Mathematisches Forschungsinstitut Oberwolfach

Report No. 37/2011

DOI: 10.4171/OWR/2011/37

Computational Group Theory

Organised by
Bettina Eick (Braunschweig)
Gerhard Hiß (Aachen)
Derek Holt (Warwick)
Eamonn O'Brien (Auckland)

July 31st – August 6th, 2011

Abstract. This sixth workshop on Computational Group Theory proved that its main themes "finitely presented groups", "p-groups", "matrix groups" and "representations of groups" are lively and active fields of research. The talks also presented applications to number theory, invariant theory, topology and coding theory.

Mathematics Subject Classification (2000): 20xx,11-04,11Hxx,13-04,13A50,16Zxx,17-04,17Bxx, 18-04,18Gxx,37F10,68-04,68Nxx,68Wxx.

Introduction by the Organisers

The workshop *Computational Group Theory* was the sixth of this title held at Oberwolfach. It was attended by 57 participants of international provenance. Among the participants were four Oberwolfach Leibniz Graduate Students, visiting Oberwolfach for the first time.

The lecture program was divided into two sections, the first of which consisted of a series of five invited one-hour lectures. The speakers were selected to cover a broad variety of topics, suggested by the organisers. Three of the five invited lectures were intended as surveys. The first of these was given by László Babai (*Polynomial time theory of matrix groups*), who covered the theoretical background of the matrix groups computation project from its very beginnings to the state of the art. Meinolf Geck (*Problems in Representation Theory*) gave an overview of computational methods in the representation theory of finite groups and presented a very nice example of a rather theoretical result on Lusztig's character sheaves,

which was nonetheless only proved with the help of computers. Colva Roney-Dougal (*Computing maximal subgroups of finite groups*) summarised her work with John Bray and Derek Holt on the classification of the maximal subgroups of the finite classical groups of small dimension. Exciting new developments were presented by Gabriele Nebe (*Extremal lattices and codes*) who sketched the construction of her recently found extremal lattice in 72 dimensions, and by Michael Vaughan-Lee, who presented joint work with Marcus du Sautoy on an old conjecture by Graham Higman on the number of p-groups of order p^n. This work uses results on the number of rational points of elliptic curves.

The other section of our scientific program was made up of 18 shorter talks of variable length between 30 and 45 minutes. Two of these short talks were each given by two speakers on joint work and very closely related work, respectively. In addition we had a session of seven five-minute presentations and a problem session. This program structure was well accepted by the participants of the workshop.

With the short talks we tried to cover the whole range of topics in computational group theory, including some applications in neighbouring areas of mathematics. The latter were presented in talks by Bartholdi (topology, dynamical systems), Kemper (invariant theory) and Klüners (Galois theory). Two of the talks went right back to the very first ideas of computational group theory: Neunhöffer's report on joint work with Stephen Linton, Richard Parker and Colva Roney-Dougal presenting new ideas in small cancellation theory, and Sims' new approach to the Reidemeister-Schreier construction of a generating set of a subgroup. A highlight was the talk by John Cannon who presented a list of problems in computational group theory. A number of talks were centered around algorithms for matrix algebras, not necessarily over finite fields. In a similar direction, two of the talks discussed methods to deal with matrix groups over infinite fields, provided that the groups are finitely generated. As to software development, the talk by Steve Linton discussed perspectives of parallelising GAP. The final talk was given by Charles Leedham-Green and was devoted to matrix group recognition, a project which provided motivation for much of the work presented at the workshop.

The program of 23 talks and two extra sessions left plenty of time for discussions. This time was well spent: the participants took the opportunities provided by the workshop and the institute to continue their collaborations and start new ones.

Workshop: Computational Group Theory

Table of Contents

Abstracts

Polynomial-time theory of matrix groups

László Babai

Over the past decades, two matrix group recognition projects have run in parallel: the black-box project, started in a 1984 paper [4] by Szemerédi and the speaker, and the geometric project, started in a 1992 paper [6] by Neumann and Praeger and driven by Charles Leedham-Green. Remarkable interaction between the two approaches has developed over the past decade.

In this talk we surveyed the history and recent major results of the polynomial-time black-box theory, culminating in the result that we can decide membership in and compute the order and the composition factors of matrix groups over finite fields of odd order in randomized polynomial time, assuming access to number theory oracles (factoring integers, discrete log.). The presentation was based on the paper [2].

Bill Kantor has been a driving force behind the project. Major credit goes to the recent papers by C. W. Parker and R. A. Wilson [7] for their remarkable analysis of Bray's algorithm to find the centralizer of an involution in odd characteristic, and a paper by Holmes-Linton-O'Brien-Ryba-Wilson [5]. A key ingredient concerning the frequency of p'-elements in simple groups appears in a paper by Pálfy, Saxl, and the speaker [3].

The general framework of these developments was outlined in a 1999 paper by R. Beals and the speaker [1] where among other things the now popular normal series

$$G \geq \mathrm{PKer}(G) \geq \mathrm{Soc}^*(G) \geq \mathrm{Rad}(G)$$

was introduced.

References

[1] L. Babai, R. Beals, *A polynomial-time theory of black box groups I.* In C. M. Campbell, E. F. Robertson, N. Ruskuc, and G. C. Smith, editors, Groups St Andrews 1997 in Bath, I, London Math. Soc. Lect. Notes, 30–64. Cambr. U. Press, 1999.

[2] L. Babai, R. Beals, Á. Seress. *Polynomial-time theory of matrix groups.* In Proc. 41st ACM STOC, 55–64, 2009.

[3] L. Babai, P. Pálfy, J. Saxl, *On the Number of p-Regular Elements in Finite Simple Groups*, LMS JCM **12**, 82–119, 2009.

[4] L. Babai, E. Szemerédi. *On the complexity of matrix group problems I.* In Proc. 25th IEEE Symp. Found. Comp. Sci., Palm Beach, FL, 229–240, 1984.

[5] P. E. Holmes, S. A. Linton, E. A. O'Brien, A. J. E. Ryba, R. A. Wilson, *Constructive membership in black-box groups*, J. Group Theory **11**, 747–763, 2008.

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

[7] C. W. Parker and R. A. Wilson, *Recognising simplicity of black-box groups by constructing involutions and their centralisers*, J. Algebra **324**, 885–915, 2010.

Computing with matrix groups over infinite fields

Alla S. Detinko and Dane L. Flannery

Our research deals with algorithms for finitely generated linear groups over infinite fields. We have developed effective methods for computing in this class of groups; used those methods to solve a number of computational problems; and designed practical software for computing with linear groups defined over a broad range of infinite domains. Part of this research was undertaken with E. A. O'Brien.

1. Methods for computing with finitely generated linear groups

1.1. **Congruence homomorphism techniques.** Our approach draws on fundamental properties of finitely generated linear groups. Such a group is residually finite; moreover, it is approximated by linear groups of the same degree over finite fields. Consequently one of the main methods used to investigate finitely generated linear groups is the method of finite approximation [12, Chapters 4 and 10]. We have developed a computational analogue of this method, based on congruence homomorphism techniques. An immediate computational advantage of our approach is that it changes the original domain of definition, thereby transferring computations to the case of, e.g., a finite field.

Suppose henceforth that $G = \langle g_1, \ldots, g_r \rangle$, $g_i \in \mathrm{GL}(n, \mathbb{F})$, where $\mathbb{F}$ is an infinite field of characteristic $p \geq 0$. Then $G \leq \mathrm{GL}(n, R)$ where R is the subring of $\mathbb{F}$ generated by the entries of the g_i and g_i^{-1}, $1 \leq i \leq r$. For an ideal ρ of R, let $\phi_\rho : \mathrm{GL}(n, R) \to \mathrm{GL}(n, R/\rho)$ be the corresponding congruence homomorphism. Denote $\ker \phi_\rho$ by Γ_ρ and $G \cap \Gamma_\rho$ by G_ρ. If ρ is a maximal ideal of R then R/ρ is a finite field.

By the Selberg-Wehrfritz theorem [12, 4.8, p. 56], G has an *SW-subgroup*, i.e., a normal subgroup of finite index in which every torsion element is unipotent; in particular, if $\mathrm{char}\, \mathbb{F} = 0$ then G has a torsion-free subgroup of finite index. Our strategy is based on the construction of a special congruence homomorphism Φ_ρ such that Γ_ρ is an SW-subgroup. For more details see [10, Section 2] and [3, Section 4].

1.2. **The main fields.** Since the group $G \leq \mathrm{GL}(n, \mathbb{F})$ is finitely generated, $\mathbb{F}$ is a finitely generated field extension. As a consequence, the main fields to be considered are number fields (including the rational field $\mathbb{Q}$); function fields $\mathbb{P}(x_1, \ldots, x_m)$ where $\mathbb{P}$ is a finite field or number field, and $x_1, \ldots, x_m$ are algebraically independent indeterminates; and finite extensions of $\mathbb{P}(x_1, \ldots, x_m)$. For each case we have developed algorithms to construct Φ_ρ and compute $\Phi_\rho(G) \leq \mathrm{GL}(n, R/\rho)$; see [10, Section 3]. An implementation of the algorithms is publicly available in Magma [2].

2. The finiteness problem; recognition algorithms

2.1. **Deciding finiteness.** One of the first issues to be settled in a class of potentially infinite groups is deciding whether a given group in the class is finite. For linear groups over various domains this problem has been considered by Babai,

Beals, Ivanyos, and Rockmore. Using our congruence homomorphism techniques, we have developed efficient finiteness testing algorithms which are uniformly applicable to finitely generated linear groups over any infinite field [10, Section 4.2]. At the first stage, the algorithm constructs a congruence image $H = \Phi_\rho(G)$. If $\operatorname{char} \mathbb{F} = 0$ then the algorithm tests whether the congruence subgroup G_ρ is trivial; if $\operatorname{char} \mathbb{F} = p > 0$ then the algorithm tests whether G_ρ is a p-group. Clearly, G is finite if and only if G_ρ satisfies these conditions in either case.

A key task is the construction of a presentation of H. Knowing such a presentation, we can then apply the 'normal generators' method to answer the questions about G_ρ. Since H is a matrix group over a finite field, we construct a presentation using algorithms as described in [1] and [11]. For $\mathbb{F} = \mathbb{P}(x_1, \ldots, x_m)$, we have developed alternative algorithms which test finiteness of G by comparing the dimensions of enveloping algebras over $\mathbb{P}$ of G and of $\phi_\rho(G) \leq \mathrm{GL}(n, \mathbb{P})$; see [7] and [8]. Note that the latter algorithms do not involve computing presentations.

2.2. **Computing with finite matrix groups over infinite fields.** Let G be a finite subgroup of $\mathrm{GL}(n, \mathbb{F})$. We have developed algorithms to construct an isomorphic copy $\widetilde{G} = \Phi_\rho(G)$ of G over a finite field, via application of a suitable congruence homomorphism Φ_ρ [10, Section 4.3]. With $\widetilde{G}$ in hand, we can use available algorithms for matrix groups over finite fields ([1] and [11]) to investigate the structure and properties of the original group G. In particular, we can compute a composition series and a presentation of G; find the derived subgroup, and Sylow subgroups of G; and test membership of $h \in \mathrm{GL}(n, \mathbb{F})$ in G. For details see [10, Section 4.3].

3. A computational analogue of Tits alternative, and related algorithms

The Tits alternative famously states that a finitely generated linear group over a field is either solvable-by-finite, or it contains a free non-abelian subgroup. This theorem partitions finitely generated linear groups into two very different classes, which require separate treatment. Therefore, in computing with finitely generated linear groups, deciding virtual solvability is a fundamental problem.

For groups over $\mathbb{Q}$ this problem has been considered by Beals, Ostheimer, and Assmann and Eick. In related work, Assmann and Eick obtained algorithms testing polycyclicity and solvability of linear groups over $\mathbb{Q}$.

3.1. **Testing virtual solvability.** Let Ψ_ρ be a congruence homomorphism Φ_ρ such that G_ρ is unipotent-by-abelian if G is solvable-by-finite. A description of such Ψ_ρ is provided by Wehrfritz in [13], for all cases of $\mathbb{F}$ except possibly when $n \geq p > 0$. Relying on Wehrfritz's description, we have developed the following algorithm for testing whether G is solvable-by-finite (see [9, Section 3]): (1) construct $\Psi_\rho(G)$; (2) find a presentation of $\Psi_\rho(G)$; (3) compute normal generators of G_ρ, and use them to test whether G_ρ is unipotent-by-abelian. Similarly to our finiteness algorithm (Section 2.1), step (2) relies on the algorithms from [1] and

[11]. By additionally testing whether the matrix group $\Psi_\rho(G)$ defined over a finite field is solvable, we obtain an algorithm to test solvability of G. Notice that if $G \leq \mathrm{GL}(n, \mathbb{Z})$ then these algorithms test whether G is polycyclic-by-finite or polycyclic, respectively.

3.2. **Related algorithms.** Modifications of the algorithm for testing virtual solvability yield algorithms to test whether G is nilpotent-by-finite or abelian-by-finite [9, Section 5]. These algorithms are based on testing whether G_ρ is nilpotent (respectively, abelian). Notice that for this purpose R must be a Dedekind domain of characteristic zero, because for such R the congruence subgroup G_ρ is (Zariski-)connected. However, we can test whether G is nilpotent over any perfect field $\mathbb{F}$ [6, Section 4.6]. An algorithm to test whether $G \leq \mathrm{GL}(n, \mathbb{F})$ is central-by-finite when $\mathrm{char}\,\mathbb{F} = 0$ is given in [9, Section 5.3].

Furthermore, given a solvable-by-finite subgroup G of $\mathrm{GL}(n, \mathbb{F})$, $\mathrm{char}\,\mathbb{F} \geq 0$, we can test whether G is completely reducible [9, Section 4]. We also point out that [4], [5], and [6] provide a number of algorithms for computing with nilpotent linear groups. T. Rossmann has developed algorithms for irreducibility and primitivity testing of nilpotent linear groups over infinite fields.

Note that all of the algorithms discussed in Sections 2 and 3 have been implemented and are publicly available in Magma.

References

[1] H. Bäärnhielm, D. F. Holt, C.R. Leedham-Green, and E.A. O'Brien, *A new model for computation with matrix groups*, preprint (2011).

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

[3] A. S. Detinko, B. Eick, and D. L. Flannery, *Computing with matrix groups over infinite fields*, London Math. Soc. Lecture Note Ser. **387** (2011), 256–270.

[4] ———, *Nilmat—Computing with nilpotent matrix groups*; http://www.gap-system.org/Packages/nilmat.html (2007).

[5] A. S. Detinko and D. L. Flannery, *Computing in nilpotent matrix groups*, LMS J. Comput. Math. **9** (2006), 104–134 (electronic).

