. This aspect of the workshop was certainly also a major highlight of this workshop and will no doubt lead to many new and interesting projects in computational group theory in the future.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1049268, “US Junior Oberwolfach Fellows”. Moreover, the MFO and the workshop organizers would like to thank the Simons Foundation for supporting Heiko Dietrich in the “Simons Visiting Professors” program at the MFO.

Workshop: Computational Group Theory

Table of Contents

Abstracts

Complexity of the conjugacy problem in groups and cryptography

Alexei G. Myasnikov

In this talk I discuss various aspects of complexity of the conjugacy problem in infinite groups and its relations to public key cryptography.

To see what kind of properties group-based cryptography requires from the conjugacy problem in groups we consider an example of a group-based public key-exchange scheme. In 2000 Ko and Lee introduced the following conjugacy-based analogue of Diffie-Hellman scheme: a group G, a fixed $q \in G$, and two commuting subgroups $A, B \leq G$ are public. Alice takes $a \in A$ and publishes: $a^* = a^{-1}qa = q^a$ (keeping a secret). Bob, likewise, takes $b \in B$ and publishes $b^* = b^{-1}qb = q^b$. Then they both can get the same element in G, their common private key $(b^*)^a = (q^b)^a = q^{ba} = q^{ab} = (a^*)^b$. To hide the private keys a, b when publishing the elements $a^{-1}qa, b^{-1}qb$, one needs to "scramble" the words $a^{-1}qa$ and $b^{-1}qb$ by taking its "normal form" in the group G. This also allows Alice and Bob to get precisely the same common private key (as a word, not an element of G) by taking the normal form of the element $(b^*)^a = (a^*)^b$.

This brings several obvious requirements on G to make the scheme work: G should have easily computable normal forms of elements (hence the word problem is easy) and the conjugacy problem (CP) in G should be "hard to solve". In fact, immediately we see a new twist, here one needs hardness of the *Search conjugacy problem (SCP)*, when the task is to find a conjugator (already knowing that it exists), while in the classical decision CP one needs to check whether two given elements in G are conjugate. A bit more careful consideration reveals that tacitly it is assumed here that the security of the scheme is based on two things: that breaking the scheme gives a practical algorithm to solve the search CP, and also that the search CP is a "one-way" function, i.e., for a given a it is easy to compute the normal form of q^a and when given the normal form a^* of q^a and the element q it is hard to find x with $q^x = a^*$. Furthermore, since the element $q \in G$ is fixed we are dealing here with the *Individual Conjugacy Problem (ICP)*: equations of the type $q^x = y$ have to be solved for x where $q \in G$ is fixed and $y \in G$ is arbitrary. Another group-based crypto scheme, the so-called AAG (Anshel-Anshel-Goldfeld) scheme, brings into the play one more version of CP in groups, the *Simultaneous Conjugacy Problem* when the task is to solve a system $a_1^x = b_1, \ldots, a_n^x = b_n$ of conjugacy equations in G. Complexity of these three versions of CP in groups was the focus of an intense research during the last two decades, which produced a host of remarkable results. And yet another very important development in algorithmic group theory (now also in the theory of algorithms and recursion theory) is underway, which is closely related to the security of the schemes above. Namely, to avoid the standard "statistical attacks" one has to choose in the scheme above all the "keys" a, b and public "parameters" q, A, B randomly. This changes the whole picture rather dramatically. Indeed, in this case we are not interested in complexity on all inputs of the problem (the worst-case complexity), but only on the random, most typical, *generic* inputs. To explain, let X^* is the set of all words in a finite alphabet X and X_n^* the finite subset of all words of length at most n. For a subset $S \subseteq X^*$ define $\rho_n(S) = \frac{|S \cap I_n|}{|I_n|}$, so $\rho_n(S)$ is the probability to hit S by choosing randomly and uniformly from X_n^*. The *asymptotic density* of S is the limit (if it exists) $\rho(S) = \lim_{n\to\infty} \rho_n(S)$. In this set-up S is called *generic* (*negligible*) if $\rho(S) = 1$ ($\rho(S) = 0$). Perhaps even more important, S is called *exponentially generic/negligible* if $\rho_n(S)$ goes to its limit exponentially fast. Now to understand the generic behaviour of an algorithmic problem it suffices to consider *generic decision or search algorithms*, which are correct partial decision/search algorithms with generic halting sets. This leads to a generic complexity, i.e., the complexity based on generic algorithms. It is important to mention that the generic complexity is rather different from the average-case complexity. Indeed, if a problem is easy on average then it is easy generically, but if a problem is hard on average it does not mean it is hard on most inputs. In fact, as was explained by Gurevich, the average-case analysis describes the trade-off between the time of computation on hard instances and the measure of the subset of these hard instances. Generic complexity is much more suitable in crypto applications. In my talk I discuss some recent results that illustrate all these new developments in algorithmic group theory.

Canonical realisations of finite Chevalley groups

Meinolf Geck

Let $\mathfrak{g}$ be a semisimple complex Lie algebra and G_K be a corresponding Chevalley group over a field K. For various applications, it is useful to be able to write down explicit matrix representations for $\mathfrak{g}$ and G_K; such applications include, for example: the computation of nilpotent orbits and unipotent classes (especially in bad characteristic); the determination of composition multiplicities in Weyl modules for finite Chevalley groups; or algorithmic questions in the "matrix group recognition project".

The traditional construction of G_K relies on the choice of certain signs for a Chevalley basis of $\mathfrak{g}$. There are algorithms to make consistent choices, using so-called "special/extra-special" pairs of roots; see Carter [1]. Recently, Lusztig [5] simplified this construction, by using a highly remarkable basis of the adjoint representation of $\mathfrak{g}$ on which the Chevalley generators $e_i, f_i \in \mathfrak{g}$ act via explicitly given matrices with entries in $\mathbb{N}_0$ (in particular, no signs involved at all!). That basis can in fact be interpreted as a "canonical basis" (in the sense of the theory of quantum groups). In [2] we observed that this idea also leads to a new, and quite elementary construction of $\mathfrak{g}$ itself from its root system. Furthermore, this set-up explicitly determines two Chevalley bases of $\mathfrak{g}$ in terms of the two "canonical" orientations of the Dynkin diagram of $\mathfrak{g}$ in which every vertex is either a sink or a source. (Thus, no need any more to work with "special/extra-special" pairs of roots!)

Finally, note that Lusztig's simplified construction yields groups G_K of adjoint type (e.g., $\mathrm{PGL}_n(K)$). In [3], it is shown that there is an analogous simplification for groups G_K which are not necessarily of adjoint type (e.g., $\mathrm{Spin}_n(K)$). This relies on Jantzen's description [4] of "canonical" models for the minuscule highest weight representations of $\mathfrak{g}$.

The resulting matrix representations of G_K (adjoint or non-adjoint) are completely explicit and can be easily implemented on a computer.

References

[1] R. W. Carter, *Simple groups of Lie type*, Wiley, New York, 1972.

[2] M. Geck, *On the construction of semisimple Lie algebras and Chevalley groups*, preprint at `arXiv:1602.04583`.

[3] M. Geck, *Minuscule weights and Chevalley groups*, preprint at `arXiv:1603.07179`.

[4] J. C. Jantzen, *Lectures on quantum groups*, Graduate Studies in Mathematics, **6**. Amer. Math. Soc., Providence, RI, 1996.

[5] G. Lusztig, The canonical basis of the quantum adjoint representation, preprint at `arXiv:1602.07276`.

On the number of p'-degree characters of a finite group

Gunter Malle

In the talk we presented the following joint result with Attila Maróti:

Theorem. *Let G be a finite group and p a prime divisor of its order. Then the number of irreducible characters of G of degree prime to p is at least $2\sqrt{p-1}$.*

We also discussed the case when equality occurs; then the structure of G is quite restricted.

The proof of our result relies on a corresponding lower bound, due to Maróti, for the number of conjugacy classes of a finite group, as well as on the classification of finite simple groups. It is also tightly connected to the McKay conjecture, which relates the number of p'-degree characters of a group to those of the normalizer of a Sylow p-subgroup.

We ended by phrasing several open questions. For example, one might ask whether the stated bound holds for the number of irreducible characters in any p-block of G with non-trivial defect. Furthermore, a similar bound, linear in p, might hold if we assume that p^2 divides the order of G.

A method for building permutation representations of finitely presented groups

Gabriele Nebe
(joint work with Richard Parker and Sarah Rees)

Let $G = \langle X \mid R \rangle$ be a finitely presented group such that $X = X^{-1}$. Then **jump data** (C, J, S) for X consists of

- a finite set C, the **cement**, with an involution $\bar{\ }$ and a map $\xi : C \to X$ such that $\xi(c)^{-1} = \xi(\overline{c})$ for all $c \in C$,
- defining the **jumps** $J = \{j(c) = (c, \xi(c), \overline{c}) \mid c \in C\}$
- and a set $S \subset C \times F(X) \times C$ of **stays** so that for any two $(c, \mathsf{w}_1, c_1) \neq (c, \mathsf{w}_2, c_2) \in S$ then w_1 and w_2 are incomparable.

The jump data is **compatible with** R if for each $r \in R$, for each $c \in C$, and for each position k, where $\xi(c)$ occurs in r, the k-th cyclic shift r_k of r can be factorised as a product

$$(\star)\ \xi(c_1)\mathsf{w}_1\xi(c_2)\mathsf{w}_2 \cdots \xi(c_s)\mathsf{w}_s$$

with $c_1 = c$ and $(\overline{c_j}, \mathsf{w}_j, c_{j+1}) \in S$ (where addition is taken mod s) for all j.

Assume that jump data is given that is compatible with R. We designed and implemented an algorithm, the **brick finder algorithm**, that constructs transitive cemented partial permutation representations of G, the **bricks**. These bricks may be combined to construct (usually infinitely many) transitive permutation representations of G, where the law to combine bricks is given be a permutation representation of the associated **jump groupoid** defined as follows.

(a) The stays define a graph, where the vertices are the elements of C. Two vertices c_1, c_2 are connected by an edge, if there is some $\mathsf{w} \in F(X)$ such that $(c_1, \mathsf{w}, c_2) \in S$.
(b) Two elements in C are called equivalent, if they are in the same connected component of this graph. Let $C_1, \ldots, C_h$ be the distinct equivalence classes.
(c) Each jump $j(c)$ then has a source, n, and a target, m, so that $c \in C_n$ and $\overline{c} \in C_m$. Denote this by ${}_n j(c)_m$.
(d) The factorisations of the relators as in $(\star)$ define words

$$_{n_1}j(c_1)_{n_2}\ _{n_2}j(c_2)_{n_3} \cdots\ _{n_s}j(c_s)_{n_1}$$

in the free groupoid generated by J.
(e) Then the associated jump groupoid $\mathcal{G}(J, R)$ is the quotient of the free groupoid generated by J by the normal closure of the subgroups generated by all these words as in (d).

As an application we consider the hyperbolic reflection group

$$H = \left\langle \begin{array}{l} a, b, c, d, e \mid a^2, b^2, c^2, d^2, e^2, \\ (ab)^3, (ac)^2, (ad)^2, (ae)^2, (bc)^3, (bd)^3, (be)^2, (cd)^2, (ce)^3, (de)^3 \end{array} \right\rangle.$$

Our method constructs permutation representations of H on N letters whose image contains the alternating group of degree N for any $N \geq 703$.

Construction of characters of $\mathrm{Syl}_p(Y_r(p^f))$, where $Y_r(p^f)$ is a Chevalley group.

Kay Magaard

Let p be a prime, $q = p^f$ and $Y_r(q)$ be a finite quasisimple group of untwisted rank r defined over the field $\mathbb{F}_q$. Let T be a split torus of $Y_r(q)$, Φ be a root system of type $Y_r(q)$, and let Φ^+ denote the set of positive roots with respect to some choice of simple roots. For $\alpha \in \Phi$ let X_α be the root subgroup of $Y_r(q)$ corresponding to α with respect to T. So

$$\prod_{\alpha \in \Phi^+} X_\alpha =: UY_r(q) \in \mathrm{Syl}_p(Y_r(q)).$$

The group $UY_r(q)$ carries much of the structural information of $Y_r(q)$. Additionally its representation theory of of the fusion system $\mathcal{F}_{Y_r(q)}(UY_r(q))$ must be relatively uniform for all primes $\ell \neq p$ and thus seems well suited for studying the cross characteristic representations of $UY_r(q)$. For theses reasons it seems timely to study $\mathrm{Irr}(UY_r(q))$ from a Lie theoretic point of view.

For $\chi \in \mathrm{Irr}(UY_r(q))$ we define the *r*oot center, *r*oot kernel and *c*entral root support by

$$\mathrm{rz}(\chi) := \{\beta \in \Phi^+ \mid X_\beta \subset Z(\chi)\}$$
$$\mathrm{rk}(\chi) := \{\beta \in \Phi^+ \mid X_\beta \subset \mathrm{Ker}(\chi)\}$$
$$\mathrm{rs}(\chi) := \mathrm{rz} \setminus \mathrm{rk}.$$

$\Sigma \subset \Phi^+$ *r*epresentable if $\Sigma = \mathrm{rs}(\chi)$ for some $\chi \in \mathrm{Irr}(UY_r(q))$.

