Mathematisches Forschungsinstitut Oberwolfach

Report No. 30/2006

Computational Group Theory

Organised by
Gerhard Hiß (Aachen)
Derek Holt (Coventry)
Mike Newman (Canberra)

July 2nd – July 8th, 2006

Abstract. This workshop on Computational Group Theory revealed the close connections between its main themes "finitely presented groups", "permutation groups", "matrix groups" and "representations of groups". The meeting also presented applications to the classification of Lie algebras and linear codes.

Mathematics Subject Classification (2000): 20-04,20-xx,17-08,22-04,05E20,68Q25,68W40.

Introduction by the Organisers

The workshop *Computational Group Theory* was the fifth of this title held at Oberwolfach. It was attended by 54 participants with broad geographic representation from four continents. Among the participants were 10 young researchers, visiting Oberwolfach for the first time, some of them still graduate students. We are grateful for the special EU funds making their visits possible.

The lecture program was divided into two sections. In the first we had a series of four invited longer lectures, 50 minutes each, given by distinguished, selected participants, surveying recent major developments in their fields. The first of these lectures was held by Eamonn O'Brien (Auckland), who gave a talk on "The latest developments in the matrix groups computation project". The second was given by Bill Kantor (Eugene) on "A presentation of presentations", introducing the remarkable result that all finite simple groups (except possibly ${}^2G_2(3^{2k+1})$) can be presented by a bounded number of generators and relations. In the third talk in this series Michael Vaughan-Lee (Oxford) reported on the recently completed classification of all p-groups of orders p^6 and p^7. Finally, Gregor Kemper (München) surveyed new developments in Computational Invariant Theory.

The other section was made up of 37 short twenty-minute lectures on new work or work in progress. We aimed at giving preference to the younger participants to present their results. This program structure prompted positive feedback by many participants.

The short talks reported on various computational aspects—data structures, algorithms, complexity, computer experiments—in a broad range of topics, including matrix groups, p-groups, finitely presented groups, permutation groups, representation theory of groups, invariant theory, group cohomology, Lie algebras and combinatorics. The analysis of algorithms requires a thorough theoretical background in the respective fields.

The talks also revealed the close interrelationship between the different topics. Work for finite p-groups uses Lie rings and algebraic groups, matrix group algorithms rely on methods for finitely presented groups as well as on representation theory, work on permutation groups uses representation theoretic information. The computational solution of open problems such as the construction of Brauer character tables or the cohomology rings of sporadic groups usually requires the application of almost all the known techniques. Methods from other parts of computer algebra, e.g., Gröbner bases, come into play in computational cohomology theory as well as in the construction of matrix groups which are factor groups of specific finitely presented groups, e.g., Hurwitz groups.

Despite the relatively large number of talks at this workshop, there was plenty of time for discussions. Needless to say that this time was well spent: numerous collaborations were continued and various others were started.

Workshop: Computational Group Theory

Table of Contents

Eamonn A. O'Brien
The matrix group recognition project: recent developments 1801

Henrik Bäärnhielm
The explicit isomorphism problem for the Big Ree groups 1803

Şükrü Yalçınkaya
Black box recognition of finite groups and related group theoretic constructions 1804

Mark Stather
Constructive Sylow Theorems 1805

Anton Betten
Computing Linear Codes and Orbits on Sets 1806

Leonard H. Soicher
Computational group theory problems arising from computational design theory 1809

Willem de Graaf
Constructing algebraic Lie algebras 1811

Csaba Schneider
LieAlgDB — A database of Lie algebras 1813

Peter A. Brooksbank (joint with Eugene M. Luks)
Algorithms for finite-dimensional modules 1814

Klaus Lux (joint with Thomas Hoffman, Robert Pawloski)
Homological Algebra in GAP 1814

Felix Noeske
Generating condensed algebras in practice 1816

Robert A. Wilson
Elementary constructions of the Ree groups 1818

John N. Bray (joint with Beth Holmes and Robert Wilson)
Explicit constructions of maximal subgroups of the Monster 1819

Götz Pfeiffer
Algorithms for Descent Algebras. 1822

William M. Kantor (joint with R. M. Guralnick, M. Kassabov, A. Lubotzky)
Short bounded presentations of finite simple groups 1824

Ákos Seress (joint with Max Neunhöffer)
A data structure for a uniform approach to computations with finite groups 1826

Charles R. Leedham-Green (joint with Eamonn O'Brien)
Finding standard generators in Classical Groups 1828

Michael Vaughan-Lee (joint with Mike Newman, Eamonn O'Brien)
The groups of order p^6 and p^7 1830

Bettina Eick
Computing with p-groups by coclass 1831

Edmund F. Robertson
Computer assisted proofs of the $F^{a,b,c}$ conjecture 1832

George Havas
Experiences with the Knuth-Bendix procedure 1834

Charles C. Sims
Computational Investigations of 4-Engel Groups 1837

Gregor Kemper
Computational Invariant Theory – new developments 1839

Gabriele Nebe
The invariants of the Clifford-Weil groups 1840

Daniel Robertz (joint with Wilhelm Plesken)
Representations, commutative algebra, and Hurwitz groups 1842

Max Neunhöffer (joint with Cheryl Praeger)
Computing minimal polynomials 1843

Anne Henke (joint with R. Hartmann, S. Koenig, R. Paget)
Stratification of diagram algebras 1845

Björn Assmann
Algorithmic use of the Mal'cev correspondence 1848

Laurent Bartholdi
Groups generated by automata 1849

Alexander Hulpke (joint with Alice Niemeyer)
Computing nonsolvable quotients of finitely presented groups 1852

David J. Green
Regularity in group cohomology: the groups of order 128 1854

Matthias Künzer
Comparison of spectral sequences 1856

Cheryl E. Praeger (joint with Steve Linton, Alice C. Niemeyer and Sven Reichard)
Permutations having order a multiple of the degree 1857

Alice C. Niemeyer (joint with Cheryl E. Praeger, Steve Linton)
Recognising k-set actions of symmetric groups 1859

Jürgen Müller (joint with Max Neunhöffer and Rob Wilson)
Enumeration of big orbits 1861

Colva M. Roney-Dougal (joint with John N. Bray, Derek Holt)
Maximal subgroups of finite groups: new developments 1864

Derek Holt (joint with John N. Bray and Colva M. Roney-Dougal)
Computing maximal subgroups of finite groups 1866

Alexander Konovalov (joint with Victor Bovdi)
Integral group ring of the first Mathieu simple group 1867

Frank Himstedt
Computing Character Tables of Parabolic Subgroups 1869

William R. Unger
Character Tables in MAGMA 1871

Scott H. Murray (joint with Arjeh Cohen, Willem de Graaf, Sergei Haller, and Don Taylor)
Computing in linear algebraic groups 1872

Abstracts

The matrix group recognition project: recent developments

Eamonn A. O'Brien

In this lecture we surveyed recent developments on the matrix group recognition project. This project seeks to develop effective well-understood algorithms for the study of subgroups of $\mathrm{GL}(d, q)$.

The *geometric approach* investigates whether a linear group G satisfies certain natural and inherent properties in its action on its underlying vector space. If so, it determines an *Aschbacher category* of G, identifies an $N \lhd G$ naturally associated with this category, and recursively studies G/N and N.

We reported on two new algorithms to decide membership in Aschbacher categories: work of Glasby, Leedham-Green and O'Brien [7] for the "smaller field modulo scalars" case; and work of Brooksbank, Niemeyer and Seress [6] for the "normaliser of extra-special group" case. At this time, algorithms exist to decide membership in the geometric categories; however not all have a rigorous analysis.

The *black-box group approach*, initiated by Babai and Beals [1], determines the abstract group-theoretic structure of G. Every finite group G has a series of characteristic subgroups

$$1 \leq O_\infty(G) \leq \mathrm{Soc}^*(G) \leq \mathrm{Pker}(G) \leq G,$$

where $O_\infty(G)$ is the largest soluble normal subgroup of G. Here $\mathrm{Soc}^*(G)/O_\infty(G)$ is the socle of the factor group $G/O_\infty(G)$, and so $\mathrm{Soc}^*(G)/O_\infty(G)$ is isomorphic to a direct product $T_1 \times \cdots \times T_k$ of nonabelian simple groups that are permuted by conjugation in G; further $\mathrm{Pker}(G)$ is the kernel of this permutation action. Variations of these ideas are used by Cannon and Holt as components of group-theoretic algorithms. Recently Mark Stather has developed a version of Kantor's Sylow p-subgroup algorithm which exploits this structure.

The immediate goal is to construct the composition or chief factors of the group. The major outstanding task is to write an element of the group as a straight-line program in the generators of the group.

We also considered the algorithm of Bray [4] to construct the centraliser of an involution. Recent results of Parker and Wilson [11] establish that this algorithm runs in polynomial time. We then discussed some recent algorithmic applications of involution centralisers. These include:

(1) Determine the characteristic of a black-box group of Lie type (Liebeck and O'Brien, [10]). This is significant since knowledge of the characteristic is a prerequisite both to applying the algorithms of [3] to name a finite simple group and to the various black-box constructive recognition algorithms.

(2) Decide whether a matrix group or black-box group of known characteristic is simple. Parker and Wilson [11] and Sukru Yalcinkaya independently answer this challenge problem originally posed by Babai and Shalev [2].

(3) The "centraliser-of-involution" constructive membership algorithm which is applicable to groups of Lie type in odd characteristic and to sporadic groups [9].
(4) Constructive recognition of classical groups: ongoing work of Leedham-Green and O'Brien.

Most of the algorithms for working with matrix groups are Monte Carlo. To upgrade them to Las Vegas requires knowledge of "short presentations" for finite simple groups. Recently there has been spectacular progress in this direction. Guralnick, Kantor, Kassabov, and Lubotzky [8] prove that every non-abelian finite simple group of rank n over GF(q) with the possible exception of ${}^2G_2(q)$ has a presentation with a bounded number of generators and relations and total length $O(\log n + \log q)$.

Components of this work are of independent interest. In particular their work and that of Bray, Conder, Leedham-Green and O'Brien [5] show that S_n and A_n have bounded presentations of length $O(\log n)$.

References

[1] László Babai and Robert Beals. A polynomial-time theory of black box groups. I. In *Groups St. Andrews 1997 in Bath, I*, volume 260 of *London Math. Soc. Lecture Note Ser.*, pages 30–64, Cambridge, 1999. Cambridge Univ. Press.

[2] László Babai and Aner Shalev. Recognizing simplicity of black-box groups and the frequency of p-singular elements in affine groups. In *Groups and Computation* III, Ohio State Univ. Math. Res. Inst. Publ., pages 39–62. de Gruyter, Berlin, 2001.

[3] László Babai, William M. Kantor, Péter P. Pálfy, and Ákos Seress. Black-box recognition of finite simple groups of Lie type by statistics of element orders. *J. Group Theory*, 5(4):383–401, 2002.

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

[5] J.N. Bray, M.D.E. Conder, C.R. Leedham-Green, and E.A. O'Brien. Short presentations for alternating and symmetric groups. Preprint 2006.

[6] Peter Brooksbank, Alice C. Niemeyer and Ákos Seress. A reduction algorithm for matrix groups with an extraspecial normal subgroup. *Finite Geometries, Groups and Computation*, (Colorado). De Gruyter, Berlin, 2006.

[7] S.P. Glasby, C.R. Leedham-Green and E.A. O'Brien. Writing projective representations over subfields. *J. Algebra*, 295:51–61, 2006.

[8] R.M. Guralnick, W.M. Kantor, M. Kassabov and A. Lubotzky. Presentations of finite simple groups: a quantitative approach. Preprint, 2006.

[9] P.E. Holmes, S.A. Linton, E.A. O'Brien, A.J.E. Ryba and R.A. Wilson. Constructive membership testing in black-box groups. Preprint, 2006.

[10] Martin W. Liebeck and E.A. O'Brien. Finding the characteristic of a group of Lie type. Preprint, 2006.

[11] Christopher W. Parker and Robert A. Wilson. Recognising simplicity of black-box groups. Preprint, 2006.

The explicit isomorphism problem for the Big Ree groups

Henrik Bäärnhielm

In the *matrix recognition project* a goal is to develop efficient algorithms for the study of subgroups of $\mathrm{GL}(d, q)$. The classification due to Aschbacher (see [1]) provides one framework for this, and the first aim is to develop an algorithm that finds a composition series of a matrix group given by a set of generators. It is possible to do this with a recursive algorithm, and the recursion is described in [8]. However, we still have to deal with the base cases, which are the finite simple groups.

The simple group is given as $G = \langle X \rangle$ where $X \subseteq \mathrm{GL}(d, q)$ for some degree d and field size q, and some problems that arise in the base cases are the following:

(1) The problem of *recognition* or *naming* of G, *i.e.* decide the name of G, as in the classification of the finite simple groups.

(2) The *constructive membership* problem. Given any $g \in \mathrm{GL}(d, q)$, decide whether or not $g \in G$, and if so express g as a word in X.

(3) The *explicit isomorphism* problem. Construct an isomorphism ψ from G to a *standard copy* H of G such that $\psi(g)$ and $\psi^{-1}(h)$ can be computed efficiently for any $g \in G$ and $h \in H$.

Here we are concerned with the last problem for the Big Ree groups, one of the exceptional families of finite simple groups, denoted ${}^2F_4(q)$ where $q = 2^{2m+1}$ for some $m > 0$. By [7] and [11], we are only interested in the case when we are given a representation of ${}^2F_4(q)$ in characteristic 2. By [12], any such representation is a tensor product of twisted copies of representations of dimensions 26, 246 and 4096.

Using [9], we can restrict ourselves to one of these representations, and here we will only consider dimension 26, the *natural representation.* All subgroups of $\mathrm{GL}(26, q)$ that are isomorphic to ${}^2F_4(q)$ are conjugate, and the standard copy is one of these conjugates. The explicit isomorphism problem then reduces to the following:

Let $S \leqslant \mathrm{GL}(26, q)$ be the standard copy of ${}^2F_4(q)$. Given $X \subseteq \mathrm{GL}(26, q)$ such that $\langle X \rangle \cong {}^2F_4(q)$, find $g \in \mathrm{GL}(26, q)$ such that $\langle X \rangle^g = S$.

Since we have no method for finding standard generators of $\langle X \rangle$, the problem is not a trivial MeatAxe module isomorphism problem (see [5] and [6]). Instead, we use the fact that ${}^2F_4(q)$ has a maximal subgroup of shape $\mathrm{Sz}(q) \wr 2$ (see [10]). We have an algorithm that finds involutions in ${}^2F_4(q)$, and using this together with [4] we can find this maximal subgroup in $\langle X \rangle$ and S.

Using [2] we can then find standard generators of these Suzuki groups, solve a module isomorphism problem and end up with an algorithm for our explicit isomorphism problem.

This way we obtain a polynomial time algorithm, given an oracle for the discrete logarithm problem in $\mathbb{F}_q$. It has been implemented in Magma (see [3]) and performs very well in practice.

References

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

[2] Henrik Bäärnhielm, *Recognising the Suzuki groups in their natural representation*, J. Algebra **300** (2006), no. 1, 171–198.

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

[4] J. N. Bray, *An improved method for generating the centraliser of an involution*, Arch. Math. (Basel) **74** (2000), no. 4, 241–245.

[5] D. F. Holt and S. Rees, *Testing modules for irreducibility*, J. Aust. Math. Soc. Series A **57** (1994), 1–16.

[6] G. Ivanyos and K. Lux, *Treating the exceptional cases of the MeatAxe*, Experiment. Math. **9** (2000), 373–381.

[7] V. Landazuri and G. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443.

[8] C. R. Leedham-Green, *The computational matrix group project*, Groups and Computation III, Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, 2001, pp. 113–121.

[9] Charles R. Leedham-Green and Eamonn A. O'Brien, *Recognising tensor products of matrix groups*, Intern. J. Algebra Comput. **7** (1997), 541–559.

[10] G. Malle, *The maximal subgroups of* ${}^2\mathrm{F}_4(q^2)$, J. Algebra **139** (1991), 52–69.

[11] G. M. Seitz and A. E. Zalesskii, *On the minimal degrees of projective representations of the finite Chevalley groups, ii*, J. Algebra **158** (1993), 233–243.

[12] R. Steinberg, *Representations of algebraic groups*, Nagoya Math. J. **22** (1963), 33–56.

Black box recognition of finite groups and related group theoretic constructions

Şükrü Yalçinkaya

Let X be a black box group with the property that $X/O_p(X)$ is a finite simple group of Lie type of odd characteristic p, where $O_p(X)$ is the p-core (or "unipotent radical") of X. Our principal aim is to recognize the group X, namely, determining whether $O_p(X) \neq 1$ and finding the structure of $X/O_p(X)$ with any given degree of certainty. The main algorithm is the construction of long root $\mathrm{SL}_2(q)$-subgroup in a finite quasi-simple group Lie type over a field of odd size q. The algorithm is based on the analysis of the structure of centralizers of involutions which is in turn a computational version of Aschbacher's "Classical Involution Theorem" [1]. In this talk, I will also present an algorithm which decides whether $O_p(X) \neq 1$. For the recognition of $X/O_p(X)$, Curtis-Tits presentations [4, 5] will be constructed, in other words, we will construct all "subsystem" subgroups of $X/O_p(X)$ which can be read from the extended Dynkin diagram of the corresponding simple group.

References

[1] M. Aschbacher, *A characterization of Chevalley groups over fields of odd order, I, II*, Ann. of Math. **106** (1977), 353–468.

[2] A. V. Borovik, *Centralisers of involutions in black box groups*, Contemp. Math. **298** (2002), 7–20.

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

[4] C. Curtis, *Central extensions of groups of Lie type*, J. fur Math. **220** (1965), 174–185.

[5] J. Tits, *Groupes semi-simples isotropes*, Colloque sur la théorie des groupes algébriques, Bruxelles (1962), 137–147.

Constructive Sylow Theorems

Mark Stather

Let G be a finite group and r a prime. Sylow's Theorem states that if r^k is the largest power of r dividing the order of G then there exists a subgroup of G of order r^k, moreover any two subgroups of order r^k are conjugate in G. Computationally one may view Sylow's Theorem as the following two problems -

Given a finite group G and a prime r -

(1) Write down generators for a Sylow r-subgroup of G.

(2) Given $P, S \in \mathrm{Syl}_r(G)$ find $g \in G$ such that $P^g = S$.

We present algorithms to solve these problems for any finite group G. These methods are based on those by Kantor in [1] and Kantor, Luks and Mark in [2]. If T is a nonabelian simple group occurring as a composition factor of G then we reduce problems (1) and (2) above to the following 4 problems in T:

(I) Construct a Sylow r-subgroup of T.

(II) Given $P, S \in \mathrm{Syl}_r(T)$, find $g \in T$ such that $P^g = S$.

(III) Compute a PC presentation of a Sylow r-subgroup of T.

(IV) Given an automorphism θ of T with $|\theta| \not| \, |T|$, find a Sylow p-subgroup of T normalised by θ, where p is the characteristic of T.

Practical solutions to problems (I),(II) and (III) in the case where T is a classical group are given in [3]. We also make use of well known algorithms to solve problems (1) and (2) in soluble groups defined by a PC presentation.

The major difference between this approach and that of Kantor is the use of the, so called, Trivial Fitting model for G. In short, Kantor's algorithms involves lifting a Sylow r-subgroup through a normal series of the group using the Frattini argument. That is, given $H \trianglelefteq G$ with $[G : H] = r$, and $S \in \mathrm{Syl}_r(H)$ we construct a Sylow r-subgroup P of G as follows:

Let $g \in G/H$. Find $h \in H$ such that $S^{gh} = S$, then $|gh| = r^\alpha b$, with $(r, b) = 1$. Then $P = \langle S, (gh)^b \rangle \in \mathrm{Syl}_r(G)$.

In particular Kantor's algorithms require a large number of recursions into subgroups of G.

We attempt to minimise the number of these recursions by making use of the Trivial Fitting model. Every finite group has a series of characteristic subgroups

$$1 \leq O_\infty(G) \leq \mathrm{soc}^*(G) \leq \mathrm{Pker}(G) \leq G$$

We define $\mathrm{soc}^*(G)$ to be such that $\mathrm{soc}^*(G)/O_\infty(G) = \mathrm{soc}(G/O_\infty(G))$ and so is isomorphic to a direct product of nonabelian simple groups. Let Δ be the set of all nonabelian simple groups contained in $\mathrm{soc}^*(G)/O_\infty(G)$, then G acts on Δ by conjugation. We define $\mathrm{Pker}(G)$ to be the kernel of this action and so $G/\mathrm{Pker}(G)$ is isomorphic to a subgroup of $\mathrm{Sym}(\Delta)$. Now conjugation by G induces a monomorphism $\alpha : G \to \mathrm{Aut}(\mathrm{soc}^*(G)/O_\infty(G))$ and $\alpha(\mathrm{Pker}(G))$ lies inside the subgroup of $\mathrm{Aut}(\mathrm{soc}^*(G)/O_\infty(G))$ that fixes all the nonabelian simple groups. So

$$\alpha(\mathrm{Pker}(G))/\alpha(\mathrm{soc}^*(G))$$

lies inside a direct product of outer automorphism groups of nonabelian simple groups, hence $\mathrm{Pker}(G)/\mathrm{soc}^*(G)$ is soluble by the Schreier conjecture and the Classification of Finite Simple Groups. For more details see [4], chapter 10.

If G is a matrix group defined over a finite field then we may use the methods described in my PhD thesis [5] to construct this characteristic series. If G is a permutation group then we may use the methods described by Cannon and Holt in [6]. Either of these methods will give us a PC presentation of $O_\infty(G)$ and $\mathrm{Pker}(G)/\mathrm{soc}^*(G)$. It should also be noted that constructive recognition algorithms are required for the nonabelian simple groups in $\mathrm{soc}^*(G)/O_\infty(G)$ so that we may work in the *standard copy*.