[6] ———, *Algorithms for computing with nilpotent matrix groups over infinite domains*, J. Symbolic Comput. **43** (2008), 8–26.

[7] ———, *On deciding finiteness of matrix groups*, J. Symbolic Comput. **44** (2009), 1037–1043.

[8] A. S. Detinko, D. L. Flannery, and E. A. O'Brien, *Deciding finiteness of matrix groups in positive characteristic*, J. Algebra **322** (2009), 4151–4160.

[9] ———, *Algorithms for the Tits alternative and related problems*, J. Algebra (to appear).

[10] ———, *Recognizing finite matrix groups over infinite fields*, preprint (2011).

[11] E. A. O'Brien, *Algorithms for matrix groups*, London Math. Soc. Lecture Note Ser. **388** (2011), 297–323.

[12] B. A. F. Wehrfritz, *Infinite linear groups*, Springer-Verlag, 1973.

[13] ———, *Conditions for linear groups to have unipotent derived subgroups*, J. Algebra **323** (2010), 3147–3154.

Computing with nilpotent linear groups

Tobias Rossmann

In this talk, we considered irreducibility testing of nilpotent linear groups over number fields. Let K be a number field and $V \neq 0$ be a finite-dimensional vector space over K. Let $G \leq \mathrm{GL}(V)$ be finitely generated and nilpotent. We can assume that G is non-abelian and completely reducible. Our strategy for irreducibility testing of G is built around the following tasks.

(1) Find a proper $K[G]$-submodule of V.
(2) Find a subspace $U < V$ such that G acts irreducibly on V if and only if $\mathrm{Stab}_G(U)$ acts irreducibly on U, and $\{Ug : g \in G\}$ is a G-system of imprimitivity.
(3) Find a homogeneous maximal abelian normal subgroup of G.

Using congruence homomorphism techniques and Clifford theory, we can always perform one of these tasks. In case (2), we replace G by the induced linear group acting on U and start again. In case (3), we find that the enveloping algebra of G is in an explicit way a crossed product. We can then decide irreducibility of G directly using computational Galois cohomology [3]; this step, however, is usually non-constructive. Hence, we obtain a "partially constructive" algorithm for irreducibility testing of nilpotent linear groups over K [6, §5.5].

In the case of a nilpotent group $G \leq \mathrm{GL}(V)$ which is finite instead of merely finitely generated, we can do much better. In this case, we employ the following variation (based on ideas from [2]) of the above strategy. If G has a non-cyclic abelian normal subgroup, then we can perform task (1) or (2). If, on the other hand, all the abelian normal subgroups of G are cyclic, then the structure of G is sufficiently restricted to allow us to constructively test irreducibility and primitivity of G directly. Consequently, we obtain fully constructive algorithms for both irreducibility and primitivity testing of finite nilpotent linear groups over K [4, 5]. Implementations are included in Magma.

References

[1] W. Bosma, J. Cannon, C. Playoust. *The Magma algebra system I: The user language*, Journal of Symbolic Computation **24** (1997), 235-265.
[2] A. Detinko, D. Flannery, *Computing in nilpotent matrix groups*, LMS Journal of Computation and Mathematics **9** (2006), 104–134.
[3] C. Fieker, *Minimizing representations over number fields II: Computations in the Brauer group*, Journal of Algebra **322** (2009), 752–765.
[4] T. Rossmann, *Irreducibility testing of finite nilpotent linear groups*, Journal of Algebra **324** (2010), 1114–1124.
[5] T. Rossmann, *Primitivity testing of finite nilpotent linear groups*, LMS Journal of Computation and Mathematics **14** (2011), 87–98.
[6] T. Rossmann, *Algorithms for Nilpotent Linear Groups*, PhD Thesis, National University of Ireland, Galway (2011).

Towards automorphism groups of p-groups: principle and practices

Peter A. Brooksbank and James B. Wilson

The structure of the automorphism group a p-group is in general quite difficult to predict, so new ideas are needed as well as new algorithms. Our general strategy uses those structural properties that are forced upon the automorphism group solely by the commutation in the p-group. While this does not consider every aspect of a p-group it is known that these conditions are one of the hardest to resolve.

Let p be an odd prime, and let G be a p-group of class 2 and exponent p. Baer showed that commutation in G gives rise to a bilinear map $b\colon V \times V \to W$, where $V = G/Z(G)$ and $W = G'$. The group

$$\Psi\mathrm{Isom}(b) = \{(g,h) \in \mathrm{GL}(V) \times \mathrm{GL}(W)\colon b(ug, vg) = b(u,v)h \ \forall u, v \in V\}$$

of *pseudo-isometries* of b is then a quotient of $\mathrm{Aut}(G)$ with a well known kernel. Hence understanding the pseudo-isometry group and its important normal subgroup $\mathrm{Isom}(b) = \{(g,1) \in \Psi\mathrm{Isom}(b)\}$ of *isometries* is a main component of understanding the full automorphism group.

In this talk we report on recent progress towards understanding the structure of $\Psi\mathrm{Isom}(b)$ by discussing the structure of the group and using that to produce polynomial time algorithms to construct:

(i) $\mathrm{Isom}(b)$ for general *Hermitian* bilinear maps $b\colon V \times V \to W$; and

(ii) $\Psi\mathrm{Isom}(b)$ for alternating bilinear maps $b\colon V \times V \to W$, where $\dim W = 2$.

The basic technique uses $*$-algebras and exploits a Galois correspondence between such algebras and tensor products. We describe the full structure of the pseudo-isometry groups of all tensor products in this correspondence.

Finally, we briefly report on ongoing projects involving the authors and E. A. O'Brien that uses such algorithms to explore the structure of $\Psi\mathrm{Isom}(b)$ for a broader range of alternating bilinear maps.

Element proportions in finite groups

Cheryl E. Praeger

Many Monte Carlo algorithms for group computation rely on estimates for the proportions of various kinds of elements in nearly simple groups. Increased precision in these estimates pays off both in terms of better theoretical complexity estimates for the algorithms, and also for better practical performance: for example, in group recognition algorithms where the input group is *not* the one being tested for, less time is wasted in fruitless searches for elements which may not exist in the input group.

The kinds of mathematics involved in estimating element proportions is quite varied and new approaches have been explored recently. I report on several approaches that have been used successfully, in several projects involving various coauthors: Jason Fulman, Simon Guest, Frank Lübeck, Peter Neumann, Alice Niemeyer, Tomasz Popiel, Ákos Seress, and Şükrü Yalçınkaya.

1. Estimation via nice generating functions

Tim Wall [W] proved that the limiting proportion of cyclic matrices in finite general linear groups $\mathrm{GL}(n,q)$, as $n \to \infty$ is $\frac{1-q^{-5}}{1+q^{-3}}$. This involved determining the generating function, and finding its radius of convergence and analytic properties. Similar (but more complicated) methods enabled Fulman, Neumann and Praeger [FNP] to determine the limiting proportions in all classical groups for cyclic, separable, semisimple, and regular matrices.

These methods worked unexpectedly in a new situation: Chris Parker and Rob Wilson [PW] had shown that involution-centraliser methods could be used for solving several problems which appeared to be computationally hard, and gave complexity analyses for methods to construct involutions and their centralisers in quasisimple Lie type groups in odd characteristic. Crucial to their analyses are conjugate involution pairs whose products are regular semisimple, possibly in an induced action on a subspace. Using generating functions Ákos Seress and I studied conjugate involution pairs, in finite general linear groups $\mathrm{GL}(n,q)$ with q odd, for which the product is regular semisimple on the underlying vector space. Such involutions form essentially a single conjugacy class $\mathcal{C}(n,q)$.

Theorem 1. [PS2, Theorem 2] *For a fixed parity of n, the proportion of pairs from $\mathcal{C}(n,q) \times \mathcal{C}(n,q)$ with regular semisimple product converges exponentially quickly to a limit, as n approaches ∞, the limit being $(1-q^{-1})^2\Omega(q)^3$ for even n, and $(1-q^{-1})\Omega(q)^3$ for odd n, where $\Omega(q) = \prod_{i=1}^{\infty}(1-q^{-i})$.*

Although not directly comparable, the general arguments in [PW, Theorem 19] lead to a lower bound of order $O(n^{-1})$.

2. And not so nice generating functions

Sometimes the generating function can be determined but not analysed. We then resort to a rather messy analysis, using geometrical methods and messing with the recursion, etc.

2.1. **Generating balanced involutions.** An involution in a finite n-dimensional classical group G over a field of odd order q is called (α,β)-balanced if the dimension of its fixed point subspace is between αn and βn (where $0 < \alpha \le \frac{1}{2} \le \beta < 1$). Constructing balanced involutions x and their centralisers is a central component of the recognition algorithm of Leedham-Green and O'Brien [LO] for n-dimensional classical groups G over fields of odd order. A balanced involution x can be constructed by powering a pre-involution and only $O(\log n)$ random elements are needed before finding a suitable preinvolution with high probability (see work with Frank Lübeck and Alice Niemeyer in [LNP]). The centraliser $C_G(x)$ involves a direct product of two classical groups, acting on the ± 1 eigenspaces $E_{\pm}(x)$ of x, and this direct product can be constructed, with high probability, by a constant number of involutions in $C_G(x)$ which project to balanced involutions in each factor (proved in [PS1, Theorem 1.1]). Finding such involutions should be easy, and

in the linear case we have shown that it requires testing only $O(1/\log n)$ random conjugates of x.

Theorem 2. [PS3] *Let x be an (α, β)-balanced involution in $G = \mathrm{GL}(n, q)$ with q odd. Then there is a constant c such that, with probability at least $c/\log n$, for a uniformly distributed random element $g \in G$, xx^g has even order and is $(\gamma, \frac{2}{3})$-balanced on each $E_\pm(x)$, where $\gamma = \frac{\alpha'}{3(1-\alpha')}$ with $\alpha' = \min\{\alpha, 1-\beta\}$.*

Ákos Seress and I determined the appropriate generating function for this probability, and employed a 'dirty hands-on analysis' to get the answer.

2.2. **Pre-semiregular permutations.** A permutation of a finite set Ω is called *semiregular* if all of its cycles have the same length, ℓ say, and $\ell > 1$. In particular semiregular elements have no fixed points in Ω, that is to say, they are fixed point free. Semiregular automorphisms of graphs give useful structural information about the graph, as well as assisting with graph construction and enumeration and graph drawing. Marušič and Jordan independently conjectured that every finite vertex-transitive graph should have a semiregular automorphism (see discussion in [NPPY]). It is not difficult to see that the proportion of semiregular elements in S_n lies between $\frac{1}{n}$ and $\frac{2}{n}$. Often semiregular permutations in S_n may be more readily constructed by powering a *pre-semiregular permutation* found by random selection. These are permutations for which some power is semiregular.

Theorem 3. [NPPY] *Suppose that an integer n has a divisor at most d (and $d \geq 4$). Then there is a constant c depending only on d such that the proportion of pre-semiregular elements in S_n is at least $cn^{-1+1/2d}$.*

In this situation Alice Niemeyer, Tomasz Popiel, Şükrü Yalçınkaya and I found a generating function, but the proportions we sought seemed to have periodic "sudden downspikes" and were very difficult to estimate. Obtaining the theorem required a delicate analysis of the recursion.

3. Lie type methods for estimation

Recognition algorithms for Lie type simple groups have involved estimation problems for various classes of elements: irreducible and nearly-irreducible elements; ppd elements, pre-involutions. The classes of each of these kinds of elements share properties that enables us to estimate their proportions using tools from the theory of groups of Lie type: each class is conjugacy closed, and membership of an element is determined by membership of its semisimple-part. The methods were developed independently by Gus Lehrer to study the character theory of Weyl groups, and by Isaacs, Kantor and Spaltenstein to estimate the proportion of p-singular elements in permutation groups (see the discussion in [NP]).

Alice Niemeyer and I developed this approach in [NP] as a general estimation theory for subsets with these properties. The first new application had already been made with Frank Lübeck in [LNP]. The method has also been used successfully with Tomasz Popiel to study preinvolutions powering to a given involution

conjugacy class in [NPP1], and to estimate the proportion of p-abundant elements in classical groups [NPP2], and with Simon Guest [GP] to estimate the proportions of elements g with a given 2-part order (that is, a given power of 2 divides $|g|$) in classical groups in odd characteristic.

References

[FNP] J. E. Fulman, Peter M. Neumann and Cheryl E. Praeger, *A Generating Function Approach to the Enumeration of Matrices in Classical Groups over Finite Fields*, Memoirs of the Amer. Math. Soc. **830**, 2005.

[GP] S. Guest and C. E. Praeger, Proportions of elements with given 2-part order in finite classical groups of odd characteristic, Submitted July 15, 2010.

[LO] C. R. Leedham-Green, and E. A. O'Brien, Constructive recognition of classical groups in odd characteristic. *J. Algebra* **322** (2009), 139–181.

[LNP] Frank Lübeck, Alice C. Niemeyer and Cheryl E. Praeger. Finding involutions in finite Lie type groups of odd characteristic, *J. Algebra*, **321** (11), (2009), 3397–3417.

[NP] Alice C. Niemeyer and C. E. Praeger, Estimating proportions of elements in finite simple groups of Lie type, *J. Algebra* **324** (2010), 122–145.

[NPP1] A. C. Niemeyer, T. Popiel and C. E. Praeger, On proportions of pre-involutions in finite classical groups, *J. Algebra* **324** (2010), 1016–1043.

[NPP2] Alice C. Niemeyer, Tomasz Popiel and Cheryl E. Praeger, Abundant p-singular elements in finite classical groups, Submitted March 21, 2011.

[NPPY] A. C. Niemeyer, T. Popiel, C. E. Praeger and Şükrü Yalçınkaya, On semiregular permutations of a finite set, *Math. Comp.* (to appear).

[PS1] C. E. Praeger and Ákos Seress Probabilistic generation of finite classical groups in odd characteristic by involutions, *J. Group Theory*. In press. doi: 10.1515/JGT.2010.061

[PS2] C. E. Praeger and Ákos Seress Regular semisimple elements and involutions in finite general linear groups of odd characteristic, preprint 2011.

[PS3] C. E. Praeger and Á. Seress, Balanced involutions in centralisers of balanced involutions for finite classical groups of odd characteristic. In preparation.

[PW] 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.

[W] G. E. Wall. Counting cyclic and separable matrices over a finite field. *Bull. Austral. Math. Soc.* **60** (1999), 253–284.

Extremal lattices and codes

Gabriele Nebe

Using invariant theory of finite complex matrix groups, Andrew Gleason has shown in his ICM talk in Nice 1970, that the minimum distance of a doubly-even self-dual binary code of length n cannot exceed $4 + 4\lfloor \frac{n}{24} \rfloor$. A similar bound has been proven by Siegel for even unimodular lattices of dimension n, where the minimum is always $\leq 2 + 2\lfloor \frac{n}{24} \rfloor$. Lattices and codes achieving equality are called **extremal**. Of particular interest are extremal lattices and codes in the "jump dimensions" - the multiples of 24.