For roots $\alpha, \beta \in \Phi^+$ we write $\alpha \preceq \beta$ if $\beta - \alpha$ is a non-zero sum of positive roots or $\alpha = \beta$. This defines a partial order $\preceq$ on Φ^+.

Proposition. *(Himstedt, Le, Magaard 2016)*
For a subset $\Sigma \subseteq \Phi^+$ the following are equivalent:

(a) Σ *is representable.*
(b) Σ *is an antichain of the root poset* $(\Phi^+, \preceq)$.

Denote the antichains of Φ by $\mathcal{A}$ and set $\mathrm{Irr}(UY_r(q))_\Sigma := \{\chi \in \mathrm{Irr}(UY_r(q)) \mid \mathrm{rs}(\chi) = \Sigma\}$. The proposition above implies that

$$\mathrm{Irr}(UY_r(q)) = \cup_{\Sigma \in \mathcal{A}} \mathrm{Irr}(UY_r(q))_\Sigma$$

leading to a natural partition of $\mathrm{Irr}(UY_r(q))$.

Recently Goodwin, Le, Magaard and Paolini, were able to construct the characters of $\mathrm{Irr}(UY_r(q))_\Sigma$ via sequences of character correspondences for all groups of rank

≤ 4. In particular they show that the number of characters of fixed degree is an element of $\mathbb{N}[v]$ where $v = q - 1$ whenever p is a good prime for Φ.

Recognition of finite exceptional groups of Lie type

Martin W. Liebeck

This is a contribution to the Matrix Group Recognition Project. Suppose we are given a group $G = \langle X \rangle \leq GL_n(F)$, where F is a finite field, such that G is quasisimple – so that $G/Z(G) \cong S$, a finite non-abelian simple group. There are algorithms that name the simple group S. The *Constructive Recognition Problem* is the following: construct an isomorphism ϕ from $G/Z(G)$ to the *standard copy* of S, and construct also ϕ^{-1}. Here, the standard copy of the alternating group A_n is the usual permutation group of degree n; it comes with standard generators (a 3-cycle and an n- or $(n-1)$-cycle), together with a presentation they satisfy. The standard copy of a classical group is the natural representation (modulo scalars), and again comes with standard generators and presentation. The standard copy of an exceptional group of Lie type is a copy of the group in its representation of minimal degree – for example, $E_6(q) < SL_{27}(q)$; its standard generators are the root elements $x_{\alpha_i}(t)$ for fundamental roots α_i and elements t in a basis of $\mathbb{F}_q$ over the prime field (some small degree extensions of $\mathbb{F}_q$ are required for twisted groups), and these generators satisfy a presentation given by the standard Curtis-Steinberg-Tits presentation for groups of Lie type.

The constructive recognition problem has been solved for alternating and classical groups, by the work of many authors. Here we announce the solution for the exceptional groups of Lie type:

Theorem (Liebeck-O'Brien [1])**.** *There is a Las Vegas algorithm that constructively recognises G in the case where $S = S(q)$ is an exceptional group of Lie type over $\mathbb{F}_q$ and S is not of type ${}^2B_2$, ${}^2G_2$, ${}^2F_4$ or ${}^3D_4$ (q even), assuming that* $\mathrm{char}(F) = \mathrm{char}(\mathbb{F}_q)$. *The algorithm runs in polynomial time, subject to the existence of a discrete log oracle.*

Work on constructive recognition for types ${}^2B_2$, ${}^2G_2$, ${}^2F_4$ has been done by H. Bäärnhielm. For ${}^3D_4(q)$ with q even, we give an algorithm in [1] but it runs in time $O(q)$, so is not polynomial time.

The algorithms in the theorem perform two main steps:

1. Find standard generators in G (i.e. find the elements $\phi^{-1}(x_{\alpha_i}(t))$).
2. Rewriting: express an arbitrary element of G as a word in the standard generators.

Step 1 is achieved in [1], and the algorithms are Black Box. Algorithms for Step 2 have been published by Cohen, Murray and Taylor, and these require the assumption in the theorem that G is a matrix group with $\mathrm{char}(F) = \mathrm{char}(\mathbb{F}_q)$. Once the standard generators have been found, it is straightforward to compute the highest weight of the representation.

The algorithms for Steps 1 and 2 have been implemented, and will be publicly available in Magma.

References

[1] M.W. Liebeck and E.A. O'Brien, *Recognition of finite exceptional groups of Lie type*, Trans. Amer. Math. Soc. **368** (2016), 6189–6226.

Generators of arithmetic groups

Willem A. de Graaf

Let $G \subset \mathrm{GL}(n, \mathbb{C})$ be an algebraic group defined over $\mathbb{Q}$. For an n-dimensional lattice $L \subset \mathbb{Q}^n$ set

$$G_L = \{g \in G \mid g(L) = L\}.$$

The arithmetic subgroups of G are the various G_L and their subgroups of finite index. By a theorem of Borel and Harish-Chandra, these groups are finitely-presented. Here we consider the problem to compute a generating set of an arithmetic subgroup of G (when G is given, for example, by a set of defining polynomials). Grunewald and Segal ([5]) have given a general algorithm for this purpose which, however, cannot be used in practice. Here we give a series of examples for which some kind of practical algorithm exists.

- Let G be a semisimple algebraic group, split over $\mathbb{Q}$. This group is generated by elements $x_\alpha(t) = \exp(t\rho(x_\alpha))$, where x_α are certain elements of a semisimple Lie algebra $\mathfrak{g}$, ρ is a representation of $\mathfrak{g}$, and α runs over the root system of $\mathfrak{g}$. In [6] it is shown that $G(\mathbb{Z})$ is generated by the elements $x_\alpha(1)$.
- Let A be a semisimple associative algebra over $\mathbb{Q}$, and let $\Lambda \subset A$ be an order in it. Then the unit group Λ^* can be viewed as an arithmetic group. If A is a number field, then there are algorithms for computing a generating set of Λ^* ([2]). If A is a quaternion algebra then there are at least two different approaches to computing generators of Λ^* ([7], [1]).
- In [4] an algorithm is given for the case where G is a torus. The main idea is to take the associative algebra A generated by the Lie algebra of G. The unit group of an order in A is computed (by splitting the algebra as a direct sum of fields, using the previously mentioned algorithm for number fields, and combining the resulting units into units of the chosen order in A). Then G is described inside A^* as the intersection of the kernels of a number of characters. Finally the intersection of the kernels of the restriction of these characters to the aforementioned unit group is computed. A set of generators of the latter also generates an arithmetic group in G.
- Let G be unipotent. For these groups an algorithm to compute generators of $G(\mathbb{Z})$ was given in [3]. Let $V = \mathbb{C}^n$. Then there is a flag $0 = V_0 \subset V_1 \subset \cdots \subset V_s = V$ such that G acts trivially on the quotients V_i/V_{i+1}. Here we take the V_i maximal with this property (so that s is minimal).

Set $V^* = V_{s-1} \oplus V/V_1$. Then we have a natural representation $\rho : G \to \mathrm{GL}(V^*)$. Let $Q = \rho(G)$. The point is that in V^* we can find a shorter flag for the action of G. So by recursion we can compute generators of $Q(\mathbb{Z})$. Secondly, we have a characterization of $\rho(G(\mathbb{Z}))$ inside $Q(\mathbb{Z})$, making it possible to compute generators of the former. Mapping these back into G, and adding generators of an arithmetic subgroup of the kernel of ρ, we obtain generators of $G(\mathbb{Z})$.

References

[1] Oliver Braun, Renaud Coulangeon, Gabriele Nebe, and Sebastian Schönnenbeck. *Computing in arithmetic groups with Voronoï's algorithm.* J. Algebra, **435**, 263–285, 2015.

[2] Johannes Buchmann. *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields.* In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 27–41. Birkhäuser Boston, Boston, MA, 1990.

[3] Willem A. de Graaf and Andrea Pavan. *Constructing arithmetic subgroups of unipotent groups.* J. Algebra, **322**(11), 3950–3970, 2009.

[4] Paolo Faccin, Willem A. de Graaf, and Wilhelm Plesken. *Computing generators of the unit group of an integral abelian group ring.* J. Algebra, **373**, 441–452, 2013.

[5] Fritz Grunewald and Daniel Segal. *Some general algorithms. I. Arithmetic groups.* Ann. of Math. (2), **112**(3), 531–583, 1980.

[6] R. Steinberg. *Lectures on Chevalley groups* Yale University, New Haven, Conn., 1967. Notes prepared by John Faulkner and Robert Wilson.

[7] John Voight. *Computing fundamental domains for Fuchsian groups.* J. Théor. Nombres Bordeaux, **21**(2), 469–491, 2009.

Recent advances in computing with infinite linear groups

Alla Detinko
(joint work with Dane Flannery)

We report on recent developments in computing with linear groups given by a finite set of generating matrices over an infinite field. In previous research [1] we developed effective methods for computing in this class of groups, used those methods to solve a number of computational problems, and designed software for practical computing. The problems solved include finiteness testing and testing (virtual) solvability over an arbitrary field, as well as structural investigation of solvable, nilpotent, and finite groups.

Further developments have occurred in two directions: (i) computing in solvable-by-finite groups; (ii) algorithms for groups containing a free non-abelian subgroup.

1. Algorithms for (virtually) solvable groups

Motivation. The theory of infinite solvable groups has played a central role in group theory over the past seventy years. Furthermore, solvable linear groups constitute a major component in the investigation of (abstract) solvable groups.

Challenges (solvable vs polycyclic). In contrast to (virtually) polycyclic groups, solvable groups may not be finitely presentable, they may contain subgroups that are not finitely generated, and they do not satisfy the maximal condition on subgroups. The failure of these properties poses severe difficulties in the design of algorithms for solvable groups.

Method. We initiated and developed a new approach to computing with (virtually) solvable linear groups, based on rank restrictions. Notice that finitely generated linear groups have finite Prüfer rank if and only if they are solvable-by-finite and $\mathbb{Q}$-linear.

Algorithms. Given a finitely generated solvable-by-finite subgroup G of $\mathrm{GL}(n, \mathbb{F})$, the following algorithms have been developed.

- Computing the torsion-free rank of G and bounds on its Prüfer rank [5, Section 4.4] when $\mathbb{F}$ is a number field.
- If H is a finitely generated subgroup of G, we can test whether $|G : H|$ is finite.
- Construction of a generating set of the completely reducible part of G. This includes testing whether G itself is completely reducible, and whether G is unipotent (i.e., is upper unitriangular in some basis) [5, Section 4.2].

Software. The algorithms are implemented in the package [6].

This research is joint with Eamonn O'Brien.

Applications. Applying the above results, we obtained a practical algorithm for arithmeticity testing of finitely generated subgroups of solvable algebraic $\mathbb{Q}$-groups. This involves a new efficient algorithm for testing integrality of a finitely generated solvable subgroup of $\mathrm{GL}(n, \mathbb{Q})$.

This is joint with Willem de Graaf.

2. Algorithms for semi-simple arithmetic groups

Most finitely generated linear groups are not virtually solvable, and comprise a broad variety of different types of groups. At this stage we restrict our attention to arithmetic subgroups of a semi-simple algebraic $\mathbb{Q}$-group $\mathcal{G}$.

Motivation.

- The class of arithmetic groups is an important class of finitely generated linear groups; moreover, computing with arithmetic subgroups is currently in high demand, especially due to the connections with number theory, topology, and physics.
- Fundamental algorithmic problems are known to be decidable (for *explicitly given* arithmetic groups, as defined by Grunewald & Segal, 1980).

We consider $\mathcal{G} = \mathrm{SL}$ or Sp, $n > 2$. These are prominent examples of groups with the congruence subgroup property (CSP): i.e., each arithmetic subgroup H of $\Gamma_n := \mathrm{SL}(n, \mathbb{Z}), \mathrm{Sp}(n, \mathbb{Z})$ contains a principal congruence subgroup (PCS) $\Gamma_{n,m}$ of level m, which is the kernel $\Gamma_{n,m}$ of the reduction modulo m homomorphism on $\mathcal{G}(\mathbb{Z})$.

Method. We developed methods for practical computing with arithmetic subgroups based on the congruence homomorphism technique. The two main components are computing the level M of the maximal principal congruence subgroup of an arithmetic group H; and computing with congruence images of H, which are matrix groups over the finite ring $\mathbb{Z}_m$.

Algorithms. Let H be an arithmetic subgroup of Γ_n given by a finite set S of generating matrices. We list below the functions designed to handle these groups via computer.

2.1. **Computing the level and related procedures.**

- `LevelMaxPCS`(H) computes the level M of the maximal principal congruence subgroup $\Gamma_{n,M}$ of H. More generally, `LevelMaxPCS` takes as input a generating set of a dense subgroup and returns the level of its minimal arithmetic overgroup.
- `Index`(Γ_n, H) returns the index of H in Γ_n. As an application, we can test whether $H = \Gamma_n$.
- `IsIn`(H, g) tests membership of $g \in \Gamma_n$ in H. More generally, `IsSubgroup` (H, H_1) returns `true` if and only if the finitely generated subgroup H_1 of Γ_n is in H.
- `Intersect`(H, H_1) returns a generating set of the intersection of H and an arithmetic subgroup H_1 of Γ_n.

2.2. **Investigating subgroup structure.** The structure of an arithmetic group is defined to some extent by its (sub)normal subgroups (e.g., its PCS).