During the talk we outlined a practical solution to problem (IV) in the classical groups and gave an overview of a solution to (1) for a general finite group. It remains to provide solutions to problems (I),(II),(III),(IV) for the exceptional groups and problems (I),(II) and (III) for the sporadic groups ((IV) does not arise in this case). Henrik Bäärnhielm has provided solutions to (I),(II) and (III) for the Suzuki groups and a number of the sporadics are small enough to be dealt with using standard techniques. The author is in the process of developing a practical implementation of these algorithms in Magma.

References

[1] W. Kantor, *Sylow's Theorem in Polynomial Time*, Journal of Computer and System Sciences **30** (1985), 359–394.

[2] W. Kantor, E. Luks, P. Mark, *Sylow Subgroups in Parallel*, Journal of Algorithms, **31** (1990), 132-195.

[3] M. Stather, *Constructive Sylow Theorems for the Classical Groups*, preprint.

[4] D.F. Holt, *Handbook of Computational Group Theory*, Chapman & Hall, 2005.

[5] M. Stather, *Algorithms for Computing with Finite Matrix Groups*, PhD thesis, University of Warwick, 2006.

[6] J.J. Cannon, D.F. Holt, *Computing chief series, composition series and socles in large permutation groups*, J. Symb. Comp., **24(3/4)**, 285–301, 1997.

Computing Linear Codes and Orbits on Sets

Anton Betten

The purpose of this note is two-fold. First we consider the problem of computing isometry classes of linear codes. Secondly, we consider the general problem of computing orbits of groups on sets, including the problems of computing set-stabilizers and set-isomorphisms. This gives the famework in which the problem of computing codes can be solved. On the algorithmic side, we discuss the algorithm

$n\backslash k$	3	4	5	6	7	8	9	10	11	12	13	14
10	5^{2}	4^{19}	4^{4}	3^{4}								
11	6	5	4^{30}	4^{2}	3^{3}							
12	6^{6}	6	4^{214}	4^{41}	4^{2}	3^{2}						
13	7	6^{6}	5^{15}	4^{580}	4^{45}	4	3					
14	8	7	6^{6}	5^{11}	4^{1488}	4^{48}	4	3				
15	8^{3}	8	7	6^{5}	5^{6}	4^{3473}	4^{43}	4	3			
16	8^{12}	8^{4}	8	6^{180}	6^{3}	5	4^{7456}	4^{47}	4			
17	9^{2}	8^{18}	8^{4}	7^{3}	6^{377}	6	5	4^{14390}	4^{39}	3^{129}		
18	10	8^{108}	8^{34}	8^{2}	7^{2}	6^{918}	6		4^{25024}	4^{33}	3^{113}	
19	10^{6}	9^{7}	8^{411}	8^{28}	8	7	6^{1700}	5^{31237}		4^{39302}	4^{25}	3^{91}
20	11	10^{3}	9^{3}	8^{1833}	8^{26}	8	7	6^{1682}	5^{14135}			4^{24}
21		10^{27}	10^{2}			8^{12}	8	7	6^{739}	5^{2373}		
22			10^{37}	9^{248}			8^{9}	8	7	6^{128}	5^{128}	
23				10^{29}	9^{29}			8^{8}	8	7	6^{8}	5
24					10^{6}				8^{9}	8		6

Table 1. Isometry Classes of Optimal Indecomposable Binary Codes

known as "Orderly Generation" as well as the more recent invention of Schmalz, known as "Snakes and Ladders" (or "Leiterspiel" [9]).

In 1960, David Slepian writes in [10]:

> *"The task of analyzing group codes would be greatly simplified if a* `canonical form` *could be found for each equivalence class of Ω-matrices. That is, for a given n and k, we should like to be able to write down* `one generator matrix from each equivalence class.` *This would provide a simple means of describing each of the essentially different (n, k)-codes."*

The purpose of this note is to report on a practical approach for solving this problem. The solution relies on machinery from Computational Group Theory.

Contrary to many other approaches for computing codes (cf. [4], Chapter 7), we refine the problem by requiring that the minimum distance of the codes searched for be high.

As a result of the search, the author determined the number of isometry classes of optimal indecomposable binary linear codes as presented in Table 1. For small n and k, the table indicates the optimal minimum distance of binary (n, k)-codes as well as the number of isometry classes (in the exponent).

The construction of isometry classes turns out to be an orbit-type problem. In essence, the semilinear isometry classes of (n, k) codes over $\mathrm{GF}(q)$ with minimum distance at least d are in one-to-one correspondence to the orbits of $\mathrm{P\Gamma L}(n-k, q)$ on n-sets of points from $\mathrm{PG}(n-k-1, q)$ with the property that any $d-1$ points are independent. To compute these orbits, the author applied the algorithm "Snakes and Ladders" which proceeds inductively in a breadth first manner.

On the other hand, the algorithms of orderly generation due to Read [8], Faradžev [3] and McKay [7] also allow to compute orbits of groups on sets. These algorithms rely on a technique known as "partition backtrack" (cf. [5, 6]) to compute a "canonical form", which is simply a well-defined representative of an orbit (it may be the lexicographically least element in the orbit or it may be something else). The purpose of these canonical representatives is to do "isomorph rejection", which means that within the search we should never consider isomorphic partial solutions (i.e., sets which come from the same G-orbit, where G is the acting group). The complexity of partition backtrack is exponential in the size of the input, which makes it the dominating step in these algorithms. The idea behind "Snakes and Ladders" is to avoid backtrack as much as possible and thereby gain speed. The price is an increased demand in terms of storage. Essentially, one trades times versus memory. This may pay off well in the top of the search tree, where the pruning due to the symmetry group is very effective. On the other hand, it may become too costly at deeper levels of the search, in which case one might consider doing no group reduction at all from a certain point on.

For a more detailed description of the search, we refer to Chapter 9 of [2].

References

[1] I.F. Blake (ed.). *Algebraic coding theory: history and development.* Dowden Hutchinson & Ross Inc., Stroudsburg, Pa., 1973. Benchmark Papers in Electrical Engineering and Computer Science.

[2] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, A. Wassermann *Error-Correcting Linear Codes.* Springer-Verlag, Berlin, 2006 (in print).

[3] I.A. Faradžev. Constructive enumeration of combinatorial objects, Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976.) Colloq. Internat. CNRS 260, 131–135, Paris 1978.

[4] P. Kaski, P. Östergård. *Classification algorithms for codes and designs.* Algorithms and Computation in Mathematics 15, Springer-Verlag, Berlin, 2006.

[5] J.S. Leon. Permutation group algorithms based on partitions. I. Theory and algorithms. *J. Symbolic Comput.*, 12(4-5):533–583, 1991. Computational group theory, Part 2.

[6] J.S. Leon. Partitions, refinements, and permutation group computation. In *Groups and computation, II (New Brunswick, NJ, 1995)*, volume 28 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 123–158. Amer. Math. Soc., Providence, RI, 1997.

[7] B.D. McKay. Isomorph-free exhaustive generation. *J. Algorithms*, 26(2):306–324, 1998.

[8] R.C. Read. Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations. *Ann. Discrete Math.*, 2:107–120, 1978. Algorithmic aspects of combinatorics (Conf., Vancouver Island, B.C., 1976).

[9] B. Schmalz. t-Designs zu vorgegebener Automorphismengruppe. *Bayreuth. Math. Schr.*, 41:1–164, 1992. Dissertation, Universität Bayreuth, Bayreuth, 1992.

[10] D. Slepian. Some Further Theory of Group Codes. *Bell System Tech. J.*, 39:1219–1252, 1960. Also reprinted in [1] pp. 118–151.

Computational group theory problems arising from computational design theory

Leonard H. Soicher

1. DESIGN

The DESIGN package [9] for GAP [4] can construct, classify, partition and study block designs satisfying a very wide range of user-specified properties. The designs may be t-designs (simple or non-simple), but in general need not have constant block-size nor constant replication-number. The DESIGN package has already been used to generate, classify and study many new designs of interest to combinatorialists and statisticians; see, for example [1, 2, 3].

2. Linton's SmallestImageSet

In the course of developing the DESIGN package and using it to classify block designs, some interesting problems in (computational) group theory arose, the first being the need for algorithms to determine canonical orbit representatives. One very useful such algorithm I now use in design (and clique) classification is Steve Linton's `SmallestImageSet`, which, given a permutation group G on $\Omega = \{1, \dots, n\}$, and a subset S of Ω, determines the lexicographically least set in the G-orbit of S (see [8]). The use of canonical set-orbit representatives allows pairwise G-isomorph-rejection to be accomplished by determining the canonical representative of each set under consideration, sorting these representatives, and removing duplicates.

I now suggest that for every action of a group G on a finite set Ω we should consider how best to define a canonical element in a G-orbit, and given such a definition, develop algorithms to determine:

- given $\alpha \in \Omega$, whether or not α is the canonical element in α^G;
- given $\alpha \in \Omega$, the canonical element in α^G;
- given $\alpha \in \Omega$, an element $g \in G$ such that α^g is the canonical element in α^G.

3. Friendly subgroups

When John Arhin (my PhD student) and I were classifying various designs invariant under given groups, the following concept naturally arose twice.

Definition A subgroup H of a group K is a *friendly* subgroup of K if every subgroup of K isomorphic to H is conjugate in K to H.

Proposition 1. *Suppose G acts on a set Ω, and let $\alpha, \beta \in \Omega$, with H a friendly subgroup of G_α and H a subgroup of G_β. Then α and β are in the same G-orbit if and only if they are in the same $N_G(H)$-orbit.*

Proof. The if-part is trivial. For the converse, suppose $x \in G$ with $\alpha^x = \beta$. Then $G_\beta = (G_\alpha)^x$, and so H^x is a friendly subgroup of G_β. Since $H \leq G_\beta$, it must be conjugate in G_β to H^x, and so there is a $y \in G_\beta$ with $H^{xy} = H$. We thus have $xy \in N_G(H)$ and $\alpha^{xy} = \beta^y = \beta$. □

Proposition 2. *Suppose G acts on a set Ω, and let $\alpha, \beta \in \Omega$, with H a friendly subgroup of G_α. Then if β is in the same G-orbit as α, every subgroup of G_β that is isomorphic to H is conjugate in G to H.*

Proof. Suppose $x \in G$ with $\alpha^x = \beta$. Then $G_\beta = (G_\alpha)^x$, and so H^x is a friendly subgroup of G_β. Thus, if $J \leq G_\beta$ with $J \cong H$, then J is conjugate in G_β to H^x, and so J is conjugate in G to H. □

When classifying H-invariant objects up to G-equivalence (that is, up to being in the same G-orbit), for a given $H \leq G$, Proposition 1 allows us to avoid many tests to determine G-equivalence when $N_G(H)$-orbit representatives of the H-invariant objects have been determined. (For such an $N_G(H)$-orbit representative α, if H is a friendly subgroup of G_α then no G-equivalence tests involving α are required.)

When classifying H_i-invariant objects for various pairwise isomorphic, but non-conjugate, subgroups H_i of G, Proposition 2 allows us to avoid many tests to determine when an H_i-invariant object is G-equivalent to an H_j-invariant one. (For a given H_i-invariant α, if H_i is a friendly subgroup of G_α, then α cannot be in the same G-orbit as an H_j-invariant object, when $i \neq j$.)

It is often possible to use cheap computational tests to confirm that a subgroup H of a finite group K is a friendly subgroup (when it is such a subgroup), making use of the following result.

Theorem 1. *Let K be a finite group and H a subgroup of K. Then H is a friendly subgroup of K if one or more of the following holds:*

1. *$H = K$;*
2. *K is cyclic;*
3. *H is a Hall subgroup of K (i.e. $\gcd(|H|, |K:H|) = 1$) and H is supersoluble (see [7]);*
4. *H is a nilpotent Hall subgroup of K (such as a Sylow subgroup), or more generally, H is a friendly subgroup of a nilpotent Hall subgroup of K (see [10]);*
5. *K is soluble and H is a Hall subgroup of K, or more generally, K is soluble and H is a friendly subgroup of a Hall subgroup of K (see [6]).*

It is worth noting that F. Gross employs the Classification of Finite Simple Groups to prove that an odd-order Hall subgroup of a finite group is a friendly subgroup of that group (see [5]), but I prefer not to use this sledgehammer to crack the odd nut.

References

[1] R.A. Bailey, P.J. Cameron, P. Dobcsányi, J.P. Morgan and L.H. Soicher, *Designs on the web*, Discrete Math., to appear. Preprint available at: `http://designtheory.org/library/preprints/`

[2] P. Dobcsányi, D.A. Preece and L.H. Soicher, *On balanced incomplete-block designs with repeated blocks*, European J. Combinatorics, to appear. Preprint available at: `http://designtheory.org/library/preprints/`

[3] P. Dobcsányi and L.H. Soicher, *An online collection of t-designs*, 2005, `http://designtheory.org/database/t-designs/`

[4] The GAP Group, *GAP — Groups, Algorithms, and Programming*, Version 4.4; Aachen, St Andrews, 2004, `http://www.gap-system.org/`

[5] F. Gross, *Conjugacy of odd order Hall subgroups*, Bull. London Math. Soc. **19** (1987), 311–319.

[6] P. Hall, *A note on soluble groups*, J. London Math. Soc. **3** (1928), 98–105.

[7] P. Hall, *Theorems like Sylow's*, Proc. London Math. Soc. (3) **6** (1956), 286–304.

[8] S. Linton, *Finding the smallest image of a set*, ISSAC 2004, 229–234, ACM, New York, 2004.

[9] L.H. Soicher, *The DESIGN package for GAP*, Version 1.1, 2004, `http://designtheory.org/software/gap_design/`

[10] H. Wielandt, *Zum Satz von Sylow*, Math. Z. **60** (1954), 407–408.

Constructing algebraic Lie algebras

Willem de Graaf

Here we work over a field F of characteristic 0. A Lie algebra of $n\times n$-matrices over F is called algebraic if it is the Lie algebra of an algebraic group. Chevalley ([1]) has developed a theory of algebraic Lie algebras from which it follows that there is a unique smallest algebraic Lie algebra containing a given Lie algebra L. This is called the algebraic hull of L. In this talk we address the problem of computing a basis of the algebraic hull of a given matrix Lie algebra.

Results by Chevalley reduce the problem of finding the algebraic hull of L to the case where L is spanned by a single semisimple matrix X. Moreover, in this case Chevalley described the algebraic hull as follows. Let $\alpha_1,\dots,\alpha_n$ be the eigenvalues of X in an extension $F'\supset F$. Set

$$\Lambda = \{(e_1,\dots,e_n)\in\mathbb{Z}^n \mid \sum_i e_i\alpha_i = 0\}.$$

Let U be an $n\times n$-matrix over F' such that $UXU^{-1}=Y$ is diagonal with the α_i on the diagonal. Then the algebraic hull of (the Lie algebra spanned by) Y is

$$\mathfrak{g}(Y) = \{\mathrm{diag}(a_1,\dots,a_n) \mid a_i\in F',\ \sum_i e_ia_i = 0 \text{ for all } (e_1,\dots,e_n)\in\Lambda\}.$$

Furthermore, the algebraic hull of X is $\mathfrak{g}(X) = U^{-1}\mathfrak{g}(Y)U$. This Lie algebra is defined over F', but has a basis over F, which spans the algebraic hull over that field. Chevalley has also proved that $\mathfrak{g}(X)$ is contained in the associative algebra generated by X. This leads to an elegant algorithm for computing $\mathfrak{g}(X)$. We write down a basis of the associative algebra $A(Y)$ generated by Y. The description above of $\mathfrak{g}(Y)$ leads to linear equations on the coefficients of an element of $A(Y)$

that have to be satisfied in order that it belongs to $\mathfrak{g}(Y)$. These equations have a solution basis over F, which immediately gives a basis of $\mathfrak{g}(X)$.

The main problem with the algorithm above is the need for constructing the splitting field F' of the characteristic polynomial of X. Since in practice the construction of F' can pose severe problems, we would like to have an algorithm that avoids constructing this field. In the talk an algorithm is presented that works in many special cases. For this we suppose that the ground field is $\mathbb{Q}$, and that the characteristic polynomial of X is irreducible. In that case there are algorithms to compute the Galois group G of the characteristic polynomial of X.

It is straightforward to see that $\Lambda_{\mathbb{Q}} = \Lambda \otimes \mathbb{Q}$ is a G-module, in fact it is a submodule of the permutation module M of G. Let M be spanned by $v_1, \dots, v_n$. Then M splits as a direct sum of G-modules $M = M_0 \oplus M_1$. Here M_0 consists of all $\sum_i a_i v_i$ such that $\sum_i a_i = 0$ and M_1 is spanned by $v_1 + \cdots + v_n$. Now M_0 cannot be a submodule of $\Lambda_{\mathbb{Q}}$ as in that case all α_i would be equal. It is well-known that if G is 2-transitive then M_0 is irreducible. It can be proved that the same holds (over $\mathbb{Q}$) when n is prime. So in these cases we have $\Lambda_{\mathbb{Q}} = 0$ or $\Lambda_{\mathbb{Q}} = M_1$. Moreover, it can be shown that $\Lambda_{\mathbb{Q}} = M_1$ if and only if $\mathrm{Tr}(X) = 0$. Hence if G is 2-transitive or n is prime we can determine Λ without constructing F'. Finally, if $\Lambda_{\mathbb{Q}} = M_1$ then it can be shown that $\mathfrak{g}(X)$ consists of all X' in $A(X)$ with $\mathrm{Tr}(X') = 0$. It follows that in the special cases where G is 2-transitive or n is prime we have a straightforward algorithm for determining $\mathfrak{g}(X)$.

More generally if M has a unique direct sum decomposition as G-module we can determine $\Lambda_{\mathbb{Q}}$. This works as follows. In every direct summand we take a vector. Then we use p-adic approximations to the roots to determine whether this vector occurs in $\Lambda_{\mathbb{Q}}$. It does if and only if the whole direct summand is contained in $\Lambda_{\mathbb{Q}}$. This can be carried out in practice because there are algorithms for computing G that also supply p-adic approximations to the roots, in the order in which G acts on them ([2]). These algorithms are implemented in the computer algebra system Magma.

Once we have Λ we construct the splitting ring of the characteristic polynomial of X. To the defining ideal of this ring we add relations that immediately follow from Λ. We compute a Gröbner basis of this ideal, and work in the quotient ring. Then we use this ring in place of F'. It is higher dimensional than F', but in many cases easier to work with. However, there are also cases where the Gröbner basis computation does not terminate in reasonable time. One advantage of this algorithm is that it can also be used "symbolically". Using it we have determined the algebraic hull of every semisimple 4×4-matrix.

This research is part of an ongoing project. Remaining problems are to determine Λ from decimal or p-adic approximations to the roots, without constructing G, or assuming that the characteristic polynomial is irreducible. The second problem is to determine $\mathfrak{g}(X)$ from Λ, again using approximations to the roots. In the research a lot of use was made of the computer algebra system Magma ([3]).

References

[1] C. Chevalley, *Théorie des groupes de Lie. Tome II. Groupes algébriques*, Hermann & Cie., Paris, 1951.

[2] K. Geissler and J. Klüners, Galois group computation for rational polynomials, *Journal of Symbolic Computation* **30** (2000), 653–674.

[3] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *Journal of Symbolic Computation*, 24, 1997, 235–265.

LieAlgDB — A database of Lie algebras

Csaba Schneider

I reported on an ongoing project whose aim is to extend and verify some known classifications of small-dimensional Lie algebras and to make such classifications available in computational algebra packages, such as GAP [2]. This has been carried out in collaboration with Willem de Graaf and Marco Costantini.

Databases now form an important feature of computational algebra systems. They provide an easy means for accessing classifications theorems, and they also make it easier to verify the validity of such results. The Millennium Project [1] led by Besche, Eick and O'Brien aimed at classifying finite groups of order up to 2000 and making the classification available in computational algebra systems, such as GAP [2]. Our aim is to classify small-dimensional Lie algebras, as far as we can proceed, and also to make our results accessible in GAP.

I reported in more details on a particular aspect of this work, namely the classification of nilpotent Lie algebras over finite fields. I implemented an adaptation of O'Brien's p-group generation algorithm in GAP and used it to classify 7-dimensional nilpotent Lie algebras over $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, and nilpotent Lie algebras up to dimension 9 over $\mathbb{F}_2$; see [5]. Using the theory of the algorithm, I also obtained a classification of 6-dimensional Lie algebras over finite fields of odd characteristic. These classifications are available on my Web page (www.sztaki.hu/~schneider).

I also reported on related work by Willem de Graaf and Helmut Strade. Using a method based on Gröbner bases, de Graaf obtained a classification of solvable Lie algebras of dimension at most 4 over an arbitrary field [3], and a classification of nilpotent Lie algebras of dimension 6 over a field whose characteristic is not 2 [4]. Using recent results on simple modular Lie algebras, Strade obtained a classification of non-solvable Lie algebras of dimension at most 6 over finite fields [6].

The classifications mentioned above will be included in the forthcoming GAP package LieAlgDB.

References

[1] H. U. Besche, B. Eick, and E. A. O'Brien. *A millennium project: constructing small groups.* Internat. J. Algebra Comput. **12** (2002), 623–644.

[2] The GAP Group. GAP — *Groups, Algorithms, and Programming, Version 4.4,* 2004. (www.gap-system.org)

[3] W. A. de Graaf. *Classification of solvable Lie algebras*, Experiment. Math. **14** (2005), 15–25. (arxiv.org/abs/math.RA/0404071)

[4] Willem A. de Graaf. *Classification of* 6*-dimensional nilpotent Lie algebras over fields of characteristic not* 2, to appear in J. Algebra. (arxiv.org/abs/math.RA/0511668)

[5] Csaba Schneider. *A computer-based approach to the classification of nilpotent Lie algebras*, Experiment. Math. **14** (2005), 153–160. (arxiv.org/abs/math.RA/0406365)

[6] Helmut Strade. *Lie algebras of small dimension.* (arxiv.org/abs/math.RA/0601413)

Algorithms for finite-dimensional modules

Peter A. Brooksbank

(joint work with Eugene M. Luks)

Let Ω be a finitely generated algebra over an arbitrary field F. Assume that Ω-modules are given by specifying the action of a fixed generating set $\{\omega_1, \ldots, \omega_n\}$ of Ω on an appropriate F-space. Thus an Ω-module M is given by a set $A \subset \mathbb{M}_d(F)$.