Number of extremal lattices L and codes C.

n	8	16	24	32	48	72	80	≥ 3952	$\geq 163,264$
C	1	2	1	5	1	?	≥ 4	0	0
L	1	2	1	$\geq 10^7$	≥ 3	≥ 1	≥ 5	?	0

A very intensively studied question is the existence on an extremal code of length 72. This survey talk reports on recent progress in the study of possible automorphism groups of such a code. I will also give a construction of the extremal even unimodular lattice Γ of dimension 72 I discovered in summer 2010. The existence of such a lattice was a longstanding open problem. The construction that allows to obtain the minimum by computer is similar to the one of the Leech lattice from E_8 and of the Golay code from the Hamming code (Turyn 1967). Γ can also be obtained as a tensor product of the Leech lattice (realised over the ring of integers R in the imaginary quadratic number field of discriminant -7) and the 3-dimensional Hermitian unimodular R-lattice of minimum 2, usually known as the Barnes lattice. This Hermitian tensor product construction shows that the automorphism group of Γ contains the absolutely irreducible rational matrix group $(\mathrm{SL}_2(25)\times\mathrm{PSL}_2(7)) : 2$.

Constructive recognition of classical matrix groups in even characteristic

Heiko Dietrich

(joint work with C. R. Leedham-Green, F. Lübeck, E. A. O'Brien)

Let $G = \langle X \rangle$ be isomorphic to a classical matrix group $H = \langle \mathcal{S} \rangle \leq \mathrm{GL}(d, q)$ in natural representation, where $\mathcal{S}$ is a *nice* generating set. For example, one can efficiently write an arbitrary element of H as a word in $\mathcal{S}$. Informally, a constructive recognition algorithm constructs an *effective* isomorphism from G to H, and vice versa. An approach for doing this is to consider a generating set $\mathcal{S}' \subseteq G$ corresponding to $\mathcal{S}$, and to write the elements of $\mathcal{S}'$ as words in X. If every element of G can efficiently be written as a word in $\mathcal{S}'$, then the isomorphisms $G \leftrightarrow H$ defined by $\mathcal{S}' \leftrightarrow \mathcal{S}$ are *effective* since images can be computed readily. For example, if $g \in G$ is written as a word $w(\mathcal{S}')$ in $\mathcal{S}'$, then the image of g in H is easily determined as $w(\mathcal{S})$. Thus, instead of working in G, this allows us to work in the *nice* group H.

An interesting special case is $G = H$, where the constructive recognition problem is reduced to writing $\mathcal{S}$ as words in the given generators X. In 2009, Leedham-Green & O'Brien [4] presented a solution to this problem for odd q. Their chosen generating set $\mathcal{S}$ contains at most seven elements, and Costi [2] developed an algorithm to write $g \in G$ as a word in $\mathcal{S}$. *Practical* implementations of both algorithms are publicly available in the computer algebra system Magma [1]. The approach of Leedham-Green & O'Brien is to use a reduction to classical groups of smaller degree. These groups are constructed as subgroups of a centraliser of a *strong* involution, which can be found efficiently in G by a random search.

Now let q be even. Guralnick & Lübeck [3] showed that the proportion of elements of even order in a classical group over the field with q elements is at most $5/q$; thus a random search is not efficient to construct an involution. Moreover, the structure of involution centralisers is significantly different from those in odd characteristic. Consequently, the approach of Leedham-Green & O'Brien does not

immediately carry over to even characteristic. (We mention that Costi's algorithm also works for even characteristic.) It is the aim of this talk to describe a constructive recognition algorithm for classical matrix groups in natural representation and even characteristic. Our main result is a Las Vegas algorithm which, subject to the existence of a discrete logarithm oracle, needs $O(d^4 \log q)$ field operations. At present, we try to improve our analysis to obtain $O(d^3 \log d \log q)$. In addition, we also discuss modifications of this algorithm which allow an efficient construction of involutions in G. Implementations of our algorithms are publicly available in Magma. Our results rely on recent work of Bray, Wilson & Parker, and Praeger, Seress & Yalzinkaya.

This work contributes to the *Matrix Group Recognition Project*; its goal is to provide efficient algorithms to investigate matrix groups defined over finite fields. For an overview of this project and references to related significant results of other authors we refer to the survey articles [5, 6].

References

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

[2] E. M. Costi. Constructive membership testing in classical groups. PhD thesis, Queen Mary, University of London, 2009.

[3] R. Guralnick and F. Lübeck. On p-singular elements in Chevalley groups in characteristic p. Groups and computation, III (Columbus, OH, 1999), 169–182, Ohio State Univ. Math. Res. Inst. Publ., 8, de Gruyter, Berlin, 2001.

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

[5] E. A. O'Brien. Towards effective algorithms for linear groups. *Finite Geometries, Groups and Computation*, (Colorado), pp. 163–190. De Gruyter, Berlin, 2006.

[6] E. A. O'Brien. Algorithms for matrix groups. Groups St Andrews 2009 in Bath II, London Math. Soc. Lecture Note Series **388** (2011), 297–323.

Problems I Would Like to Solve in CGT

John Cannon

A substantial body of sophisticated algorithms have been developed in CGT over the past 40 years. With the wide availability of software packages, the techniques of CGT find wide application both within mathematics and in other areas. The growing use of CGT techniques has highlighted areas where there is a current lack of effective algorithms.

Finitely presented groups are commonplace in topology and other areas. A basic question concerns whether a given presentation defines the trivial group, a finite group or an infinite group. A second question asks for an isomorphic group with a soluble word problem. Both problems are known to be insoluble in general. However, I argue that with the current tools we can frequently solve one or both problems in the case of a particular group. I reported on two experiments. In one I constructed a program which is highly successful in proving that a group is infinite. In a second case study I applied Derek Holt's Knuth-Bendix to a large number

of fundamental groups of hyperbolic 3-manifolds and was able to determine the automatic structure for a high proportion (1150 out of 1300).

In the case of finite groups, the current approach to structure investigations proceeds by reducing the problem to the non-abelian composition factors. I reported on some recent successes with large matrix groups and also noted limitations which are often due to incomplete machinery for constructive recognition of simple groups.

Finally, I briefly considered representation theory and observed that very recent algorithmic advances mean that ordinary characters and representations of nearly simple groups can now be produced on an industrial scale. I identified a number of problems which have yet to be solved.

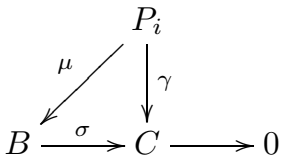
Computing with Basic Algebras

Jon F. Carlson

For several years, I have been developing a package in Magma for computations with basic algebras. This report emphasizes the new developments. The basic definition is that a (split) basic algebra is an algebra for which all of the simple modules have dimension one. For the purposes of this project, we assume that basic algebras are split and that all algebras have a unit element.

A primary motivation for the project is the theorem that every algebra is Morita equivalent to a basic algebra. This means that any finite dimensional algebra A has an equivalent module category as its basic algebra. Hence, when doing any sort of homological calculations, it is often convenient to do the calculation at the level of the basic algebra, which is often much smaller The computer data of a basic algebra A is a collection of pairs $\{(P_i, pt_i)|i = 1, \ldots, n\}$ where P_i is a projective A-module, and pt_i is a path tree that tells us how to construct homomorphisms.

The path tree is an algorithm for solving the lifting problem: Given σ, which is surjective, and γ, find μ such that the diagram



commutes.

So the philosophy is that we build the data structure to solve the problem that we want to solve, - then figure out how to get structures we want into the data structure. In practice, we can define basic algebras in many ways, as we see in the examples below. We can also construct a basic algebra using generators and relation, regarding it as a quiver with relations.

I give two examples of things that we can do with the package and comment on the new developments. Include in the examples are some running times of an actual calculation on my Apple laptop.

Example 1: Here we look at the question of whether the basic algebra of a Schur algebra is Koszul.

> time A := BasicAlgebraOfSchurAlgebra(3,8,GF(3)); Time: 24.480

(This was obtained by condensing a matrix algebra of dimension 461559 that is a subalgebra of all 1647×1647 matrices.)

> print A;
Basic algebra of dimension 41 over GF(3)
Number of projective modules: 10
Number of generators: 24

One of the issues that must be decide is whether the algebra is graded. We accomplish this by showing the algebra is isomorphic to its associated graded algebra.

> time B := AssociatedGradedAlgebra(A); Time: 0.060
> time a,b :=IsIsomorphic(B,A); Time: 4.120
> print a; true

This is sufficient to prove that A is Koszul.

Another marker of a Koszul algebra is that it is isomorphic to its double ext-algebra. The ext-algebra is $\mathrm{Ext}^*_A(S,S)$ where S is the direct sum of the simple A-modules.

> time C := BasicAlgebraOfExtAlgebra(A,10); Time: 2.110
> time D := BasicAlgebraOfExtAlgebra(C,10); Time: 2.040
> time a, b := IsIsomorphic(A,D); Time: 4.080
> print a; true

The program for automorphisms and isomorphisms for basic algebras has only recently been implemented in Magma. It should be available in the next release near the end of this year (2011). It follows an algorithm of Eick and O'Brien. Basically, we find the automorphism group of $A/\operatorname{Rad}^2(A)$. Then inductively assuming that we have the automorphism group of $A/\operatorname{Rad}^m(A)$, we compute the automorphism group of $A/\operatorname{Rad}^{m+1}(A)$, continuing until done. In the induction step we must compute a cover for $A/\operatorname{Rad}^m(A)$ that is universal with respect to the properties of having the same factor modulo Rad^m as A and having Rad^{m+1} zero. Then previously constructed automorphisms lift to this cover, and the automorphism group of the next factor of A is is the stabilizer of the homomorphism of the cover onto A.

In the next example we compute the cohomology of a group algebra by computing in the basic algebra.

Example 2: We begin by calling the group out of the library.

> load m12;
Loading "/usr/local/magma/libs/pergps/m12"
M12 - Mathieu group on 12 letters - degree 12

Order 95 040 = $2^6 \cdot 3^3 \cdot 5 \cdot 11$; Base 1,2,3,4,5
Group: G

Next we create the projective indecomposables and sort them by blocks. The principal block should be the first one.

```
> time PR := ProjectiveIndecomposables(G,GF(3));  Time: 13.910
> XX := SortByBlocks(PR);
> [[Dimension(y): y in x]:x in XX];
[[594, 297,297, 378, 378, 297, 351, 351],[189,243],[54]]
```

Next we created the basic algebra of the block algebra of the principal block.

```
> time B := BasicAlgebraOfBlockAlgebra(XX[1]);    Time: 64.130
> DimensionsOfProjectiveModules(B);
[ 15, 15, 18, 20, 20, 17, 17, 41 ]
```

Next we take the projective resolution of the trivial module which is the top of the eighth projective module.

```
> time cpr := CompactProjectiveResolution(SimpleModule(B,8),6);    Time: 0.080
> cpr‘BettiNumbers;
[   [ 0, 0, 3, 1, 1, 2, 2, 0 ],
[ 0, 0, 1, 1, 1, 1, 1, 1 ],
[ 0, 0, 1, 0, 0, 0, 0, 2 ],
[ 0, 0, 1, 0, 0, 1, 1, 1 ],
[ 1, 1, 2, 0, 0, 1, 1, 0 ],
[ 0, 0, 1, 1, 1, 1, 1, 0 ],
[ 0, 0, 0, 0, 0, 0, 0, 1 ]   ]
```

The projective resolution has the form

$$\ldots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow k \longrightarrow 0$$

and in the rows in the above display indicate the number of copies of each indecomposable projective module that is a direct summand of the modules $P_0, P_1, \ldots$. So the bottom row says that P_0 is one copy of indecomposable projective number 8. The next to bottom row says that P_1 is a direct sum of indecomposable projectives number 3, 4, 5, 6 and 7. In a recent discussion with a colleague in the generation of endotrivial modules it was important to know that structure of $\mathrm{H}^6(G,k)$. The zero in the 8^{th} column of the 7^{th} row (from bottom) says that the projective cover of the trivial module is not involved in P_6. Hence, $\mathrm{Ext}^6_{kG}(k,k) \cong \mathrm{H}^6(G,k) = 0$.

Other recent work has focused on algebra homomorphisms. We now have things like center and centralizers of elements and subset, ideals and quotient algebras, subalgebra, random subalgebras, kernels and images of homomorphisms, homomorphism testing.

Computation of Galois groups over p-adic fields

Jürgen Klüners
(joint work with Christian Greve)

Let $K/\mathbb{Q}_p$ be a p-adic field and $g \in K[x]$ be an irreducible monic polynomial. The goal is to compute its Galois group. The "trivial" approach would be to compute the splitting field which we would like to avoid. One crucial part in the algorithms over number fields [2] is that we have easy access to (approximations of) the roots of the given polynomial, e.g. we can use complex approximations or p-adic approximations for some unramified prime p. In the p-adic case we have no access to the roots (except in the splitting field). Therefore we cannot express the final result as a permutation group acting on its roots. We present the Galois group by generators with relations. On the other hand there is much more structure for p-adic fields, e.g. the Galois groups are solvable and the Galois group of the maximal pro-p-extension is known.

In case the given extension is at most tame, the Galois group can be easily computed as a group with two generators in probabilistic polynomial time (we need to factor polynomials over finite fields).

For Eisenstein polynomials of p–power degree we introduce the ramification polynomial and its corresponding ramification polygon. If this polygon is one-sided, we can easily write down the splitting field and its Galois group. The latter one is a semidirect product, where a group $H \leq \mathrm{GL}_m(p)$ is acting on C_p^m. The group H is the Galois group of a tame subextension of the splitting field of g which can be explicitly computed.

In case the ramification polygon has more than one segment, we can compute in probabilistic polynomial time a tame subextension T of the splitting field of g such that the Galois group of g over T is a p-group. Furthermore we know a tower of subfields of the stem field of g such that each relative step is elementary abelian. In case of two segments the complete Galois group can be computed by the use of the canonical class. These computations are difficult to carry out and will not be practical for more than two segments. More details can be found in the PhD-thesis [1] of Christian Greve.

References

[1] C. Greve, *Galoisgruppen von Eisensteinpolynomen über p-adischen Körpern*, Dissertation Universität Paderborn, 2010.

[2] K. Geißler and J. Klüners, *Galois Group Computation for Rational Polynomials*, J.Symb.Comput. **30** (2000), 675–716.

Graham Higman's PORC conjecture — Dead or Alive?