- `IsSubnormal`(H): tests whether H is subnormal in Γ_n.
- `Normalizer`(H) returns a generating set of $N_{\Gamma_n}(H)$.
- `NormalClosure`(H) returns a generating set of $\langle H\rangle^{\Gamma_n}$; here H is an arbitrary finitely generated subgroup of Γ_n.

Method: All algorithms are based on `LevelMaxPCS`(H) and our library of functions for subnormal subgroups of matrix groups over $\mathbb{Z}_m$; see [2, Section 3.1]. The algorithms also involve computing the ideal generated by the entries of the matrices in S [2, Section 1.5, 3.2].

2.3. **Orbit-stabilizer problem.** Let H be an arithmetic subgroup H of Γ_n given by a finite generating set of matrices, and let u, v be vectors in $\mathbb{Q}^n$.

- `Orbit`(H, u, v) tests whether $\exists\ g \in H$ such that $g(u) = v$, and returns such an element if such exists.
- `Stabilizer`(H, u) returns a generating set of $\mathrm{Stab}_H(u)$.

N.B.: $\mathrm{Stab}_H(u)$ is a finitely generated group.

Method: solution of the orbit-stabilizer problem for $\varphi_m(H)$ acting on $\mathbb{Z}_m^n$ and for a PCS $\Gamma_{n,m}$ of H; see [2, Section 4].

2.4. **Application.** We extended our methods and algorithms to the wider class of Zariski dense subgroups of $\mathcal{G}(\mathbb{C})$. This includes computing the 'arithmetic closure' (i.e. the minimal arithmetic overgroup) of a finitely generated subgroup $H \leq \mathcal{G}(\mathbb{Z})$ dense in $\mathcal{G}(\mathbb{C})$; here $\mathcal{G} = \mathrm{SL}$ or Sp. Using our GAP implementation of the algorithms, we solved various problems for classes of groups which have emerged recently in areas of mathematics and its applications [3].

The results of Section 2 are joint work with Alexander Hulpke.

We also present a number of open problems that are important for further development of the area.

References

[1] A. Detinko, D. Flannery *Computing with matrix groups over infinite fields*, Oberwolfach Reports, Volume **8**, Issue 3, 2011, 2118–2121.

[2] A. Detinko, D. Flannery, A. Hulpke, *Algorithms for arithmetic groups with the congruence subgroup property*, J. Algebra **421** (2015), 234–259.

[3] A. Detinko, D. Flannery, A. Hulpke, *Zariski density and computing in arithmetic groups*, preprint.

[4] A. Detinko, D. Flannery, W. de Graaf *Integrality and arithmeticity of solvable linear groups*, Journal of Symbolic Computation, **68** (2015) 138-145.

[5] A. Detinko, D. Flannery, E. O'Brien *Algorithms for linear groups of finite rank*, Journal of Algebra, **393** (2013), 187-196.

[6] A. Detinko, D. Flannery, E. O'Brien, *Infinite—Computing with matrix groups over infinite fields*, `http://magma.maths.usyd.edu.au/magma/handbook/matrix_groups_over_infinite_fields`, (2012).

Minimal Fields for Representations over Number Fields

Claus Fieker

Given some absolutely irreducible representation

$$\rho : G \to \mathrm{GL}(n, K)$$

for some finite group G and a number field K, I discuss algorithms to change the field K and some consequences for integral representations.

Going back to Springer, Plesken and Brückner, we can associate a 2-cocycle to the given representation:

$$\rho \simeq s \in H^2(\mathrm{Gal}(K/k), K^*) = H^2(K/k, K^*)$$

Here k denotes the character field. Furthermore, ρ can be realised over $E = K^V$ for some subfield $K/E/k$, fixed by V, iff $s|_{V\times V} = 0 \in H^2(K/E, K^*)$. If we can find $t \in H^1(K/k, K^*)$ proving this, ie. $\delta(t) = s|_{V\times V}$, then Brückner gave a procedure to find $T \in \mathrm{GL}(n, K)$ s.th.

$$\rho^T : G \to \mathrm{GL}(n, E).$$

Based on Derek Holt's algorithms for explicit calulations in H^1 and H^2 as well as a theoretical reduction to find $t \in H^1(K/k, U_S)$ where U_S is the group of S-units for some set S depending on K and the values of s, this is now practical.

As an application, one can, in the presence of Schur indices, look at all fields of minimal degree affording ρ. Experimental evidence suggests that in this situation one can always find both field where ρ can be made integral over as well as fields where this cannot be done. In particular, we have a large number of explicit fields and representations that cannot be made integral.

A short survey on Coclass Graphs

Heiko Dietrich

Leedham-Green & Newman [11] defined the coclass of a p-group of order p^n and nilpotency class c as $r = n - c$. The investigation of the p-groups of a fixed coclass led to deep results in p-group theory (see the book of Leedham-Green & McKay [10]), applications (see for example [1, 12]), and generalisations to other algebraic objects (see for example [5, 8]). In the last decade, the focus in coclass theory is on the investigation of the coclass graph $\mathcal{G}(p, r)$ associated with the finite p-groups of coclass r. It is conjectured that this infinite graph can be described by a finite subgraph and several "periodic patterns". The aim of this talk is to give a survey on the known periodicity results, the outstanding problems, and a recent new result [4] for the graph $\mathcal{G}(p, 1)$. Some details are given below.

1. Coclass graphs

The coclass graph $\mathcal{G}(p, r)$ has as vertices the isomorphism type representatives of the finite p-groups of coclass r, and there is an edge $H \to G$ if and only if H is isomorphic to $G/\gamma(G)$ where $\gamma(G)$ is the last non-trivial term in the lower central series of G. It is a deep result that $\mathcal{G}(p, r)$ can be partitioned into a finite subgraph and finitely many so-called coclass trees, which are infinite trees having exactly one infinite path starting at their root. Let $\mathcal{T}$ be such a coclass tree with maximal infinite path $S_t, S_{t+1}, \ldots$ where S_n has order p^n. The n-th branch $\mathcal{B}_n$ of $\mathcal{T}$ is the finite subtree of $\mathcal{T}$ induced by all descendants of S_n which are not descendants of S_{n+1}; clearly, the structure of these branches determines $\mathcal{T}$. For a positive integer k let $\mathcal{B}_n(k)$ be the pruned subtree of $\mathcal{B}_n$ induced by the groups in $\mathcal{B}_n$ of distance at most k to the root S_n of $\mathcal{B}_n$.

2. Periodicity results

Motivated by computational work of Newman & O'Brien, it has been proved by du Sautoy [14] and Eick & Leedham-Green [6] that for every coclass tree $\mathcal{T}$ and every positive integer k there exist integers $f = f(\mathcal{T}, k)$ and $d = d(\mathcal{T})$ such that the pruned branches $\mathcal{B}_n(k)$ and $\mathcal{B}_{n+d}(k)$ are isomorphic for all $n \geq f$. This shows that the pruned tree $\mathcal{T}_{(k)}$ with branches $\mathcal{B}_t(k), \mathcal{B}_{t+1}(k), \ldots$ has a periodic structure and can be described by a finite subgraph. There exists $k > 0$ such that $\mathcal{T} = \mathcal{T}_{(k)}$ for all coclass trees in $\mathcal{G}(p, r)$ if and only if $p = 2$ or $(p, r) = (3, 1)$; in these cases the structure of $\mathcal{G}(p, r)$ is already determined by a finite subgraph. However, for all other values of p and r there exist coclass trees with $\mathcal{T} \neq \mathcal{T}_{(k)}$ for all k, and the periodic pattern proved in [6, 14] is not able to describe the structure of such a coclass tree completely. In other words, it remains to describe the growth (in depth and width) of the branches in such coclass trees. Computer experiments and results for $\mathcal{G}(5,1)$ and $\mathcal{G}(3,2)$ suggest that this can be done by using a second periodic pattern, see [2, 3, 9, 13] for some conjectural descriptions. Most recently, Conjecture W in [7] suggests another construction of $\mathcal{T}$ from a finite subgraph. In [4] we give the first explicit evidence in support of Conjecture W in the context of coclass trees whose branches grow in depth and width. More precisely, we consider the (unique) coclass tree in $\mathcal{G}(p,1)$ with $p \geq 7$ and define $\mathcal{S}_n^*$ to be the subtree induced by the so-called skeleton groups in $\mathcal{B}_n(n-2p+8)$ with automorphism group order divisible by $p-1$. We show that Conjecture W holds for these subtrees $\mathcal{S}_n^*$; we refer to [4] for details and a report on further computational evidence.

References

[1] M. Couson. *Character degrees of finite p-groups by coclass.* J. Algebra **418**, 91–109 (2014).

[2] H. Dietrich, B. Eick, and D. Feichtenschlager. *Investigating p-groups by coclass with GAP.* Contemp. Math. AMS, Providence, RI, Vol. **470**, 45–61 (2008).

[3] H. Dietrich. *A new periodic pattern in the graph of p-groups of maximal class.* Bull. London Math. Soc., **42**, 1073–1088 (2010).

[4] H. Dietrich and B. Eick. *Finite p-groups of maximal class with 'large' automorphism groups.* To appear in J. Group Theory (2016).

[5] A. Distler. *Finite nilpotent semigroups of small coclass.* Comm. Algebra **42**, 1136–1150 (2014).

[6] B. Eick and C. R. Leedham-Green. *On the classification of prime-power groups by coclass.* Bull. London Math. Soc. **40**, 274–288 (2008).

[7] B. Eick, C. R. Leedham-Green, M. F. Newman, and E. A. O'Brien. *On the classification of groups of prime-power order by coclass: The 3-groups of coclass 2*, Internat. J. Algebra Comput. **23**, 1243–1288 (2013).

[8] B. Eick and T. Moede. *Nilpotent associative algebras and coclass theory.* J. Algebra **434**, 249–260 (2015).

[9] C. R. Leedham-Green and S. McKay. *On the classification of p-groups of maximal class.* Quart. J. of Math. Oxford **35**, 293–304 (1984).

[10] C. R. Leedham-Green and S. McKay. The structure of groups of prime power order. London Mathematical Society Monographs. Oxford Science Publications, 2002.

[11] C. R. Leedham-Green and M. F. Newman. *Space groups and groups of prime-power order I.* Archiv der Mathematik **35** (1980), 193–203.

[12] P. Moravec. *On the Schur multipliers of finite p-groups of given coclass.* Israel J. Math. **185**, 189–205 (2011).

[13] M. F. Newman. *Groups of prime-power order* Groups-Canberra 1989, Lecture notes in math., **1456**, Springer, 49-62 (1990).

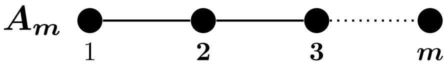
[14] M. du Sautoy. *Counting p-groups and nilpotent groups.* Inst. Hautes Etudes Sci. Publ. Math. **92**, 63–112 (2001).

On the Complexity of Multiplication in the Iwahori–Hecke Algebra of the Symmetric Group

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

Iwahori–Hecke algebras play an important role in many areas of mathematics and science. A well known example is the Iwahori-Hecke algebra $H = H(A_m)$ of the symmetric group $\mathsf{Sym}(m+1)$ of degree $m+1$. For more information on Hecke algebras see [3].

The symmetric group $\mathsf{Sym}(m+1)$ is a Coxeter group of type A_m with Dynkin diagram



It is generated by the set of reflections $S = \{s_1, \ldots, s_m\}$, where $s_i = (i, i+1)$ for $1 \leq i \leq m$. Every element $w \in \mathsf{Sym}(m+1)$ can be expressed in the form $w = s_{i_1} \cdots s_{i_k}$ with $s_{i_j} \in S$ for $1 \leq j \leq k$. If k is minimal such that there is an expression for w with k reflections in S, then we say k is the *length* of w denoted $\ell(w)$.

Let Z be a commutative ring with one, and let $q \in Z$. The Iwahori–Hecke algebra H of $\mathsf{Sym}(m+1)$ is the Z-free Z-algebra with basis $\{T_w \mid w \in W\}$. Thus a basis of H contains $M = (m+1)!$ elements. The multiplication in H satisfies

$$T_w T_s = \begin{cases} T_{ws}, & \ell(ws) > \ell(w), \\ (q-1)T_w + qT_{ws}, & \ell(ws) < \ell(w), \end{cases}$$

for all $w \in \mathsf{Sym}(m+1)$ and $s \in S$. Note that the Iwahori–Hecke algebra H is generated by $\{T_s \mid s \in S\}$.

The GAP 3 algebra package CHEVIE [1] facilitates in particular computing with Coxeter groups, and Iwahori-Hecke algebras. Working with H is difficult, since a basis of H consists of M elements. Current algorithms store elements of the Iwahori–Hecke algebra H as *coefficient lists* in this basis and multiplying two elements of H can require as many as $O(m^2 \cdot M^2)$ operations in the ring Z.

We introduce a new recursive data structure to represent elements of the Iwahori–Hecke algebra H. This data structure relies on considering the chain of subgroups $\mathsf{Sym}(1) \leq \mathsf{Sym}(2) \leq \cdots \leq \mathsf{Sym}(m) \leq \mathsf{Sym}(m+1)$ of $\mathsf{Sym}(m+1)$ and representing elements $w \in \mathsf{Sym}(m+1)$ as products of coset representatives of the cosets of $\mathsf{Sym}(j+1)$ inside $\mathsf{Sym}(j)$ rather than as words in S.