We present a deterministic algorithm to decide whether two given Ω-modules are isomorphic and, if they are, produce an isomorphism. The algorithm works over any field in which it is possible to perform basic linear algebra, and the total number of field operations it uses is polynomial in $d|A|$.

The algorithm employs an efficient method for constructing non-nilpotent elements of non-nilpotent algebras. More precisely, if $\mathrm{Env}(X) = \mathrm{span}_F(\overline{X})$ is the enveloping algebra generated by $X \subset \mathbb{M}_d(F)$ (here $\overline{X}$ denotes the semigroup generated by X), and $\mathrm{Env}(X)$ is not nilpotent, then there is a (deterministic) polynomial-time algorithm to construct a non-nilpotent element of $\overline{X}$.

The algorithm for module isomorphism appears to have practical possibilities and implementations tailored to specific algorithmic settings are being developed. Other applications for non-nilpotent elements of non-nilpotent algebras are also being investigated.

Homological Algebra in GAP

Klaus Lux

(joint work with Thomas Hoffman, Robert Pawloski)

We report on two packages for the computer algebra system GAP that deal with homological Algebra for finite groups. The general aim of these packages is to compute the so called Ext-algebra for the group algebra FG of a finite group G over a finite splitting field F. The main emphasis of the approach described in the sequel is on the case where G is a finite simple group. The Ext-algebra is an important homological invariant and can be used to recover FG-modules from their composition factors. It is defined as

$$\mathrm{Ext}(FG) := \oplus \mathrm{Ext}^k_{FG}(S, T)$$

where the sum is over all simple FG-modules S, T (up to isomorphism) and all $k \in \mathbb{N}$. Here $\mathrm{Ext}^k_{FG}(S, T)$ is the set of exact sequences of FG-modules starting in T and ending in S modulo a suitable equivalence relation. Splicing of long exact sequences induces a multiplication on $\mathrm{Ext}(FG)$, which turns $\mathrm{Ext}(FG)$ into a finitely generated, graded, associative F-algebra.

The first package, Basic, by T. Hoffman and K. Lux, deals with the construction of the basic algebra B for the group algebra FG. B is defined as the smallest (up to isomorphism) F-algebra Morita equivalent to FG. The package constructs the basic algebra as a matrix algebra over F but a presentation of B as a quotient of a particular path algebra can be easily derived from this matrix representation. The basic algebra B is therefore both interesting from the theoretical and the algorithmic point of view. For applications in homological Algebra the important fact is that the Ext-algebra of B and the Ext-algebra of FG are isomorphic as graded F-algebras. It is therefore sufficient to determine $\mathrm{Ext}(B)$ in order to determine $\mathrm{Ext}(FG)$.

The computation of the basic algebra is performed in two steps:

First, Basic finds a subgroup H of G whose order is not divisible by the characteristic of F, such that the subalgebra $e_H FG e_H$ of FG is Morita equivalent to FG. Here we denote by e_H the fixidempotent of FG that is $e_H := \frac{1}{|H|}\sum_{h\in H} h$.

In a second step the package constructs all the projective indecomposable modules of $e_H FG e_H$ up to isomorphism and derives the basic algebra as the $e_H FG e_H$-endomorphism ring of the progenerator that is the direct sum of all the projective indecomposable modules (upto isomorphism). This leads to the explicit description of B as a matrix algebra. A wide range of examples of basic algebras computed with Basic can be downloaded from T. Hoffman's home page.

The second package, Homology, by R. Pawloski and K. Lux, takes as input the basic algebra in the form as computed by Basic. Moreover, in order to compute the Ext-spaces $\mathrm{Ext}_B^k(S,T)$ it uses the computationally preferable description of theses spaces using minimal projective resolutions of the corresponding simple B-modules. More specifically it computes the minimal projective resolutions for all the simple B-modules up to a certain bound. From these projective resolutions the Ext-spaces are derived in a straightforward manner. The product of two elements $\alpha \in \mathrm{Ext}_B^k(S,T)$ and $\beta \in \mathrm{Ext}_B^m(T,U)$ is performed by using a lift of α to a chain map between the corresponding minimal projective resolutions.

To find a minimal set of generators for the Ext-algebra up to the bound given, the package then uses an inductive approach. A complete set of relations satisfied by the generators found is determined and an application of a Gröbner basis algorithm gives a Gröbner basis for the corresponding ideal.

At the moment a crucial improvement would be a criterion which guarantees that a generating set for the Ext-algebra of FG can be found below a certain bound. Up to now, no practical bound seems to exist.

References

[1] D. J. Benson, Representations and cohomology. I, Cambridge Studies in Advanced Mathematics, **30**, 2nd ed., Cambridge University Press, Cambridge, 1998.

[2] Jon F. Carlson, Modules and group algebras, Lectures in Mathematics ETH Zürich, Birkhäuser Verlag, Basel, 1996.

[3] Jon F. Carlson, Edward L. Green, and J. A. .Schneider, *Computing* Ext *algebras for finite groups*, J. Symbolic Comput., 3-4(**24**), 1997, 317–325.

[4] Edward L. Green, *Noncommutative Gröbner bases and projective resolutions*, Progr. Math., **173**, Birkhäuser, Basel, 1999, 29–60.

[5] Thomas R. Hoffman, Constructing Basic Algebras for the Principal Block of Sporadic Simple Groups, Ph.D. thesis, Department of Mathematics, University of Arizona, 2004.

[6] Robert M. Pawloski, Computing the Cohomology Ring and Ext-Algebra of Group Algebras, Ph.D. thesis, Department of Mathematics, University of Arizona, 2006.

Generating condensed algebras in practice

Felix Noeske

The Modular Atlas project [4] strives to compute the modular character tables, or equivalently the decomposition matrices, of the almost simple groups whose ordinary tables are given in the Atlas of finite groups [1]. For the sporadic simple groups in particular there are still many open problems whose sizes render a direct computational approach with the MeatAxe [7] infeasible. A valuable tool to regain computational tractability is the condensation method (see, for example, [8]), as it allows us to restrict our attention to subspaces of the considered modules, thus leading to much smaller problem sizes.

To make this transition precise let G be a finite group, F a field of characteristic $p > 0$ and $e \in FG$ an idempotent. For practical purposes we usually consider $e := 1/|K| \sum_{k \in K} k$ for some subgroup $K \leq G$ whose order is coprime to p. Then instead of the FG-module V we consider its subspace Ve which is a module for the condensed algebra $eFGe$. There is a strong link between the algebras FG and $eFGe$, as, for example, condensation maps composition series of FG-modules to composition series of $eFGe$-modules and both algebras may even be Morita-equivalent. Therefore many questions regarding the FG-module V may be answered by studying the generally much smaller $eFGe$-module Ve.

The drawback of applying condensation is the problem that in general we do not know how to generate the condensed algebra $eFGe$ with sufficiently few elements that still adhere to a computational treatment. This constitutes the so called *generating problem*. In particular, it is in general not true that a generating set of FG condenses to a generating set of $eFGe$. It is important to remember that we can only study a module V for a particular algebra A with the MeatAxe by providing the latter with a set of matrices which generate an algebra isomorphic to the image of A under the representation afforded by V. Hence if we cannot assert that the proposed generators (the input to the MeatAxe) generate the whole condensed algebra, we have to assume that the information given by the MeatAxe refers to the restricted module V_C for some subalgebra $C \leq A$. Gaining results for the condensed module from this can be tedious and in the past a lot of effort has gone into developing techniques to bridge this gap.

Here we present two new methods to assure generation (see also [5]).

Firstly, let $H \leq G$ be any subgroup and choose any idempotent $e \in FH$ as the condensation idempotent. We may assume that we know how to generate the condensed algebra $eFHe$. Let $\mathcal{H} \subseteq eFHe$ denote the corresponding set of generators and set $\mathcal{S}$ to be a set of representatives for the isomorphism classes of simple $eFHe$ modules. Furthermore for some subset $\mathcal{E} \subseteq eFGe$ let $C := \langle \mathcal{E} \cup \mathcal{H} \rangle$ be the algebra generated by the union $\mathcal{E} \cup \mathcal{H}$. Then $C = eFGe$ if and only if for every $S \in \mathcal{S}$ we have $\dim(S \otimes_{eFHe} C) = \dim(S \otimes_{eFHe} eFGe)$. This criterion generalizes the previously known criterion due to Markus Wiegelmann (see [9]).

Secondly, consider the situation that there exists an intermediate subgroup $K \leq N \leq G$, which normalizes the condensation subgroup K, and the condensation idempotent e is the central primitive idempotent of some 1-dimensional FK-module (a so called *linear* idempotent). Then a guaranteed generating set for the condensed algebra is obtained by condensing representatives of the double cosets of the inertia subgroup T in N which corresponds to the character associated to e, as well as the generators of T itself. These generating sets are called *inert*. In the case where the cardinality of an inert generating set exceeds the computationally possible, there are methods to deal with a large amount of generators, too (see [5, Section 3]).

The application of inert generating sets has lead to recent results in the Modular Atlas project. With their help the 2- and 3-modular character tables of the bicyclic extensions of Fischer's sporadic simple group Fi_{22}, which are given in the Atlas, as well as the 2-modular decomposition matrix of Fi_{23} have been computed (see [2, 6]). They have also lead to the completion of the 5-modular character table of the Harada-Norton group HN and its automorphism group in [3].

References

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups, Oxford University Press, Eynsham, 1985, maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[2] G. Hiss, M. Neunhöffer, F. Noeske, The 2-modular characters of the Fischer group Fi_{23}, J. Algebra 300 (2) (2006), 555-570.

[3] K. Lux, F. Noeske, A. Ryba, The 5-modular characters of the sporadic simple Harada-Norton group HN and its automorphism group, in preparation.

[4] The Modular Atlas Homepage, `http://www.math.rwth-aachen.de/~MOC/`.

[5] F. Noeske, Tackling the generation problem in condensation, J. Algebra, *to appear*.

[6] F. Noeske, The 2- and 3-modular characters of the sporadic simple Fischer group Fi_{22} and its cover, J. Algebra, *to appear*.

[7] R. Parker, The computer calculation of modular characters, in: M. Atkinson (Ed.), Computational Group Theory, Academic Press, 1984, pp. 267–274.

[8] A. J. E. Ryba, Computer condensation of modular representations, J. Symbolic Comput. 9 (5-6) (1990), 591–600.

[9] M. Wiegelmann, Fixpunktkondensation von Tensorproduktmoduln, Diplomarbeit, RWTH Aachen University (1994).

Elementary constructions of the Ree groups

Robert A. Wilson

The two families of Ree groups were the last families of finite simple groups to be discovered, and they remain the least understood of these families. They arise from the Chevalley groups $G_2(3^{2n+1})$ and $F_4(2^{2n+1})$ as the centralizers of certain outer automorphisms of order 2. The standard construction first builds the Chevalley groups acting on their respective Lie algebras, and then makes the outer automorphism from a linear map on the root system which maps short roots to long roots and long roots to multiples of short roots. There are technical difficulties with these constructions which make them hard to use for applications.

In an attempt to make these groups more accessible, I take a completely elementary approach. The smallest representation has dimension exactly half that of the Lie algebra, so should be easier to build. Instead of starting with the BN-pair, I start with the non-toroidal local subgroups. These subgroups have the very useful property that they act irreducibly on the smallest module. Thus in $G_2(q)$ for any odd q there is a subgroup $2^3{\cdot}L_3(2)$ acting irreducibly on the 7-dimensional module. This subgroup has an outer automorphism which centralizes $2^3{:}7{:}3$, and in the case when $q = 3^{2n+1}$ this can be extended to an outer automorphism of $G_2(q)$, whose centralizer is the (small) Ree group $R(q)$.

Similarly in $F_4(q)$ for any q prime to 3 there is a subgroup $3^3{:}L_3(3)$ acting irreducibly on the 26-dimensional module. This subgroup has an outer automorphism which inverts the normal 3^3 and centralizes a complementary $L_3(3)$. In the case when $q = 2^{2n+1}$ this can be extended to an outer automorphism of $F_4(q)$, whose centralizer is the (large) Ree group $R(q)$.

To build these representations explicitly, we need only a little representation theory. In the first case, take a 7-dimensional faithful irreducible representation of $2^3{\cdot}L_3(2)$ in characteristic 3, which is unique up to automorphisms. Its exterior square is a uniserial module with three 7-dimensional constituents. The top and bottom constituents are isomorphic to the one we started with, and these isomorphisms give the octonion algebra (without identity) or co-algebra. The middle constituent is different, but on restriction to $2^3{:}7{:}3$ the two modules become isomorphic. This isomorphism gives us an algebraic structure which I call a *middle algebra*: it is neither an algebra nor a co-algebra, but somewhere in the middle! Twisting this structure by a field automorphism gives us a *twisted middle algebra* whose automorphism group is naturally the small Ree group.

To be precise, take a basis $\{i_0, \ldots, i_6\}$ with subscripts read modulo 7, such that the co-algebra is generated by the maps $i_t \mapsto i_{t+1} \wedge i_{t+3} + i_{t+2} \wedge i_{t+6} + i_{t+4} \wedge i_{t+5}$. Then the twisted middle algebra is defined by $i_t^* = i_{t+1} \wedge i_{t+3} - i_{t+2} \wedge i_{t+6}$ modulo the co-algebra, together with the semilinearity condition $(\sum_{t=0}^{6} \lambda_t i_t)^* = \sum_{t=0}^{6} \lambda_t^* i_t^*$, where $\lambda^* = \lambda^{3^{n+1}}$.

Similarly for the large Ree groups, take a 26-dimensional faithful irreducible representation in characteristic 2 of $3^3{:}L_3(3)$ which remains irreducible on restriction to $L_3(3)$. There are two such, interchanged by the outer automorphism. Again, the exterior square has both a submodule and a quotient module isomorphic to the original, giving rise to the exceptional Jordan algebra, and the co-algebra. Explicit computation with the Meataxe gives formulae for the algebra and co-algebra. Stripping off these two consituents from the module leaves a direct sum of non-isomorphic modules, of which one is the image under the outer automorphism of the module we first thought of. Thus on restriction to $L_3(3)$ these two modules become isomorphic, and using the Meataxe again we can find an explicit isomorphism, and write down a definition of the corresponding twisted middle algebra.

The formulae in this case are not quite so simple, but can be expressed entirely in terms of a certain code of length 13 over the field of order 3, and the action of $L_3(3)$ on this code and the projective plane of order 3.

In both cases, the representation theory gives us almost for free both the algebra (respectively the octonion algebra and the exceptional Jordan algebra) and the additional structure required to define the Ree groups.

I wish to do more, however, and prove all of the elementary properties of the Ree groups from first principles. In the case of the small Ree groups, by careful change of basis so that a maximal torus becomes diagonal, I obtain the 2-transitive action q^3+1 points, the order of the group, and a proof of simplicity (except when $q = 3$), as well as explicit generators for most of the maximal subgroups. In the case of the large Ree groups, the calculations are somewhat more formidable and not entirely complete. However, with this proviso I have a basis with respect to which a maximal torus is diagonal, an explicit construction of the generalised octagon and the BN-pair, an elementary calculation of the order of the group, and proof of simplicity (except for $q = 2$), as well as explicit generators for most of the maximal subgroups.

Explicit constructions of maximal subgroups of the Monster

John N. Bray

(joint work with Beth Holmes and Robert Wilson)

1. Introduction

For various reasons, such as verifying the Alperin weight conjecture and Dade's conjecture from representation theory, it is useful to have explicit representations of the Monster sporadic simple group $\mathbb{M}$. The representations of $\mathbb{M}$ are somewhat unwieldy, requiring approximately 10^{20} points for a permutation representation, and at least 196882 dimensions for a matrix representation. (It should be noted that the constructions in [5] and [3] of $\mathbb{M}$ in 196882 dimensions over $\mathbb{F}_2$ and $\mathbb{F}_3$ work implicitly rather than explicitly with matrices of this degree.) Thus it was decided to provide somewhat smaller and more convenient representations of all the maximal subgroups of the Monster.

So far 43 conjugacy classes of maximal subgroups of the Monster are known, and the remaining ones (if any) must be an almost simple group with socle $L_2(13)$, $U_3(4)$, $U_3(8)$ or $Sz(8)$, see [1] and the references therein. We have so far succeeded in constructing all of these (including the potential maximal subgroups), except for some of the 2-locals, which seem to be very hard to make. The representations we have made are available on the Web-Atlas [6].

2. Construction

Four of the Monster maximal subgroups were 'chopped' out of one of the 196882-dimensional representations of $\mathbb{M}$ by locating the subgroup and permuting a suitable orbit of objects (sparse vectors). The maximal subgroups made this way were $2^{2+11+22}{}^{\cdot}(M_{24} \times S_3)$, $2^{3+6+12+18}{}^{\cdot}(3{}^{\cdot}S_6 \times L_3(2))$, $3^{2+5+10}{}^{\cdot}(M_{11} \times 2{}^{\cdot}S_4^+)$ and $3^{3+2+6+6}\colon (SD_{16} \times L_3(3))$. We could express other subgroups in terms of the Monster generators, such as $3^8{}^{\cdot}O_8^-(3){}^{\cdot}2_3$, but could not find a suitable orbit of objects to permute within the Monster representations. For (most of) the remainder of the groups, we had to employ the following strategy.

- Determine the shape of the group, and determine all isomorphism classes of groups with that shape.
- Decide what representations of the groups we are going to try to construct.
- Make representations of all the groups.
- Determine which of our groups is a subgroup of the Monster.

The non-local maximal subgroups are all low index subgroups in direct products of almost simple groups or wreath products of almost simple groups with S_2 or S_3. The only problem for these maximal subgroups is to decide which subgroup to take. This was decidedly non-trivial in some cases, in particular for the group $(A_6)^3{}^{\cdot}(2 \times S_4)$, of index 8 in $(\mathrm{Aut}A_6) \wr S_3$. The structure of $(A_7 \times (A_5 \times A_5)\colon 2^2)\colon 2$ had previously been listed incorrectly as $(A_7 \times (A_5 \times A_5).4).2$.

Some of the p-local subgroups are affine groups, or subdirect products of affine groups and almost simple groups. These are routine (for us) to construct once we know the group that must be made. The extraspecial normalisers other than $3_+^{1+12}{}^{\cdot}(2{}^{\cdot}Suz\colon 2)$ caused us no problems. We made an $\mathbb{F}_3$-representation of shape $(1^- \cdot 64^+ \cdot 1^+) \oplus (1^- \cdot 12^+ \cdot 1^+)$ for $3_+^{1+12}\colon (6{}^{\cdot}Suz\colon 2)$. The subquotients of shape $1^- \cdot (64^+ \oplus 12^+) \cdot 1^+$ represent $3_+^{1+12}{}^{\cdot}(2{}^{\cdot}Suz\colon 2)$, with both groups $3_+^{1+12}{}^{\cdot}(2{}^{\cdot}Suz\colon 2)$ being obtained in this manner. The subgroup $7^{2+1+2}\colon GL_2(7)$ was proven to be isomorphic to a maximal parabolic of $G_2(7)$. The group $5^{2+2+4}\colon (S_3 \times GL_2(5))$ was constructed by extending a representation of an index 6 subgroup as permutations on 15625 points; the index 6 subgroup is also contained in $5_+^{1+6}\colon 2J_2.4$.

The possibilities for p-locals such as $3^8{}^{\cdot}O_8^-(3){}^{\cdot}2_3$ and $5^{3+3}{}^{\cdot}(2 \times L_3(5))$ were decided using various cohomological calculations. Representations of $O_8^-(3){}^{\cdot}2_3$ over $\mathbb{F}_3$ were glued together until a group that had to be $3^8{}^{\cdot}O_8^-(3){}^{\cdot}2_3$ (represented in 204 dimensions over $\mathbb{F}_3$) was obtained. Suitable objects in this representation were permuted with the help of a Schreier tree in order to get a permutation representation of (minimal) degree 805896. Gluing plus the subdirect product construction used for $3_+^{1+12}{\cdot}(2{\cdot}\mathrm{Suz}{:}\ 2)$ was used to obtain 46-dimensional representations of both groups $5^{3+3}{\cdot}(2 \times \mathrm{L}_3(5))$ over $\mathbb{F}_5$. We eventually obtained both groups as permutations on 7750 points, and decided containment in $\mathbb{M}$ by testing isomorphism of their Sylow 5-subgroups with the known Sylow 5-subgroup of $\mathbb{M}$.

3. Problematic subgroups

$2{\cdot}\mathbb{B}$. No small (degree less than 10^{15}) permutation representations exist, and the smallest representations in characteristic not 2 are known to be 96256 [4]. The smallest faithful subquotient of the restriction of the 196882-dimensional $\mathbb{F}_2$-module for $\mathbb{M}$ to $2{\cdot}\mathbb{B}$ appears to have degree about 90000. A faithful $\mathbb{F}_2$-representation of degree less than 10000 has not been ruled out.

$2_+^{1+24}{\cdot}\mathrm{Co}_1$. There are two groups of this shape, and it is well-known which one is a subgroup of the Monster. This group has a faithful representation of degree 98304 over $\mathbb{F}_3$. This representation is a tensor product of representations of degrees $2^{12} = 4096$ and 24, and was used (in its detensored state) as the basis for the 2-local construction of $\mathbb{M}$ over $\mathbb{F}_3$. The minimal degree in characteristic not 2 is 98304, and the smallest permutation degree comfortably exceeds 10^{11}. A smaller representation over $\mathbb{F}_2$ is being sought. A representation of degree 300 (and shape $24{\cdot}274{\cdot}(1 \oplus 1)$) exists for the quotient $2^{24}{\cdot}\mathrm{Co}_1$ (as opposed to a minimum of 98280 in odd characteristic), but we are having problems amalgamating $\mathbb{F}_2$-representations of $2^{24}{\cdot}\mathrm{Co}_1$ to give either $2_+^{1+24}{\cdot}\mathrm{Co}_1$.