Michael Vaughan-Lee

For $p > 3$ the number of groups of order p^6 is

$$3p^2 + 39p + 344 + 24\gcd(p-1,3) + 11\gcd(p-1,4) + 2\gcd(p-1,5).$$

So for $p > 3$ the number of groups of order p^6 is one of 8 polynomials in p, with the choice of polynomial depending on the residue class of p modulo 60. In other words, the number of groups of order p^6 is PORC — polynomial on residue classes. In precise terms, we say that a function $f(p)$ defined on prime numbers is PORC if there is a finite set $g_1(p), g_2(p), \ldots, g_k(p)$ of polynomials in p, and a fixed positive integer N, such that for any prime p the value of $f(p)$ equals $g_i(p)$ for some i $(1 \le i \le k)$, with the choice of i depending on the residue class of p modulo N. In 1959 Graham Higman conjectured that for any given n the number of groups of order p^n is PORC. This has been confirmed for $n \le 7$, though the case $n = 8$ is still open and is likely to be extremely difficult to settle. Higman proved that the number of p-class 2 groups of order p^n is PORC (for all n). Anton Evseev has extended this result to show that the number of class 2 groups of order p^n with derived group of exponent p is PORC (for all n).

Nowadays the classification of p-groups of small order makes use of the lower exponent-p-central series of a group. If G is any group then the lower exponent-p-central series of G,

$$G = G_1 \ge G_2 \ge \ldots \ge G_i \ge \ldots,$$

is defined by setting $G_1 = G$, $G_2 = G'G^p$, and in general setting $G_{i+1} = [G_i, G]G_i^p$. If G is a finite p-group then $G_{c+1} = \{1\}$ for some c, and we say that G has p-class c if $G_c \ne \{1\}$, $G_{c+1} = \{1\}$. If G is a finite p-group of p-class $c > 1$ then we say that G is an *immediate descendant* of G/G_c. Apart from the elementary abelian group of order p^n, every group of order p^n is an immediate descendant of a group of order p^k for some $k < n$. To list the groups of order p^n, first list the groups of order p^k for all $k < n$. Then for each group G of order p^k for $k < n$, find all the immediate descendants of G which have order p^n.

So (for example) the formula given above for the number of p-groups of order p^6 $(p > 3)$ can be obtained as follows. It turns out that for $p > 3$ there are 42 groups of order at most p^5 which have immediate descendants of order p^6. Each of these 42 groups is given by a presentation involving the prime p symbolically — for example one of the 42 groups has presentation

$$\langle a, b \mid a^p[b,a,a]^{-1}, b^p, \text{class } 3\rangle. \tag{1}$$

For each of these 42 groups we compute the number of immediate descendants of order p^6, and the formula given above is obtained by adding together each of these individual contributions. For example, group (1) above has $p + \gcd(p-1,3) + 1$ descendants of order p^6. Finally, we have to add one to this total to account for the elementary abelian group of order p^6. Each of the individual contributions is PORC, and as a consequence the formula above is PORC.

Marcus du Sautoy has found a way of encoding elliptic curves into finite p-groups. Let M be the group that Marcus associates with the elliptic curve $y^2 = x^3 - x$ over the finite field GF(p). (M for Marcus.) Then M is a class 2 group of order p^9 and exponent p. Several important group theoretic properties of M, such as the number of conjugacy classes and the size of the automorphism group, are related to the number of points on the curve $y^2 = x^3 - x$ over GF(p). And this number is *not* PORC. In particular, the number of immediate descendants of M of order p^{10} is *not* PORC.

Marcus's group is a class 2 group of exponent p with generators

$$x_1, x_2, \ldots, x_6, X, Y, Z$$

and with all commutators trivial except for

$$[x_1, x_5] = [x_2, x_4] = [x_3, x_6] = X,$$
$$[x_1, x_6] = [x_3, x_4] = Y,$$
$$[x_1, x_4] = [x_2, x_5] = Z.$$

Thus M has Frattini quotient of order p^6, and elementary abelian derived group generated by X, Y, Z.

It turns out that if $p = 1 \bmod 12$ then the order of the automorphism group of M depends on whether or not the two equations

$$x^4 + 6x^2 - 3 = 0,$$
$$y^2 = x^3 - x.$$

have solutions in GF(p). If $p = 1 \bmod 12$ and if these two equations have no solutions in GF(p) then the automorphism group of M has order $|GL(2,p)| \cdot 4 \cdot p^{18}$, but if $p = 1 \bmod 12$ and the two equations have solutions in GF(p) then the automorphism group of M has order $|GL(2,p)| \cdot 36 \cdot p^{18}$. This has an impact on the number of descendants of M of order p^{10}. If $p = 1 \bmod 12$ and there are no solutions to the equations then there are $\frac{(p+1)^2}{4} + 3$ descendants of order p^{10} and exponent p, but if there are solutions to the equations then there are $\frac{(p-1)^2}{36} + \frac{p-1}{3} + 4$ descendants of order p^{10} and exponent p. However this behaviour is not PORC. There are infinitely primes $p = 1 \bmod 12$ for which the two equations have solutions in GF(p) — in fact these primes have Dirichlet density $\frac{1}{16}$. But you cannot capture these primes in a subcongruence class of $\{p \mid p = 1 \bmod 12\}$. Any such subcongruence class contains infinitely many primes p such that $x^4 + 6x^2 - 3 = 0$ has no solutions in GF(p).

So the number of immediate descendants of M of order p^{10} is not PORC, but this does not settle the PORC conjecture. As we saw above, the total number of groups of order p^{10} can be obtained by counting the number of immediate descendants of order p^{10} of each of the groups of order less than p^{10} and then adding all these numbers together. It is feasible that the grand total is PORC even though we know that at least one of the individual summands is not PORC. My own personal opinion is that this is extremely unlikely, and that although Higman's PORC conjecture is not clinically dead, it is on life support.

Properties of invariant rings and pointwise stabilizers

Gregor Kemper

A recurrent theme in invariant theory is the question which ring-theoretic properties an invariant ring $K[V]^G$ has. This talk is in part a survey talk about the properties that are usually studied. We also present some more recent results relating properties of an invariant ring, properties of the invariant ring of a pointwise stabilizer, and the local behavior of the invariant ring.

Throughout we consider a finite subgroup $G \subseteq \mathrm{GL}(V)$ acting linearly on a finite-dimensional vector space V over a field K. We write $K[V] = K[x_1, \ldots, x_n]$ for the polynomial ring on V and

$$K[V]^G := \big\{ f \in K[V] \mid \sigma(f) = f \ \forall \sigma \in G \big\}$$

for the *invariant ring*. This is always a graded subalgebra of $K[V]$. But what are its structural properties? It is known that $K[V]^G$ is always a normal ring and finitely generated as a K-algebra. But what further properties does it have? How do they relate to properties of the group action? At which points of the affine variety associated to $K[V]^G$ does the localization look nice?

One usually considers the following hierarchy of properties, in which each property implies the following one:

- $K[V]^G$ polynomial ring,
- $K[V]^G$ complete intersection,
- $K[V]^G$ Gorenstein,
- $K[V]^G$ Cohen–Macaulay.

Associated to each of these properties is a locus where the property holds locally. There are also numbers that measure the deviation from each of the properties: the *regular defect* $\mathrm{rdef}\big(K[V]^G\big)$, the *complete intersection defect* $\mathrm{cidef}\big(K[V]^G\big)$, the *type* (also known as Cohen–Macaulay type) of $K[V]^G$, and the *Cohen–Macaulay defect* $\mathrm{cmdef}\big(K[V]^G\big)$.

In the talk we discuss the polynomial ring property and the Cohen–Macaulay property in some detail and present some results.

For a point $x \in V$, let

$$G_x := \{\sigma \in G \mid \sigma(x) = x\} \subseteq G$$

be the pointwise stabilizer. We consider the localization $K[V]^G_x$ at x and the completion $\widehat{K[V]^G_x}$.

Lemma 1. $\widehat{K[V]^G_x} \cong \widehat{K[V]^{G_x}_x}$.

An elementary proof can be found in [6]. Moreover, the The G_x-automorphism $V \to V$, $v \mapsto v + x$ induces an isomorphism

$$K[V]^{G_x}_x \xrightarrow{\sim} K[V]^{G_x}_{\mathfrak{m}}.$$

Using this and Lemma 1, one can prove the main result of this talk:

Theorem 2. *Let* $f \in \{\mathrm{rdef}, \mathrm{cidef}, \mathrm{cmdef}, \mathrm{type}\}$ *and* $x \in V$. *Then*

$$f\left(K[V]_x^G\right) = f\left(K[V]^{G_x}\right) \leq f\left(K[V]^G\right).$$

This tells us that the behavior of the invariant ring can only get better when passing to a pointwise stabilizer, and that the local behavior of the invariant ring is entirely controlled by the pointwise stabilizer. The inequality in the theorem provides a common generalization of results of Serre [1], Steinberg [8], Nakajima [7], Kac and Watanabe [3], and the author [5]. The inequality also holds if f denotes the maximal degree of an invariant in a minimal homogeneous generating set.

Using Theorem 2, one can find examples of reflection groups (in the modular case) whose invariant ring has arbitrarily large Cohen–Macaulay defect, simply because the invariant ring of a suitable pointwise stabilizer has a large Cohen–Macaulay defect by previously known results. G. Malle and the author [4] also used the theorem for classifying all finite irreducible linear groups whose invariant ring is a polynomial ring.

A further application can be obtained by considering the non Cohen–Macaulay locus. In fact, if $K[V]^G$ is not Cohen–Macaulay, then

$$\dim\left\{x \in V \mid K[V]_x^G \text{ is not Cohen–Macaulay}\right\} > 0. \tag{1}$$

This follows from the fact that a Sylow p-subgroup of G (with $p = \mathrm{char}(K)$) fixes a line, and for a point x of this line, the index of G_x in G is not divisible by p, hence $K[V]^{G_x}$ is not Cohen-Macaulay. A further property that $K[V]^G$ may or may not have is the *Buchsbaum* property, which we might have added at the bottom of the above list of properties. The Cohen–Macaulay property always implies the Buchsbaum property, and it is well-known that the non Cohen–Macaulay locus of a Buchsbaum ring consists of only one point. With this, it is clear that (1) implies that $K[V]^G$ is not Buchsbaum if it is not Cohen–Macaulay. So the Buchsbaum property and the Cohen–Macaulay property for $K[V]^G$ are equivalent. This was conjectured by Campbell et al. [2].

References

[1] N. Bourbaki, Groupes et algèbres de Lie, Chap. IV,V,VI, Herman, Paris 1968.

[2] H.E.A. Campbell, I.P. Hughes, G.Kemper, R.J. Shank, D.L. Wehlau, *Depth of Modular Invariant Rings*, Transformation Groups **5** (2000), 21–34.

[3] V.G. Kac, K.-I. Watanabe, *Finite Linear Groups whose Ring of Invariants is a Complete Intersection*, Bull. Amer. Math. Soc. **6** (1982), 221–223.

[4] G. Kemper, G. Malle, *The Finite Irreducible Linear Groups with Polynomial Ring of Invariants*, Transformation Groups **2** (1997), 57–89.

[5] G. Kemper, Die Cohen-Macaulay-Eigenschaft in der modularen Invariantentheorie, Habilitationsschrift, Universität Heidelberg 1999.

[6] G. Kemper, *Loci in Quotients by Finite Groups, Pointwise Stabilizers and the Buchsbaum Property*, J. reine angew. Math. **547** (2002), 69–96.

[7] H. Nakajima, *Rings of Invariants of Finite Groups which are Hypersurfaces, II*, Adv. Math. **65** (1987), 39–64.

[8] R. Steinberg, *Differential Equations Invariant under Finite Reflection Groups*, Trans. Amer. Math. Soc., **112** (1964), 392–400.

Uniform triples and fixed point spaces

Gunter Malle
(joint work with Robert Guralnick)

We discussed the proof of our following recent result:

Theorem 1. *Let $1 \neq G \leq \mathrm{GL}(V)$ be an irreducible subgroup of the general linear group of a finite dimensional vector space V. Then there is $g \in G$ with fixed space of dimension $\dim C_V(g) \leq \frac{1}{3}\dim V$.*

This confirms a conjecture of Peter Neumann's 1966 thesis.

After various reductions, using in particular Scott's lemma on fixed spaces, the claim essentially follows from:

Theorem 2. *Let G be a non-abelian finite simple group, $G \neq \mathrm{SL}_2(2^f), \mathrm{PSL}_2(7)$. Then there is a conjugacy class $C \subset G$ and $(x, y, z) \in C \times C \times C^{-2}$ such that $xyz = 1$ and $G = \langle x, y\rangle$.*

This implies in particular:

Corollary 3. *Let G be non-abelian finite simple, $G \neq \mathrm{SL}_2(2^f)$. Then there exists an element $g \in G$ such that all its eigenspaces on any non-trivial absolutely irreducible G-module V have dimension at most $\frac{1}{3}\dim V$.*

Theorem 2 is proved using the Deligne–Lusztig character theory and information on the maximal subgroups of finite groups of Lie type, and ad hoc methods for the alternating and the sporadic groups.

We also mentioned several results pertaining to larger dimensions and of an asymptotic nature. For example, over the field of complex numbers we can show that eigenspaces for simple groups become arbitrarily small when the dimension increases:

Theorem 4. *For all $\epsilon > 0$ there exists $N = N_\epsilon$ such that for all non-abelian finite simple groups G and all non-trivial absolutely irreducible $\mathbb{C}G$-modules V of dimension $\dim V \geq N$ there is $g \in G$ with $\dim C_V(g) \leq \epsilon \dim V$.*

Our methods can also be adapted to show the following extension of a 1994 result of Malle–Saxl–Weigel:

Theorem 5. *Let G be non-abelian finite simple. Then there are classes $C_1, C_2 \subset G$ such that $C_1C_2 \cup \{1\} = G$.*

Together with a result of Chernousov–Ellers–Gordeev this implies:

Corollary 6. *Let G be finite non-abelian simple, and m a prime power or $m = 6$. Then all elements of G are products of two mth powers.*

Rethinking Reidemeister-Schreier

Charles C. Sims

Let a and b be free generators of $B(2,5)$, the two-generator Burnside group of exponent 5. In $B(2,5)$, let H be the subgroup generated by $x = b$, $y = b^a$, and $z = b^{a^{-1}}$. It is very easy to show that the index of H in $B(2,5)$ is 125. Only a small number of fifth powers are needed and the coset enumeration defines very few extra cosets. Recently I tried to find a finite set $\mathcal{T}$ of (group) words over $\{x, y, z\}$ such that the elements of $\mathcal{T}$ are relators for H and the order of the largest nilpotent, exponent-5 quotient of

$$\langle x, y, z \mid \mathcal{T} \rangle$$

has order 5^{31}, the order of the largest finite quotient of H. (Note: Nilpotent, exponent-5 quotients of a finitely presented group can be computed using the *anupq* package.)