For $1 \leq j \leq m$ define the cycle $a(j,i) = (j-i+1, \ldots, j+1)$ in $\mathsf{Sym}(m+1)$. Then the set $\{a(j,i) \mid 0 \leq i \leq j\}$ is a set of coset representatives of $\mathsf{Sym}(j+1)$ inside $\mathsf{Sym}(j)$. Every element $w \in \mathsf{Sym}(m+1)$ can be expressed uniquely as a product $a(1,a_1) \cdot a(2,a_2) \cdots a(m,a_m)$, where $0 \leq a_j \leq j$ for $1 \leq j \leq m$. Therefore, the set $\{T_{a(j,i)} \mid 1 \leq j \leq m, 0 \leq i \leq j\}$ is a generating set for H.

In our new data structure we represent an element $h \in H$ as $h = \sum_{k=0}^{m} h_k T_{a(m,k)}$ where h_k is an element of the Iwahori–Hecke algebra of $\mathsf{Sym}(m)$. The elements h_k in turn can be represented as $h_k = \sum_{i=0}^{m-1} h_{ki} T_{a(m-1,i)}$ where h_{ki} is an element of the Iwahori–Hecke algebra of $\mathsf{Sym}(m-1)$. This process terminates when we reach the Iwahori–Hecke algebra of $\mathsf{Sym}(1)$, which is the ring Z. We call this data structure a *nested coefficient list*.

Multiplying two elements in H relies on the following identities between the newly defined generators (see [4, Lemma 3.1]). For $m \geq j \geq 1$ and $k, l \geq 1$ we have

$$T_{a(m,k)}\, T_{a(j,l)} = \begin{cases} T_{a(j,l)}\, T_{a(m,k)}, & k < m - j, \\ T_{a(m,k+l)}, & k = m - j, \\ (q-1)\, T_{a(j-1,j-m+k-1)}\, T_{a(m,m-j+l)} & \\ \qquad + q\, T_{a(j-1,l-1)}\, T_{a(m,k-1)}, & m - j < k \leq m - j + l, \\ T_{a(j-1,l)}\, T_{a(m,k)}, & k > m - j + l. \end{cases}$$

Comparing the complexity of multiplying two elements in H we prove the following theorem (see [4, Theorem 1.1]).

Theorem. *Let m be a positive integer, Z a ring with one, H the Iwahori–Hecke algebra of the Symmetric group $\mathsf{Sym}(m+1)$. Let $M = (m+1)!$.*

(a) *The cost of multiplying two elements in H each represented as a coefficient list over Z, based on Equations (1), is at most $\frac{m^2+m+4}{2} M^2$ operations in Z.*

(b) *The cost of multiplying two elements in H, each represented as a nested coefficient list over the Iwahori–Hecke algebra of $\mathsf{Sym}(m)$, is at most $(1 + \exp(1))M^2$ operations in Z.*

The new data structure yields a theoretical improvement in complexity, and experiments with a prototype implementation in the computer algebra system GAP [2] indicate an even better practical performance improvement.

References

[1] Meinolf Geck, Gerhard Hiß, Frank Lübeck, Gunter Malle, and Götz Pfeiffer, CHEVIE — *A system for computing and processing generic character tables*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), 175–210. MR 99m:20017

[2] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.4*, 2016.

[3] Meinolf Geck and Götz Pfeiffer, *Characters of finite Coxeter groups and Iwahori-Hecke algebras*, London Mathematical Society Monographs. New Series, **21**, Oxford University Press, New York, 2000. MR 2002k:20017

[4] Alice C. Niemeyer, Götz Pfeiffer and Cheryl E. Praeger, *On the Complexity of Multiplication in the Iwahori–Hecke Algebra of the Symmetric Group*, J. Symbolic Computation (to appear) (arXiv:1512.05319 [math.GR]).

Computing zeta functions of groups, algebras, and modules

Tobias Rossmann

Over the past decades, zeta functions associated with algebraic counting problems have received considerable attention. In particular, following the seminal paper [3] of Grunewald, Segal, and Smith, the theory of subobject zeta functions evolved into a distinct branch of asymptotic algebra.

While the initial focus in the area was on the enumeration of subgroups of finitely generated nilpotent groups, it was already observed in [3] that the Mal'cev correspondence all but reduces this problem to the enumeration of subalgebras of associated nilpotent Lie algebras. More formally, let R be $\mathbf{Z}$ or the ring $\mathbf{Z}_p$ of p-adic integers. Then, given a possibly non-associative R-algebra L whose underlying R-module is free of finite rank d, we define the *subalgebra zeta function* of L to be $\zeta_L(s) = \sum_{n=1}^{\infty} a_n(L)n^{-s}$, where $a_n(L)$ denotes the number of R-subalgebras of L of additive index n and s is a complex variable. It is easy to see that if L is a $\mathbf{Z}$-algebra, then we obtain the Euler product factorisation $\zeta_L(s) = \prod_p \zeta_{L\otimes\mathbf{Z}_p}(s)$, where p ranges over all primes. A deep result from [3], derived using non-constructive model-theoretic techniques, asserts that each *local zeta function* $\zeta_{L\otimes\mathbf{Z}_p}(s)$ is a rational function in p^{-s}. In another key paper in the area, du Sautoy and Grunewald [2] showed that, excluding finitely many exceptional primes, the functions $\zeta_{L\otimes\mathbf{Z}_p}(s)$ can all be expressed in terms of a single formula. Specifically, they showed that there are $\mathbf{Q}$-varieties $V_1, \dots, V_r$ and rational functions $W_1, \dots, W_r \in \mathbf{Q}(X, Y)$ such that, for almost all primes p,

$$(\star) \qquad \zeta_{L\otimes\mathbf{Z}_p}(s) = \sum_{i=1}^{r} \#\bar{V}_i(\mathbf{F}_p)\cdot W_i(p, p^{-s}),$$

where $\bar{\cdot}$ denotes "reduction modulo p". While their proof is constructive, it is usually impractical due to its reliance on resolution of singularities.

This talk was devoted to describing a practical method [5] for computing a formula $(\star)$ in favourable situations. This method combines techniques from a number of areas. In particular, it relies on

- the formalism for expressing local subobject zeta functions in terms of p-adic integrals from [3, 2],
- results from singularity theory and toric geometry due to Khovanskii [4] and others,
- algorithms of Barvinok and others from computational convex geometry (see, in particular, [1]), and
- ideas from the theory of Gröbner bases.

In practice, we can frequently do much better than merely producing a formula $(\star)$. Namely, for many examples of interest, the $\zeta_{L\otimes\mathbf{Z}_p}(s)$ are "uniform" in the sense that there exists a single rational function $W \in \mathbf{Q}(X, Y)$ such that $\zeta_{L\otimes\mathbf{Z}_p}(s) = W(p, p^{-s})$ for almost all primes p; our goal is then to find W. Among other things, this involves symbolically counting rational points on certain types of varieties.

As an application, we discussed the computation of the subalgebra zeta function of $\mathfrak{gl}_2(\mathbf{Z}_p)$ for $p \gg 0$. We also presented the author's "semi-simplification conjecture" [6, Conj. E] which asserts that given a rational unital matrix algebra, the behaviour of its associated generic local submodule zeta functions at zero only depends on the action of the largest semi-simple quotient of the algebra.

References

[1] A. Barvinok, K. Woods, *Short rational generating functions for lattice point problems* J. Amer. Math. Soc. **16**(4) (2003), 957–979.

[2] M. du Sautoy, F. Grunewald, *Analytic properties of zeta functions and subgroup growth* Ann. of Math. (2) **152**(3) (2000), 793–833.

[3] F. Grunewald, D. Segal, G. Smith, *Subgroups of finite index in nilpotent groups* Invent. Math. **93**(1) (1988), 185–223.

[4] A. Khovanskii, *Newton polyhedra, and toroidal varieties* Funkcional. Anal. i Priložen. **11**(4) (1977), 56–64,96.

[5] T. Rossmann, *Computing local zeta functions of groups, algebras, and modules (preprint)*, `arXiv:1602.00919`

[6] T. Rossmann, *Enumerating submodules invariant under an endomorphism (preprint)*, `arXiv:1606.00760`

Enumerating graded ideals in graded rings associated to free nilpotent Lie rings

Christopher Voll

Let $\mathcal{O}$ be the ring of integers of a number field and $d \in \mathbb{N}_{\geq 2}$. Denote by $\mathfrak{f}_d(\mathcal{O})$ the free d-generator $\mathcal{O}$-Lie algebra with lower central series $(\gamma_i(\mathfrak{f}_d(\mathcal{O})))_{i=1}^{\infty}$. For $c \in \mathbb{N}$, the quotient $\mathfrak{f}_{c,d}(\mathcal{O}) = \mathfrak{f}_d(\mathcal{O})/\gamma_{c+1}(\mathfrak{f}_d(\mathcal{O}))$ is called the free nilpotent d-generator $\mathcal{O}$-Lie algebra of nilpotency class c. The associated graded $\mathcal{O}$-Lie algebra is

$$\mathrm{gr}(\mathfrak{f}_{c,d}(\mathcal{O})) = \bigoplus_{i=1}^{c} \gamma_i(\mathfrak{f}_d(\mathcal{O}))/\gamma_{i+1}(\mathfrak{f}_d(\mathcal{O})).$$

An $\mathcal{O}$-ideal I of $\mathrm{gr}(\mathfrak{f}_{c,d}(\mathcal{O}))$ is called graded if $I = \bigoplus_{i=1}^{c} I \cap (\gamma_i(\mathfrak{f}_d)/\gamma_{i+1}(\mathfrak{f}_d))$, written $I \triangleleft_{\mathrm{gr}} \mathrm{gr}(\mathfrak{f}_{c,d}(\mathcal{O}))$. The graded ideal zeta function of $\mathfrak{f}_{c,d}(\mathcal{O})$ is the Dirichlet series

$$\zeta^{\triangleleft_{\mathrm{gr}}}_{\mathfrak{f}_{c,d}(\mathcal{O})}(s) = \sum_{I \triangleleft_{\mathrm{gr}} \mathrm{gr}(\mathfrak{f}_{c,d}(\mathcal{O}))} |\mathrm{gr}(\mathfrak{f}_{c,d}(\mathcal{O})) : I|^{-s},$$

where s is a complex variable. It satisfies an Euler product decomposition of the form

$$\zeta^{\triangleleft_{\mathrm{gr}}}_{\mathfrak{f}_{c,d}(\mathcal{O})}(s) = \prod_{\mathfrak{p}} \zeta^{\triangleleft_{\mathrm{gr}}}_{\mathfrak{f}_{c,d}(\mathcal{O}_{\mathfrak{p}})}(s), \tag{1}$$

indexed by the (non-zero) prime ideals $\mathfrak{p}$ of $\mathcal{O}$. Here, $\mathcal{O}_{\mathfrak{p}}$ denotes the completion of $\mathcal{O}$ at $\mathfrak{p}$; each Euler factor enumerates the graded $\mathcal{O}_{\mathfrak{p}}$-ideals of $\mathrm{gr}(\mathfrak{f}_{c,d}(\mathcal{O}_{\mathfrak{p}})) = \mathrm{gr}(\mathfrak{f}_{c,d}(\mathcal{O})) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}}$.

Graded ideal zeta functions of Lie algebras such as $\mathfrak{f}_{c,d}(\mathcal{O})$ may be viewed as approximations of their "ungraded" relatives, viz. the so-called ideal zeta functions enumerating all $\mathcal{O}$-ideals of finite index. Via the Mal'cev correspondence, ideal zeta functions of nilpotent Lie rings ($\mathbb{Z}$-algebras), in turn, are closely related to the normal subgroup zeta functions enumerating normal subgroups of finite index in nilpotent groups. It was in this context of subgroup growth of nilpotent groups that ideal zeta functions of nilpotent Lie rings were introduced and studied by Grunewald, Segal, and Smith in the seminal paper [2]. Writing q for the cardinality of the residue field of the local ring $\mathcal{O}_\mathfrak{p}$, a deep result – essentially a corollary (or rather porism) of [2, Theorem 3.5] – establishes that each factor of the Eulerian product (1) is a rational function in q^{-s} with rational coefficients.

We present recent joint work with Seungjai Lee ([3]) in which we compute all the factors of Euler products of the form (1) for $c \leq 2$ and $(c,d) \in \{(3,3),(3,2),(4,2)\}$. Our explicit formulae show, in particular, that the relevant Euler factors

- ∘ are rational functions in q^{-s} *and* q and
- ∘ satisfy functional equations upon the operation $q \to q^{-1}$.

Moreover, their associated reduced and topological zeta functions – two related but distinct "limits" of Euler factors as "$q \to 1$" – exhibit a number of intriguing arithmetic features, for instance pertaining to their degrees, poles, and behaviour at zero resp. infinity.

For $c \leq 2$ and $(c,d) = (3,2)$, our computations have "ungraded" counterparts, establishing formulae for the relevant ideal zeta functions of the $\mathcal{O}$-Lie algebras $\mathfrak{f}_{c,d}(\mathcal{O})$ (cf. [5] for $c = 2$ and [1, Theorem 2.35] for $(c,d) = (3,2)$). For $(c,d) \in \{(3,3),(2,4)\}$, however, the ideal zeta functions the relevant free nilpotent Lie algebras are unknown.