$2^{5+10+20}{\cdot}(\mathrm{S}_3 \times \mathrm{L}_5(2))$. A faithful permutation action of this group whose degree is probably 7618560 is known to exist. (Uncertainties in how the quotient $\mathrm{S}_3 \times \mathrm{L}_5(2)$ act on the normal $2^{5+10+20}$ prevent us being precise about this.) We will probably chop this group out of one of the Monster representations, provided a suitable orbit of objects to permute can be located.

$2^{10+16}{\cdot}\mathrm{O}_{10}^+(2)$. It is known that the 2^{10+16} is special, and that the quotient $2^{16}{\cdot}\mathrm{O}_{10}^+(2)$ is non-split (and unique). Subject to these restrictions, it is known that there are two groups of this shape, which are barely distinguishable. We have succeeded in constructing various representations of $2^{16}{\cdot}\mathrm{O}_{10}^+(2)$, $2^{10}{\cdot}\mathrm{O}_{10}^+(2)$ and $\mathrm{O}_{10}^+(2)$ over $\mathbb{F}_2$, but have been unable to glue them together to give a representation of either of the groups $2^{10+16}{\cdot}\mathrm{O}_{10}^+(2)$. Permutation and odd characteristic matrix representations of this group are on the large side.

References

[1] J. N. Bray and R. A. Wilson. Explicit representations of maximal subgroups of the Monster. *J. Algebra* **300** (2006), 834–857.

[2] J. N. Bray, P. E. Holmes and R. A. Wilson. Explicit representations of maximal 2-local subgroups of the Monster. *In preparation.*

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

[4] Ch. H. Jansen. The minimal degrees of faithful representations of the sporadic simple groups and their covering groups. *LMS J. Comput. Math.* **8** (2005), 122–144.

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

[6] R. A. Wilson, S. J. Nickerson, J. N. Bray *et al.* A World Wide Web ATLAS of group representations. `http://brauer.maths.qmul.ac.uk/Atlas`.

Algorithms for Descent Algebras.

GÖTZ PFEIFFER

Let (W, S) be a finite Coxeter system. The descent algebra $\Sigma(W)$ of the finite Coxeter group W is a subalgebra of the group algebra $\mathbb{Q}W$ with a basis $\{x_J : I \subset S\}$, where x_J is the sum in $\mathbb{Q}W$ of the distinguished coset representatives of the parabolic subgroup W_J in W. It is a non-commutative preimage of the ring of parabolic permutation characters of W, with respect to the homomorphism θ which associates to x_J the permutation character of W on the cosets of W_J. Solomon [9] discovered it as the real reason why the sign character of W is a linear combination of parabolic permutation characters. He also showed that $\ker \theta$ (which is spanned by the differences $x_J - x_K$, where J and K are conjugate subsets of S) is the radical of $\Sigma(W)$.

The special case where W is the symmetric group on n points, i.e., a Coxeter group of type A_{n-1}, has received particular attention. This type of descent algebra occurs as the dual of the Hopf algebra of quasi-symmetric functions. Atkinson [1] has determined the Loewy length of $\Sigma(W)$ in this case. Garsia and Reutenauer [5] have found a basis for $\Sigma(W)$ consisting of primitive idempotents and other nilpotent elements. From their work, the quiver for $\Sigma(W)$ in type A_{n-1} is known to be the graph of a restricted partition refinement on the partitions of n.

For general W, the descent algebra has been further studied as an interesting object in its own right. Bergeron, Bergeron, Howlett and Taylor [2] have constructed explicit idempotents, decomposing $\Sigma(W)$ into projective indecomposable modules. Recently, Blessenohl, Hohlweg and Schocker [3] could show that θ satisfies the remarkable symmetry $\theta(x)(y) = \theta(y)(x)$ for all $x, y \in \Sigma(W)$. In a joint work with C. Bonnafé [4], we have determined the Loewy length of $\Sigma(W)$ for all types of irreducible finite Coxeter groups W, with the exception of type D_n, n odd.

It is obvious, from its known properties, that $\Sigma(W)$ is a basic algebra and as such has a presentation as a quiver with relations. In my talk I have introduced a new combinatorial object, an algebra of *arrow classes* derived from the lattice of subsets of the set S of simple reflections of W, which can be used to calculate this quiver and the relations.

Here, an *arrow* is a pair $(L; s, t, \dots)$ consisting of a subset $L \subseteq S$ and a list of pairwise distinct elements $s, t, \dots \in L$. The *length* of such an arrow is the number of elements $\#\{s, t, \dots\}$. Two arrows $(L; s, t, \dots)$ and $(L'; s', t', \dots)$ can be joined provided $L \setminus \{s, t, \dots\} = L'$, in which case

$$(L; s, t, \dots) \circ (L'; s', t', \dots) = (L; s, t, \dots, s', t', \dots).$$

The conjugation action of W on itself gives rise to an action of the *free monoid* S^* on the set of all arrows as follows. For $L \subseteq S$ denote by w_L the *longest element* of the parabolic subgroup W_L of W. Then conjugation by w_L induces a permutation on the subset L. And if $L \subseteq M$ and $d_L^M = w_L w_M$ then $L^{d_L^M} \subseteq M$. Given an arrow $(L; s, t, \dots)$, and an element $r \in S$, we let $M = L \cup \{r\}$ and $d = d_L^M$ and define

$$(L; s, t, \dots).r = (L^d; s^d, t^d, \dots).$$

The S^*-orbits of arrows are called *arrow classes.* Denote by $\Psi(W)$ the set of all arrow classes.

Let us consider the special case of arrows $(L, \emptyset)$ of length 0, i.e., the subsets L of S, and let us call the set of conjugates of L within S the *shape* of L. This notion generalizes the notion of cycle shape in type A_{n-1}, where the conjugacy classes of parabolic subgroups (as well as the conjugacy classes of elements) are parametrized by the partitions of n, the set of all possible cycle shapes. Denote by $\Lambda(W)$ the set of all shapes of W. It is well-known [7, Theorem 2.3.3] that the shape of $L \subseteq S$ is the S^*-orbit of L in the above action. Bergeron, Bergeron, Howlett and Taylor [2] have constructed a parametrized basis $\{e_J : J \subseteq S\}$ of $\Sigma(W)$ with the properties that the radical of $\Sigma(W)$ is spanned by the differences $e_J - e_K$ where $J, K \subseteq S$ have the same shape, and that (for a suitable choice of parameters) the orbit sums

$$\epsilon_\lambda = \sum_{L \in \lambda} e_L, \quad \lambda \in \Lambda(W)$$

form a complete set of primitive idempotents for $\Sigma(W)$.

Given this background, we identify an arrow class with the sum of its elements in the algebra spanned (over $\mathbb{Q}$) by all arrows. It turns out that a product of two arrow classes is a sum of arrow classes. The arrow classes thus form a basis of a *graded subalgebra* $\Xi(W)$ of the graded algebra $A(W) = A_0 \oplus \cdots \oplus A_n$ spanned by all arrows, where the grade i component A_i is spanned by the arrows of length i. The algebra $\Xi(W)$ has a simple presentation as quiver with relations. Here the quiver is the graph with vertex set $\Lambda(W)$ and edge set $\Psi(W)$, and the relations are given by the multiplication table of the arrow classes. Moreover, there exists a linear map $\Delta\colon A(W) \to A_0$ which maps $\Xi(W)$ surjectively to A_0. The grade 0 component A_0 can be identified with $\Sigma(W)$ by setting $(L; \emptyset) = e_L$.

I have verified, for all finite irreducible Coxeter groups W of rank up to 8, that under this identification the restricted map $\Delta\colon \Xi(W) \to \Sigma(W)$ is an algebra homomorphism. It is therefore natural to conjecture that for all finite Coxeter groups the image of the arrow class algebra $\Xi(W)$ under Δ is isomorphic to the descent algebra $\Sigma(W)$. In any case, a presentation of $\Delta(\Xi(W))$ as a quiver with relations can be computed along the following lines.

Algorithm Q. Given a finite Coxeter system (W, S), compute a directed graph (V, E) and a set $\mathcal{R}$ of relations between the paths in (V, E) such that the path algebra of (V, E) modulo $\mathcal{R}$ is isomorphic to $\Delta(\Xi(W))$.

```
1. $V \leftarrow \Lambda(W)$, the set of all shapes of $W$;
2. $M \leftarrow \{\alpha \in \Psi(W) : l(\alpha) > 0$ and $\Delta(\alpha) \neq 0\}$;
```

```
$i \leftarrow 0$;
while $M \neq \emptyset$:
    $i \leftarrow i + 1$;    $E_i \leftarrow M$;
    add to $\mathcal{R}$ the nullspace of $\Delta$ on $E_1 \cup \cdots \cup E_i$;
    remove redundant elements from $E_1$;
    $M \leftarrow M \circ E_1$;
return $(V, E_1)$ and $\mathcal{R}$ in terms of $E_1$.
```

This algorithm and many other tools for the investigation of descent algebras are part of a forthcoming GAP package ZigZag [8], which is based on the CHEVIE package [6] for generic character tables of finite groups of Lie type, finite Coxeter groups, Iwahori–Hecke algebras and related structures in GAP3.

Acknowledgment. The author is supported by NUI, Galway's Millennium Fund.

References

[1] M. D. Atkinson, *Solomon's descent algebra revisited*, Bull. London Math. Soc. **24** (1992), 545–551. MR 93i:20012

[2] F. Bergeron, N. Bergeron, R. B. Howlett, and D. E. Taylor, *A decomposition of the descent algebra of a finite Coxeter group*, J. Algebraic Combinatorics **1** (1992), 23–44. MR 93g:20079

[3] Dieter Blessenohl, Christophe Hohlweg, and Manfred Schocker, *A symmetry of the descent algebra of a finite Coxeter group*, Adv. Math. **193** (2005), 416–437. MR 2005m:20089

[4] C. Bonnafé and G. Pfeiffer, *Around Solomon's descent algebras*, submitted, 2006. arXiv:math.RT/0601317.

[5] A. M. Garsia and C. Reutenauer, *A decomposition of Solomon's descent algebra*, Adv. Math. **77** (1989), 189–262.

[6] M. Geck, G. Hiss, F. Lübeck, G. Malle and G. Pfeiffer, *CHEVIE - A system for computing and processing generic character tables*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), 175–210.

[7] M. Geck and G. Pfeiffer, *Characters of finite Coxeter groups and Iwahori-Hecke algebras*, London Mathematical Society Monographs, New Series **21**, The Clarendon Press, Oxford University Press, New York (2000).

[8] G. Pfeiffer, *ZigZag - A GAP3 package for Descent Algebras of Finite Coxeter Groups*, http://schmidt.nuigalway.ie/zigzag.

[9] L. Solomon, *A Mackey formula in the group ring of a Coxeter group*, J. Algebra **41** (1976), 255–268. MR 56 #3104

Short bounded presentations of finite simple groups

William M. Kantor

(joint work with R. M. Guralnick, M. Kassabov, A. Lubotzky)

This talk reported on the following "implausible"

Theorem [4]**.** *Each nonabelian finite simple group of rank n over $\mathbf{F}_q$ (except perhaps ${}^2G_2(3^{2k+1})$) has a presentation with a bounded number of generators and relations* ("bounded") *and length $\leq C(\log n + \log q)$* ("short").

In fact fewer than 500 generators and relations are needed, and the constant $C < 1000$.

We view alternating groups as over "the field $\mathbf{F}_1$ with 1 element". The *length* of a presentation $\langle X \mid R\rangle$ is $\sum_{r\in R} l_X(r)$, so that relators such as x^n or x^{q-1} do not occur in our presentations. The length in the theorem is optimal as a function of n and q (up to the specific constant C). The theorem also is true for all perfect central extensions of these simple groups (this turns out to be not at all as obvious a variation as it might seem).

The theorem is stated so as to be independent of the classification of the finite simple groups.

A few special cases of this result known. Campbell-Robertson-Williams [3] obtained a bounded presentation for $PSL(2, q)$; variations on their ideas were crucial for the rank 1 case of the above theorem. Babai-Goodman-Kantor-Luks-Pálfy [1], together with Suzuki [9] and Hulpke-Seress [7] in the rank 1 case, obtained presentations of the above group G of length $O((\log|G|)^2) = O(n^4 \log^2 q)$ except in the case ${}^2G_2(3^{2k+1})$; we used their results or methods in our proof. Korchagina-Lubotzky [8] obtained related presentations for some simple groups (also based on the Campbell-Robertson-Williams result).

More recently, Bray-Conder-Leedham Green-O'Brien [2] obtained bounded presentations for A_n and S_n that are "short" for a less stringent notion of length (namely: they view a power x^n as having length $\log_2 n$); but their presentations can be made short and bounded in our sense with very little effort.

One nice feature of this theorem is that it is counterintuitive: even for the symmetric or alternating groups it is very different from the familiar types of presentations of these groups.

Another feature is that it can be used to prove a 1987 conjecture of Holt [6] (this time using the classification of the finite simple groups):

Theorem [4]. *For any faithful irreducible $\mathbf{F}_p$-module M of any finite group G,*

$$\dim H^2(G, M) \le C' \dim M.$$

Even composition factors ${}^2G_2(3^{2k+1})$ are allowed here. In fact $C' \le 500$; the authors are in the process of improving this to $C' < 20$ [5].

Wilson [10] has made the interesting conjecture that the universal central extension of every finite simple group has a presentation with 2 generators and 2 relations. While I do not believe this, it would be nice at least to have such a presentation for $SL(2, q), q \neq 4, 9$.

References

[1] L. Babai, A. J. Goodman, W. M. Kantor, E. M. Luks and P. P. Pálfy, Short presentations for finite groups. J. Algebra 194 (1997) 79–112.

[2] J.N. Bray, M.D.E. Conder, C.R. Leedham-Green and E.A. O'Brien. Short presentations for alternating and symmetric groups, submitted.

[3] C. M. Campbell, E. F. Robertson and P. D. Williams, On presentations of $PSL(2, p^n)$. J. Austral. Math. Soc. 48 (1990) 333–346.

[4] R. M. Guralnick, W. M. Kantor, M. Kassabov and A. Lubotzky, Presentations of finite simple groups: a quantitative approach, to appear in JAMS.

[5] R. M. Guralnick, W. M. Kantor, M. Kassabov and A. Lubotzky, Presentations of finite simple groups: profinite and cohomological approaches, in preparation.

[6] D. F. Holt, On the second cohomology group of a finite group. Proc. Lond. Math. Soc. (3) 55 (1987) 22–36.

[7] A. Hulpke and Á. Seress, Short presentations for three-dimensional unitary groups. J. Algebra 245 (2001) 719–729.

[8] I. Korchagina and A. Lubotzky, On presentations and second cohomology of some finite simple groups (submitted).

[9] M. Suzuki, On a class of doubly transitive groups. Ann. of Math. 75 (1962) 105–145.

[10] J. S. Wilson, Finite axiomatization of finite soluble groups, preprint.

A data structure for a uniform approach to computations with finite groups

Ákos Seress
(joint work with Max Neunhöffer)

We describe a recursive data structure for the uniform handling of permutation groups and matrix groups. This data structure allows the switching between permutation and matrix representations of segments of the input group, and has wide-ranging applications. It provides a framework to process theoretical algorithms which were considered too complicated for implementation such as the asymptotically fastest algorithms for the basic handling of large-base permutation groups and for Sylow subgroup computations in arbitrary permutation groups. It also facilitates the basic handling of matrix groups. The data structure is general enough for the easy incorporation of any matrix group or permutation group algorithm code; in particular, the library functions of the *GAP* computer algebra system [3] dealing with permutation groups and matrix groups work as they are, or with minimal modification.

The mathematical principles behind the data structure are not new. An appropriate homomorphism φ is searched for and then applied to break the input group G into the image and kernel of φ. Then we recursively process these smaller groups, and finally put together the results to obtain the desired information for G. In the permutation group setting, the use of homomorphic images to break a computation into manageable pieces was introduced by Luks, in the context of parallel (NC) computations (see [2]). In the matrix group setting this seems to be the only feasible approach [1], [4].

The devil (and the novelty of our approach) is in the details. Here we list only four of these.

(i) In search of an appropriate homomorphism, a ranking of possible homomorphisms is created, similarly of the method selection process of *GAP*; however, these rankings are individualized for the nodes of the recursion tree and the nodes can pass information to their children to speed up the search at those nodes and to balance the search tree.

(ii) An automated mechanism is set up to add "memory" to group elements (so they can "remember" how they were created from input generators of their node) and suppress this memory when a library function like the MeatAxe is called, which expects only matrices as inputs (not records consisting of a matrix and of its memory). A user or potential developer writing a subroutine working with matrices or permutations does not even have to be aware of the existence of the memory.

(iii) A generalization of strong generating sets is introduced for black-box groups (including permutation groups, matrix groups, and the genuine black-box group applications), which reduces the length of straight-line programs to reach group elements from the generators dramatically, compared to straight-line programs from the input generators.

(iv) The data structure can also be used for the clean design of algorithms with complicated case analysis. Instead of a tree of `if-then` statements, the properties used in these statements can be assigned as attributes of objects and the method selection process automatically guides the flow of the algorithm.

The first success story of our approach is the basic handling (i.e., finding the order and setting up a scheme for membership testing) in permutation groups. This is the first-ever practical algorithm which works for *arbitrary* inputs (both small-base and large-base groups). Of course, the major motivation for the development of the data structure is the handling of matrix groups. Currently, we have homomorphism methods which may work on some inputs in any of the seven reductive Aschbacher classes and recognition algorithms for some almost simple groups (which are the end nodes in the recursive scheme). However, our guiding principle is not the recognition of Aschbacher classes, but rather to find any applicable homomorphism. Some of our most useful (and therefore highly ranked) reduction methods may be successful for inputs in more than one Aschbacher class. The (loosely coordinated) development of further algorithms is under way by a lot of people.

References

[1] L. Babai and R. Beals, *A polynomial-time theory of matrix groups and black box groups I*, In Groups St. Andrews 1997 in Bath, I (ed. by C. M. Campbell, E. F. Robertson, N. Ruskuc, G. C. Smith). London Math. Soc. Lecture Note Ser. 260, 1999, 30–64.

[2] L. Babai, E. M. Luks, and Á. Seress, *Permutation groups in NC*, In Proc. 19th ACM Symp. on the Theory of Computing, ACM Press, New York 1987, pp. 409–420.

[3] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version* 4.4 Aachen–St Andrews 2005. `http://www.gap-system.org`

[4] C. R. Leedham-Green, *The computational matrix group project*, In Groups and Computation III (ed. by W. M. Kantor, Á. Seress), deGruyter, Berlin–New York 2001, pp. 229–247.

[5] M. Neunhöffer and Á. Seress, *A data structure for a uniform approach to computations with finite groups*, In Proc. International Symposium on Symbolic and Algebraic Computation (ISSAC 2006), ACM Press, New York 2006, pp. 254–261.

Finding standard generators in Classical Groups

Charles R. Leedham-Green
(joint work with Eamonn O'Brien)

A central issue in the matrix group recognition project is finding a set of standard generators in a perfect classical matrix group G, given in terms of some (small) generating set X. Any definition of 'standard generators' is acceptable provided that the set of standard generators is small, and that some efficient algorithm should be available to construct any element of the classical group as a word (strictly, as a straight line program) in the standard generators. There are many subdivisions of the problem, of which the most important are as follows.

1. Is G a classical group in its natural representation, or some other matrix representation of G in the natural characteristic, or are no assumptions made about the representation (the black box case)?

2. To which family of classical groups does G belong? (Linear, Symplectic, Unitary, or an Orthogonal family).

3. Is the natural characteristic of the group odd or even?

There is another issue at stake. The output of the procedure is a straight line program that defines the standard generators in terms of the given input matrices. It is at least as important to keep this straight line program short as to have the program run quickly. This gives another dichotomy, and we have versions of our programs that concentrate on speed of performance, and versions that concentrate on producing a short straight line program.

One serious obstruction is the difficulty, even in $\mathrm{SL}(2,q)$, of finding a unipotent element if q is large. This problem is solved in [1] and [2] at the cost of using discrete logarithms in $\mathrm{GF}(q)$. Given a discrete logarithm oracle, our algorithms have complexity that is polynomial in $\log q$.

Our algorithms have been developed in the context of the natural representations of the classical groups, in the expectation that these will be the most challenging problems, given the ambient vector space, or in terms of the size of the input. However, the algorithms generalise without serious changes to deal with arbitrary representations in the given characteristic. The algorithms could be adapted to work in black box generality, though this would require more serious changes to made, and these would affect the complexity of the algorithms. If the group is given in the natural characteristic the recursive calls on which the algorithm is based should soon reduce to smaller classical groups in their natural representations.

In odd characteristic the basic idea behind the algorithms is to find an involution whose eigen-spaces are of approximately equal dimension, to find the centraliser C in G of this involution, using the Bray algorithm, and to work recursively in the direct factors of the derived subgroup of C. The standard generators for these direct factors then need to be 'glued together' to construct standard generators for G. This recursion is naturally based on dealing with the small rank groups in a different way.

We have two classes of algorithms, let us call them 'class A' and 'class B'. The class A algorithms, using the above divide and conquer strategy, produce two recursive calls to deal with the two direct factors of the derived subgroup of C. The space and time complexity of the algorithms make the cost of these recursive calls unimportant (except for the use of discrete logarithms in base cases). However, the length of the straight line program is $\mathrm{O}(d)$ (with suitable conventions), and the contribution of the recursive calls to this length is significant. The class B algorithms arrange, when possible, for the direct factors in question to have equal dimension, and thus succeed in requiring, when this is possible, for a single recursive call to a group of half the Lie rank to suffice. This reduces the length of the straight line program to $O(\log d)$.

The time complexity of the class A algorithms for fixed q is $\mathrm{O}(d^4)$ for the natural representations, and the class B algorithms may be as good asymptotically. To achieve such a bound requires considerable care, both in the construction of the algorithms and in their analysis. It is also important to ensure that the 'gluing' operations do not overwhelm the asymptotically more expensive parts of the algorithm in practical ranges. These considerations have resulted in the algorithms, and their analysis, becoming rather complex.