My first attempts to solve this problems involved using various implementations of the Reidemeister-Schreier procedure, including my own. These efforts were quite unsatisfactory and led me to consider alternatives. The alternative presented in this talk is based heavily on the Knuth-Bendix procedure for strings. Information about the Knuth-Bendix procedure and the standard Reidemeister-Schreier procedure can be found in [1].

Let G be a group generated by a finite set X and let $\mathcal{R}$ be a finite set of relators over X that define G. Let H be a subgroup of finite index in G. By adding additional generators if necessary, we may assume that H is generated by a subset X_2 of X. Define X_1 to be $X - X_2$.

An ordinary coset enumeration of the cosets of H in G produces an ordinary coset table, from which it is possible to write down a finite set $\mathcal{S}$ of words over X that define a set of Schreier generators for H.

To find the Reidemeister-Schreier presentation for H, we need the extended coset table. The secondary labels in that table express the Schreier generators as words over X_2. Traditionally these secondary labels have been found by an extended coset enumeration process, but in the approach proposed here, they will be found with the Knuth-Bendix procedure for strings using an order on words I call the right-to-left wreath product ordering. Any word over X can be written in the form

$$U_0 x_1 U_1 x_2 ... U_{n-1} x_n U_n,$$

where $x_1 ... x_n$ is a word over X_1 and the U_i are words over X_2. To compare two words, construct this decomposition of each word and then compare the associated words over X_1 using the len-lex order. If these words are equal, then compare the two words U_n, again using the len-lex order. If these are equal, compare the words U_{n-1}, and so on.

Start the Knuth-Bendix procedure for strings going with the generators X and the relators $\mathcal{R}$ using the right-to-left wreath product ordering. If H really has finite index in G and the Knuth-Bendix systematically computes all overlaps of rules, then eventually the elements of $\mathcal{S}$ will rewrite to words over X_2. Periodically

interrupt the computation and check whether each element of $\mathcal{S}$ rewrites to a word over X_2. If this is the case, stop the Knuth-Bendix computation.

Using the rewritten Schreier generators and the ordinary coset table, it is now possible to write down an extended coset table for H. The Reidemeister-Schreier relators for H can now be computed. One may add the new relators to the previous Knuth-Bendix computation and run it for a while longer. This may reduce the lengths of the Schreier generators as words over X_2 and thus reduce the length of the Reidemeister-Schreier relators. These relators are consequences of those determined earlier, but it might take the Knuth-Bendix procedure a long time to discover them.

Using the methods outlined here, the original problem in $B(2,5)$ was solved. A set $\mathcal{T}$ was found such that

$$\langle x, y, z \mid \mathcal{T} \rangle$$

has largest nilpotent, exponent-5 quotient of order 5^{31}. The cardinality of $\mathcal{T}$ is 15, the minimum possible, and the longest words in $\mathcal{T}$ have length 38. I believe this cannot be shortened, but I do not have a proof.

References

[1] C. C. Sims, *Computation with finitely presented groups*, Encyclopedia of Mathematics and Its Applications 48, Cambridge University Press (1994).

Computing maximal subgroups of finite groups

Colva M. Roney-Dougal

(joint work with John N. Bray and Derek F. Holt)

The maximal subgroups of a finite group G yield much information about the internal structure and representations of G. Additionally, they have many computational applications.

An *almost simple* group is a group G such that there exists a nonabelian simple group T with $T \trianglelefteq G \leq \operatorname{Aut} T$.

Work of Cannon and Holt [2], or (independently) Eick and Hulpke [3] reduces the problem of computing the maximal subgroups of an arbitrary permutation or matrix group G to that of computing the maximal subgroups of all almost simple groups with socle a composition factor of G. Constructive recognition further reduces the problem of computing maximal subgroups to that of constructing the maximal subgroups of the almost simple groups in their natural representations.

After briefly surveying the current state of knowledge of the maximal subgroups of the alternating and sporadic groups, this talk will concentrate on the maximal subgroups of the finite classical groups. For these groups, Aschbacher's theorem [1] provides a detailed description of nine classes of subgroups, such that any maximal subgroup is a maximal member of one of these classes. Kleidman and Liebeck [5] describe the structure of the candidate maximal subgroups in the first eight of these classes; the ninth class consists (projectively) of almost simple groups G such

that $\operatorname{Soc} G$ is absolutely irreducible, written over a minimal field, and preserves an appropriate classical form.

For $n \geq 13$, Kleidman and Liebeck in [5] describe exactly when a candidate maximal subgroup in the first eight of the Aschbacher classes is in fact maximal. Work of Hiß and Malle [4] and Lübeck [6] yields a list of socles of candidate maximal subgroups in the ninth class. This talk will end with presenting recent work which classifies the maximal subgroups of all almost simple groups of Lie type that have projective representations in dimension at most 12.

References

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

[2] J. J. Cannon and D. F. Holt. Computing maximal subgroups of finite groups. *J. Symbolic Comput.* **37** (2004), 589–609.

[3] B. Eick and A. Hulpke Computing the maximal subgroups of a permutation group I. In W.M. Kantor and Á Seress, eds, Groups and Computation III, Ohio, 1999, pages 155-168. *Walter de Gruyter*, 2001.

[4] G. Hiß and G. Malle. Low-dimensional representations of quasi-simple groups. *LMS J. Comput. Math.* **4** (2001), 22–63. Corrigenda: *LMS J. Comput. Math.* **5** (2002), 95–126.

[5] P. B. Kleidman and M. W. Liebeck. The subgroup structure of the finite classical groups. London Mathematical Society Lecture Note Series, 129. *Cambridge University Press, Cambridge,* 1990.

[6] F. Lübeck. Small degree representations of finite Chevalley groups in defining characteristic. *LMS J. Comput. Math.* **4** (2001), 135–169.

Computations in exceptional groups and Lie algebras

Robert A. Wilson

(joint work with Kay Magaard)

Before the main talk, I announced two recent results. The first was completed last week:

Theorem 1. *There is exactly one conjugacy class of subgroups isomorphic to* $\mathrm{PSL}_2(41)$ *in the Monster sporadic simple group. Such subgroups are maximal.*

The second was completed this morning:

Theorem 2. *(with Laszlo Babai) The Guest–Praeger lower bound of* $c/n^{3/4}$ *for the proportion of odd-order elements in a symplectic or orthogonal group in dimension* n *over a field of odd order is best possible.*

The main talk was on algorithmic construction of a Chevalley basis in a Lie algebra. Given a Lie algebra in a computational setting, perhaps in the adjoint representation, as a vector space of dimension n with the n^3 structure constants defined on the basis, one wants to change basis so that it appears in canonical form. This generally means that we want a Chevalley basis. For applications to constructive recognition of matrix groups, we assume the input is written over a

finite field, and the Lie algebra is (say) simple. We are most interested in the Lie algebras of exceptional type, but the algorithms should work more generally.

The essential problem, in dealing with a field which is not algebraically closed, is that we want a split toral subalgebra (a Cartan subalgebra), whereas most toral subalgebras are non-split.

Several such algorithms are already in the literature, due to Ryba [3], Cohen and Murray [1], and others. They generally work by a process of successive approximation, making a series of toral subalgebras, each more split than the last (in the sense that it splits into more pieces, not in the sense that it has more 1-dimensional pieces). They also divide the calculation into two phases: first find a split toral subalgebra, and second, diagonalise it, label the root spaces, and choose suitable basis vectors.

In our algorithm, we split off one dimension of the Cartan subalgebra at a time, and compute the subalgebra and the root spaces simultaneously, constructing the Dynkin diagram and labelling the roots as we go. The main idea is to pick random elements x of the Lie algebra, until we find one such that $\mathrm{ad}\,(x)$ has a pair of 1-dimensional eigenspaces. Then we build the $\mathfrak{a}_1$-subalgebra $\langle e_\alpha, e_{-\alpha}, h_\alpha \rangle$ they generate. Next we compute suitable eigenspaces V^+, V^- of $\mathrm{ad}\,(h_\alpha)$, so that they contain the next root vectors $e_\beta, e_{-\beta}$, for the next root β along the Dynkin diagram. To find these explicitly, we take random $x \in [V^+, V^-]$ until we get 1-dimensional eigenspaces of $\mathrm{ad}\,(x)$. Iterate this process until all nodes of the Dynkin diagram are found. (It is not necessary to know the Dynkin diagram in advance, as there is only a small number of possibilities for where to draw the next node at each stage, and one can try them all.) Finally we adjust the scalars to get the standard Chevalley basis.

There are extra complications in characteristics 2 and 3, which we do not yet address: these have been largely solved already by Cohen and Roozemond [2], although they do assume that a split Cartan subalgebra has already been found, which may not be the case in practice.

In the case when the characteristic is at least 5, the complexity of our algorithm is essentially r^7, where r is the Lie rank, which improves on Cohen and Murray's quoted complexity of r^9 (and Ryba's r^{11}).

References

[1] A. M. Cohen and S. H. Murray, *An algorithm for Lang's theorem*, J. Algebra **322** (2009), 675–702.

[2] A. M. Cohen and D. Roozemond, *Computing Chevalley bases in small characteristics*, J. Algebra **322** (2009), 703–721.

[3] A. J. E. Ryba, *Computer construction of split Cartan subalgebras*, J. Algebra **309** (2007), 455–483.

Algorithmic Generalisations of Small Cancellation Theory

Max Neunhöffer
(joint work with Stephen Linton, Richard Parker, Colva Roney-Dougal)

This talk gives an overview over our project to generalise Small Cancellation Theory in an algorithmic direction. As of now, there are no publications of results or software that have come out of this project although we are already working on it for about 4 years. I will describe the envisioned generalisations briefly.

The first idea is to change the ambient group. We want to replace the free group in classical Small Cancellation Theory (SCT) by the following construction:

Let Γ be a groupoid, i.e. a small category in which every morphism is invertible. Let

$$A := \bigcup_{X,Y \in \mathrm{ob}_\Gamma} \mathrm{Mor}_\Gamma(X, Y)$$

be our alphabet. Then the set A^* of finite words in A with concatenation is a monoid.

The multiplication in Γ defines a terminating and confluent RW-system on A^*. Let $F := A^*/\sim$ where $\sim$ is rewrite-equivalence. Then F is a group.

In our generalised SCT we are going to do the following: Let $R \subseteq A^*$ be a finite set of relators. We want to devise an algorithm $\mathcal{SC}$ that:

- delivers and proves correct an algorithm $\mathcal{WP}$ that decides whether or not a $w \in F$ is a product of conjugates of relators, and
- delivers a function $f : \mathbb{N} \to \mathbb{N}$ and proves for it that every rewrite-reduced $w \in F$ of length n that is equal to a product of conjugates of elements of R at all, is actually equal to such a product with at most $f(n)$ factors,
- or fails.

As in the classical SCT it is possible that a given presentation is not susceptible to this method, after all, the word problem for this presentation could be unsolvable, i.e. no algorithm $\mathcal{WP}$ as above exists.

In this talk I explain how we have generalised the notion of van Kampen diagrams to the above generalised setup, how we use a notion of combinatorial curvature and local redistribution of such together with an algorithmic local analysis of van Kampen diagrams to produce the above mentioned algorithm $\mathcal{SC}$. Finally I give an outlook at further generalisation ideas in this area.

We expect that in a few years time we will have developed, proved correct and analysed algorithms fulfilling the above task. They should run successfully on rather large presentations of hyperbolic groups, which actually arise in applications in other fields like topology. This ought to give us a completely new way to work with such finitely presented groups on a computer.

Splitting full matrix algebras over algebraic number fields

Lajos Rónyai
(joint work with Gábor Ivanyos, Josef Schicho)

We consider the following algorithmic problem, which we call *explicit isomorphism problem*: *let $\mathbb{K}$ be an algebraic number field, A an associative algebra over $\mathbb{K}$. Suppose that A is isomorphic to the full matrix algebra $M_n(\mathbb{K})$. Construct explicitly an isomorphism $A \to M_n(\mathbb{K})$. Or, equivalently, give an irreducible A module.*

Recall that for an algebra A over a field $\mathbb{K}$ and a $\mathbb{K}$-basis $a_1, \ldots, a_m$ of A over $\mathbb{K}$ the products $a_i a_j$ can be expressed as linear combinations of the a_i

$$a_i a_j = \gamma_{ij1} a_1 + \gamma_{ij2} a_2 + \cdots + \gamma_{ijm} a_m.$$

The elements $\gamma_{ijk} \in \mathbb{K}$ are called structure constants. Here an algebra is considered to be given as a collection of structure constants. The usual representation of a number field $\mathbb{K}$ over $\mathbb{Q}$ with the minimal polynomial $f \in \mathbb{Z}[x]$ of an algebraic integer $\alpha \in \mathbb{K}$ with $\mathbb{K} = \mathbb{Q}(\alpha)$ can also be considered this way.

For basic definitions and facts from the theory of finite dimensional associative algebras the reader is referred to [14] and [16].

To obtain a decomposition of A into minimal left ideals, one has to be able to solve the explicit isomorphism problem for simple algebras over $\mathbb{K}$. In [18] this was shown to be possible in randomized polynomial time when $\mathbb{K}$ is finite. This method was derandomized recently in [9] in the case when the dimension of A over $\mathbb{K}$ is bounded. In [17] and [20] evidence (randomized reduction) is presented, that over algebraic number fields the explicit isomorphism problem problem is at least as difficult as the task of factoring integers, a problem not known to be amenable to polynomial time algorithms. For simple algebras over a number field $\mathbb{K}$ polynomial time Las Vegas algorithms were given in [4] and [1] to find a number field $\mathbb{L} \supseteq \mathbb{K}$ such that $A \otimes_{\mathbb{K}} \mathbb{L} \cong M_n(\mathbb{L})$ for a suitable n, together an explicit representation of the isomorphism. In [5] a real version was established: if $\mathbb{K} \subset \mathbb{R}$, and A splits over $\mathbb{R}$, then it can be achieved that $\mathbb{L} \subset \mathbb{R}$. These results have been derandomized.

We recall the notion of an *ff-algorithm*. It is an algorithm which is allowed to call an oracle for two types of subproblems. These are the problem of factoring integers, and the problem of factoring polynomials over finite fields. We have no deterministic polynomial time algorithms for these problems (but the latter one admits polynomial time randomized algorithms). In both cases the cost of the oracle call is the length of the input to the call.

In [19] the problem of deciding if $A \cong M_n(\mathbb{K})$ holds for an algebra A over a number field $\mathbb{K}$ was shown to be in $NP \cap coNP$. The proof relies on properties of maximal orders $\Lambda \leq A$ for central simple algebras A over $\mathbb{K}$. Maximal orders are in many ways analogous to the full ring of algebraic integers in $\mathbb{K}$. The principal result of [10] is a polynomial time ff-algorithm to construct maximal orders in simple algebras over $\mathbb{Q}$. A very similar algorithm is presented in [13]. In [20] a more direct method is given for quaternion algebras.