We make a number of conjectures making precise the expectation that the arithmetic features we establish hold – mutatis mutandis – for all values of c and d. Our conjecture regarding the "uniform rationality" in q^{-s} and q is a "graded analogue" of a conjecture in [2]. Local functional equations for the "ungraded" ideal zeta functions of the Lie algebras $\mathfrak{f}_{c,d}(\mathcal{O})$ have been established in [6, Theorem 4.4]. Our conjectures on the topological zeta functions, finally, are analogous to certain "ungraded" conjectures of Rossmann (cf., for instance, [4, Section 8].

References

[1] M. P. F. du Sautoy and L. Woodward, Zeta functions of groups and rings, Lecture Notes in Mathematics, vol. 1925, Springer-Verlag, Berlin, 2008.

[2] F. Grunewald, D. Segal, G. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), 185–223.

[3] S. Lee, C. Voll, *Enumerating graded ideals in graded rings associated to free nilpotent Lie rings*, preprint, arXiv:1606.04515, 2016.

[4] T. Rossmann, *Computing topological zeta functions of groups, algebras, and modules, I*, Proc. Lond. Math. **110** (2015), 1099–1134.

[5] C. Voll, *Normal subgroup growth in free class-2-nilpotent groups*, Math. Ann. **332** (2005), 67–79.

[6] C. Voll, *Local functional equations for submodule zeta functions associated to nilpotent algebras of endomorphisms*, preprint, arXiv:1602.07025, 2016.

Hubris

Michael Vaughan-Lee

In 2012 Marcus du Sautoy and I gave an example of a group of order p^9 with a non-PORC number of descendants of order p^{10}.

We wrote: *It seems likely that there are other groups of order* p^9 *with a non-PORC number of immediate descendants of order* p^{10}*, and so it is possible that the grand total [of groups of order* p^{10} *] is PORC, even though not all of the summands are PORC. The authors' own view is that this is extremely unlikely.*

The last sentence above is now looking rather foolish. Seunjai Lee has recently found a class two group K of order p^8 with exponent p which has a non-PORC number of descendants of order p^9 with exponent p. But in apparent contradiction to this result, I have a complete list of the 70 class two groups of exponent p with order dividing p^8. For every single group G in my list the number of descendants of G of order p^9 with exponent p is PORC.

The explanation for this "contradiction" is that Lee's group K is really a family of groups, one for each p, as are the groups in my list. For any given p, Lee's group K must lie in one of my families. But it does not have to lie in the same family for every p.

It turns out that there are four (families of) groups in my list A, B, C, D. If $p = 3$ then $K \cong A$, if $p = 2 \bmod 3$ then $K \cong B$, if $p = 1 \bmod 3$ and $t^3 - 2$ has no roots in $\mathrm{GF}(p)$ then $K \cong C$, and if $p = 1 \bmod 3$ and $t^3 - 2$ has three roots in $\mathrm{GF}(p)$ then $K \cong D$.

The non-PORC properties of Lee's group K arise from the fact that the number of roots of $t^3 - 2$ over $\mathrm{GF}(p)$ is *not* PORC.

Computing axial algebras

Sergey V. Shpectorov

Axial algebras are a new class of algebras related to groups. Examples include Jordan algebras for classical groups and the group F_4, Matsuo algebras for groups of 3-transpositions, as well as the 196,884-dimensional Griess-Norton algebra for the Monster sporadic simple group. Hence axial algebras provide a unified platform from which one can study all simple groups.

1. Axial algebras

Axial algebras are commutative non-associative algebras generated by non-zero idempotents called *axes*, whose action on the algebra are governed by prescribed *fusion rules*. Fusion rules are represented by a (finite) set $\mathcal{F}$ of numbers from the ground field $\mathbb{F}$ and a binary operation $\mathcal{F} * \mathcal{F} \to 2^{\mathcal{F}}$. An axis a in an algebra A satisfies these fusion rules if the adjoint action $\mathrm{ad}_a : A \to A$ (defined by $u \mapsto au$ for $u \in A$) is semisimple with all eigenvalues in $\mathcal{F}$, while the operation $*$ restricts multiplication of eigenvectors. More in detail, let $A_\lambda(a)$ denote the λ-eigenspace of ad_a

and, for $\Lambda \subset \mathbb{F}$, $A_\Lambda(a) := \oplus_{\lambda\in\Lambda} A_\lambda(a)$. Then the conditions on axes coming from fusion rules amount to the following: $A = A_{\mathcal{F}}(a)$ and $A_\lambda(a)A_\mu(a) \subseteq A_{\lambda*\mu}(a)$. For example, the Griess-Norton algebra belongs to the class of axial algebras defined by the fusion rules $\mathcal{F} = \mathcal{M}(\frac{1}{4}, \frac{1}{32})$ over $\mathbb{F} = \mathbb{R}$, where $\mathcal{M}(\alpha, \beta) = \{1, 0, \alpha, \beta\} \subseteq \mathbb{F}$ and the operation $*$ is as follows:

$*$	1	0	α	β
1	1		α	β
0		0	α	β
α	α	α	$1+0$	β
β	β	β	β	$1+0+\alpha$

Usually, axes are also required to be *primitive*, which means that the 1-eigenspace $A_1(a)$ must be 1-dimensional: $A_1(a) = \langle a\rangle$.

When fusion rules $\mathcal{F}$ are *T-graded* for an abelian group T, every axial algebra has a separate T-grading for every axis. This allows to introduce the *axis group* $T_a \leq \mathrm{Aut}(A)$, corresponding to an axis a and indexed by the linear characters of T. Hence every axial algebra becomes associated with its group of automorphisms generated by all groups T_a. For example, the above fusion rules $\mathcal{M}(\alpha, \beta)$ are C_2-graded, and so for every axis a we get an involution $\tau_a \in \mathrm{Aut}(A)$. In case of the Griess-Norton algebra, the associated group is the Monster M and the involutions τ_a are the $2A$ involutions in M.

2. Some theoretical results

The concept of axial algebras originates from the Majorana algebras of A.A. Ivanov [3]. These are axial algebras with fusion rules $\mathcal{M}(\frac{1}{4}, \frac{1}{32})$ satisfying several additional conditions derived from the properties of the Griess-Norton algebra. One key theoretical result is the Sakuma Theorem [4] classifying all Majorana algebras generated by two axes: every such algebra is one of the eight concrete *Sakuma algebras*, all of them arising inside the Griess-Norton algebra. There is now a version of this theorem [5, 1], where most additional Majorana conditions are removed.

The fusion rules $\mathcal{J}(\alpha)$ are the minor of the fusion rules $\mathcal{M}(\alpha, \beta)$ on the subset $\{1, 0, \alpha\}$. This means that axial algebras for the rules $\mathcal{J}(\alpha)$ are a subclass of the class corresponding to $\mathcal{M}(\alpha, \beta)$. The paper [2] contains a “Sakuma Theorem” for this subclass, classifying all 2-generated algebras. Furthermore, the paper also contains the proof that any axial algebra with fusion rules $\mathcal{J}(\alpha)$, $\alpha \neq \frac{1}{2}$, is a factor algebra of a Matsuo algebra. These are axial algebras corresponding to groups of 3-transpositions, defined uniformly in terms of the group for all fields of characteristic not two.

3. Computational results

So far computations of algebras for concrete small groups were done only for Majorana algebras and other axial algebras with fusion rules $\mathcal{M}(\frac{1}{4}, \frac{1}{32})$. This is because the explicit Sakuma theorem, available in this case, allows to restrict possible groups G for such algebras and also to classify algebras A for a given G in terms of their *shape*, prescribing which Sakuma algebras arise inside A.

The GAP program created by A. Seress [6] allows to calculate 2-closed algebras, that is, algebras spanned by length two products of axes. The program is fast and it was used to construct some large algebras, like the algebra of dimension 286 for the group M_{11}.

The GAP program created by the speaker, overcomes the 2-closeness restriction at the expense of a more complicated logic and slower speed. The idea for the program comes from the paper [1] providing an explicit construction of the universal k-generated axial algebra. This allowed to formalize the expansion operation, via which the available partial algebra is extended to include longer products of axes. This extension is then reduced using relations coming from the fusion rules. One calculations may involve several expansion/reduction cycles until the partial algebra converges to a complete algebra. This algorithm is certain to construct all finite dimensional algebras existing for the given group and shape. In practice, this is limited by the size of the systems of linear equations arising in this calculation. Note that even when the final algebra has a small dimension, the intermediate partial algebras can be significantly bigger. To date, the best achievement of this program has been the calculation of algebras for all twelve shapes for the group S_4. The largest of the algebras is of dimension 25 and it is not 2-closed. For two shapes no algebra exists. The dimension of the intermediate algebras in some cases is in the thousands.

There is also a version of this written by F. Rehren. It is based on the same ideas and has similar limitations. Note that both the speaker's and Rehren's programs only use the fusion rules and the list of Sakuma algebras.

Finally, the universal construction from [1] leads to further interesting finiteness questions and links to algebraic geometry. The restrictions on the group G also indicate links with the Burnside problem.

References

[1] J.I. Hall, F. Rehren, S. Shpectorov, *Universal axial algebras and a theorem of Sakuma*, J. Algebra, **421** (2015), 394–424.

[2] J.I. Hall, F. Rehren, S. Shpectorov, *Primitive axial algebras of Jordan type*, J. Algebra, **437** (2015), 79–115.

[3] A.A. Ivanov, *The Monster Group and Majorana Involutions*, Cambridge Univ. Press, Cambridge, Cambridge Tracts in Mathematics **176** (2009).

[4] A.A. Ivanov, D.V. Pasechnik, A. Seress, S. Shpectorov, *Majorana representations of the symmetric group of degree 4*, J. Algebra, **324** (2010) 2432–2463.

[5] F. Rehren, *Axial algebras*, PhD Thesis, University of Birmingham, 2015.

[6] A. Seress, *Construction of 2-closed M-representations*, in Proceedings ISAAC12, AMS, New York (2012), 311–318.

Group isomorphism is tied up in knots

James B. Wilson

With a century of attention, our understanding of isomorphisms between groups is both rich with answers and full of open questions. The implications have grown from original use in topology, to questions of computational complexity, problems in logic, and spawned the creation of numerous important concepts in algebra. Some recent projects are moving beyond established barriers while others are demonstrating why lack of progress is to be expected.

Among the hardest cases left is that of nilpotent groups. To get a handle on these groups we look at what grows like groups. We recognize that theorems of Pyber, Higman, Sims, Kruse-Price, Neretin and Poonen have all been point the way to a common structure involving tensors. With this insight not only do we recover the counts from those authors we begin to see new ways to attack isomorphism of nilpotence.

Several recent projects of Brooksbank, Eick, Leedham-Green, Maglione, O'Brien, and Wilson can be put into a common framework that introduces a recursive process to find characteristic subgroups. Each discovery increases the probability of finding the next. These methods begin with ideas in matroid theory, finite geometry, and nonassociative algebra. The result is to reduce to the extremely uniform cases.

In the final case when a product has a uniform product we demonstrate a recent result of First-Maglione-Wilson which replaces Whitney's tensor products with derivations-tensors, called "densors". These collapse the dimension by incredible amounts. For example, a 19683 dimensional space in the standard Whitney tensor space collapses to dimension 5. The impact on isomorphism is immediate. Even more exciting, these works on tensors apply in situations of interest across mathematics including the quantum phases of matter. The future is bright.

Condensation and Virtual Condensation

Alexander Ryba

The Meataxe is applied to analyze a module V for a finite group G over a finite field k of characteristic p — here analyze means obtain submodules, quotients and one or more composition series. Input for the Meataxe is a set of representing matrices for some generating group elements. Condensation is a preprocessor that cuts the size of matrix input.

A condensation program replaces matrices by (tiny) top left corners. The condensed results are analyzed by the Meataxe and an analysis of the original module is read off from the condensed result.

To be precise, we extract top left corners that correspond to a decomposition $V = Ve \oplus V(1-e)$, where e is an idempotent in the group algebra. Good idempotents are obtained as the sum of the elements in a p'-subgroup H — this will lead to a decrease in matrix size by a factor of about $|H|$. The condensed matrices give a representation of the Hecke algebra $ekGe$. One difficulty is that no efficient method is known for identifying a small set S of group elements for which eSe generates the Hecke algebra. Any method for doing this would be very much appreciated! Richard Parker has observed that generation of the Hecke algebra seems to be a difficult problem even in the very concrete case where the condensation subgroup H is cyclic of order 2 (and p is odd).

In practice condensation is only applied to a module that is too large to specify by explicit representing matrices. The module is instead specified by a recipe that is applied to explicit "small" input. For example, tensor products or symmetrized tensor products of small modules, permutation modules or vector permutation modules. There are also virtual tensor condensations that condense modules from ingredients which are themselves only known in condensed form.

A recent application is my computation with Klaus Lux of the 5-modular character table of the Lyons sporadic simple group. This computation was carried out entirely by condensation (and the Meataxe). Our computational result can only be said to be correct with probability extremely close to 1 because of the previously mentioned problem about identifying generators of the Hecke algebra. However, we hope to be able to apply virtual condensation to give a full proof.

Subgroups of sporadic groups

Robert A. Wilson

Since the 1980s, mainstream group theory has shifted focus from the classification of simple groups, to the study of their representation theory. This includes permutation representations, or equivalently the study of subgroups. Maximal subgroups correspond to primitive permutation representations, that is, the 'simple' objects in the theory.