The case of even characteristic is considerably harder; but again we find suitable involutions, and recursively consider smaller classical groups involved in the involution centraliser, again having one or two recursive calls.

We thank R. Wilson for his very expert assistance in the case of the even characteristic.

We acknowledge the important work of others in this field, such as [3], [5] and [4].

References

[1] Marston Conder, Charles R. Leedham-Green *Fast recognition of classical groups over large fields* in Groups and Computation III, Ed. W.M. Kantor and Á. Serres. de Gruyter, Berlin, New York, 2001, 112–121.

[2] M.D.E. Conder, C.R. Leedham-Green, E.A. O'Brien *Constructive recognition of* $\mathrm{PSL}(2, q)$, Trans. Amer. Math. Soc. **358(3)** (2006) 1203–1221.

[3] W.M. Kantor and À. Seress *Black box classical groups* Mem. Amer. Math. Soc. **149**, Nr. 708, Amer. Math. Soc., Providence, RI, 2001.

[4] Peter A. Brooksbank and William M. Kantor *On constructive recognition of a black box* $\mathrm{PSL}(d, q)$ in Groups and Computation III, Ed. W.M. Kantor and Á. Serres. de Gruyter, Berlin, New York, 2001, 112–121.

[5] P.A. Brooksbank *A constructive recognition algorithm for the matrix group* $\Omega(d, q)$ in Groups and Computation III, Ed. W.M. Kantor and Á. Serres. de Gruyter, Berlin, New York, 2001, 79–93.

The groups of order p^6 and p^7

Michael Vaughan-Lee
(joint work with Mike Newman, Eamonn O'Brien)

Newman, O'Brien and Vaughan-Lee [3] have classified the groups of order p^6 and O'Brien and Vaughan-Lee [4] have classified the groups of order p^7. For $p \geq 5$ there are

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

groups of order p^6 and for $p > 5$ there are

$$\begin{aligned}&3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455\\&+(4p^2 + 44p + 291)\gcd(p-1,3) + (p^2 + 19p + 135)\gcd(p-1,4)\\&+(3p+31)\gcd(p-1,5) + 4\gcd(p-1,7) + 5\gcd(p-1,8) + \gcd(p-1,9)\end{aligned}$$

groups of order p^7.

Our classification is according to the p-class of the groups. If P is a p-group, then the lower p-central series of P is defined recursively by $P_1 = P$ and $P_{i+1} = [P_i, P]P_i^p$ for $i \geq 1$. The p-class of P is the length of this series. Each p-group P, apart from the elementary abelian ones, is an *immediate descendant* of the quotient P/R where R is the last non-trivial term of the lower p-central series of P. Thus all the groups of order p^6, apart from the elementary abelian one, are immediate descendants of groups with order p^k for $k < 6$. Similarly all the groups of order p^7, apart from the elementary abelian one, are immediate descendants of groups with order p^k for $k < 7$.

For $p \geq 5$, there are 42 groups with order p^k for $k < 6$ which have immediate descendants with order p^6. These groups are listed in both [3] and [4]. For each group P in this list of 42 groups, we determine the groups of order p^6 which are immediate descendants of P. Together with the elementary abelian group of order p^6, this gives us a complete classification of the groups of order p^6.

It turns out that 17 of these 42 groups also have immediate descendants of order p^7. So for $p \geq 5$ a complete list of the groups of order p^7 is given by:

- the elementary abelian group of order p^7,
- the immediate descendants of order p^7 of 17 groups of order at most p^5,
- the immediate descendants of order p^7 of the groups of order p^6.

For $p > 5$ we actually classify the nilpotent Lie rings of order p^6 and p^7, and then use the Baker-Campbell-Hausdorff formula [2] and the Lazard correspondence [1] to obtain presentations for the corresponding groups. The classification contains 5087 parametrized presentations of the form

$$\{a, b \mid a^p = [b,a,a][b,a,b,b]^\lambda,\ b^p = [b,a,b,b][b,a,b,b,a]^\mu,\ \text{class } 5\}.$$

In addition to the parameter p this presentation involves two parameters λ and μ and (for each prime $p > 5$) we obtain p^2 different groups of order p^7 and class 5, as λ and μ range over the set $\{0, 1, \ldots, p-1\}$. Our results have been incorporated in Magma Version 2.12 as databases of the groups of order p^6 and p^7.

References

[1] N. Bourbaki, *Groupes et algèbres de Lie*, Hermann, Paris, 1972.

[2] N. Jacobson, *Lie algebras*, Wiley-Interscience, New York, 1962.

[3] E.A. O'Brien M.F. Newman and M.R. Vaughan-Lee, *Groups and nilpotent Lie rings whose order is the sixth power of a prime*, J. Algebra **278** (2004), 383–401.

[4] E.A. O'Brien and M.R. Vaughan-Lee, *The groups with order p^7 for odd prime p*, J. Algebra **292** (2005), 243–258.

Computing with p-groups by coclass

Bettina Eick

The coclass of a group G of order p^n and nilpotency class c is defined as $cc(G) = n - c$. Leedham-Green and Newman [13] proposed to classify and investigate p-groups using the coclass as primary invariant. A central idea towards this aim is to visualise the p-groups of coclass r by the graph $\mathcal{G}(p, r)$: the vertices of $\mathcal{G}(p, r)$ correspond to the isomorphism types of p-groups of coclass r and two vertices G and H are adjoined by an edge if there exists an $N \trianglelefteq H$ with $|N| = p$ and $H/N \cong G$. The central aim in coclass theory is to understand the structure of $\mathcal{G}(p, r)$ and its underlying groups. See also [12] for detailed information and further references.

In this talk a collection of algorithms is described which can be used to investigate the structure of the infinite graph $\mathcal{G}(p, r)$ for given prime p and natural number r. These algorithms include:

- A method to construct all infinite pro-p-groups of coclass r up to isomorphism. The infinite pro-p-groups of coclass r correspond one-to-one to the infinite paths in $\mathcal{G}(p, r)$. See also [6] and [7] for a description of part of the algorithms and further details.
- A method to draw finite parts of the descendant tree of a given infinite pro-p-group of coclass r. It is known that all but finitely many groups in $\mathcal{G}(p, r)$ are contained in such a descendant tree. See also [12] for background on such descendant trees.

An implementation of these algorithms in GAP [11] is also presented in this talk. This implementation uses various GAP packages such as [9], [1] and [10]. It will be made available as GAP package in preparation [8] shortly.

The resulting collection of algorithms has been a fundamental tool in finding many of the recent results in coclass theory. For example, the algorithms have been used to investigate the following problems which are all theorems now:

Theorem. (Eick and Leedham-Green [2])
The 2-groups of coclass r can be classified by finitely many parametrised presentations.

Theorem. (Eick [5])
Almost all 2-groups of coclass r satisfy $|G| \mid |Aut(G)|$.

Theorem. (Eick [3] and [4])
Almost all p-groups of coclass r $(p > 2)$ have a non-trivial Schur multiplicator.

References

[1] F. Celler, M. Neunhöffer, *XGAP - A GAP package, Version 4.21*, (2004)
[2] B. Eick, C.R. Leedham-Green, *Periodic patterns in coclass graphs and the classification of 2-groups by coclass*, Submitted.
[3] B. Eick, *Schur multiplicators of infinite pro-p-groups with finite coclass*, Submitted.
[4] B. Eick, *Schur multiplicators of finite p-groups with fixed coclass*, Submitted.
[5] B. Eick, *Automorphism groups of 2-groups*, J. Algebra 300, 91 - 101 (2006).
[6] B. Eick, *On the determination of the uniserial space groups with a given coclass*, J. London Math. Soc. 71, 622 - 642 (2005)
[7] B. Eick, *On the number of infinite branches in the graph of all p-groups of coclass r*, J. Group Theory 8, 687 - 700 (2005)
[8] B. Eick, *Coclass - A GAP package*, In preparation.
[9] B. Eick, W. Nickel, *Polycyclic - A GAP package, Version 1.1*, (2003)
[10] G. Gamble, W. Nickel, E.A. O'Brien, *ANUPQ - A GAP package, Version 3.0*, (2006)
[11] The GAP Group, *GAP – Groups, Algorithms and Programming, Version 4.4*, Available at www.gap-system.org (2006)
[12] C.R. Leedham-Green, S. McKay, *The structure of groups of prime power order*, London Math. Soc. Monographs (2002)
[13] C.R. Leedham-Green, M.F. Newman, *Space groups and groups of prime-power order I*, Archiv der Mathematik 35, 193 - 203 (1980)

Computer assisted proofs of the $F^{a,b,c}$ conjecture

Edmund F. Robertson

The groups
$$F^{a,b,c} = \langle r, s | r^2 = 1, rs^a rs^b rs^c = 1 \rangle$$
arose during a census of symmetric trivalent graphs begun by R. M. Foster in the 1960s. In 1975 C. M. Campbell, H. S. M. Coxeter and E. F. Robertson made the "$F^{a,b,c}$ conjecture" in [1]. Let $n = a+b+c$, $d = (a-b, b-c)$. First they classified the groups
$$H^{a,b,c} = \langle r, s | r^2 = s^{2n} = rs^a rs^b rs^c = 1 \rangle.$$
If $t = (a, b, c) \neq 1$ then $F^{a,b,c}$ is infinite except when $H^{a/t,b/t,c/t}$ is abelian, in which case $F^{a,b,c} \cong H^{a,b,c} \cong C_{2n}$. Provided $(a, b, c) = 1$, $n \neq 0$ and $(d, 6) \neq 6$, the groups $H^{a,b,c}$ are finite metabelian groups. If $(a, b, c) = 1$ and $d \geq 6$ the groups $F^{a,b,c}$ are infinite. The $F^{a,b,c}$ conjecture is as follows. Suppose $(a, b, c) = 1$ and $n \neq 0$. Let $\theta : F^{a,b,c} \to H^{a,b,c}$ be the natural homomorphism. Let $N = \ker \theta$. Then

$N = 1$ if $d = 1$,
$N = 1$ if $d = 2$,
$N \cong C_2$ if $d = 3$,
$N \cong Q_8$ if $d = 4$,
$N \cong SL(2, 5)$ if $d = 5$.

The conjecture was proved true when $d = 1$ in [2] and recently it was proved true when $d = 5$ in [5]. To attack the remaining cases we looked to see how the computer was able to solve small examples. George Havas (with Colin Ramsay) had written a package PEACE (Proof Extraction After Coset Enumeration) that produced an algebraic proof after completing a coset enumeration, see [4]. Here is a PEACE proof that $s^{22} = 1$ in $F^{1,3,7}$. (Note: Upper case letters are inverses of lower case letters) It is called a “proofword”.

$$
\begin{aligned}
&sssssssssssssssrsr(sssrsssssssrsr)RSRSSSSSSS(RR)S(RR)rsr\\
&(sssrsssssssrsr)RSRSSSSSSSRSR(rr)RSR(rr)(RSRSSSSSSSRSSS)\\
&sssrsssssssrsr(sssrsssssssrsr)RSRSSSSSSr(RSRSSSSSSSRSSS)RR\\
&(rr)SSSrsr(RR)rsr(RR)rsrsssssssrsr(RSRSSSSSSSRSSS)RSRSSS\\
&(RR)rr(sssrsssssssrsr)RRS(RR)SSS(sssrsssssssrsr)RSR
\end{aligned}
$$

Freely cancel as it stands. One obtains s^{22}. Remove the relations inside round brackets. Now freely cancel to obtain 1. Hence $s^{22} = 1$.

Dale Sutherland wrote GAP code [3] to translate these proofwords into a lemma based line by line proof. After studying the proofs produced for small examples we observed a significant type of relation appearing regularly in the proofs. For example, in the group $F^{3,5,7}$ we observed relations of the form

$$(rs^{10}rs^5)^2 = 1, (rs^{12}rs^3)^2 = 1, (rs^{14}rs)^2 = 1$$

held. Proving that relations in such a sequence all hold is sufficient since $(rs^0rs^{15})^2 = 1$ is a member of the sequence and this reduces to $s^{30} = 1$ as required. Examining different proofs for small k led us to observe that for $F^{3,5,k}$ relations of the form $(rs^{2i+3}rs^{k-2i+5})^2 = 1$ held. Having discovered what we should try to prove, we used induction on i to obtain a proof of this result. Since k is odd, $k + 5$ is even. Put $i = (k + 5)/2$ to obtain $s^{2k+16} = 1$ as required.

We decided next to look at the groups $F^{a-2,a,a+2}$ for small odd a. The presentation here exhibited more symmetry which helped us to recognise significant lemmas in the PEACE proofs. Again we observed that the proofs involved certain squares. This time the relations were of the form $(rs^{2i}rs^{3a-2i})^2 = 1$. Now $i = 0$ gives $s^{6a} = 1$ as required.

We then proceeded to examine the groups $F^{a-2,a,a+4}$ followed by $F^{a-2,a,a+2k}$, again finding that we could construct a proof from a sequence of squares, although a harder induction was involved at each stage. Finally, generalising to $F^{a-2j,a,a+2k}$ where $(j, k) = 1$ led us to conjecture that squares of the form

$$(rs^{2a+id+kd-jd}rs^{a-id})^2 = 1$$

held. Once we had an inductive proof that such squares held, we had completed the proof of the conjecture for $d = 2$. A similar investigation in the cases $d = 3$ and $d = 4$ eventually led to us completing the proof of the $F^{a,b,c}$ conjecture. This is presented in [6]. More details of how we used PEACE to construct the proof appear in [7]. Also in [7] further results of when $F^{a,b,c} = H^{a,b,c}$ in the case $(a, b, c) \neq 1$ are also given. As an example we note that equality holds when $(a, b, c) \neq 1$ for all the cases $1 \leq d \leq 5$ covered by the original conjecture.

References

[1] C. M. Campbell, H. S. M. Coxeter, E. F. Robertson, Some families of finite groups having two generators and two relations, *Proc. Roy. Soc. London Ser. A* **357** (1977), 423–438.

[2] C. M. Campbell, E. F. Robertson, On 2-generator 2-relation soluble groups, *Proc. Edinburgh Math. Soc. (2)* **23** (1980), 269–273.

[3] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version* 4.3, 2000.

[4] George Havas, Colin Ramsay, On proofs in finitely presented groups, in *Groups St Andrews 2005*, London Math. Soc. Lecture Note Series, Cambridge University Press, in press.

[5] George Havas, Edmund F. Robertson, The $F^{a,b,c}$ Conjecture, I, *Irish Math. Soc. Bulletin* **56** (2005), 75–80..

[6] George Havas, Edmund F. Robertson, Dale. C. Sutherland, The $F^{a,b,c}$ conjecture is true, II, *J. Algebra* **300** (2006), 57–72.

[7] George Havas, Edmund F. Robertson, Dale. C. Sutherland, Behind and beyond the proof of the $F^{a,b,c}$ conjecture, *in preparation.*

Experiences with the Knuth-Bendix procedure

George Havas

This is based on joint work with Michael Vaughan-Lee, with assistance from Charles Sims. It was partially supported by the Australian Research Council.

Vaughan-Lee and I proved that 4-Engel groups are locally nilpotent [2] and we wrote about some of the computations that were involved in [3]. These papers cover the relevant background material and include some history of the problem.

A group G is said to be an n-Engel group if

$$[x, \underbrace{y, y, \ldots, y}_{n}] = 1 : \forall x, y \in G.$$

Our proof that 4-Engel groups are locally nilpotent is quite long and complicated. It relies heavily on the result of Traustason [9] that 2-generator 4-Engel groups are nilpotent. A proof of this result of Traustason which uses the Knuth-Bendix procedure was discussed by Charles Sims [8] at this Oberwolfach meeting.

Our proof that 4-Engel groups are locally nilpotent is modelled on the proof used by Vaughan-Lee [11] to show that 4-Engel 5-groups are locally finite. Indeed we started by extending that result to p-groups for primes greater than 5. Vaughan-Lee's proof relies on both hand and machine calculations. In that case the machine work involved use of the p-quotient algorithm and of coset enumeration. To prove the more general result, namely local nilpotence for 4-Engel groups, the previous machine computation tools were no longer directly adequate. Where Vaughan-Lee previously used the p-quotient algorithm to prove properties of p-groups, we use a nilpotent quotient algorithm to prove properties of more general nilpotent groups. Where Vaughan-Lee previously used coset enumeration to prove finiteness of finitely presented groups, we use the Knuth-Bendix procedure to prove nilpotence.

The use of the Knuth-Bendix process as a tool for group theory was pioneered by Charles Sims. The basic procedure (in its application to groups) is described by Gilman [1] and (in great detail) by Sims [7]. A major success of the Knuth-Bendix procedure in group theory was its use by Sims [6] to verify nilpotency of a finitely presented group. The nilpotent quotient algorithm was used initially to construct a polycyclic presentation for the nilpotent quotient Q of the finitely presented group G. Then, using some relations of this presentation as part of an initial set of rewrite rules, and a special term-ordering, Sims developed an effective algorithm for verifying the triviality of the kernel of the quotient Q.

We followed a similar approach to address one particular group which plays a crucial role in our overall proof. This group, which we call T, is a 3-generator 4-Engel group which has nilpotency conditions applying to the subgroups generated by each pair of its given generators. One pair of generators commute, another pair generate a subgroup with class 2, and the remaining pair generate a subgroup with class 3. We start with the following presentation for T:

$$\langle u, v, w \mid [u,v],\ [w,u,u,u],\ [w,u,u,w],\ [w,u,w,w],\ [w,v,v],\ [w,v,w],\ \text{4-Engel}\rangle\,.$$

T arises as a preimage of a number of groups which we need to prove nilpotent. The proof that those groups are nilpotent follows directly from the fact T is nilpotent. Our computations which prove that T is nilpotent are quite subtle.

Knuth-Bendix implementations well-suited to group theory which are available include `RKBP` by Sims and `KBMAG` by Derek Holt [4] which is available in GAP and Magma. Both of these packages may be used in proving enough about T. The final result is that the Knuth-Bendix procedure (initially together with some now surplus “hand” work) shows that the group T is nilpotent.

A simple-minded approach to solving this problem is as follows. Use the nilpotent quotient algorithm (we used the implementation by Werner Nickel [5]) to find a polycyclic presentation (PCP) for the largest nilpotent quotient. Define an input group for Knuth-Bendix on the PCP generators, then run the Knuth-Bendix process using a wreath-product ordering with this input group, adding sufficient instances of the 4-Engel law till the process terminates with a confluent presentation for the group.

This approach works well with easier problems about 3-generator groups. It readily shows the nilpotency of any 3-generator 4-Engel group in which two pairs of generators commute and the remaining pair generate a subgroup with class 3. With more effort, but still easily, it shows the nilpotency of any 3-generator 4-Engel group in which one pair of generators commute and the other two pairs generate a subgroup with class 2. We have not been able to make this approach work directly for T.

When we start this way, we find that the Knuth-Bendix procedure finds many thousands of consequences of the defining relations but does not terminate even when given large amounts of time and space. Various unsuccessful attempts ran for several cpu days and used up to a gigabyte of memory. Instead, our first proof relied on some hand calculations and on our inspecting incomplete Knuth-Bendix computations and deducing useful consequences by hand.

As we did this we discovered two important facts. First, it could be useful to introduce additional, redundant generators. Second, even though the wreath-product ordering implies that the simple approach should lead (eventually) to a finite confluent presentation, we found we could make more rapid progress using lenlex ordering. We point out that the reduction to just the nilpotency problem for the group T came after we had solved similar problems for various other groups. Also, the final proof for T, which requires only one Knuth-Bendix run, was developed after we had done very many other runs.

Our published proof uses one extra generator beyond those which appear in a PCP for (the nilpotent quotient of) T. The Knuth-Bendix procedure then gives us enough additional relations to show that T is nilpotent (with some extra hand calculations). In that proof, we prefaced use of the Knuth-Bendix procedure by determining separately some additional relations which hold in T, beyond the six initial relations in the presentation given for T earlier.

Further study of the relevant computations, aided by suggestions from Charles Sims, reveals that we can use the Knuth-Bendix procedure to prove nilpotence without explicitly adding these extra relations. By adding more redundant generators and by altering the sequence of Knuth-Bendix iterations we can first obtain all of the required additional relations and subsequently deduce that T is nilpotent. It suffices to introduce definitions for all six left normed commutators of weight 5 (instead of just defining one of these, as we did originally). This makes that part of the proof both shorter and faster. Using this would have reduced our complete paper by about 10% in total length, and the proof of the nilpotence of T from about $4\frac{1}{2}$ pages to about 1 page. Furthermore, this proof of the nilpotence of T does not require arguments involving the Hirsch-Plotkin radical.

These observations raise important questions about how one should approach use of the Knuth-Bendix procedure to solve problems in group theory.

It should be noted that Traustason [10] has found a very clever proof of the nilpotence of the group T which does not use the Knuth-Bendix procedure. However both our paper and Traustason's proof of the nilpotence of T still make essential use of detailed information about the free 4-Engel group of rank 2 obtained with the nilpotent quotient algorithm. Also, our complete proof relies on a number of computations using the nilpotent quotient algorithm applied to groups of class 4 and 5.

References

[1] R.H. Gilman, *Presentations of groups and monoids*, J. Algebra **57** (1979) 544–554.

[2] George Havas and M.R. Vaughan-Lee, 4-*Engel groups are locally nilpotent*, Internat. J. Algebra Comput. **15** (2005) 649–682.

[3] George Havas and M.R. Vaughan-Lee, *Computing with* 4-*Engel groups*, Groups St Andrews 2005, London Math. Soc. Lecture Note Ser., Cambridge Univ. Press (to appear).

[4] D.F. Holt, `KBMAG` (Knuth-Bendix on Monoids and Automatic Groups, Version 2.4), Software Package (2000). Available from `http://www.maths.warwick.ac.uk/ dfh/download/kbmag2/`

[5] Werner Nickel, *Computing nilpotent quotients of finitely presented groups*, Geometric and computational perspectives on infinite groups, 175–191, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **25**, Amer. Math. Soc. (1996).