Several of the algorithms mentioned here have implementations in the computer algebra system Magma, see for example [12].

We mention also a somewhat surprising application of the algorithms for orders: they have been applied in the construction and analysis of high performance space time block codes for wireless communication, see [8]. In fact, in addition to an application of the algorithm of [10], in [8] an improvement is suggested for the orders relevant there.

A very recent result, joint work with Gábor Ivanyos and Josef Schicho, is a polynomial time ff-algorithm for the case when A is a central simple algebra of bounded dimension over a small extension field $\mathbb{K}$ of $\mathbb{Q}$. This was known before only in the smallest nontrivial case $\dim_{\mathbb{Q}} A = 4$, see [11] and the more recent papers [3], [20]. We have proved the following.

Theorem 1. *Let $\mathbb{K}$ be an algebraic number field of degree d and discriminant Δ over $\mathbb{Q}$. Let A be an associative algebra over $\mathbb{K}$ given by structure constants such that $A \cong M_n(\mathbb{K})$ holds for some positive integer n. Then an isomorphism $A \to M_n(\mathbb{K})$ can be constructed by an ff-algorithm. The time bound of our algorithm depends polynomially on $|\Delta|$ and the size of the structure constants of A, and exponentially on n and d.*

In particular, we have a polynomial time ff-algorithm when n, d and Δ are bounded.

In addition to computational representation theory where the problem naturally originates from, the explicit isomorphism problem arises also in connection with computing parametrizations in algebraic geometry: [3] considers parametrizations of conics, and [7] gives algorithms for rational parametrization of Severi-Brauer surfaces. In fact, in [7] an algorithm is given which solves the explicit isomorphism problem when $A \cong M_3(\mathbb{Q})$. This, however, uses a procedure for solving norm equations whose complexity was not clear so far. For example it was not known if they can be solved in ff-polynomial time. The case $A \cong M_4(\mathbb{Q})$ is treated similarly in [15]. An algorithm based on ideas similar to those of Theorem 1 is outlined in [2] for the case $\mathbb{K} = \mathbb{Q}$ and is detailed for the cases $n = 3, 5$.

Applications of our result include a polynomial time ff-algorithm to compute isomorphisms of central simple algebras of bounded degree over $\mathbb{K}$.

By the well known connection between split cyclic algebras and relative norm equations our results imply that for a number field $\mathbb{K}$ and a cyclic extension $\mathbb{L}$ of $\mathbb{K}$ if a norm equation $N_{\mathbb{L}/\mathbb{K}}(x) = a$ is solvable, then there is a solution whose standard representation has polynomial size (in terms of the size of the standard representation of a and the input size of $\mathbb{L}$). Moreover, for fixed $\mathbb{K}$ and fixed degree $|\mathbb{L} : \mathbb{K}|$, a solution can be found by a polynomial time ff-algorithm.

Potential directions to improve our results would be to obtain polynomial time ff-algorithms when the dimension of the algebra over $\mathbb{K}$ may be allowed to grow, or when $\mathbb{K}$ is allowed to vary (even if its degree over $\mathbb{Q}$ remains fixed), or both. Existence of ff-algorithms with similar time bounds for finding an explicit isomorphism of a non-split central simple algebra with a suitable algebra of matrices over a skewfield is also left open (even in the case of fixed base field, or fixed dimension).

References

[1] L. Babai, L. Rónyai, *Computing irreducible representations of finite groups*, Mathematics of Computation **192** (1990), 705-722.
[2] J. Cremona, T. Fisher, C. O'Neil, D. Simon, M. Stoll, *Explicit n-descent on elliptic curves III. Algorithms*, ArXiv 1107.3516
[3] J. E. Cremona, D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), 1417-1441.
[4] W. M. Eberly, *Computations for algebras and group representations*, Ph. D. Thesis, Dept. of Computer Science, University of Toronto, 1989.
[5] W. M. Eberly, *Decompositions of algebras over* $\mathbb{R}$ *and* $\mathbb{C}$, Computational Complexity **1** (1991), 207-230.
[6] T. Fisher, *How to trivialise an algebra*, http://www.faculty.jacobs-university.de/mstoll/workshop2007/fisher2.pdf
[7] W. A. de Graaf, M. Harrison, J. Pílniková, J. Schicho, *A Lie algebra method for rational parametrization of Severi-Brauer surfaces*, Journal of Algebra **303** (2006), 514–529.
[8] C. Hollanti, J. Lahtnonen, K. Ranto, R. Vehkalahti, *On densest MIMO lattices from cyclic division algebras*, IEEE Trans. Inform. Theory **55** (2009), 3751-3780.
[9] G. Ivanyos, M. Karpinski, L. Rónyai, N. Saxena, *Trading GRH for algebra: algorithms for factoring polynomials and related structures*, Mathematics of Computation, to appear.
[10] G. Ivanyos, L. Rónyai, *Finding maximal orders in semisimple algebras over* $\mathbb{Q}$, Comput. complexity **3** (1993), 245–261.
[11] G. Ivanyos, Á. Szántó, *Lattice basis reduction for indefinite forms and an application*, Discrete Math. **153** (1996), 177–188.
[12] http://magma.maths.usyd.edu.au/magma/handbook/text/840
[13] G. Nebe, A. Steel, *Recognition of division algebras*, Journal of Algebra **322** (2009), 903–909.
[14] R. S. Pierce, *Associative algebras*, Springer-Verlag, 1982.
[15] J. Pílniková, *Trivializing a central simple algebra of degree 4 over the rational numbers*, *J. Symbolic Comput.* **42** (2007), 579–586.
[16] I. Reiner, *Maximal orders*, *Academic Press, 1975.*
[17] L. Rónyai, *Zero divisors in quaternion algebras*, Journal of Algorithms **9** (1988) 494–506.
[18] L. Rónyai, *Computing the structure of finite algebras,* Journal of Symbolic Computation **9** (1990) 355–373.
[19] L. Rónyai, *Algorithmic properties of maximal orders in simple algebras over* $\mathbb{Q}$, Comput. Complexity, **2** (1992), 225–243.
[20] J. Voight, *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, manuscript, 2010.

Problems in Representation Theory

Meinolf Geck

This is a survey talk, upon invitation by the organisers. It is divided into two parts: (1) ATLAS projects and (2) group-theoretical applications.

The ATLAS projects that we are referring to are concerned with properties of finite simple groups and related algebraic structures:

Cambridge Atlas	Oxford University Press, 1985
Modular Atlas	`http://www.math.rwth-aachen.de/~MOC`
Atlas of Finite Group Representations	`http://brauer.maths.qmul.ac.uk/Atlas/v3/`
CHEVIE	`http://www.math.rwth-aachen.de/~CHEVIE`

The systematic collection of information about the various types of finite simple groups is in itself a formidable project and, at the present state of knowledge, far from completion (especially as far as modular representations are concerned). At the same time, the available information contained in these ATLASES is tremendously helpful in connection with the classification of finite simple groups. We are now seeing a growing number of problems or conjectures about general finite groups for which a reduction to the simple case has been achieved. Since finite simple groups have a rich structure and so much is known about them, there is at least a reasonable hope that it might be possible to verify the required properties for this class of groups. For example, this approach appears to be close to a successful completion as far as the McKay Conjecture is concerned; see [4] where the relevant reduction theorem is established.

In the second part of the talk we discuss two situations in which purely group-theoretical problems have been solved using character-theoretic methods. In both cases, it was well-known that reformulations in terms of character theory did exist but it was not immediately clear that these reformulations would indeed lead to a reasonable strategy for attacking the problem. The two situations are:

Problem 1: Let C_1, C_2, C_3 be conjugacy classes in a finite group G. Is it possible to find elements $x \in C_1$ and $y \in C_2$ such that $xy \in C_3$?

Problem 2: Let H be a subgroup of a finite group G and C be a conjugacy class in G. Then determine the cardinality $|C \cap HxH|$ for $x \in G$.

Problem 1 has a positive solution if and only if

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1)\chi(g_2)\chi(g_3^{-1})}{\chi(1)} \neq 0 \qquad \text{(where } g_i \in C_i \text{ are fixed).}$$

This criterion has been successfully applied, for example, in connection with the "rigidity criteria" for realising finite groups as Galois groups (see [9]), or in questions concerning the generation of finite simple groups by suitable elements (see [3], [10]). It is remarkable that this even works uniformly for infinite families of groups of Lie type, in the general framework of Lusztig's theory [6]; a useful feature in the above-mentioned applications is the fact that the classes C_i are such that many terms in the above sum are actually zero. In a different direction, Lusztig [7] has used this to classify embeddings of the alternating group A_5 (which is generated by an element of order 2 and an element of order 3 such that the product has order 5) into groups of exceptional Lie type. In this context, there are many non-zero terms in the above sum and it is quite remarkable that it is possible at all to compute the above sum with sufficient precision.

In order to deal with the second problem, consider the corresponding Hecke algebra $\mathcal{H}$, that is, the endomorphism algebra of the permutation module $\mathbb{C}[G/H]$. This algebra has a standard basis $\{T_x \mid x \in D\}$ where D is a complete set of representatives of the double cosets of H in G. Furthermore, we have a canonical bijection from the set of irreducible characters of $\mathcal{H}$ onto the set of those irreducible characters of G which occur in $\mathbb{C}[G/H]$; given $\varphi \in \mathrm{Irr}(\mathcal{H})$, we denote by χ_φ the

corresponding irreducible character of G. With this notation, we have

$$|C \cap HxH| = \frac{|H|}{|C_G(g)|} \sum_{\varphi \in \mathrm{Irr}(\mathcal{H})} \varphi(T_x)\, \chi_\varphi(g) \qquad \text{(with } g \in C \text{ fixed)}.$$

Lusztig [8] has recently constructed a natural surjective map from the set of conjugacy classes in a finite Weyl group W to the unipotent classes of the underlying algebraic group $\mathbf{G}$. For $\mathbf{G}$ of exceptional type, the proof relies on the above formula, applied to the case where $G = \mathbf{G}(\mathbb{F}_q)$ is the finite group of $\mathbb{F}_q$-rational points of $\mathbf{G}$ and H consists of the $\mathbb{F}_q$-rational points in a Borel subgroup of $\mathbf{G}$. Then the formula can be evaluated explicitly using the general theory developed in [6], tables of Green functions (see [5]) and character tables of Hecke algebras (see [2]). The actual computations were performed in GAP; for further details and worked examples, see the survey [1]. In this way, explicit computations with GAP and CHEVIE are used to establish a geometric result about algebraic groups.

References

[1] M. Geck, *Some applications of* CHEVIE *to the theory of algebraic groups*, Carpath. J. Math., **27** (2011), 64–94.

[2] M. Geck, G. Pfeiffer, *Characters of finite Coxeter groups and Iwahori–Hecke algebras*, London Math. Soc. Monographs, New Series **21**, Oxford University Press, New York 2000.

[3] R. Guralnick, G. Malle, *Products of conjugacy classes and fixed point spaces*, J. Amer. Math. Soc. (2011), in press.

[4] I. M. Isaacs, G. Malle, G. Navarro, *A reduction theorem for the McKay conjecture*, Invent. Math. **170** (2007), 33–101.

[5] F. Lübeck, *Tables of Green Functions for Exceptional Groups*, online data electronically available at `http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/Green`.

[6] G. Lusztig, *Characters of reductive groups over a finite field*, Annals Math. Studies, vol. 107, Princeton University Press, 1984.

[7] G. Lusztig, *Homomorphisms of the alternating group A_5 to reductive groups*, J. Algebra **260** (2003), 298–322.

[8] G. Lusztig, *From conjugacy classes in the Weyl group to unipotent classes*, Represent. Theory **15** (2011), 494–530.

[9] G. Malle, *Exceptional groups of Lie type as Galois groups*, J. Reine Angew. Math. **392** (1988), 70–109.

[10] G. Malle, J. Saxl, T. Weigel, *Generation of classical groups*, Geom. Dedicata **49** (1994), 85–116.

Computing generators of the unit group of an integral abelian group ring

Willem A. de Graaf

(joint work with Paolo Faccin)

Let G be a finite abelian group. Consider the group of units of the integral group ring of G:

$$(\mathbb{Z}G)^* = \{u \in \mathbb{Z}G \mid u^{-1} \in \mathbb{Z}G\}.$$

By a theorem of Higman, $(\mathbb{Z}G)^* = \pm G \times F$, where F is a free abelian group. Moreover, a straightforward formula is known for the rank of F. We refer to [4] for an introduction into these matters.

The question remains what the generators of $(\mathbb{Z}G)^*$ are. In 1966 Bass gave a construction of a set of generators of a finite-index subgroup of $(\mathbb{Z}G)^*$. This was refined by Hoechsmann in 1992 ([3]), who gave a generating set of a subgroup of generally much smaller index. He called the elements of this group *constructible units*. Units lying outside this group are called *exotic*. Now the question is for what groups G the group ring $\mathbb{Z}G$ has exotic units. Regarding the group of constructible units, Hoechsmann wrote ([3]): "Does this method ever yield all units if $n = |G|$ is not a prime power? The answer seems to be affirmative for all $n < 74$." Moreover, for $n = 74$ he showed that there are exotic units. However, he did not answer the question for $n < 74$.

This talk outlines an algorithm for computing generators of $(\mathbb{Z}G)^*$. With its implementation in Magma we have computed generators of $(\mathbb{Z}G)^*$ for G of size ≤ 50 (except three cases), and for some G with $|G| > 50$. We found that for the groups of the orders 40, 48, 60, 63 the constructible units do *not* generate the full unit group. Here one possible exception is the group $C_2 \times C_2 \times C_2 \times C_6$ for which our computation did not terminate. (Here C_m denotes the cyclic group of order m.) However, for all other orders, that we tested, we found that either no group of that order yields exotic units, or that all groups of that order yield them. Therefore, we conjecture that also the above mentioned group has exotic units in its integral group ring. The index of the group of constructible units, for the groups that we considered, is small, i.e., 1, 2, 3, or 4.

The algorithm is based on the construction of two groups: the subgroup $\mathcal{H}$ of constructible units and a group U that comes from the isomorphism of $\mathbb{Q}G$ with a sum of cyclotomic fields. We have $\mathcal{H} \subset (\mathbb{Z}G)^* \subset U$, with both indices finite. We use these inclusions to compute generators of $(\mathbb{Z}G)^*$.

Roughly, this works as follows. Initially we set $H := \mathcal{H}$. We compute the primes dividing the index of H in U. If $(\mathbb{Z}G)^*$ is strictly bigger than H, there is an element of order p in the quotient $(\mathbb{Z}G)^*/H$, where p is one of the primes computed previously. This leads to a nontrivial coset in $M_p = (U^p \cap H)/H^p$. We enumerate this last set, and see whether we find nontrivial cosets $u^p H$ such that $u \in (\mathbb{Z}G)^*$. If we find such a u then we add it to H, and start from the beginning. In order to make this work we have to change it slightly: we have to run through the set of all $v \in U$ with $v^p = 1$, and see whether there is such a v with $uv \in (\mathbb{Z}G)^*$.