The systematic classification of maximal subgroups of sporadic groups was started by Donald Livingstone and his students in the 1960s, and continued by others. All except the Monster were completed by 1999, and the Monster itself has been 'almost complete' since about 2008. The problem was reduced to classifying simple subgroups isomorphic to one of a few named groups.

In a recent paper [3], I showed that the Suzuki group $Sz(8)$ is not a subgroup of the Monster. More recently still (18th July 2016) I showed that there is a unique class of $U_3(8)$ in the Monster [4]. The strategy is to build $U_3(8)$ from subgroups $3 \times L_2(8)$ and $(9 \times 3).S_3$ intersecting in $3 \times D_{18}$.

First I show there is a unique class in the Monster of subgroups $3 \times L_2(8)$ in which all elements of order 9 are in the same Monster class. Such a group has normalizer $3S_6 \times L_2(8){:}3$. The normalizer in the Monster of the appropriate group 9×3 has shape $(9 \times 3).3^4.(S_3 \times A_6)$, in which the relevant class of involutions contains 3^6 elements.

But the group of allowable symmetries is $9 \times 3A_6$, of order $2^3.3^5.5$, so every group built as described has centralizer of order at least $2^3.3^5.5/3^6 = 40/3$. Since this centralizer lies in $C(19) = 19 \times A_5$, it is the whole of A_5, and the result follows.

This work leaves just four cases remaining:

- $L_2(8)$, containing $7B$-elements. In this case, there are three possibilities for the subgroup $2^3{:}7$, and 49×105 ways of extending 7 to D_{14}. By using the symmetries, the number of cases can be reduced substantially. The computations are in progress, and should be completed with a few more days work.
- $L_2(13)$, containing $13A$-elements. Since the centralizer of a $13A$ element is $13 \times L_3(3)$, there are five classes of 13:6 to consider, and this will take considerably more effort.
- $L_2(16)$, containing $5B$-elements. In this case, the best strategy would seem to be to start with an A_5 and extend D_{10} to D_{30}. There are three classes of $5B$-type A_5 subgroups, with centralizers D_{10}, S_3 and 2.
- $U_3(4)$, in which all elements of order 5 are in $5B$. Here one can employ the analogous construction to the $U_3(8)$ case above, that is start with $5 \times A_5$ and extend $5 \times D_{10}$ to $5^2{:}S_3$. Such an A_5 has normalizer $D_{10} \times A_5$, and the normalizer of the 5^2 is $5^4{:}4 \circ SL_2(5)$. The number of cases is small, but since the centralizer is trivial, computation will be required.

Once all these computations are complete, one could say that the maximal subgroup problem for sporadic groups is solved. However, the issues of reliability and reproducibility of the results remain. Some sort of revision of the proof would seem to be called for. Many delicate arguments have been employed, and in some cases serious mistakes have been made. For example, a 'proof' that $L_2(41)$ is not in the Monster stood for several years before the mistake was found, and eventually replaced by a computational proof by direct construction that $L_2(41)$ is in fact a subgroup of the Monster [2].

Partly as an experiment in such revision, I re-computed the maximal subgroups of ${}^2E_6(2)$ and its automorphism groups. This result is part of the folklore, but no published proof exists. The list in the Atlas [1] is complete, and correct except that the $3C$ normalizer has a quotient $3^2{:}2$ but not $3 \times S_3$.

References

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

[2] S. P. Norton and R. A. Wilson, *A correction to the* 41*-structure of the Monster, a construction of a new maximal subgroup* $L_2(41)$*, and a new Moonshine phenomenon*, J. London Math. Soc. **87** (2013), 943–962.

[3] R. A. Wilson, *Is* Sz(8) *a subgroup of the Monster?*, Bull. London Math. Soc. **48** (2016), 355–364.

[4] R. A. Wilson, *The uniqueness of* $\mathrm{PSU}_3(8)$ *in the Monster*, Preprint (2016).

A Characteristic Zero Approach to Computing Modular Representations

John J. Cannon

1. Introduction

Modular representations of finite groups arise in many areas of mathematics and it is frequently necessary to construct them for a given group G. For an arbitrary group the usual way is start with a KG-module affording a faithful representation of G in the desired characteristic and to obtain the irreducible modular representations for G as constituents of tensor powers of G. An algorithm along these lines (*Tensor Algorithm*) was developed by Cannon and Holt in the early 2000's and its implementation in Magma is very widely used. However, it suffers from a number of defects. Firstly, it is typically very expensive to split tensor powers much beyond the second. Secondly, while for many applications just one particular KG-module is required, the above approach may need to construct most irreducible KG-modules before the desired module is found. Finally, it is often difficult to find a suitable faithful KG-module for the initial input.

In this note we show how recent advances in algorithms for constructing complex irreducible characters and representations provide a new approach to constructing modular representations.

2. The Unger Character Table Algorithm

In 2006 Unger published a new algorithm for computing the table of ordinary irreducible characters. This algorithm is based on Brauer's Theorem which states that every irreducible character of G is a Z-linear combination of characters induced from linear characters of elementary subgroups of G. The input for the algorithm is a set of permutation or matrix generators for G. Initially the algorithm was thought to be applicable only to groups of moderate order. However, in 2014 I discovered that the algorithm was capable of computing the ordinary irreducible characters of very large non-soluble groups including most of the groups in the Atlas of Finite Groups.

In March 2014, J.P Serre gave a talk at Harvard University in which he observed that while the character tables in the Atlas were used in the proof of many recent theorems, no proofs of their correctness existed. It occurred to me that we could compute almost all of the Atlas character tables using the Magma implementation of Unger's algorithm. Since the tables appearing in the Atlas were originally computed mainly by hand using methods entirely distinct from Brauer's Theorem, this would be a completely independent computation.

Unger and myself have been able to compute the character tables for 87 out of the 93 simple groups listed in the Atlas. The groups which can not be done directly using Unger's algorithm are BM, M, $E_6(4)$, $E_7(4)$, $E_8(2)$, and $E_8(4)$. In total we have completed verifying 360 out of approximately 430 tables. The remaining groups are decorated versions of simple groups and their tables are steadily being constructed. Our tables are compared with those stored in the GAP library of character tables. The table for $E_6(2)$ was found to be incorrect. (While $E_6(2)$ is discussed in the Atlas its character table only appears in the GAP/Atlas character table library.)

3. Modular Representations

It is often convenient to specify an irreducible complex representation of a group G by giving its character χ. Given the character table $\mathrm{Irr}(G)$ of G and an irreducible character χ it is not difficult to produce a recipe for constructing χ from a character of some small subgroup of G. The recipe specifies character induction or extension operations working up some short chain of subgroups of G until χ is reached. Recently, Allan Steel developed algorithms that can apply this recipe to construct the irreducible representation affording χ.

In the case of modular representations it seems to be very difficult to construct the table of irreducible Brauer characters ($\mathrm{IBr}(G)$) without computing many of the modular representations. If G is a soluble group then $\mathrm{IBr}(G)$ is easily obtained from the complex character table. In the non-soluble case the best guide we currently have for constructing a modular representation is $\mathrm{Irr}(G)$. So assuming that we know the complex irreducible character χ whose reduction mod p contains the Brauer character of the desired representation then we can proceed as we did when constructing a complex irreducible representation. However, the *Black Box data structure* introduced by Allan Steel to represent a complex representation allows us to write down its reduction mod p without ever actually constructing the corresponding complex representation. The final step is to apply the F_p-Meataxe to obtain the irreducible constituents. If all the irreducible modular representations of G are required then one can reduce the work considerably by using a knowledge of the p-blocks of G.

An important advantage of this algorithm over Tensor Algorithm is that the dimension of the largest KG-module that has to be split is bounded by the maximum degree of a complex irreducible character. At this stage the algorithm is at an early stage of development but it appears that it will become the algorithm of choice when constructing certain types of irreducible modular representations, particularly those for which the relevant complex irreducible character can be identified.

A new method for verifying the hyperbolicity of finitely presented groups

Derek F. Holt

Let $G = \langle X \mid R \rangle$ be a group defined by a finite presentation, where the defining relators R are cyclically reduced. We are interested in attempting to decide whether G is hyperbolic. It is known that there is no general algorithm for this purpose, but the condition of G can be verified. There are many equivalent conditions for hyperbolicity of G [1]. These include: (i) geodesic triangles in the Cayley graph are uniformly slim; (ii) the Dehn function of G is linear; and (iii) G has a Dehn presentation (so the word-problem of G is solvable efficiently in linear time).

The programs in the author's KBMAG package [2](available as a standalone program or via GAP or Magma) can verify hyperbolicity. They do this by first finding a shortlex automatic structure for G, and then verifying that geodesic bigons in the Cayley graph are uniformly slim. A result of Papasoglu [4] then implies hyperbolicity of G.

The alternative methods that we are discussing now are based on generalizations of small cancellation theory [3, Chapter V]. The project was initiated by Richard Parker in about 2008. Significant contributions have been made by Roney-Dougal, Neunhöffer, Linton and others. Experimental programs have been written by Parker and Neunhöffer, a new implementation in GAP by Markus Pfeiffer is nearing completion, and there is also a very recent Magma implementation by the author.

Given enough resources, KBMAG can verify the hyperbolicity of any hyperbolic group, and it has been successful on difficult examples, such as the Fibonacci group $F(2,9)$. It can also calculate the growth series of G as a rational function. But it provides no reasonable estimate of the slimness constant or of the Dehn function of G, and it enables only a quadratic-time solution of the word problem.

In contrast, the new methods are *not* guaranteed to succeed on all presentations of hyperbolic groups, and KBMAG is more likely to succeed on short difficult examples. The new methods always finish in polynomial time, and when they work they do so much more quickly than KBMAG, but they often report failure. Unlike KBMAG, they can be used on presentations with large numbers of generators or relators, and they can sometimes be applied by hand, and to infinite families of group presentations. They provide a reasonable estimate of the Dehn function of G, which can be used to estimate the slimness constant. If the presentation is itself a Dehn presentation, then the programs may be able to verify this property, and hence enable a fast linear-time solution of the word problem.

The methods work by analysing reduced van Kampen (vK-)diagrams for G [3, Section V.1], and they are based on small cancellation theory, using curvature techniques based on those developed by Dehn, Greendlinger, and Lyndon & Schupp.

For a vK-diagram Δ, let $F = F_\Delta$, $V = V_\Delta$ and $E = E_\Delta$ be the internal faces, the vertices, and the edges of Δ. A *curvature function* $\kappa = \kappa_\Delta$ on Δ is a function

$$\kappa : F \cup V \cup E \to \mathbb{R} \quad \text{with} \quad \sum_{f\in F} \kappa(f) + \sum_{v \in V} \kappa(v) + \sum_{e\in E} \kappa(e) = 1.$$

For example, we could define $\kappa(f) = \kappa(v) = 1$ and $\kappa(e) = -1$ for all $f \in F$, $v \in V$, $e \in E$, and the condition holds by Euler's formula. A *curvature distribution scheme* on G is an assignment of a curvature function κ_Δ to each reduced diagram Δ for G. The idea is that, if we can find such a scheme in which the curvature of non-boundary faces is bounded below 0 and all of the positive curvature is in the boundary faces, then we can conclude that the Dehn function of G is linear and hence that it is hyperbolic.

We describe the simple curvature distribution scheme RSym, which is nevertheless powerful enough to rapidly prove hyperbolicity of many examples, and to reprove some results of this type in the literature. We plan to develop more powerful schemes in the future. Our main computational procedure attempts to prove that RSym succeeds in proving hyperbolicity of G by analysing the possible neighbours of a non-boundary face in an arbitrary vK-diagram for G. It can also try to verify that the presentation is Dehn.

A problem with small cancellation based methods is that many presentations involve relators x^k for small values of k and, since x will typically be a piece, this means that $C(k+1)$ cannot be satisfied and RSym is unlikely to succeed in proving hyperbolicity. To handle this, we extend the power and scope of RSym by treating certain short relators separately from the others. We designate these short relators as being *red* and call the remaining relators *green*, and colour our vK-diagrams accordingly. The underlying theory is based on the theory of *pregroups*, which was developed in the 1970s by Stallings [5]. Examples that can be successfully proved hyperbolic using these extended methods include the groups

$$(\ell, m, n; p) = \langle x, y \mid x^\ell, y^m, (xy)^n, [x,y]^p \rangle,$$

which were studied originally by Coxeter, and can be proved hyperbolic for all sufficiently large ℓ, m, n, p.

References

[1] J. Alonso, T. Brady, D. Cooper, V. Ferlini, M. Lustig, M. Mihalik, M. Shapiro and H. Short, *Notes on word-hyperbolic groups*, in E. Ghys, A. Haefliger and A. Verjovsky, eds., Proceedings of the Conference *Group Theory from a Geometric Viewpoint* held in I.C.T.P., Trieste, March 1990, World Scientific, Singapore, 1991.

[2] D.F. Holt, "KBMAG - Knuth–Bendix in monoids and automatic groups", software package (1995), available from `http://homepages.warwick.ac.uk/~mareg/download/kbmag2/`

[3] R.C. Lyndon & P.E. Schupp. *Combinatorial group theory.* Springer-Verlag, 1977.