[6] Charles C. Sims, *Verifying nilpotence*, J. Symbolic Comput. **3** (1987) 231–247.

[7] Charles C. Sims, *Computation with finitely presented groups*, Encyclopedia of Mathematics and its Applications **48**, Cambridge Univ. Press (1994).

[8] Charles C. Sims, *Computational investigations of 4-Engel groups*, Oberwolfach Report 30/2006 1837–1838.

[9] Gunnar Traustason, *Two generator* 4-*Engel groups*, Internat. J. Algebra Comput. **15** (2005) 309–316.

[10] Gunnar Traustason, *A note on the local nilpotence of* 4-*Engel groups*, Internat. J. Algebra Comput. **15** (2005) 757–764.

[11] Michael Vaughan-Lee, *Engel*-4 *groups of exponent* 5, Proc. London Math. Soc. **74** (1997) 306–334.

Computational Investigations of 4-Engel Groups

Charles C. Sims

A group G satisfies the 4-Engel condition if for all elements x and y of G the left-normed commutator $[x, y, y, y, y]$ is trivial. In [3] Traustason proved that two-generator 4-Engel groups are nilpotent. Using this result, Havas and Vaughan-Lee [1] then showed that all 4-Engel groups are locally nilpotent.

Let $E(2, 4)$ denote the freest two-generator 4-Engel group. By Traustason, $E(2, 4)$ is nilpotent and hence finitely presented. Thus $E(2, 4)$ is defined as a two-generator group by a finite number of instances of the 4-Engel identity. Traustason's proof is nonconstructive in the sense that it makes heavy use of properties of the Hirsch-Plotkin radical. This makes it difficult to determine an explicit finite set of instances of the 4-Engel identity that defines $E(2, 4)$.

The main purpose of this talk is to report that the speaker has obtained a direct computational proof that $E(2, 4)$ is nilpotent, a proof that uses no more than 10^8 instances of the 4-Engel identity. It is almost certain that a much smaller set of instances suffices. Work continues to construct such a set.

The only reasonable computational tool for demonstrating the nilpotence of $E(2, 4)$ is the Knuth-Bendix procedure for strings. An introduction to this procedure can be found in Chapter 2 of [2]. Attempts to use the Knuth-Bendix procedure to study $E(2, 4)$ were initially unsuccessful. Only when a large number of redundant generators were added was progress possible.

One set of generators that "works" is the set of commutators of weight at most 10 in two generators. More precisely, let a and b denote the standard generators of $E(2, 4)$ and define a sequence of commutators as follows: The commutators of weight 1 in the sequence are a and b, in that order. Suppose that the commutators of weight up to n have been defined. Then the commutators of weight $n + 1$ in the sequence are all $[v, u]$, where u and v are already in the sequence, u precedes v, and the sum of the weights of u and v is $n + 1$. The new commutators are ordered first by v and then by u.

There are 2363 commutators in this sequence with weight at most 10. Let these commutators be denoted a_1, …, a_{2363}. The initial input to the Knuth-Bendix procedure consists of these 2363 generators, their definitions in terms of $a = a_1$

and $b = a_2$, and approximately 10^8 instances $[u, v, v, v, v]$ of the 4-Engel identity, where u and v are words of length at most 3 in the a_i.

After several days of cpu time on a SunFire computer, a number of the a_i have been shown to be trivial, some have been shown equal to others, and two, a_{1206} and a_{1991}, have been determined to be central. Quite quickly the groups $\langle a_1, a_3\rangle$ and $\langle a_2, a_3\rangle$ are found to be nilpotent of class at most 4. It takes quite a bit longer to get any additional information.

Since a group is nilpotent if and only if the quotient of the group by its center is nilpotent, the elements a_{1206} and a_{1991} may be set equal to 1. If this is done, then after another couple of days of cpu time, some more generators have been shown to be trivial and some others have been shown to be central. Again, these central generators are set equal to 1 and the computation continued. Setting central elements equal to 1 twice more leads to a group that is obviously nilpotent.

The bound one gets for the nilpotence class of $E(2, 4)$ from this computation is too high. As shown by the implementation of the nilpotent quotient algorithm by Werner Nickel, the correct class is 6. One could try to see if the Knuth-Bendix procedure can correctly obtain the class. This would be done by setting all commutators of weight 8 equal to 1 and seeing whether the Knuth-Bendix procedure can deduce that all commutators of weight 7 are also 1.

The total cpu time required for this computation was about 10 days. Roughly 16 gigabytes of memory were needed. Substantial modifications to the speaker's implementations of the Knuth-Bendix procedure had to be made and the programs needed to be run in a 64-bit environment.

More thought should be given to the question of what redundant generators to add in a Knuth-Bendix computation. With $E(2, 4)$, the defining relators are commutators and to prove nilpotence one wants to prove that commutators of high weight are trivial. Thus adding commutators as extra generators makes a lot of sense.

One would also like to study Burnside groups computationally. Here again one is trying to prove nilpotence or solvability but now the relators being added are powers. The proper choice of additional generators in this situation is less obvious.

A great deal of additional experimentation with 4-Engel groups has been performed. For example, it was shown that both $H = \langle a, b \,|\, a^2 = 1, \text{4-Engel}\rangle$ and $K = \langle a, b \,|\, a^4 = 1, \text{4-Engel}\rangle$ have finite confluent rewriting systems on the given generators with respect to the lenlex ordering with $a < a^{-1} < b < b^{-1}$. In H, b^{16} commutes with a. Thus in a 4-Engel group, the 16th power of every element commutes with all involutions.

References

[1] G. Havas and M. R. Vaughan-Lee, *4-Engel groups are locally nilpotent*, Internat. J. Alg. Comp. **15** (2005), 649–682.

[2] C. C. Sims, *Computation with Finitely Presented Groups.* Cambridge University Press 1994.

[3] G. Traustason, *Two generator 4-Engel groups*, Internat. J. Alg. Comp. **15** (2005), 309–316.

Computational Invariant Theory – new developments

Gregor Kemper

This talk gives a survey of some old topics and some new developments in invariant theory. The basic setting is as follows: Let G be a linear algebraic group and X an affine variety on which G acts by a morphism $G \times X \to X$. Then G also acts on the ring $K[X]$ of regular functions, and we consider the invariant ring $K[X]^G$. An important special case occurs when X is affine n-space and G acts linearly. There are a number of classical problems in invariant theory:

- Hilbert's 14th problem: Is $K[X]^G$ finitely generated (as a K-algebra)?
- If so, find generators (and/or teach a computer to do so).
- What structural properties does the algebra $K[X]^G$ have?
- Orbit separation: For $x, y \in X$ with $G(x) \neq G(y)$, does there exist $f \in K[X]^G$ with
$$f(x) \neq f(y)?$$

It is the second problem that we will be particularly interested in. Progress has been made on various fronts here. To give an account of the present state of the art, it is useful to distinguish between various classes of groups. Notably, we have the finite groups, the reductive groups, and the linearly reductive groups. For computing invariant rings of finite groups, algorithms have been found by Sturmfels and by the author. For G linearly reductive, an algorithm was given by Harm Derksen in 1999. Various other algorithms are available for infinite groups, with various degrees of generality. It is striking that one ideal, which we propose to call the *Derksen ideal*, appears in all these algorithms. The Derksen ideal D comes in various flavors. We assume that G acts on a K-algebra R, and $x_1, \dots, x_n \in R$.

Algebraically:: $D := \bigcap_{\sigma \in G} \langle y_1 - \sigma(x_1), \dots, y_n - \sigma(x_n) \rangle_{R[y_1,\dots,y_n]}$ (ideal in polynomial ring $R[y_1, \dots, y_n]$). This may be taken as the definition of D.

Geometrically:: If $R = K[V] = K[x_1, \dots, x_n]$, then D is the vanishing ideal of
$$\mathcal{D} = \{(x, y) \in V \times V | G(x) = G(y)\}.$$

Computationally:: If $G \subseteq K^m$ with vanishing ideal $I_G \subseteq K[t_1, \dots, t_m]$, and $\sigma(x_i) = f_i(\sigma)$ with $f_i \in R[t_1, \dots, t_m]$, then
$$D = \langle I_G \cup \{y_1 - f_1, \dots, y_n - f_n\} \rangle_{R[\underline{t}, \underline{y}]} \cap R[y_1, \dots, y_n].$$

Thus computing D amounts to the computation of an elimination ideal, which can be done by Gröbner basis computations. This is the main computational step in most of the algorithms.

The Derksen ideal is used in Derksen's algorithm, whence its name. But it is also the main protagonist in an algorithm for computing invariant fields, which was found in 1999 by Müller-Quade and Beth and was generalized in 2006 by the author. This algorithm works for all algebraic groups and has a stunningly simple proof of correctness. A theorem of Rosenlicht on separating properties of rational invariants can be derived as a consequence.

We continue by considering *separating invariants*, which is a weakening of the concept of generating invariants. It turns out that in many respects separating invariants have nicer properties than generating invariants. Moreover, using separating invariants as an intermediate step yields an algorithm for computing invariant rings of reductive groups. This algorithm also uses the Derksen ideal.

The invariants of the Clifford-Weil groups

Gabriele Nebe

There is a beautiful analogy between most of the notions for lattices and codes provided by construction A (see for instance [2], [3], [6]). Theta-series of lattices correspond to weight-enumerators of codes. Whereas theta-series of unimodular lattices are modular forms for certain Siegel modular groups, weight-enumerators of self-dual codes are polynomials invariant under a certain finite group, called the associated Clifford-Weil group, and in fact the main result of [3] shows that these weight-enumerators generate the invariant ring. Many structures from modular forms, such as Siegel's Φ-operator that maps the genus-m Siegel theta-series of a lattice to its Siegel theta-series of genus $m-1$, have analogues on the coding theory side. One missing concept was the one of Hecke-operators which play an important role for the investigation and construction of modular forms. For codes over finite fields these are introduced in the two papers [4] and [5], which therewith answer a question raised in 1977 in [1].

For $N \in \mathbf{N}$ let

$$\mathcal{F}_N := \{C = C^\perp \leq \mathbf{F}_q^N\}$$

denote the family of self-dual codes of length N over $\mathbf{F}_q$. The genus-m complete weight enumerator $p_C^{(m)}$ of a code $C \in \mathcal{F}_N$ is a homogeneous polynomial of degree N in q^m variables that encodes important information about the code. The main theorem of [3] constructs a finite complex matrix group $\mathcal{C}_m \leq \mathrm{GL}_{q^m}(\mathbf{C})$, the associated *Clifford-Weil group*, such that the space of homogeneous polynomials of degree N that are invariant under $\mathcal{C}_m$ is the linear span of the $p_C^{(m)}$ with $C \in \mathcal{F}_N$,

$$\mathrm{Inv}_N(\mathcal{C}_m) = \langle p_C^{(m)} \mid C \in \mathcal{F}_N \rangle.$$

Since the genus-$\frac{N}{2}$ weight enumerators of inequivalent codes in $\mathcal{F}_N$ are linearly independent, the Molien series of $\mathcal{C}_m$ tends monotonically to the generating function of the number of equivalence classes of codes in $\mathcal{F}_N$ when m goes to infinity. The coding-theoretic analogue of the Siegel Φ-operator introduced by Runge [6] maps $p_C^{(m)}$ to $p_C^{(m-1)}$ and therewith yields a surjective linear mapping

$$\Phi_m : \mathrm{Inv}_N(\mathcal{C}_m) \to \mathrm{Inv}_N(\mathcal{C}_{m-1})$$

between invariant rings of linear groups of different degree. This gives rise to an orthogonal decomposition (with respect to the natural $\mathcal{C}_m$-invariant hermitian product on $\mathrm{Inv}_N(\mathcal{C}_m)$)

$$\mathrm{Inv}_N(\mathcal{C}_m) = \ker(\Phi_m) \perp \ker(\Phi_m)^{\perp} \cong \ker(\Phi_m) \perp \mathrm{Inv}_N(\mathcal{C}_{m-1}) \cong \perp_{j=0}^{m} \ker(\Phi_j) \quad \star\,.$$

We present two constructions of a commutative subalgebra of $\mathrm{End}(\mathrm{Inv}_N(\mathcal{C}_m))$ that has $\star$ as eigenspace decomposition. The first one uses codes, the second one expresses these Hecke-operators as linear combinations of $\mathcal{C}_m$-double cosets.

1) Codes: The family $\mathcal{F}_N$ is the union of, say, h equivalence classes of codes $\mathcal{F}_N = \cup_{i=1}^{h}[C_i]$. Note that equivalent codes have the same complete weight enumerators. Regarding $([C_1],\dots,[C_h])$ as a basis of a complex vector space V, define the Kneser-Hecke operator $T \in \mathrm{End}(V)$ by

$$T([C_i]) := \sum_{D \in \mathcal{F}_N} [D]$$

where the sum runs over all D such that $\dim(D \cap C_i) = N/2 - 1$. The action of T on the genus-m complete weight enumerators gives a linear operator $\delta_m(T) \in \mathrm{End}(\mathrm{Inv}_N(\mathcal{C}_m))$. The eigenspaces of $\delta_m(T)$ are the non-zero direct summands of $\star$ with explicitly known eigenvalues.

2) Double-cosets: For lattices the analogue of the operator $\delta_m(T)$ is a linear combination of double cosets of the associated modular group. In the coding theory case one finds a similar expression using the fact that $\mathcal{C}_m$ is a finite Weil representation, which means that there is a Heisenberg group $E_m \leq \mathrm{GL}_{q^m}(\mathbf{C})$ that is normalized by $\mathcal{C}_m$. The paper [5] constructs a commutative algebra $\mathcal{H}(\mathcal{C}_m)$ generated by double-cosets $\mathcal{C}_m p_U \mathcal{C}_m$ of orthogonal projections p_U onto the fixed space of suitable elementary abelian subgroups $U \leq E_m$. Its action on $\mathrm{Inv}_N(\mathcal{C}_m)$ coincides with the algebra generated by $\delta_m(T)$.

References

[1] M. Broué, *Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et formes quadratiques entières définies positives à discriminant* +1. Discrete Math. **17** (1977), no. 3, 247–269.

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 1998, 3rd. ed. 1998.

[3] G. Nebe, E. M. Rains and N. J. A. Sloane, *Self-dual codes and invariant theory.* Springer-Verlag ACM 17 (2006).

[4] G. Nebe, *An analogue of Hecke-operators in coding theory.* (submitted)

[5] G. Nebe, *Finite Weil-representations and associated Hecke-algebras.* (submitted)

[6] B. Runge, *Codes and Siegel modular forms,* Discrete Math. **148** (1996), 175–204.

Representations, commutative algebra, and Hurwitz groups

Daniel Robertz
(joint work with Wilhelm Plesken)

In [13] we have constructed characteristic zero representations of the $(2, 3, 7)$-triangle group

$$G_{2,3,7} := \langle a, b \mid a^2,\, b^3,\, (ab)^7 \rangle$$

in degrees up to seven. Some families of Hurwitz groups [3, 8, 9, 14, 15], i.e. finite epimorphic images of $G_{2,3,7}$ were found as images of these representations. The employed method was already suggested in [11] and applied in [4], but nowadays more powerful computational techniques are available.

The procedure to construct matrix representations is in principle applicable to any finitely presented group G. We assign matrices with indeterminate entries to the generators of the presentation and translate the relators into relations between these commuting variables. Hence, the set of all matrix representations of G with entries in a field K is viewed as the set of K-rational points of an affine variety. The corresponding system of algebraic equations is handled by Janet's algorithm [5], which is an earlier and rather successful version of a Gröbner basis type algorithm, cf. [12, 1]. The dimension of the variety is easily obtained from Janet's algorithm. In the zero-dimensional case the result gives finitely many matrix representations over some number field.

This method was applied to $G = G_{2,3,7}$ for small degrees. When restricting to irreducible representations, i.e. cyclic KG-modules M, the number of indeterminates can drastically be reduced by choosing a structurally rigid K-basis of M. To this end, a total order $<$ on the free monoid F generated by a, b is defined which is compatible with the left multiplication in F. We start with an eigenvector e_1 for ab. Suppose we have already defined i basis vectors $e_1, \ldots, e_i$ of M. Then we choose e_{i+1} to be $w\, e_1$, where w is the smallest word in F with respect to $<$ such that $(e_1, \ldots, e_i, w\, e_1)$ is K-linearly independent.

In [13], a total order $<$ with $b < a$ was chosen which led to a unique K-basis for the KG-modules up to degree 5; for larger degrees case distinctions had to be made. We classified the irreducible projective representations of $G_{2,3,7}$ completely up to degree 5 and solved some cases in degree 6 and 7.

The outlined approach sometimes allows to prove that the considered group G is infinite. If it is not, then group recognition routines [2, 10, 6] may identify the image of the representation. Moreover, further relations can easily be added to the presentation when using the above method. In [13] the additional relator $[a, b]^n$ was imposed for $n \in \{4, \ldots, 19\}$ when considering degree 6 in finite characteristic (for computational reasons). Some finite groups, e.g. the second Janko group J_2, came up, but the construction of an infinite factor group of $G_{2,3,7}$ was not rigorously carried out. In general, one may ask if it is possible to decide whether there are additional relations which can be imposed, still admitting solutions. If it is possible, of course, one would like to find such relations. Since the method can be applied over $\mathbb{Z}$ as well, it can for instance be used to find all prime powers q for which epimorphisms onto $\mathrm{PSL}_2(q)$ exist.

References

[1] Y. A. Blinkov, C. F. Cid, V. P. Gerdt, W. Plesken, D. Robertz. *The MAPLE Package "Janet": I. Polynomial Systems.* In *Proc. of Computer Algebra in Scientific Computing CASC 2003*, edited by V. G. Ganzha, E. W. Mayr, E. V. Vorozhtsov, 31–40. Garching, Germany: Institut für Informatik, TU München, 2003. Also available together with the package from WWW (`http://wwwb.math.rwth-aachen.de/Janet`).

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

[3] L. Di Martino, M. C. Tamburini, A. E. Zalesskii. *On Hurwitz groups of low rank.* Comm. Algebra 28 (2000), no. 11, 5383–5404.

[4] D. F. Holt, W. Plesken, B. Souvignier. *Constructing a Representation of the Group* $(2,3,7,11)$. J. Symbolic Computation **24** (1997), 489–492.

[5] M. Janet, *Leçons sur les systèmes des équationes aux dérivées partielles.* Cahiers Scientifiques IV, Gauthiers-Villars, Paris, 1929.

[6] C. R. Leedham-Green. *The computational matrix group project*, in W. M. Kantor, Á. Seress (eds.), *Groups and computation III. Proceedings of the international conference at the Ohio State University, Columbus, OH, USA, June 15-19, 1999.* Berlin: Walter de Gruyter. Ohio State Univ. Math. Res. Inst. Publ. 8, 229–247 (2001).

[7] A. Lubotzky, A. R. Magid. *Varieties of representations of finitely generated groups.* Mem. Amer. Math. Soc. 58 (1985), no. 336.

[8] A. M. Macbeath. *Hurwitz Groups and Surfaces.* in S. Levy (ed.) *The Eightfold Way.* Cambridge University Press, 1999, 103–113.

[9] G. Malle. *Hurwitz groups and* $G_2(q)$. Canad. Math. Bull. **33** (1990), no. 3, 349–357.

[10] A. C. Niemeyer, C. E. Praeger. *A recognition algorithm for classical groups over finite fields.* Proc. London Math. Soc. (3) **77** (1998), no. 1, 117–169.

[11] W. Plesken, B. Souvignier. *Analyzing finitely presented groups by constructing representations.* J. Symbolic Computation **24** (1997), 335–349.

[12] W. Plesken, D. Robertz. *Janet's approach to presentations and resolutions for polynomials and linear pdes.* Arch. Math. **84**:1 (2005), 22–37.

[13] W. Plesken, D. Robertz. *Representations, commutative algebra, and Hurwitz groups.* J. Algebra **300** (2006), 223–247.

[14] M. C. Tamburini, M. Vsemirnov. *Hurwitz groups and Hurwitz generation.* Handbook of Algebra, vol. 4, edited by M. Hazewinkel, Elsevier. Preprint: http://www.dmf.unicatt.it/semmat/preprints/2003.

[15] M. C. Tamburini, A. E. Zalesski. *Classical groups in dimension 5 which are Hurwitz.* in: C. Y. Ho, P. Sin, P. H. Tiep and A. Turull (eds.). *Finite groups 2003. Proceedings of the conference held in Gainesville, FL, March 6–12, 2003.* Walter de Gruyter, Berlin, 2004, 363–371.

Computing minimal polynomials

Max Neunhöffer
(joint work with Cheryl Praeger)

We present an algorithm to compute minimal polynomials of matrices that is in practice over finite fields noticeably faster than the algorithms currently implemented in GAP and Magma. The algorithm consists of a Monte Carlo algorithm to actually compute the minimal polynomial with a prescribed maximal error probability, and a deterministic verification phase. The procedure was inspired by, and developed from, a deterministic minimal polynomial algorithm for cyclic matrices by Peter Neumann and Cheryl Praeger in [1].

Let F be a finite field and $M \in F^{n\times n}$ a matrix acting from the right on the row space $V := F^{1\times n}$.

We first compute the characteristic polynomial with the standard approach. That is, we first compute the order polynomial of a random vector v_1 and then inductively the relative order polynomials of further random vectors v_i modulo the spaces $\langle v_1, \ldots, v_{i-1}\rangle_M$ respectively until we have $V = \langle v_1, \ldots, v_k\rangle_M$. We carefully store all intermediate results, such that we end up with a new F-basis of V:

$$(v_1, v_1M, \ldots, v_1M^{d_1-1}, \ldots, v_k, v_kM, \ldots, v_kM^{d_k-1})$$

The data structures involved in this part are as in [1]. A probability analysis then shows that for each $\epsilon > 0$ we can determine some small number u with $1 \le u \le k$ such that the probability, that the least common multiple of the absolute order polynomials of $v_1, \ldots, v_u$ is equal to the minimal polynomial of M, is greater than $1 - \epsilon$.