In the algorithm we need unit groups of cyclotomic fields. To compute those we use a construction due to Greither ([2]) of a finite-index subgroup, as well as a Magma program by Claus Fieker for "saturating" a subgroup at a given prime p.

A very important role in all our constructions is played by an algorithm to obtain multiplicative relations of elements of an algebraic number field (which in our case is always a cyclotomic field). For this we used a Magma program by Fieker, based on an algorithm by Ge ([1]).

References

[1] G. Ge. *Algorithms related to multiplicative representations of algebraic numbers*. PhD thesis, University of California, Berkeley, 1993.

[2] Cornelius Greither. Improving Ramachandra's and Levesque's unit index. In *Number theory (Ottawa, ON, 1996)*, volume 19 of *CRM Proc. Lecture Notes*, pages 111–120. Amer. Math. Soc., Providence, RI, 1999.

[3] Klaus Hoechsmann. Constructing units in commutative group rings. *Manuscripta Math.*, 75(1):5–23, 1992.

[4] César Polcino Milies and Sudarshan K. Sehgal. *An introduction to group rings*, volume 1 of *Algebras and Applications*. Kluwer Academic Publishers, Dordrecht, 2002.

Building a Platform for Parallel Computational Algebra

Stephen A. Linton

Recent developments in computer technology force us to consider parallel programming if we wish to continue exploiting more powerful hardware. Some previous software has supported particular models of parallel computations in group theory (ParGAP/MPI, Cooperman '99 and SCSCP, Freundt et al. '09). This talk describes an ongoing project to provide wide-ranging and flexible support in GAP for the development and and exploitation of parallel algorithms.

Our programming model for users focuses on "skeletons", parallel programs into which sequential content can be slotted to solve a particular problem. A challenge for the computational group theory community is to identify an appropriate set of skeletons small enough that they can be implemented efficiently but powerful enough to cover the most important group-theoretic computations.

The present state of the project is that a version of GAP is now available for interested parties with extensions to support threaded programming and synchronization primitives. Feedback and ideas are invited.

S^2

Laurent Bartholdi

1. Branched coverings

We consider *branched self-coverings* of spheres, namely continuous maps $f : S^2 \to S^2$ that locally, in complex charts, look like $z \mapsto z^d$ for some $d \geq 1$. The *post-critical set* of f is $P = \bigcup_{n\geq 1} f^n(\text{critical points of } f)$, and is assumed to be finite. We are interested in such f up to isotopy rel P; namely, $f \sim g$ if there exists a path of branched self-coverings from f to g whose post-critical set moves smoothly.

On the one hand, many examples of branched self-coverings can be constructed combinatorially, via triangulations; for these, it is natural to consider the maps up to isotopy. On the other hand, a fundamental theorem by Thurston claims

Theorem (Thurston)**.** *Let f be branched self-covering with $\#P \geq 3$. Then f is isotopic to a rational map if and only if f admits no "Thurston obstruction", namely, if and only if, for every collection $\mathcal{C}$ of non-peripheral curves on $S^2 \setminus P$, the $\mathbb{Q}\mathcal{C}$-endomorphism $c \in \mathcal{C} \to \sum_{d \in f^{-1}(c) \cap \mathcal{C}} d/\deg(f|d)$ has spectral radius < 1.*

Furthermore, in that case, the rational map is unique up to conjugation by a Möbius transformation.

2. Bisets

Questions on branched coverings can in fact readily be translated to group-theoretical questions as follows. The maps $f, i : S^2 \setminus f^{-1}(P) \to S^2 \setminus P$, with i the inclusion, induce group homomorphisms $f_*, i_* : H = \pi_1(S^2 \setminus f^{-1}(P)) \to G = \pi_1(S^2 \setminus P)$ on fundamental groups. Furthermore, f is a covering whence f_* is injective, and i is in general position whence i_* is split. These maps f_*, i_* are only well-defined up to inner automorphisms, because of the problem of choosing basepoints. The appropriate object to consider is the G-G-biset

$$B_f := (G \times G)/\{(g_1 i_*(h), g_2) = (g_1, f_*(h) g_2)\},$$

with its natural actions $g_0 \cdot [(g_1, g_2)] \cdot g_3 = [(g_0 g_1, g_2 g_3)]$. Say two G-G-bisets B, C are isomorphic if there exists a bijection $\phi : B \to C$ and an automorphism ψ of G such that $\psi(g)\phi(b)\psi(g') = \phi(gbg')$ holds.

Theorem (Kameyama [2], Nekrashevych [4])**.** *The biset B_f is, up to isomorphism, a complete invariant for f up to isotopy.*

The biset B_f is free qua left G-set, because f_* is injective; so B_f may be written in the form $G \times X$ for a set X, of cardinality the degree of f. The structure of the biset is then given by a multiplication table of the form $x \cdot g = g' \cdot x'$ for every $x \in X$ and (generator) $g \in G$. This makes these bisets amenable to computation.

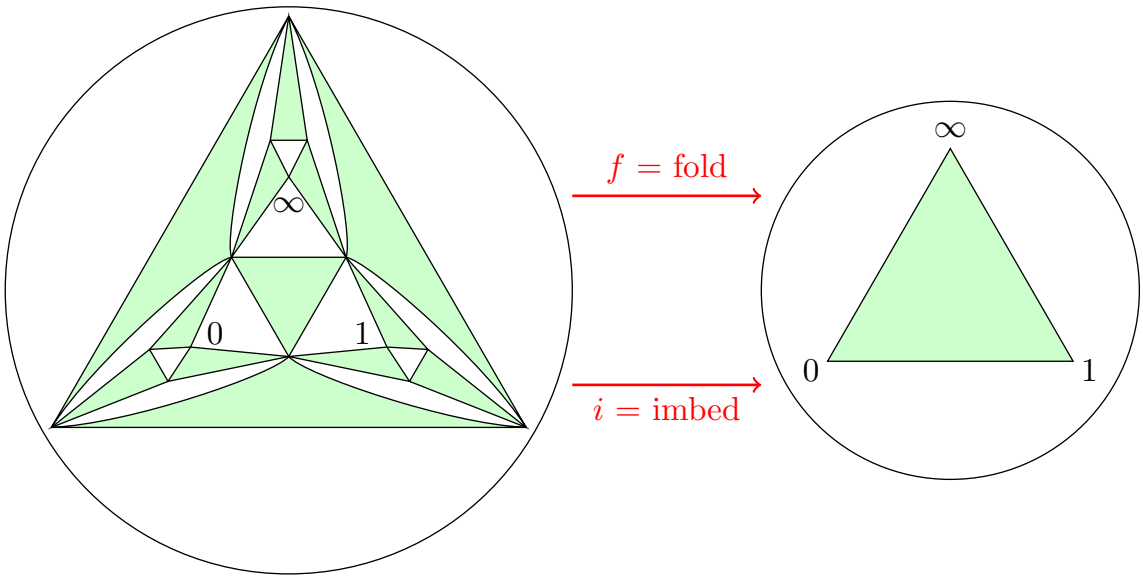
I explained, in my talk, how I developed algorithms (implemented in [1]) to solve the following tasks. They are implemented in the GAP package `fr`.

- **A1:** Given a complex approximation of a rational map, construct its associated biset;
- **A2:** Given bisets representing branched coverings, construct bisets for combinatorially related maps (e.g.: given two maps f, g with fixed critical point p_f, p_g of same degree, remove a neighbourhood of p_f, respectively p_g from S^2 and glue the spheres together along the cut);
- **A3:** Given a biset, compute either its associated rational map, up to some desired precision, or its associated Thurston obstruction.

I then illustrated it on two particular examples, described in the following §§.

3. Cui's map

Cui Guizhen suggested in 2010 that a "Sierpinski map", namely a rational map whose Julia set is a Sierpinski carpet, should have an invariant non-peripheral curve with unbounded number of preimages. He then found a counterexample, given combinatorially as follows:



I have computed the associated rational map, as follows. First, the above picture translates to a biset $B \cong G \times X$, with

$$G = \langle g_0, g_1, g_\infty \mid g_0 g_1 g_\infty \rangle, \qquad X = \{1, 2, \ldots, 13\},$$

and multiplication table

$\swarrow$	$1\cdot$	$2\cdot$	$3\cdot$	$4\cdot$	$5\cdot$	$6\cdot$	$7\cdot$
$\cdot g_0$	2	$g_0 \cdot 1$	5	3	4	7	6
$\cdot g_1$	$g_0^{-1} \cdot 8$	3	2	10	1	9	4
$\cdot g_\infty$	3	4	1	6	$g_0^{-1} \cdot 11$	8	9

$\swarrow$	$8\cdot$	$9\cdot$	$10\cdot$	$11\cdot$	$12\cdot$	$13\cdot$
$\cdot g_0$	$g_1^{-1} \cdot 9$	10	$g_0^{-1} \cdot 13$	12	11	$g_\infty^{-1} \cdot 8$
$\cdot g_1$	12	$g_1 \cdot 6$	7	13	$g_0 \cdot 5$	11
$\cdot g_\infty$	2	7	5	$g_0 \cdot 10$	$g_\infty \cdot 13$	12.

Note in particular the cycles

$$\pi = (1, 3, 12, 4)(5, 9)(6, 7)(10, 13, 11)(2, 8),$$

$$\rho = (1, 5, 13, 6)(7, 10)(2, 3)(8, 11, 12)(4, 9)$$

under which the basis X is permuted by g_0, g_1 respectively. These are the monodromy actions of a small loop around $0, 1$ respectively.

Write the sought rational map as a quotient of polynomials of degree 13, and write the equations that its coëfficients must satisfy if the map is to have branch points with the desired degrees (i.e. respect the cycle structure of π, ρ). These equations may be solved modulo 11, and then (by Hensel's lemma) lifted to solutions modulo $11^{2^{14}}$, namely approximate solutions in $\mathbb{Z}_{11}$. These solutions can then be rounded to algebraic numbers using the LLL algorithm [3]. Six solutions arise. This part of the search was done by H.-C. von Bothmer and J. Kröker.

My algorithm **A1** then checked that one of these is correct. Its Julia set is displayed in Figure 1.

FIGURE 1. Julia set of Cui's map

4. Pilgrim's map

In [5, §1.3.4], Kevin Pilgrim described a self-covering of the sphere, obtained from the $z \mapsto 2z$ map on the torus by rotating and blowing up an edge. It is a degree-5 map f, and Pilgrim asked whether it can be realized as a complex map. Combinatorially, the map subdivides the standard torus as described in Figure 2.

The biset may be written as $G \times X$, with

$$G = \langle a, b, c, d \mid dcba \rangle, \qquad X = \{1, 2, 3, 4, 5\},$$

and multiplication table

$1 \cdot a = c^{-1} \cdot 5$	$1 \cdot b = 2$	$1 \cdot c = a \cdot 4$	$1 \cdot d = b \cdot 1$
$2 \cdot a = 4$	$2 \cdot b = 1$	$2 \cdot c = 3$	$2 \cdot d = 2$
$3 \cdot a = 2$	$3 \cdot b = 3$	$3 \cdot c = 5$	$3 \cdot d = d \cdot 3$
$4 \cdot a = 3$	$4 \cdot b = d \cdot 5$	$4 \cdot c = a^{-1} \cdot 1$	$4 \cdot d = a \cdot 4$
$5 \cdot a = c \cdot 1$	$5 \cdot b = d^{-1} \cdot 4$	$5 \cdot c = 3$	$5 \cdot d = c \cdot 5.$

My algorithm **A3** found after a few seconds that $\{ac\}$ is a Thurston obstruction, with Thurston endomorphism $(\frac{1}{2} + \frac{1}{2})$.

References

[1] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; 2008, (`http://www.gap-system.org`).

[2] Atsushi Kameyama, *The Thurston equivalence for postcritically finite branched coverings*, Osaka J. Math. **38(3)** (2001), 565–610.

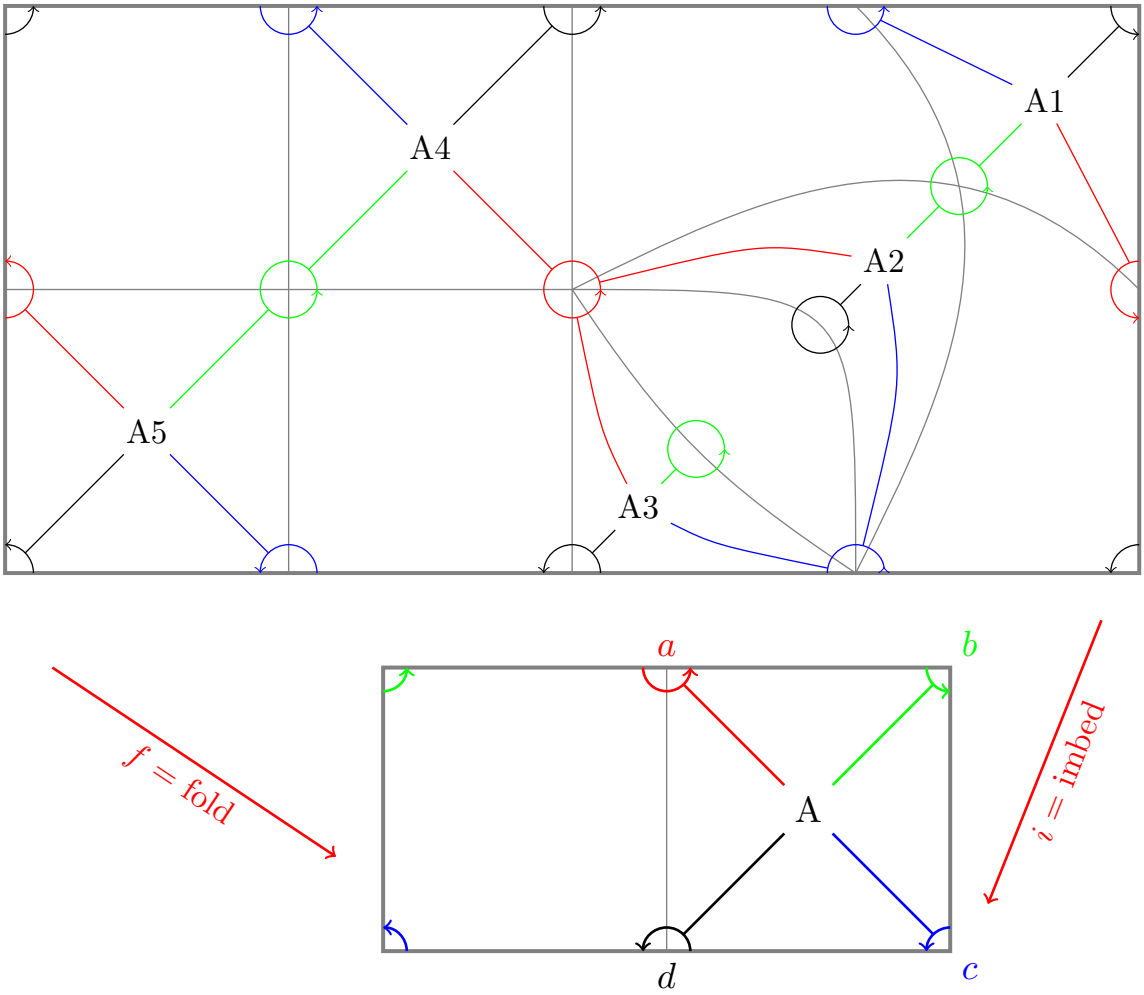


FIGURE 2. Target and source sphere of Pilgrim's map

[3] Arjen K. Lenstra, Hendrik W. Lenstra Jr. and László Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982) 4, 515–534.
[4] Volodymyr Nekrashevych, *Self-similar groups*, volume 117 of *Mathematical Surveys and Monographs*, Amer. Math. Soc., Providence, RI, 2005.
[5] Kevin M. Pilgrim, *Combinations of complex dynamical systems*, Lecture Notes in Mathematics **1827**, Springer-Verlag (Berlin), 2003, x+118 pages.