[4] P. Papasoglu. Strongly geodesically automatic groups are hyperbolic. *Invent. Math.* **121**(2) (1995), 323–334.

[5] J.R. Stallings. *Group theory and three-dimensional manifolds.* Yale University Press, New Haven, Conn., 1971.

Computational Aspects of Burnside Rings

Martin Kreuzer

Given a finite group G, the Burnside ring consists of the formal differences of isomorphism classes of finite G-sets, with the addition being induced by disjoint unions and multiplication by cartesian products. In this talk we want to examine its structure as a commutative ring. Given representatives $H_1, \dots, H_s$ of the conjugacy classes of subgroups of G, ordered such that $\#H_1 \le \#H_2 \le \dots \le \#H_s$, the matrix $T(G) = (m_{ij})$ with $m_{ij} = \#(G/H_i)^{H_j}$ is called the table of marks of G. Using $T(G)$, we can write down a presentation $B(G) = \mathbb{Z}[x_1, \dots, x_{s-1}]/I(G)$ with an explicitly given ideal $I(G)$. This presentation shows that $I(G)$ is an ideal of points and $B(G)$ is a 1-dimensional reduced Cohen-Macaulay ring.

Furthermore, we explicitly describe the minimal and maximal primes of $B(G)$, their containments (via the prime ideal graph), and the singularities of $B(G)$. The mark homomorphism $\Phi_G : B(G) \to \mathbb{Z}^s$ identifies the ghost ring $\mathbb{Z}^s$ as the integral closure of $B(G)$, and the conductor of $B(G)$ yields its quasi-idempotents and their quasi-idempotent indices. All of these objects are calculated explicitly.

The next phases of the project include explicit calculation of the restriction, induction, projection, and inflation maps between various Burnside rings, an application to the problem of whether $B(G)$ uniquely determines $T(G)$, and an extension to Burnside rings and complete Burnside rings of infinite groups.

References

[1] M. Kreuzer and D. Patil, *C*omputational aspects of Burnside rings, Part I: The ring structure, preprint 2016 (submitted)

Computing the double Burnside ring of a finite group

Goetz Pfeiffer

(joint work with B. Masterson and S. Park)

The Burnside ring $B(G)$ of a finite group G is the Grothendieck ring of the category of finite G-sets. The double Burnside ring $B(G, G)$ of group G is the Grothendieck ring of the category of finite (G, G)-bisets. As an abelian group, $B(G, G)$ is isomorphic to the Burnside group $B(G\times G)$ of the direct product of the group G with itself, and as such it has a basis labelled by the conjugacy classes of subgroups of $G \times G$. The notion of multiplication in $B(G, G)$ is based on the so-called tensor product of (G, G)-bisets, which is the usual direct product of the sets, modulo the middle G-action.

The rational double Burnside algebra $\mathbb{Q}B(G, G)$ is known to be semisimple only if G is a cyclic group. In general, the problem of describing the structure of this algebra is wide open.

Based on a recent result on a factorization of the table of marks of $G \times G$, we develop computational methods for the construction of a mark homomorphism into a low-dimensional faithful representation of the algebra $\mathbb{Q}B(G, G)$ for a given group G. In some (small) examples, a cellular structure on $\mathbb{Q}B(G, G)$ can be exhibited.

Counting conjugacy classes in Sylow p-subgroups of finite Chevalley groups (On conjectures of Higman and Alperin)

Gerhard Röhrle
(joint work with Peter Mosch and Simon Goodwin)

Let $\mathrm{GL}_n(q)$ be the general linear group of nonsingular $n \times n$ matrices over the finite field $\mathbb{F}_q$ and let $\mathrm{U}_n(q)$ be the subgroup of $\mathrm{GL}_n(q)$ consisting of upper unitriangular matrices. Then $\mathrm{U}_n(q)$ is a Sylow p-subgroup of $\mathrm{GL}_n(q)$ where q is a power of p. A longstanding conjecture states that the number of conjugacy classes in $\mathrm{U}_n(q)$ for fixed n as a function of q is an integral polynomial in q. This conjecture has been attributed to G. Higman [9], and it has been verified for $n \leq 16$, see [17] and [14]. There has also been interest in this conjecture from G. Robinson (see [15]) and J. Thompson (see [16]).

The equivalent problem of counting the number of (complex) irreducible characters of $\mathrm{U}_n(q)$ has also attracted a lot of attention, see for example [13], [11] and [12]. Thanks to work of M. Isaacs [11], the degrees of the irreducible characters of $\mathrm{U}_n(q)$ are all powers q^d of q. It was conjectured by Lehrer [13] that the number of irreducible characters of $\mathrm{U}_n(q)$ of degree q^d is a polynomial in q with integer coefficients only depending on n and d; this conjecture clearly implies Higman's conjecture.

It is natural to consider the analogue of Higman's conjecture for other finite groups of Lie type. In order to state this generalization we need to introduce some notation. Let G be a simple algebraic group defined and split over $\mathbb{F}_q$, where q is a power of a good prime p for G. Let U be a maximal unipotent subgroup of G which is also defined over $\mathbb{F}_q$.

Let $G(q)$ denote the group of $\mathbb{F}_q$-rational points of G, which is a finite Chevalley group of the same Dynkin type as that of G. Moreover, $U(q)$, the $\mathbb{F}_q$-rational points of U, is a Sylow p-subgroup of $G(q)$. Let $k(U(q))$ denote the number of conjugacy classes of $U(q)$.

The following theorem combines the results from [6], [4], and [5]:

Theorem 1. *Let G be a split simple algebraic group defined over $\mathbb{F}_q$ of rank at most 8, not of type E_8, where q is a power of a good prime. Let U be a maximal unipotent subgroup of G which is also defined over $\mathbb{F}_q$. Then there is a polynomial $h(t) \in \mathbb{Z}[t]$ which only depends on the Dynkin type of G such that the number $k(U(q))$ of conjugacy classes in $U(q)$ is $h(q)$. Furthermore, if one considers $k(U(q))$ as a polynomial in $q-1$, then the coefficients are non-negative.*

The polynomials giving $k(U(q))$ are presented in the tables in [17], [6], [4] and [5]. In types other than A_n these were calculated using an algorithm outlined in [3] by means of the computer algebra system GAP, [2]. We remark that the restriction to good primes is necessary to get the same polynomial $h(t)$ as the prime varies.

In [1], J. Alperin showed that a related question is easily answered, namely that the number of $\mathrm{U}_n(q)$-conjugacy classes in all of $\mathrm{GL}_n(q)$, for fixed n as a function of q is a polynomial in q with integer coefficients. This result gives some support for Higman's conjecture in the sense that the count over all $\mathrm{U}_n(q)$-double cosets of $\mathrm{GL}_n(q)$ is given by a polynomial with integer coefficients in q. The failure of that for $\mathrm{U}_n(q)$-conjugacy classes in $\mathrm{U}_n(q)$ is thus rather unlikely. Nevertheless, recent work does cast some doubt on Higman's original conjecture, see [8], [14].

Generalizing this result of Alperin, in [7], we give an affirmative answer to a question raised by Alperin from [1]. In order to state it, let $k(U(q), G(q))$ denote the number of conjugacy classes of $U(q)$ in $G(q)$.

Theorem 2. *Let G be a split simple algebraic group defined over $\mathbb{F}_q$, where q is a power of a good prime. Let U be a maximal unipotent subgroup of G which is also defined over $\mathbb{F}_q$. Suppose that the center of G is connected.*

(i) *if $G \neq E_8$, then there is a polynomial $f(t) \in \mathbb{Z}[t]$ which only depends on the Dynkin type of G such that the number of conjugacy classes $k(U(q), G(q))$ of $U(q)$ in $G(q)$ is $f(q)$.*

(ii) *if $G = E_8$, then there is a polynomial $f^i(t)$ in $\mathbb{Z}[t]$ $(i = \pm 1)$ such that $k(U(q), G(q)) = f^i(q)$ for $q \equiv i \mod 3$.*

In view of Alperin's philosophy namely that the polynomial count of $k(\mathrm{U}_n(q), \mathrm{GL}_n(q))$ should reflect the polynomial behaviour of $k(\mathrm{U}_n(q))$, Theorem 2(ii) suggests that for G of type E_8, $k(U(q))$ might actually be "PORC".

Finally, we also discussed the counterpart to Lehrer's conjecture for $\mathrm{U}_n(q)$ for the irreducible characters of $U(q)$. The results from [5] suggest that this conjecture might be true in this more general context under suitable restrictions as in Theorem 1.

This work is related to the one reported by K. Magaard on new methods for the computation of the complex irreducible characters of $U(q)$, [10].

References

[1] J. L. Alperin, *Unipotent conjugacy in general linear groups*, Comm. Algebra **34** (2006), no. 3, 889–891.

[2] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.3*; 2002, `http://www.gap-system.org`.

[3] S. M. Goodwin, *On the conjugacy classes in maximal unipotent subgroups of simple algebraic groups*, Transform. Groups **11** (2006), no. 1, 51–76.

[4] S. M. Goodwin, P. Mosch and G. Röhrle, *Calculating conjugacy classes in Sylow p-subgroups of finite Chevalley groups of rank six and seven*, LMS J. Comput. Math. **17** (2014), no. 1, 109–122.

[5] S. M. Goodwin, P. Mosch and G. Röhrle, *On the coadjoint orbits of maximal unipotent subgroups of reductive groups.* Transform. Groups **21** (2016), no. 2, 399–426.

[6] S. M. Goodwin and G. Röhrle, *Calculating conjugacy classes in Sylow p-subgroups of finite Chevalley groups*, J. Algebra **321** (2009), no. 11, 3321–3334.

[7] S. M. Goodwin and G. Röhrle, *Rational points on generalized flag varieties and unipotent conjugacy in finite groups of Lie type*, Trans. Amer. Math. Soc., **361** (2009), no. 1, 177–206.

[8] Z. Halasi, P. Pálfy, *The number of conjugacy classes in pattern groups is not a polynomial function.* J. Group Theory **14** (2011), no. 6, 841–854.

[9] G. Higman, *Enumerating p-groups. I. Inequalities*, Proc. London Math. Soc. (3) **10** (1960), 24–30.

[10] F. Himstedt, T. Le and K. Magaard, *On the characters of the Sylow p-Subgroups of the untwisted Chevalley Groups $Y_n(p^a)$*, preprint (2015).

[11] I. M. Isaacs, *Characters of groups associated with finite algebras*, J. Algebra **177** (1995), 708–730.

[12] I. M. Isaacs, *Counting characters of upper triangular groups*, J. Algebra **315** (2007), no. 2, 698–719.

[13] G. I. Lehrer, *Discrete series and the unipotent subgroup*, Compos. Math. **28** (1974), 9–19.

[14] I. Pak, A. Soffer, *On Higman's $k(\mathrm{U}_n(\mathbb{F}_q))$ conjecture*, `http://arxiv.org/abs/1507.00411`.

[15] G. R. Robinson, *Counting conjugacy classes of unitriangular groups associated to finite-dimensional algebras*, J. Group Theory **1** (1998), no. 3, 271–274.

[16] J. Thompson, $k(\mathrm{U}_n(F_q))$, Preprint, `http://www.math.ufl.edu/fac/thompson.html`.

[17] A. Vera-López and J. M. Arregi, *Conjugacy classes in unitriangular matrices*, Linear Algebra Appl. **370** (2003), 85–124.

Finding strong involutions in finite classical groups in odd characteristic

Cheryl E. Praeger

(joint work with J. D. (John) Dixon and Ákos Seress)

Our major objective is to improve the complexity analysis of Bray's algorithm [1] in the context of finding the centraliser $C_G(t)$ of a strong involution t in an n-dimensional classical group G over a finite field of odd order.

An involution $t \in G$ is called *strong* if both of its eigenspaces $E_+(t)$ and $E_-(t)$ in the natural n-dimensional module have dimensions in the interval $[\frac{n}{3}, \frac{2n}{3}]$. Bray's algorithm proceeds by choosing independent uniformly distributed random elements $g \in G$ and considering the product $y := tt^g$. Suppose that y has order ℓ.

'Odd Case': If ℓ is odd then $t = t^{gh}$ for some element $h \in \langle t, t^g \rangle$ and gh is a uniformly distributed random element of $C_G(t)$;

'Even Case': if ℓ is even then $y^{\ell/2}$ is the central involution of $\langle t, t^g \rangle$, and so lies in $C_G(t)$; it is random and uniformly distributed within its $C_G(t)$-conjugacy class.

The impetus to study this instance of Bray's algorithm came from our wish to understand the performance complexity of a constructive recognition algorithm due to C. R. Leedham-Green and E. A. O'Brien [3] for finite classical groups of odd characteristic in their natural representation as matrix groups. The algorithm first constructs a strong involution by randomly selecting elements $a \in G$, until one is found of even order, say k, such that $t := a^{k/2}$ is a strong involution. It was shown by Lübeck, Niemeyer and the author in [4] that this procedure succeeds with high probability using $O(\log n)$ random elements. Next $C_G(t)$ is constructed using Bray's algorithm. The cost of this step was estimated in [3], based on the analysis in [5], to require examination of at most $O(n)$ random elements g. The rest of the algorithm requires only $O(\log\log n)$ random elements [3, Section 11]. This raises the following question, a positive answer to which would imply that

$O(\log n)$ random selections are sufficient for the algorithm of Leedham-Green and O'Brien algorithm, rather than the $O(n)$ estimate given in [3].