Using the sparseness of M after a base change to the new basis we obtain a Monte Carlo algorithm with prescribed error bound ϵ to compute the minimal polynomial of M by computing the absolute order polynomials of $v_1, \ldots, v_u$ and their least common multiple using all the already acquired information.

We can show that the total number of elementary field operations (counting additions, multiplications, and inversions) needed to compute the absolute order polynomial of v_j is bounded by

$$(j + 8) \cdot D^2 + j \cdot D$$

where $D = \dim_F(\langle v_1, \ldots, v_j\rangle_M)$, assuming the results from the computations of the characteristic polynomial.

Given $\epsilon > 0$, we can bound the value u such that we end up with an analysis showing, that for every fixed $\epsilon > 0$ our Monte Carlo algorithm needs asymptotically for $n \to \infty$ less than $5n^3$ elementary field operations plus the number of operations needed for the factorisation of the characteristic polynomial plus the number of operations needed for generating k random vectors.

In many cases the algorithm in addition proves the result to be true, for example if the minimal polynomial is equal to the characteristic polynomial. For other cases, we have a deterministic verification routine that performs well in practice. However, it still needs improvement with respect to its worst case analysis.

References

[1] Peter Neumann and Cheryl Praeger, *Exploiting cyclic matrices in computer algebra: Sharpening the Meataxe*, in preparation.

Stratification of diagram algebras

Anne Henke
(joint work with R. Hartmann, S. Koenig, R. Paget)

Background. In 1937 Brauer [1] asked the question which algebra has to replace the group algebra of the symmetric group $k\Sigma_r$ in Schur-Weyl duality if one replaces the general linear groups GL_n by its orthogonal or symplectic subgroup. As an answer for $k = \mathbb{C}$, he defined an algebra which is a special case of what nowadays is called the Brauer algebra $B_k(r, \delta)$ with parameter $\delta \in k$. Brauer algebras at first were mainly studied over the complex numbers. Hanlon and Wales [5] conjectured values δ for which $B_{\mathbb{C}}(r, \delta)$ is semi-simple. This conjecture was proved by Wenzl [12]. The question about semisimplicity of $B_k(r, \delta)$ over any field k was settled only recently by Rui [11].

The interest in Brauer algebras over a field k of prime characteristic increased, when Graham and Lehrer [4] introduced the structure of cellular algebras to allow a more systematic study of Brauer algebras, Ariki-Koike algebras etc. Koenig and Xi [10] showed that they are iterated inflations of group algebras of symmetric groups, and thus reproved that Brauer algebras are cellular.

Here, more generally we are interested in algebras represented by diagrams, like Brauer algebras, BMW-algebras or partition algebras. The theoretical results presented here (for details see [6]) have been motivated by computations with Brauer algebras, using GAP and the MeatAxe and by results on Brauer algebras in [7].

Cellularly stratified algebras. Let A be an algebra which can be realised as an iterated inflation of smaller cellular algebras B_l along vector spaces V_l for $l = 1, \ldots, n$. By [9] this implies that as a vector space $A = \bigoplus_{l=1}^{n} B_l \otimes V_l \otimes V_l$. Moreover, A is cellular with a chain of ideals $0 \subset J_1 \subset \ldots \subset J_n = A$, which can be refined to a cell chain, and each subquotient J_l/J_{l-1} equals $B_l \otimes V_l \otimes V_l$ as algebra without unit. Let 1_{B_l} be the unit element of the algebra B_l. We suggest in [6] the following definition:

Definition. A finite dimensional associative algebra A over a field k is called *cellularly stratified* with stratification data $(B_1, V_1, \ldots, B_n, V_n)$ if and only if the following conditions are satisfied:

(C) Algebra A is an iterated inflation of cellular algebras B_l along vector spaces V_l for $l = 1, \ldots, n$.

(L) For each $l = 1, \ldots, n$, there exists an idempotent $e_l \in A$ such that $J_l = Ae_lA$ and $e_l = 1_{B_l} \otimes u_l \otimes v_l$ for some vectors $u_l, v_l \in V_l$.

(I) If $l > m$, then $e_l e_m = e_m = e_m e_l$.

(E) For $l = 1, \ldots, n$, map $\iota_l : B_l \to A$ with $\iota_l(b) = b \otimes u_l \otimes v_l$ is multiplicative.

Examples.

- Let $r \in \mathbb{N}$ and $\delta \in k$. If r is even, suppose $\delta \neq 0$. Then the Brauer algebra $B_k(r, \delta)$ is cellularly stratified. The B_l's are group algebras of symmetric groups.

FIGURE 1. Decomposition matrix of $B_k(7,1)$ with $char(k) = 2$

dim	*cell\simples*	1	6	14	8	20	15	48	76	35	84	1
1	(7)	1	.	.	.	.	.	.	.	.	.	.
6	$(6,1)$	.	1	.	.	.	.	.	.	.	.	.
14	$(5,2)$	.	.	1	.	.	.	.	.	.	.	.
14	$(4,3)$	.	1	.	1	.	.	.	.	.	.	.
15	$(5,1^2)$	1	.	1	.	.	.	.	.	.	.	.
35	$(4,2,1)$	1	.	1	.	1	.	.	.	.	.	.
21	$(3^2,1)$	1	.	.	.	1	.	.	.	.	.	.
21	$(3,2^2)$	1	.	.	.	1	.	.	.	.	.	.
20	$(4,1^3)$	.	2	.	1	.	.	.	.	.	.	.
35	$(3,2,1^2)$	1	.	1	.	1	.	.	.	.	.	.
14	$(2^3,1)$	.	1	.	1	.	.	.	.	.	.	.
15	$(3,1^4)$	1	.	1	.	.	.	.	.	.	.	.
14	$(2^2,1^3)$	.	.	1	.	.	.	.	.	.	.	.
6	$(2,1^5)$	.	1	.	.	.	.	.	.	.	.	.
1	(1^7)	1	.	.	.	.	.	.	.	.	.	.
21	(5)	.	1	.	.	.	1	.	.	.	.	.
84	$(4,1)$	2	.	1	.	1	.	1	.	.	.	.
105	$(3,2)$	.	1	.	1	.	1	.	1	.	.	.
126	$(3,1^2)$	.	2	.	1	.	2	.	1	.	.	.
105	$(2^2,1)$	.	1	.	1	.	1	.	1	.	.	.
84	$(2,1^3)$	2	.	1	.	1	.	1	.	.	.	.
21	(1^5)	.	1	.	.	.	1	.	.	.	.	.
105	(3)	2	.	.	.	1	.	1	.	1	.	.
210	$(2,1)$	.	2	.	1	.	2	.	1	.	1	.
105	(1^3)	2	.	.	.	1	.	1	.	1	.	.
105	(1)	.	2	.	1	.	.	.	.	.	1	1

- Let $n \in \mathbb{N}$, $\lambda, \lambda^{-1}, q, q^{-1}, \delta \in k$ satisfying $\lambda^{-1} - \lambda = (q - q^{-1})(\delta - 1)$. If n is even, suppose $\delta \neq 0$. Then the BMW algebra $BMW_k(n, \lambda, q - q^{-1}, \delta)$ is cellularly stratified. The B_l's are Hecke algebras.
- Let $n \in \mathbb{N}$ and $\delta \in k$. Suppose $\delta \neq 0$. Then the partition algebra $P_k(n, \delta)$ is cellularly stratified. The B_l's are group algebras of symmetric groups.

We define the induction functor $G_l = Ae \otimes_{eAe} B_l \otimes_{B_l} - : B_l\text{-mod} \to A\text{-mod}$. Then G is an exact functor, sending cell modules of B_l to cell modules of A. Decomposition numbers are the multiplicities of simple modules as composition factors in cell modules.

Theorem. *For each l, the decomposition matrix of B_l is a diagonal submatrix of the decomposition matrix of A.*

We computed decomposition matrices of Brauer algebras for $r \leq 9$ and $\delta \in \{0, 1\}$ for $p = 2$ and $\delta \in \{0, 1, 2\}$ for $p = 3$.

Theorem. *Let A be cellularly stratified. Then A is stratified in the sense of* [2] *with a stratification provided by the ideals J_l. Moreover, for any l there is a full recollement of bounded derived categories*

$$\begin{tikzcd} \mathcal{D}^b(A/J_l\text{-}mod) \arrow[r, shift left=1.5ex, leftarrow] \arrow[r] \arrow[r, shift right=1.5ex, leftarrow] & \mathcal{D}^b(A\text{-}mod) \arrow[r, shift left=1.5ex, leftarrow] \arrow[r] \arrow[r, shift right=1.5ex, leftarrow] & \mathcal{D}^b(B_l\text{-}mod). \end{tikzcd}$$

The second part of the theorem implies that the derived category of A has a stratification (iterated recollements) by the derived categories of the algebras B_l.

Corollary. *Let A be cellularly stratified, M, N any A/J_l-modules and X, Y any B_l-modules. Then for any $i > 0$ and any $j \geq 0$:*

$$Ext^i_A(M,N) \simeq Ext^i_{A/J_l}(M,N), \qquad Ext^j_{B_l}(X,Y) \simeq Ext^j_A(G_l(X), G_l(Y)).$$

Corollary. *Let A be cellularly stratified by the algebras $B_1, \ldots, B_n$. Then the global dimension of A is finite if and only if all B_l have finite global dimensions. The finitistic dimension of A is finite if and only if all B_l have finite finitistic dimensions. In particular, the finitistic dimension conjecture holds for Brauer algebras, BMW-algebras and partition algebras.*

Dlab and Ringel defined standardizable sets in an abelian category [3, Section 3]. If the cell modules of a cellular algebra form such a standardizable set, this implies that modules with a cell-filtration have well-defined filtration multiplicities.

Theorem. *Let A be cellularly stratified. The cell modules of A form a standardizable set iff for each l, the cell modules of B_l form a standardizable set.*

Let e be least with $1 + q^{-2} + q^{-4} + \cdots + q^{-2e} = 0$, $q \in k$. Using [8, 4.2.1, 4.4.1]:

Corollary. *Let $char(k) \neq 2, 3$. Then Brauer algebras (with $\delta \neq 0$ if r even) and partition algebras (with $\delta \neq 0$) are cellular algebras, whose cell modules form a standardizable set. Suppose $e \geq 4$. Then the BMW algebras (with $\delta \neq 0$ if n even) are cellular algebras, whose cell modules form a standardizable set. In the above algebras, modules with cell filtrations have well-defined filtration multiplicities.*

References

[1] R.Brauer, *On algebras which are connected with the semisimple continuous groups.* Annals of Math. **38**, 854–872 (1937).

[2] E.Cline, B.Parshall, and L.Scott, *Stratifying endomorphism algebras.* Memoir A.M.S. **124** (1996).

[3] V.Dlab and C.M.Ringel, *The module theoretic approach to quasi-hereditary algebras.* In: Representations of algebras and related topics (Kyoto, 1990), 200–224, London Math. Soc. Lecture Note Ser., **168**, Cambridge Univ. Press, Cambridge (1992).

[4] J.J.Graham and G.I.Lehrer, *Cellular algebras.* Invent.Math. **123**, no. 1, 1–34 (1996).

[5] P.Hanlon and D.Wales, *Computing the discriminants of Brauer's centralizer algebras.* Math. Comp. **54**, no. 190, 771-796 (1990).

[6] R.Hartmann, A.Henke, S.Koenig, R.Paget, *Cohomological stratification of diagram algebras.* Preprint (2006).

[7] R.Hartmann, R.Paget, *Young modules and filtration multiplicities for Brauer algebras.* To appear Math Z.

[8] D.Hemmer and D.Nakano, *Specht filtrations for Hecke algebras of type A.* J. London Math. Soc. (2) **69**, 623–638 (2004).

[9] S.Koenig and C.C.Xi, *Cellular algebras: inflations and Morita equivalences.* J. London Math. Soc. (2) **60**, 700–722 (1999).

[10] S.Koenig and C.C.Xi, *A characteristic free approach to Brauer algebras.* Trans. Amer. Math. Soc. **353**, 1489–1505 (2001).

[11] H.Rui, *A criterion on the semisimple Brauer algebras.* J. Combin. Theory Ser. A **111**, no. 1, 78–88 (2005).

[12] H.Wenzl, *On the structure of Brauer's centralizer algebras.* Ann. of Math. (2) **128**, no. 1, 173–193 (1988).

Algorithmic use of the Mal'cev correspondence

Björn Assmann

The connection between groups and Lie rings, respectively Lie algebras, is a well-known and mathematically very useful concept. For example, a typical way to solve a problem in a Lie group is to transfer the problem to the Lie algebra of the group, study it there with the help of tools from linear algebra and transfer the result back into the Lie group.

Mechanisms of this kind have also been shown to be useful for algorithmic applications. For instance, Vaughan-Lee and O'Brien used Lie ring techniques to construct a consistent polycyclic presentation of $R(2, 7)$, the largest finite 2-generator group of exponent 7 [7].

Mal'cev showed in the 1950s that there is a correspondence between $\mathbb{Q}$-powered nilpotent groups and rational nilpotent Lie algebras [6]. I am interested in algorithmic applications of this correspondence to computations with infinite polycyclic groups; so far I have used it for the following projects.

- **Fast collection in infinite polycyclic groups** [1, 3].
  Collection lies in the heart of most algorithms dealing with polycyclically presented groups. The current state of the art for collection in those groups is "Collection from the left" (Cftl). The Mal'cev correspondence can be used to gain a considerable speed up in comparison with Cftl.
- **Symbolic collection in infinite polycyclic groups**.
  In [4] du Sautoy showed that for a given infinite polycyclic group G, there exist certain functions (K-linear combinations of monomials in integer variables and expressions like ω^y, where K is a number field, $\omega \in K$ and y an integer variable) that describe the collection process in a subgroup of finite index of G. The Mal'cev correspondence can be used to compute these functions. This method can be seen as a generalisation of the algorithm "Deep Thought" of Leedham-Green and Soicher [5].
- **Testing polycyclicity of finitely generated rational matrix groups** (joint with Bettina Eick) [2].
  Given a finite set of matrices $g_1, \ldots, g_n \in \mathrm{GL}(d, \mathbb{Q})$ the Mal'cev correspondence can be used for testing whether $G = \langle g_1, \ldots, g_n \rangle$ is polycyclic. In particular it can be used to control possibly infinitely generated torsion-free nilpotent subgroups of G.

In the near future I plan to apply Lie methods to various other computations with soluble/polycyclic groups. For example, I want to use them for collection in p-groups and for studying the conjugacy problem in finitely generated soluble rational matrix groups.

References

[1] B. Assmann. Algorithmic use of the Mal'cev correspondence. In C. M. Campbell and E. F. Robertson, editors, *Groups - St. Andrews 2005*. To appear.

[2] B. Assmann and B. Eick. Testing polycyclicity of finitely generated rational matrix groups. *Submitted*, 2006.

[3] B. Assmann and S. Linton. Using the Mal'cev correspondence for collection in polycyclic groups. *In preparation*, 2006.

[4] M. du Sautoy. Polycyclic groups, analytic groups and algebraic groups. *Proc. London Math. Soc. (3)*, 85:62–92, 2002.

[5] C. R. Leedham-Green and L. H. Soicher. Symbolic collection using Deep Thought. *LMS J. Comput. Math.*, 1:9 – 24, 1998.

[6] A. J. Mal'cev. On certain classes of infinite soluble groups. *Mat. Sb.*, 28:567 – 588, 1951.

[7] E.A. O'Brien and M. Vaughan-Lee. The 2-generator restricted burnside group of exponent 7. *Internat. J. Algebra Comput.*, 12:575–592, 2002.

Groups generated by automata

Laurent Bartholdi

There has been considerable interest since the 1980's in groups generated by automata – these include examples by Aleshin, Grigorchuk, Gupta and Sidki, among others. They produced groups of intermediate growth, and infinite torsion groups, among others.

This note reports on a coming Gap package, Fr, for manipulation and computation with such groups. For more information on groups generated by automata and self-similar groups, consult the references [3, 4, 2, 5].

1. Machines

The basic objects are as follows: a *machine*, or *automaton* M is defined by a set X, called the *alphabet*; a set Q, called the *stateset*; and a function $\phi : Q \times X \to X \times Q$ called the *transition*.

An *element* $E = (M, q)$ is a machine M, with a distinguished internal *state* $q \in Q$. An element (M, q) induces a transformation of finite sequences X^*, or of infinite sequences X^∞, as follows. Given a sequence $x_1 x_2 \dots$, the machine reads the first letter, x_1; it then computes $\phi(q, x_1) = (y_1, q')$; it then outputs the letter y_1; puts itself in internal state q'; and proceeds with the remainder $x_2 x_3 \dots$ of the sequence.

Clearly this transformation is invertible as soon as for all $q \in Q$ the projection on the first coördinate of the restriction $\phi(q, -)$ induces a bijection $X \to X$.

There are two types of machines: either Q is a finite set, in which case ϕ is stored as a table (M is then called a *Mealy machine*); or Q is a free group on a finite generating set S, in which case ϕ is specified as a map $S \times X \to X \times Q$. The action of the element (M, q) for $q \notin S$ is simply defined by composition: the formula

$$(1) \qquad \phi(q_1 q_2, x) = (z, q_1' q_2') \quad \text{if} \quad \phi(q_1, x) = (y, q_1') \text{ and } \phi(q_2, y) = (z, q_2')$$

reduces the computation of $\phi(q, x)$ for all $q \in Q, x \in X$ to that of $\phi(s, x)$ for all $s \in S, X \in X$.

The product and inverse (if it exists) of an element is again an element, on the same alphabet. If Q, Q' are the finite statesets of M, M' respectively, one may define the product MM' as a machine with stateset $Q \times Q'$, in such a way that the element $(M, q)(M', q')$ is $(MM', (q, q'))$, using essentially Equation (1). If Q, Q' are free groups, one may take $Q * Q'$ as stateset of MM', extending naturally $\phi : (Q \cup Q') \times X \to X \times (Q \cup Q')$ to a map $(Q * Q') \times X \to X \times (Q * Q')$; the initial state of $(M, q)(M', q')$ is now qq'.

A machine can conveniently be described as a graph. One draws one vertex for each $q \in Q$, and an arrow from q to q', labeled x/x', whenever $\phi(q, x) = (x', q')$.

2. Groups

Of particular interest are the groups generated by all the elements (M, q), where q ranges over the stateset of a given machine M. This group is denoted $G(M)$, and is *state-closed*: the state of an element, after it has read any number of symbols from X, is again an element of $G(M)$. What amounts to the same thing, there is an injective map $G(M) \to G(M)^X \rtimes \mathrm{Sym}(X)$.

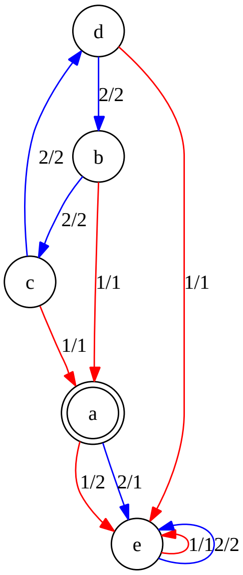
It is a common feature of almost all results on groups generated by finite automata that they involve many calculations of a finite nature. In particular, one would like to: check equality of elements of $G(M)$ given as products of generators (the "word problem"); compute the action of such elements on strings, both finite or infinite-periodic; compute small (e.g. nilpotent) quotients of $G(M)$; etc. Some of these methods have been implemented in Fr, and others will appear soon.

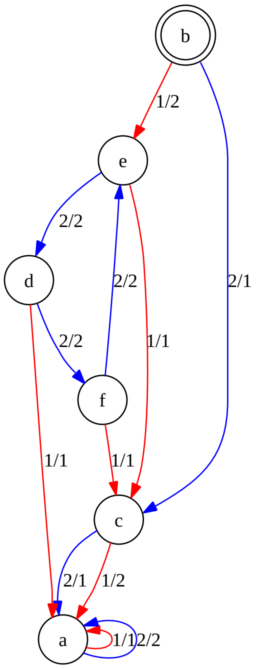
3. A sample run

Below is a sample session of Gap, showing some of the most basic commands of Fr. A machine is entered by listing the second coördinate of ϕ, using $Q = \{1, 2, 3, 4, 5\}$, and the first coördinate, given as the induced permutations of $X = \{1, 2\}$.

After defining the machine m and group g, the following code computes the orders of some elements, their action on sequences, displays (in separate windows) the elements g_1 and $g_1 g_2$, and computes as a permutation group the quotient q of g acting on sequences of length 6. It then computes the Jennings Lie algebra, leading to the observation (proved in [1]) that the ranks are alternatively 1 and 2.

```
gap> m := MealyMachine([[5,5],[1,3],[1,4],[5,2],[5,5]],
                       [(1,2),(),(),(),()]);
<Mealy machine on alphabet [ 1 .. 2 ] with 5 states>
gap> g := SCGroup(m);
<self-similar group over [ 1 .. 2 ] with 5 generators>
gap> Order(g.1);
2
gap> Order(g.1*g.2);
16
gap> [1,1]^g.1;
[ 2, 1 ]
gap> [1,1,[2]]^g.1;
[ 2, 1, [ 2 ] ]
gap> [1,[1,2]]^g.1;
[ [ 2, 1 ] ]
gap> [1,1,[2]]^g.2;
[ 1, [ 2 ] ]
gap> Draw(g.1);
gap> Draw(g.1*g.2);
gap> q := PermGroup(g,6);
<permutation group with 5 generators>
gap> LogInt(Size(q),2);
42
gap> j := JenningsLieAlgebra(q);
<Lie algebra of dimension 42 over GF(2)>
gap> List([1..20],i->Dimension(Grading(j).hom_components(i)));
[ 3, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 1, 1, 1 ]
```





4. Open questions

As of now, we know only very few algorithms that handle groups generated by automata. Some subclasses of these groups may well be more amenable to computation; for example, those that are "contracting", i.e. such that all the projections $G(M) \to G(M)^X \rtimes \mathrm{Sym}(X) \to G(M)$ are contracting for the word metric on $G(M)$. It is known that for these the word problem is solvable in polynomial (essentially linear) time; in some cases the conjugacy problem is also solvable; is some cases a recursive presentation can be computed, etc.