The matrix group recognition project, past and future

CHARLES R. LEEDHAM-GREEN
(joint work with H. Bäärnhielm, D. F. Holt, E. A. O'Brien)

Our project to construct a package to compute with matrix groups has at last, after very many years of effort by many people, reached a state in which it is functional, and has useful functionality. It is written in MAGMA, and makes use of a wide variety of sophisticated properties of that system, including some that have not otherwise been used in computational group theory.

A paper by Henrik Bäärnhielm, Derek Holt, Eamonn O'Brien, and myself describing the current state of our project, and acknowledging the contributions of many others, is in preparation.

The algorithm processes a matrix group over a finite field, given by generators, in two passes. The first pass, using Aschbacher's classification of matrix groups, and specialist code for the various families of finite simple groups, constructs a composition series (or composition tree) that passes through $O_p(G)$, where p is the characteristic of the field, but ignores other characteristic subgroups. The second pass constructs, from the composition tree, a more intrinsic composition series that refines a chief series that passes through each term of the series $1 \leq G_1 \leq G_2 \leq G_3 \leq G_4 \leq G$, where $G_1 = O_p(G)$, and G_2 is the soluble radical of G, and G_3/G_2 is the socle of G/G_2, and G_4 is the kernel of the permutation action of G on the set of simple factors of G_3/G_2. This series (without G_1, which is not relevant to their work) was used by Babai and Beals in [1] to initiate a very serious attack on the problem of deciding what can be determined about a finite matrix group, or a black box group, in polynomial time, with or without various oracles.

Our use of this series is to enable the use of algorithms developed by John Cannon and Derek Holt for calculating in finite groups for which the soluble radical is known.

The status of our package is roughly as follows.

The final steps in dealing with classical groups are now being put into place.

Rather more work remains to be done on some exceptional and twisted groups.

There remain problems with making Aschbacher's theorem constructive. We are not aware of any problems that we cannot deal with in a satisfactory way; but this is not the same as having a proof of a polynomial time algorithm.

A major breakthrough has very recently been made by Alex Ryba, who has finally found a polynomial time algorithm for deciding whether or not a matrix group is imprimitive or tensor decomposable. His algorithms, though not particularly fast, are practical, and are of fundamental importance. I am particularly grateful to Richard Parker for pointing out to me (and, apparently, to Ryba) that the algorithm deals with imprimitivity as well as tensor decomposition.

A further obstacle to producing a package that runs in provably polynomial time lies in dealing with groups of Lie type of small rank in characteristic 2.

For example, Henrik Bäärnhielm has some extremely interesting and original algorithms for computing in ${}^2F_4(q)$, the large Ree group over $\mathrm{GF}(q)$. Here q is an odd power of 2, and the problem arises when q is large. A randomly chosen element of G will then almost certainly be of odd order, and two randomly chosen elements will almost certainly generate the whole group, so it is not easy to obtain generators for a proper subgroup of even order. The problem then is to search symbolically, looking for a polynomial equation of $\mathrm{GF}(q)$ whose solution will give rise to an element of even order. To achieve this aim, a suitable element g of order $q-1$ is found by random search, and an element of even order is sought in random cosets of $\langle g \rangle$. The reduction of this search to the solution of a polynomial equation is subtle, but can be carried out, and the procedure is reliable and fast. However,

the polynomial time performance of the algorithm requires the even order elements to be very roughly uniformly distributed amongst the (right) cosets of $\langle g \rangle$, and to prove that this is the case seems an impossibly hard task.

As to the future, it is to be hoped that some of the work on the representation theory of finite groups that is concerned with actual representations will find its way into our project. For example, we recognise simple groups, and we should recognise their irreducible representations in so far as these are known.

A package with similar objectives is being written in GAP by A. Seress and M. Neunhöffer. We have taken from them the important idea of using 'nice generators' for the groups that appear in the nodes of the composition tree.

References

[1] L. Babai, R. Beals, *A polynomial-time theory of black box groups I*, "Groups St Andrews 1997 in Bath, I" (C.M. Campbell, E.F. Robertson, N. Ruskuc, G. C. Smith, eds.), London Math. Soc. Lect. Notes 260, Cambr. U. Press, 1999, 30–64.

Problem session

A problem session was held on August 4, 2011. The following problems and questions were presented.

Cheryl E. Praeger (joint with Frank Lübeck and Alice C. Niemeyer)**:**

Let $G = \mathrm{Class}(n, q)$ be a finite n-dimensional classical group over a field of odd order q, and let V be the natural module. Let Q consist of those $g \in G$ such that $|g|$ is even and such that the dimension of the fixed point subspace of $g^{|g|/2}$ in V lies in $[\frac{n}{3}, \frac{2n}{3})$. It was shown in [LNP] that $|Q|/|G| \geq c/\log(n)$ for some constant $c > 0$ depending on the Lie type of G. Also statistical tests reported in [LNP], and based on random samples from several classical groups, suggest that the $|Q|/|G|$ may not be statistically much different from $O(\log(n))$.

Question. What is the asymptotic value of $|Q|/|G|$? In particular, is it true that $|Q|/|G| = O(\log(n))$?

References

[LNP] F. Lübeck, A. C. Niemeyer, and C. E. Praeger. *Finding involutions in finite Lie type groups of odd characteristic*, J. Algebra **321** (2009), 3397-3417.

James B. Wilson:

Definition. If G is a group then we define the natural *central product* of G with itself as:

$$G \circ G = (G \times G)/\langle (z, z^{-1}) : z \in Z(G) \rangle.$$

It is well-known that

$$D_8 \circ D_8 \cong Q_8 \circ Q_8$$

yet D_8 and Q_8 are not isomorphic.

Question. If G and H are p-groups of class 2 and exponent p which are not themselves central products of proper subgroups, can

$$G \circ G \cong H \circ H$$

yet G and H be non-isomorphic?

It appears that an example of this sort may exist, however, a minimal counter-example appears to need order 5^{30} or greater. The interest as well as details surrounding this problem are given in [W] Section 8.2.

References

[W] J. B. Wilson, *Decomposing p-groups via Jordan Algebras*, J. Algebra 322 (2009) 2642-2679.

Laurent Bartholdi:

Let F be a free group of finite rank. Let $S = \{1, \ldots, k\}$ be a finite set, and let $\phi\colon F \to F \wr_S \mathrm{Sym}(S)$ be a homomorphism. Iterating ϕ, we get homomorphisms denoted $\phi^n\colon F \to F \wr_{S^n} \mathrm{Sym}(S^n)$, and therefore an action of F on S^n for any $n \geq 1$. Let N be the kernel of the induced action of F on $\bigsqcup_{n\geq} S^n$, the disjoint union of the previous actions.

For example, $F = \langle x, y\rangle$, $S = \{1, 2\}$, and $\phi(x) = \langle x^2, x^{-1}y, (1, 2)\rangle$, $\phi(y) = \langle xy, x, ()\rangle$. The permutation action of x on $\{1, \ldots, 2\}$ is $(1, 2)$, while that on $\{11, 12, 21, 22\}$ is $(11, 21, 12, 22)$.

Question. Can F/N have undecidable word problem?

For example, although it is not obvious, $yxy^{-1}xy^{-1}xyx^{-3} = 1$ in the above example.

Charles R. Leedham-Green:

Traditional computational group theory consists of manipulating specific elements of specific groups. In some cases, however, one needs to compute symbolically. For example, if G is a group of Lie type in characteristic 2, with defining field of size q, and if G is given by a generating set consisting of a small number of random elements, one generally needs, as a first step in computing with G, to find an involution; and since q can be exponentially large a random search may be too slow. The alternative, which we use in practice, is to reduce to a group H of small rank, such as $\mathrm{SL}(2, q)$, and then search symbolically in H for an element of even order. For example a set of $q - 1$ elements of G, a coset of some cyclic group, is defined by a parameter in $\mathrm{GF}(q)$, and a value of this parameter that will define an element of even order is obtained by solving a polynomial equation. Discrete logs are then used to express this value as a power of the chosen primitive element of $\mathrm{GF}(q)$, and hence to obtain the element as a word in the given generators.

There are increasingly many instances of symbolic computation in group theory. For example, D. Feichtenschlager, as student of B. Eick, carried out significant calculations in p-groups that were defined symbolically, and deep thought is an

algorithm that gives a symbolic formula for the product of two elements of a given p-group.

The question arises as to whether symbolic computation will play a major role in the future of computational group theory, or whether it will remain as a set of occasional tools.

Leonard H. Soicher:

Problem. For a given action of a group G on a (finite) set Ω, devise an algorithm which, given $\alpha \in \Omega$, determines a "canonical" element in the orbit α^G.

This has been done for certain specific actions, but I would like to see a general approach, if possible. Typically α^G will be extremely large and it will be impossible to enumerate the elements of α^G explicitly.

Eamonn A. O'Brien:

Problem. Construct all irreducible representations of A_n over $\mathbb{F}_q$ of degree d, where $n \leq 25$ and $d \leq n^3$.

This is motivated by the following much-studied problem: which irreducible representations of simple groups over finite fields have a base of size 2? For larger values of n, theoretical "gap results" can be used to describe such representations.

Reporter: Tobias Rossmann

Participants

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

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

Prof. Dr. Robert Beals
Center for Communications Research
IDA
805 Bunn Drive
Princeton NJ 08540
USA

Dr. Anton Betten
Department of Mathematics
Colorado State University
Weber Building
Fort Collins , CO 80523-1874
USA

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

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

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

Prof. Dr. Jon F. Carlson
Department of Mathematics
University of Georgia
Athens , GA 30602-7403
USA

Brian Corr
School of Mathematics & Statistics
The University of Western Australia
35 Stirling Highway
Crawley WA 6009
AUSTRALIA

Prof. Dr. Alla Detinko
Mathematics Department
National University of Ireland, Galway
University Road
Galway
IRELAND

Ian Gregor Dick
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
GB-London E1 4NS

Dr. Heiko Dietrich
Department of Mathematics
The University of Auckland
Private Bag 92019
Auckland
NEW ZEALAND

Prof. Dr. Bettina Eick
Institut Computational Mathematics
Technische Universität Braunschweig
Pockelsstr. 14
38106 Braunschweig

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

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

Prof. Dr. Meinolf Geck
Department of Mathematical Sciences
University of Aberdeen
King's College
Aberdeen AB24 3UE
SCOTLAND

Prof. Dr. Stephen P. Glasby
Department of Mathematics
Central Washington University
Ellensburg , WA 98926-7424
USA

Dr. Willem A. de Graaf
Dipartimento di Matematica
Universita di Trento
Via Sommarive 14
I-38050 Povo (Trento)

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

Prof. Dr. Gerhard Hiß
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

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

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

Prof. Dr. William M. Kantor
Department of Mathematics
University of Oregon
Eugene , OR 97403-1222
USA

Prof. Dr. Gregor Kemper
Zentrum Mathematik
TU München
Boltzmannstr. 3
85748 Garching b. München

Prof. Dr. Jürgen Klüners
Institut für Mathematik
Universität Paderborn
Warburger Str. 100
33098 Paderborn

Dr. Alexander Konovalov
School of Computer Science
University of St. Andrews
Jack Cole Building
North Haugh
GB-St. Andrews , Fife KY16 9SX

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

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

Dr. Frank Lübeck
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

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

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

Prof. Dr. Gunter Malle
Fachbereich Mathematik
T.U. Kaiserslautern
Erwin-Schrödinger-Straße
67653 Kaiserslautern

Dr. Jürgen Müller
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

Dr. Scott Murray
Faculty of Information Science
and Engineering
University of Canberra
Canberra , ACT 2601
AUSTRALIA

Prof. Dr. Gabriele Nebe
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

Dr. Max Neunhöffer
The Mathematical Institute
University of St. Andrews
North Haugh
GB-St. Andrews Fife KY16 9SS

Dr. Alice Niemeyer
School of Mathematics & Statistics
University of Western Australia
Nedlands WA 6009
AUSTRALIA

Dr. Felix Noeske
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

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

Richard A. Parker
62 Devonshire Road
GB-Cambridge CB1 2BL

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

Prof. Dr. Wilhelm Plesken
Lehrstuhl B für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

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

Dr. Colva M. Roney-Dougal
School of Mathematics & Statistics
University of St. Andrews
North Haugh
GB-St. Andrews Fife KY16 9SS

Prof. Dr. Lajos Ronyai
Computer and Automation Institute
Hungarian Academy of Sciences
Lagymanyosi u. 11
H-1111 Budapest

Dr. Tobias Rossmann
Mathematics Department
National University of Ireland, Galway
University Road
Galway
IRELAND

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

Dr. Csaba Schneider
Centro de Algebra
Universidade de Lisboa
Av. Prof. Gama Pinto 2
1649 - 003 Lisboa
PORTUGAL

Prof. Dr. Akos Seress
Department of Mathematics
The Ohio State University
100 Mathematics Building
231 West 18th Avenue
Columbus , OH 43210-1174
USA

Prof. Charles C. Sims
School of Mathematics & Statistics
The University of Western Australia
35 Stirling Highway
Crawley WA 6009
AUSTRALIA

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

Dr. Britta Späth
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

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

Prof. Dr. Michael R. Vaughan-Lee
Mathematical Institute
Oxford University
24-29 St. Giles
GB-Oxford OX1 3LB

Christian Weber
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

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

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