Will Bray's algorithm succeed with $O(\log n)$ random elements?

The $O(n)$-estimate for the Bray algorithm took into account only elements obtained from the 'odd case', and experimental data examined by Seress and the author suggested that elements in the 'odd case' were unlikely to be found with only $O(\log n)$ random elements g. So an improvement in the complexity would necessarily have to take into account elements from the 'even case'.

Now all involutions $y^{\ell/2}$ in $C_G(t)$ in the 'even case' have determinant 1, so the modified aim would be to generate a subgroup of $C_G(t)$ containing the quasisimple group $C_G(t)''$ (the second derived subgroup). The experimental evidence suggested further that fairly often $y^{\ell/2}$ induces a strong involution on at least one of the t-eigenspaces $E_\pm(t)$. In [6], Seress and the author proved that there is a positive constant c such that, with high probability, a finite classical group H in odd characteristic is generated by c strong involutions, with each of them random in its H-conjugacy class. It follows that $C_G(t)''$ can be constructed with high probability if we can find, for each $\varepsilon = \pm$, at least c elements $y^{\ell/2}$ which induce a strong involution on $E_\varepsilon(t)$. Thus in order to prove that the Bray algorithm for strong involutions succeeds, with high probability, after examining $O(\log n)$ random elements, it is sufficient to solve the following problem.

Problem. *Let G be an n-dimensional finite classical group G of odd characteristic, let $t \in G$ be a strong involution, and let $\varepsilon = \pm$. Prove that there is a constant c' such that, with probability at least $c'/\log n$, a random $g \in G$ produces a product tt^g with even order ℓ such that $(tt^g)^{\ell/2}$ induces a strong involution on $E_\varepsilon(t)$.*

In the talk I reported on work in [2] which solves this problem in the case where G is a special linear group. Current work jointly with Glasby and Roney-Dougal suggests we may be close to a solution for the unitary groups. The problem for symplectic and orthogonal groups is open.

References

[1] J. N. Bray, *An improved method for generating the centralizer of an involution,* Arch. Math. (Basel) **74** (2000), 241–245.

[2] J. D. Dixon, Cheryl E. Praeger and Ákos Seress, *Balanced involutions in centralisers of balanced involutions for finite special linear groups of odd characteristic*, preprint.

[3] C.R. Leedham-Green and E.A. O'Brien, *Constructive recognition of classical groups in odd characteristic,* J. Algebra **322** (2009), 833–881.

[4] Frank Lubeck, Alice C. Niemeyer and Cheryl E. Praeger, *Finding involutions in finite Lie type groups of odd characteristic,* J. Algebra **321** (2009), 3397–3417.

[5] Christopher W. Parker and Robert A. Wilson, *Recognising simplicity of black-box groups by constructing involutions and their centralisers,* J. Algebra **324** (2010), 886–915.

[6] Cheryl E. Praeger and Ákos Seress, *Probabilistic generation of finite classical groups in odd characteristic by involutions,* J. Group Theory **14** (2011), 521–545.

Finding normal subgroups in finite groups

Charles R. Leedham-Green

The matrix group recognition project has progressed, over twenty five years, from a vague and feeble hope to a successful piece of software that is widely used, and does almost everything we could hope for. We can now compute with matrix groups over finite fields with much the same functionality with which we can compute with permutation groups. None the less there remains room for significant improvement, and many people are still working on the project. Our groups are defined by a generating set contained in $\mathrm{GL}(d, q)$ for some integer d and prime power q.

The fundamental difficulty lies in the fact that, in contradistinction to the permutation case, a matrix group may have no proper subgroup of 'small' index. We resolve this difficulty by using normal subgroups instead.

Our driving principle is to use Aschbacher's theorem to reduce to almost simple groups. So if the group G is not simple we can use the action of the group on some geometrical structure, such as a tensor decomposition of the underlying space. Then the action of G on one of the tensor factors enables us to proceed by recursion on this image. and we have a mechanism to process the kernel.

The snag is that our algorithms to make Aschbacher's theorem explicit do not work well in some cases; generally when G is almost simple. Of course if G is almost simple we can treat it as though it did not preserve any Aschbacher structure. But this is unsatisfactory. Apart from wanting to know if G preserves such a structure, we can deal with G far more efficiently if this is the case.

The aim of this lecture is to reduce the difficult case to when G is a simple group, in a clean and simple way. Alex Ryba is producing algorithms to resolve the Aschbacher cases for simple groups.

It may still be more efficient to use our present methods 'in general', and to use the ideas suggested here when we hit hard Aschbacher cases.

The ideas I am presenting are largely based on work of Beals.

Summary of the problem session

A problem session was held on Tuesday, August 2, 2016. The following problems and questions were presented.

Leonard Soicher.
How can we determine whether a given small non-solvable group H (say A_5) is a quotient of a given finitely presented group G having "many" (say 16) generators in its presentation? Ideally find all quotients of G that are isomorphic to H.

Simon King.
The F_5-algorithm is an algorithm for computing a Gröbner basis of an ideal of a commutative multivariate polynomial ring. We developed a non-commutative

F_5-algorithm. We have used it for computations with cohomology rings. What are other possible applications?

Vladimir Shpilrain.
Consider the group $H(K)$ generated by the following matrices in $\mathrm{SL}(2,\mathbb{Q})$:

$$A(K) = \begin{pmatrix} 1 & K \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B(K) = \begin{pmatrix} 1 & 0 \\ K & 1 \end{pmatrix} \text{ where } K \in \mathbb{Q}, K > 0$$

It is known that $H(K)$ is free if $K \geq 2$.

- (Lyndon, Ullman, Merzlyakov) For which rational $0 < K < 2$ is $H(K)$ free? $H(K)$ is known to be **not** free for $K = \frac{m}{(nm+1)r}, K = \frac{m+n}{mnr}, m, n, r \in \mathbb{N}$.
- Solution to the subgroup membership problem (SMP) in $\mathrm{SL}(2,\mathbb{Q})$?
- Let $K \geq 2, K \in \mathbb{Z}$. Is there a sublinear time algorithm for solving SMP in $H(K)$?

Alla Detinko.
Is the membership problem for subgroups of $\mathrm{SL}(3,\mathbb{Z})$ decidable?

William R. Unger.
Let p_n be the proportion of elements of S_n which power to a (non-trivial) cycle. Is it true that $\lim\limits_{n\to\infty} p_n = 1$?

Robert A. Wilson.
The problem is to devise a reasonably generic algorithm for computing maximal subgroups of a group, using as little external information as possible. One could use such an algorithm, for example, to check results on maximal subgroups of almost simple groups of reasonable order, including sporadic groups. It would also avoid the presently necessary prodigious programming effort to work with subgroups of simple groups, and reduce the probability of errors and programming bugs.

Laurent Bartholdi.
Compute dimension-quotients of finitely presented groups G. Let k be a ring, let $\Delta(kG) \subset kG$ denote the augmentation ideal and define $\gamma_{n,k} = \{g \in G \mid g - 1 \in \Delta(kG)^n\}$. It is known that $\gamma_{n,\mathbb{F}_p} = \prod\limits_{mp^j \geq n} (\gamma_m)^{p^j}$ and $\gamma_{n,\mathbb{Q}} = \sqrt{\gamma_n}$.

- How can we (efficiently) compute $G \twoheadrightarrow G/\gamma_{n,\mathbb{F}_p}$?
- How can we compute $\gamma_{n,\mathbb{Z}}$?
- Is it true that $\gamma_{n,\mathbb{Z}} = \bigcap\limits_{p \text{ prime}} \gamma_{n,\mathbb{F}_p}$?

Sjögren proved that $\gamma_{n,\mathbb{Z}}/\gamma_n$ has exponent at most c_n for some numbers c_n; coarsely, $c_n \leq (2n)!$ and it is conjectured that $c_n = 2$. Rips has given an example where $\gamma_{4,\mathbb{Z}} \neq \gamma_4$.

Jürgen Müller.
Let $G = \mathrm{AGL}(n,q)$ act on $V = \mathbb{F}_q^n$. It also acts on $\mathcal{P}_k(V) \mathrel{\widehat{=}} k$-element subsets

of V. The goal is to find orbit representatives and stabilizers efficiently, where even the case $q = 3$, $n = 4$ and $k \leq 20$ seems to be ambitious. The number of orbits is known. We have the same goals for $\mathcal{S}_k(V) \subseteq \mathcal{P}_k(V)$ consisting of all k-element subsets not containing an affine line. In this case the number of orbits is not known.

Reporter: Tobias Moede

Participants

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

Dr. John N. Bray
School of Mathematical Sciences
Queen Mary University of London
Mile End Road
London E1 4NS
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

Giovanni De Franceschi
Department of Mathematics
The University of Auckland
Private Bag 92019
Auckland
NEW ZEALAND

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

Dr. Alla Detinko
School of Computer Science
University of St. Andrews
North Haugh
St. Andrews Fife KY16 9SS
UNITED KINGDOM

Dr. Heiko Dietrich
School of Mathematical Sciences
Monash University
Clayton, Victoria 3800
AUSTRALIA

Prof. Dr. Bettina Eick
Institut Computational Mathematics
Technische Universität Braunschweig
38106 Braunschweig
GERMANY

Prof. Dr. Graham Ellis
Mathematics Department
National University of Ireland, Galway
University Road
Galway
IRELAND

Prof. Dr. Claus Fieker
Fachbereich Mathematik
Technische Universität Kaiserslautern
Postfach 3049
67618 Kaiserslautern
GERMANY

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

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

Prof. Dr. David J. Green
Institut für Mathematik
Friedrich-Schiller-Universität
07737 Jena
GERMANY

Rafael Guglielmetti
Département de Mathématiques
Université de Fribourg
Perolles
Chemin du Musée 23
1700 Fribourg
SWITZERLAND

Prof. Dr. George Havas
School of ITEE
The University of Queensland
Queensland 4072
AUSTRALIA

Prof. Dr. Gerhard Hiß
Lehrstuhl D für Mathematik
RWTH Aachen
Pontdriesch 14-16
52062 Aachen
GERMANY

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

Prof. Dr. Max Horn
Mathematisches Institut
Justus-Liebig-Universität Gießen
Arndtstrasse 2
35392 Gießen
GERMANY

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

Prof. Dr. William M. Kantor
77 Pond Avenue #202
Brookline, MA 02445-7113
UNITED STATES

Dr. Simon A. King
Seminar für Mathematik und ihre Didaktik
Universität Köln
Gronewaldstrasse 2
50931 Köln
GERMANY

Prof. Dr. Martin Kreuzer
Fakultät für Informatik und Mathematik
Universität Passau
Innstraße 33
94032 Passau
GERMANY

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

Dr. Frank Lübeck
Lehrstuhl D für Mathematik
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

Prof. Dr. Kay Magaard
School of Mathematics and Statistics
The University of Birmingham
Edgbaston
Birmingham B15 2TT
UNITED KINGDOM

Josh Maglione
Department of Mathematics
Colorado State University
Weber Building
Fort Collins, CO 80523-1874
UNITED STATES

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

Tobias Moede
Institut Computational Mathematics
Technische Universität Braunschweig
38106 Braunschweig
GERMANY

Dr. Jürgen Müller
Mathematisches Institut
Universität Jena
Ernst-Abbe-Platz 2-4
07743 Jena
GERMANY

Prof. Dr. Alexei G. Myasnikov
Department of Mathematics
Stevens Institute of Technology
Castle Point Station
Hoboken, NJ 07030
UNITED STATES

Prof. Dr. Gabriele Nebe
Lehrstuhl D für Mathematik
RWTH Aachen
Pontdriesch 14/16, Rm 117
52056 Aachen
GERMANY

Dr. Alice Niemeyer
Lehrstuhl B für Mathematik
RWTH Aachen
Pontdriesch 10-16
52062 Aachen
GERMANY

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

Dr. Götz Pfeiffer
Mathematics Department
National University of Ireland, Galway
University Road
Galway
IRELAND

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

Prof. Dr. Gerhard Röhrle
Fakultät für Mathematik
Ruhr-Universität Bochum
44780 Bochum
GERMANY

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
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld
GERMANY

Prof. Dr. Alexander Ryba
Department of Computer Sciences
Queens College, CUNY
65-30 Kissena Boulevard
Flushing, NY 11367
UNITED STATES

Prof. Dr. Dmytro Savchuk
Department of Mathematics
University of South Florida
Tampa, FL 33620-5700
UNITED STATES

Prof. 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. Sergey V. Shpectorov
School of Mathematics
The University of Birmingham
Edgbaston
Birmingham B15 2TT
UNITED KINGDOM

Prof. Dr. Vladimir Shpilrain
Department of Mathematics
The City College of New York
Convent Avenue at 138th Street
New York, NY 10031
UNITED STATES

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

Dr. William R. Unger
School of Mathematics and Statistics
The University of Sydney
Sydney NSW 2006
AUSTRALIA

Prof. Dr. Michael R. Vaughan-Lee
Christ Church
Mathematical Institute
Oxford University
St. Aldate's
Oxford OX1 1DP
UNITED KINGDOM

Dr. Christopher Voll
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld
GERMANY

Prof. Dr. Robert A. Wilson
School of Mathematical Sciences
Queen Mary University of London
Mile End Road
London E1 4NS
UNITED KINGDOM

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