To the best of my knowledge, no algorithm is known that computes the order (in $\mathbb{N} \cup \{\infty\}$) of a Mealy element. This is striking: if an element has finite order, then this order can be determined using the solution to the word problem. Therefore, if no algorithm existed to determine the order of an element, this would mean that the function ($n \mapsto$ largest finite order of a Mealy element with $\#Q = n$) is not a recursive function — a highly unlikely event.

References

[1] L. Bartholdi and R. I. Grigorchuk. Lie methods in growth of groups and groups of finite width. In *Computational and geometric aspects of modern algebra (Edinburgh, 1998)*, 1–27, Cambridge Univ. Press, Cambridge, 2000.

[2] L. Bartholdi, R. I. Grigorchuk and V. V. Nekrashevych. From fractal groups to fractal sets. In *Fractals in Graz 2001*, 25–118, Birkhäuser, Basel, 2003.

[3] L. Bartholdi, R. I. Grigorchuk and Z. Šunik. Branch groups. In *Handbook of algebra, Vol. 3*, 989–1112, North-Holland, Amsterdam, 2003 .

[4] R. I. Grigorchuk, V. V. Nekrashevich and V. I. Sushchanskiĭ. Automata, dynamical sysytems, and groups. Tr. Mat. Inst. Steklova **231** (2000), Din. Sist., Avtom. i Beskon. Gruppy, 134–214; translation in Proc. Steklov Inst. Math. **2000**, no. 4 (231), 128–203.

[5] V. Nekrashevych. *Self-similar groups.* Amer. Math. Soc., Providence, RI, 2005.

Computing nonsolvable quotients of finitely presented groups

Alexander Hulpke

(joint work with Alice Niemeyer)

A principal tool for the study of finitely presented groups has been algorithms for computing quotient groups of a "better behaving" class, in which efficient computations are feasible.

For example one can find (and represent) subgroups of G as full preimages of subgroups in a homomorphic image. Intersection of subgroups can be treated in the same way. Words which represent different elements in the quotient clearly must represent different elements of G.

The easiest case of these is the computation of the structure of G/G' by calculating the Smith Normal form. More sophisticated algorithms have been developed over the last three decades:

(1) The *Low Index* algorithm which finds subgroups of bounded index in G (and thus homomorphisms from G into permutation groups of small degree). Its runtime is exponential in the index and thus it it only feasible for small indices, thus the name.

(2) The *p-quotient* algorithm which finds epimorphisms from G onto groups of prime-power order.

(3) The *nilpotent quotient* algorithm by Nickel, which finds epimorphisms onto (infinite) nilpotent groups.

(4) A *solvable quotient* algorithm (SQ), finding epimorphisms onto finite solvable groups, has been developed in two flavors:
   (a) Following a suggestion of Leedham-Green, Niemeyer uses consistency conditions for pc-presentations to obtain a module presentation for the next layer. These are evaluated using vector enumeration.
   (b) Plesken suggests to first enumerate all irreducible modules for the factor group (which for solvable groups can be done in an inductive process), then to calculate the 2-cohomology for each module, and finally to test whether an extension with the module can become a

quotient. This work has been extended by Brückner which introduces a criterion which can be used to determine the relevant primes.

(5) Lo described a *Polycyclic quotient* algorithm which find epimorphisms onto (infinite) polycyclic groups.

Apart from the low-index algorithm, all of these algorithms find only solvable or polycyclic quotients. In particular they will never expose nonsolvable parts of a group.

Given the rather limited "tool chest" available for investigating finitely presented groups, any extension of these algorithms will be a welcome tool for researchers investigating finitely presented groups.

In recent work I have been able to start generalizing the idea of solvable quotient algorithms to nonsolvable groups.

The basic assumption here is that a quotient $\varphi\colon G \to H$ onto a finite group H is assumed to be known. (The low index algorithm is a typical source of such a quotient.)

One now wants to find a group extension $N.H$ of an H-module N by H such that there is an epimorphism $\lambda\colon G \to N.H$ such that $\varphi = \lambda \cdot \nu$ factors through the natural homomorphism $\nu\colon N.h \to H$. We call such an epimorphism λ a *lift* of φ and N the *lift kernel* of λ.

Iteration of this process will produce solvable-by-finite quotients (which are the largest class of groups for which algorithms are feasible).

A naive way to find such an N would be to rewrite the presentation for G to its normal subgroup $\ker\varphi$. Such a rewritten presentation however becomes more complicated with the index $[G : \ker\varphi]$ thus this approach is not really practical. The argument shows however the feasibility in principle.

So far the approach has been twofold. The use of induced representations gives a criterion to test whether a lift with a given H-module N can occur. This criterion might be used to generalize the Plesken variant of the SQ. A main difficulty to this however would be the enumeration of all irreducible H-modules.

Nevertheless this method has been used successfully to answer a question by Pasechnik whether a particular epimorphism onto the sporadic group McL (of order about $8 \cdot 10^6$) has lifts for modules in characteristic 3. This problem had been unsolved with prior methods.

More recently, in collaboration with A. Niemeyer, we tried to develop a generalization of the Leedham-Green/Niemeyer solvable quotient algorithm. The idea of this work is to replace a pc-presentation for the factor group H by a confluent rewriting system. To go from the factor group H to an extension $N.H$ one then modifies each rewriting rule by adding one formal generator as element of N. Finally one can use confluence conditions and the relations for G to obtain a module presentation for the lift kernel N.

Using vector enumeration a concrete representation for this module N (a basis and matrices for the action of H on this basis) is computed. The confluence conditions used to obtain the module construction then describe the cofactors of the extension.

We call this algorithm a "hybrid quotient algorithm" (HQ). We have a prototype implementation in GAP.

The output of the solvable quotient algorithms etc. is a pc-presentation for the quotient group. While such presentations have been studied before the availability of groups given by such presentations as the result of quotient algorithms has strongly motivated the further development of algorithms for solvable groups in which such a pc-presentation is used for arithmetic. This led from the late 1970s on to much further development of computational group theory.

Once the HQ algorithm is available, similar arithmetic for the image groups becomes desirable.

For this we note that the image obtained by the hybrid quotient algorithm is an extension of an elementary abelian group by a group given with a confluent rewriting system. By combining the elementary abelian layers obtained in several steps of the algorithm, we get a structure of a larger solvable normal subgroup N extended by a finite group G which is given by a confluent rewriting system.

It thus becomes possible to represent N by a polycyclic presentation and to add "tails" to the rewriting system for G to describe the extension structure.

Regularity in group cohomology: the groups of order 128

David J. Green

My work concerns the cohomology of finite groups. Specifically I am interested in the commutative algebra of the mod-p cohomology ring and the computer calculation of such rings. Especially for p-groups.

Following Carlson's approach [3, 2] I devised efficient noncommutative Gröbner basis methods for constructing the minimal resolution [5], and created a program for cohomology calculation based on these methods. For the later stages of the program I also needed to work out Gröbner bases for graded commutative algebras.

Cohomology rings are finitely presented, but there are no useable degree bounds on the presentation. Instead one uses a test for completion. Carlson's test [2] was the original one, but Benson's new test [1] is better for theoretical and practical reasons.

Cohomology computations to date have

- Yielded the counterexample that refuted the so-called essential conjecture [5, 7].
- Led to the proofs of two conjectures [6, 8] (confidence building!)
- Provided a large sample set for testing ideas against (e.g. Carlson's calculations [4] for the groups of order 64).

Currently I am working on a second version of the cohomology program. The methods for working with presentations of graded commutative rings need a radical overhaul. The current computational goals are:

- The cohomology rings of the 2328 groups of order 128.

- Testing Benson's regularity conjecture [1].

Castelnuovo-Mumford regularity is a numerical commutative algebra invariant. Benson conjectures it always takes the value zero for a cohomology ring. He proves this happens if the "Cohen-Macaulay deficiency" is at most two: this deficiency is defined to be the Krull dimension minus the depth. Until recently there were no calculations in higher C-M deficiency.

Theorems of Quillen and Duflot provide an upper bound for the C-M deficiency: this bound is the "group-theoretic deficiency", which I define to be the difference between the p-rank of the group and that of its centre. The Small Groups library and Carlson's calculations show that the groups of order 128 are the first place to look for groups with higher C-M deficiency.

To date I have checked the conjecture for five[1] groups with C-M deficiency three, and identified another seven such groups. I have also identified a group of order 256 with C-M deficiency four.

One current issue is constructing a system of parameters which is filter-regular, meaning that only in low degrees does it fail to be a regular sequence. For an efficient calculation this system needs to lie in low degrees itself, and be defined over the prime field. Experience from constructing such systems by hand suggests an approach using lowest degree Dickson invariants for a flag of elementary abelian subgroups, but this method lacks theoretical justification at present.

References

[1] D. Benson, *Dickson invariants, regularity and computation in group cohomology*, Illinois J. Math. **48** (2004), 171–197.

[2] J. F. Carlson, *Calculating group cohomology: Tests for completion*, J. Symbolic Comput. **31** (2001), 229–242.

[3] J. F. Carlson, E. L. Green, and G. J. A. Schneider, *Computing Ext algebras for finite groups*, J. Symbolic Comput. **24** (1997), 317–325.

[4] J. F. Carlson, L. Townsley, L. Valeri-Elizondo, and M. Zhang, *Cohomology Rings of Finite Groups*, Kluwer Academic Publishers, Dordrecht, 2003.

[5] D. J. Green, *Gröbner Bases and the Computation of Group Cohomology*, Lecture Notes in Mathematics **1828**, Springer-Verlag, Berlin, 2003.

[6] D. J. Green, *On Carlson's depth conjecture in group cohomology*, Math. Z. **244** (2003), 711–723.

[7] D. J. Green, *The essential ideal in group cohomology does not square to zero*, J. Pure Appl. Algebra **193** (2004), 129–139.

[8] D. J. Green, *The essential ideal is a Cohen–Macaulay module*, Proc. Amer. Math. Soc. **133** (2005), 3191–3197.

[1] At the time of the meeting it was only four.

Comparison of spectral sequences

Matthias Künzer

To calculate $\mathrm{Ext}^k(X, Y)$, one can either resolve X projectively or Y injectively, the result is the same. Similar phenomena are observed in the context of Grothendieck spectral sequences.

By a proper spectral sequence we understand a spectral sequence with E_1-terms excluded. Suppose given left exact functors $\mathcal{A} \xrightarrow{F} \mathcal{B} \xrightarrow{G} \mathcal{C}$ between abelian categories and given $X \in \mathrm{Ob}\,\mathcal{A}$, and suppose further conditions to hold. Let A be an F-acyclic resolution of X, and let J be a Cartan-Eilenberg resolution of FA, which is a double complex injectively resolving simultaneously the entries and the homology objects of FA. Recall that by definition, the proper Grothendieck spectral sequence $\dot{\mathrm{E}}^{\mathrm{Gr}}_{F,G}(X)$ is the proper first spectral sequence associated to the double complex GJ, written $\dot{\mathrm{E}}_{\mathrm{I}}(GJ)$.

1) Suppose given functors $\mathcal{A} \times \mathcal{A}' \xrightarrow{F} \mathcal{B} \xrightarrow{G} \mathcal{C}$ and objects $X \in \mathrm{Ob}\,\mathcal{A}$ and $X' \in \mathrm{Ob}\,\mathcal{A}'$ such that $\mathcal{A}$, $\mathcal{A}'$, $\mathcal{B}$, $\mathcal{C}$ are abelian, $F(X,-)$, $F(-,X')$, G are left exact, and such that further conditions hold. We obtain an isomorphism of proper Grothendieck spectral sequences $\dot{\mathrm{E}}^{\mathrm{Gr}}_{F(X,-),G}(X') \simeq \dot{\mathrm{E}}^{\mathrm{Gr}}_{F(-,X'),G}(X)$. So instead of "resolving X' twice", we may "resolve X twice".

2) Suppose given functors $\mathcal{A} \xrightarrow{F} \mathcal{B}'$ and $\mathcal{B} \times \mathcal{B}' \xrightarrow{G} \mathcal{C}$, and objects $X \in \mathrm{Ob}\,\mathcal{A}$ and $Y \in \mathrm{Ob}\,\mathcal{B}$ such that $\mathcal{A}$, $\mathcal{B}$, $\mathcal{B}'$, $\mathcal{C}$ are abelian, F, $G(Y,-)$ are left exact, and such that further conditions hold. Let B be an injective resolution of Y, and let A be a "sufficiently acyclic" resolution of X. Then $\dot{\mathrm{E}}^{\mathrm{Gr}}_{F,G(Y,-)}(X) \simeq \dot{\mathrm{E}}_{\mathrm{I}}\big(G(B, FA)\big)$. So instead of "resolving X twice", we may "resolve X once and Y once".

In both cases, it is a priori clear that the E_2-terms conincide. The differentials, however, are another story. So we do not proceed by induction on the pages, but rather by comparison of the defining double complexes.

Barnes [1, X.5] works in a somewhat different general setup.

Applications: reproving Beyl's Theorem [2, Th. 3.5] on the Lyndon-Hochschild-Serre spectral sequence, which has also been reproven by Barnes [1]; comparison of change-of-rings spectral sequences.

References

[1] D. W. Barnes, *Spectral sequence constructors in algebra and topology*, Mem. Am. Math. Soc. **317** (1985).

[2] F. R. Beyl, *The spectral sequence of a group extension*, Bull. Sc. Math. (2), **105** (1981), 417–434.

[3] M. Künzer, *Comparison of spectral sequences involving bifunctors*, in preparation.

Permutations having order a multiple of the degree

Cheryl E. Praeger
(joint work with Steve Linton, Alice C. Niemeyer and Sven Reichard)

This research was motivated by the following algorithmic situation and problem.

Algorithmic Situation: We are given generators for a subgroup G of permutations of a set X of size $N = \binom{n}{k}$, with k bounded and n very large. Further we are given that G is isomorphic to S_n and the action is equivalent to the action of S_n on k-sets, but we do not know a permutational isomorphism. In fact n is so large that we are not willing to compute the complete cycle structure of a product g of several generating permutations. We are however willing to "trace out" several random points of X under g, and thereby find the cycles under g of these random points, and in particular the lengths of those cycles.

The subset actions of symmetric groups form a class of large base primitive permutation actions for which randomised recognition algorithms exist that run in nearly linear time, see [1]. Our aim was to explore whether more general algorithms might be possible that use only image computations (of points under permutations) rather than multiplying togther permutations. In this context the point set is very large, and we hope that our ideas may have application in large scale practical search algorithms where it is precisely fast algorithms for large-base permutation groups that are needed. One of the critical parts of constructing the natural representation on n points of the group G in the Algorithmic Situation is the construction of an n-cycle.

Algorithmic Problem: Find an element of the group G above that is an n-cycle in the natural action of G on n points.

If $g \in G$ and g is an n-cycle in the natural action of G on n points, then it turns out, not surprisingly, that most g-cycles in X have length n (see [2]), so with high probability a random point of X will lie in a g-cycle of length n in X. Even though we may 'trace out' relatively few g-cycles in X in the Algorithmic Situation, it is therefore reasonably likely that we would find one of length n, and hence we would know from this computation that $|g|$ is divisible by n. Computer experiments for small n suggested that, when a random element $g \in S_n$ has a cycle of length n in its action on k-sets, then the conditional probability that g is an n-cycle might be reasonably high.

In order to pursue this experimental observation in a rigorous theoretical setting, we decided to analyse the family $\mathcal{F}$ of elements of S_n that have order a multiple of n. In two quite different situations there are sub-families of $\mathcal{F}$ of size comparable with (sometimes larger than) the sub-family consisting of n-cycles. Our analysis needed to encompass these situations. Eventually we decided on a subdivision of $\mathcal{F}$ into six of sub-families depending on the natural action of the elements $g \in \mathcal{F}$ on n points: namely whether or not the subset $\Delta(g)$ of $\{1, \ldots, n\}$ of points lying in g-cycles with lengths dividing n was 'very large', which for the purposes of this exposition we will take to mean $|\Delta(g)| > n^{30/32}$, and whether the number of 'large' g-cycles of length dividing n was 0, 1, 2, or at least 3. Again, for the purposes of this exposition, by a 'large' g-cycle we mean a cycle of length at least $n^{23/32}$. We discovered that four of these six sub-families had negligible size compared with the other two, but that, depending on the multiplicative properties of n, it was possible for either one or both of the remaining two sub-families to dominate. We define the two important sub-families $\mathcal{F}_1$ and $\mathcal{F}_2$ as follows.

The sub-family $\mathcal{F}_1$ consists of all $g \in \mathcal{F}$ such that g has exactly one large cycle $C \subseteq \Delta(g)$, $|\Delta(g)| > n^{30/32}$, and $|\Delta(g) \setminus C| < n^{27/32}$ (so C is very large). We note that $\mathcal{F}_1$ contains all the n-cycles, so $\frac{|\mathcal{F}_1|}{n!} \geq \frac{1}{n}$. If $n = p$ or $2p$ (where p is prime) then $\mathcal{F} = \mathcal{F}_1$, while if $n = pq$ where p, q are consecutive primes, then $\mathcal{F}_1$ consists only the n-cycles, and $\mathcal{F} \setminus \mathcal{F}_1$ is of comparable size.

The sub-family $\mathcal{F}_2$ consists of all $g \in \mathcal{F}$ such that $|\Delta(g)| \leq n^{30/32}$. Here, if $n = p$ or $2p$ (where p is prime) then $\mathcal{F}_2 = \emptyset$, while if $n = pq$ where p, q are consecutive primes, then $\mathcal{F}_2$ contains all g with one p-cycle and one q-cycle and has size roughly equal to that of $\mathcal{F}_1$, namely $\frac{|\mathcal{F}_2|}{n!} \geq \frac{1}{n} - \frac{4}{n^{3/2}}$, see [3].

From a detailed study of the generating functions for $\mathcal{F}$ and various of its sub-families, we were able to prove that $\mathcal{F} \setminus (\mathcal{F}_1 \cup \mathcal{F}_2)$ is asymptotically smaller than $\mathcal{F}_1 \cup \mathcal{F}_2$. The definitions of the other sub-families and their sizes are given in the following table.

$\mathcal{F}$ – subfamily	$\lvert\Delta(g)\rvert$	# large cycles C in $\Delta(g)$	size/$n!$
$\mathcal{F}_1$	$> n^{30/32}$	1 and $\lvert\Delta(g) \setminus C\rvert < n^{27/32}$	
$\mathcal{F}_2$	$\leq n^{30/32}$	any number	
$\mathcal{S}_0$	$> n^{30/32}$	0	$O(1/n^{40/32})$
$\mathcal{S}_1$	$> n^{30/32}$	1 and $\lvert\Delta(g) \setminus C\rvert \geq n^{27/32}$	$O(1/n^{33/32})$
$\mathcal{S}_2$	$> n^{30/32}$	2	$O(1/n^{33/32})$
$\mathcal{S}_3$	$> n^{30/32}$	≥ 3	$O(1/n^{54/32})$

Thus $\frac{|\cup_i \mathcal{S}_i|}{n!} = \frac{|\mathcal{F} \setminus (\mathcal{F}_1 \cup \mathcal{F}_2)|}{n!} = O\left(\frac{1}{n^{33/32}}\right)$, and:

Theorem 2. [3] *For a random $g \in S_n$*

$$Prob(g \in \mathcal{F}_1 \cup \mathcal{F}_2 \mid n \text{ divides } |g|) = 1 - O\left(\frac{1}{n^{1/32}}\right).$$

Building on the insights gained from our analysis of the family $\mathcal{F}$, we were able to prove the following probabilistic result for the algorithmic application.

Theorem 3. [2] *For a random $g \in S_n$*

$$\mathit{Prob}\,(g \text{ is an } n\text{-cycle} \mid \text{four random } k\text{-sets lie in } g\text{-cycles of length } n)$$

is $1 - O\left(\frac{1}{n^{1/6}}\right)$.

References

[1] Maska Law, Alice C. Niemeyer, Cheryl E. Praeger and Ákos Seress, A reduction algorithm for large-base primitive permutation groups, *LMS Journal of Computational Math.* **9** (2006), 159–173.

[2] Steve Linton, Alice C. Niemeyer, Cheryl E. Praeger and Sven Reichard, Finding n-cycles in the symmetric group of degree n acting on subsets, in preparation.

[3] Alice C. Niemeyer and Cheryl E. Praeger, On the proportion of permutations of order a multiple of the degree, preprint.

Recognising k-set actions of symmetric groups

Alice C. Niemeyer
(joint work with Cheryl E. Praeger, Steve Linton)

Large base primitive permutation groups are subgroups of wreath products $H \wr S_\ell$ in product action, where H is a symmetric group acting on subsets. They can be recognised by randomised algorithms that run in nearly linear time, see [3]. Here we explore the special case of symmetric groups acting on subsets, given not necessarily as a permutation group.

Algorithmic Situation: We are given generators for a G isomorphic to a subgroup of the group of all permutations of a set X of size $N = \binom{n}{k}$, with $k \leq n/2$ and N very large. Further we are given that G is isomorphic to S_n and the action is equivalent to the action of S_n on k-sets, but we do not know a permutational isomorphism. In fact N is so large that we are not willing to compute the complete cycle structure of a product g of several generating elements. We are however willing to "trace out" several random points of X under g, that is, to find the cycles under g of several random points of X. To distinguish the action of G on X from the action of S_n on $\{1, \ldots, n\}$, we call the elements of X *points* and the elements of $\{1, \ldots, n\}$ *letters.*

In [5] we addressed the problem of finding efficiently an element of G that is an n-cycle in the natural permutation representation of G on n letters. The theoretical solution has led to a fast algorithm to solve the following algorithmic problem, which we address in this report.

Algorithmic Problem: Design a Las Vegas algorithm to construct a permutational isomorphism between G acting on X and S_n in its natural permutation representation on n letters at a cost of $o(N)$ (sub-linear in N) computations of the image of a point in X under an element in G and $O(n)$ random elements in G.

Solution to Algorithmic Problem: Our algorithm has the following components.

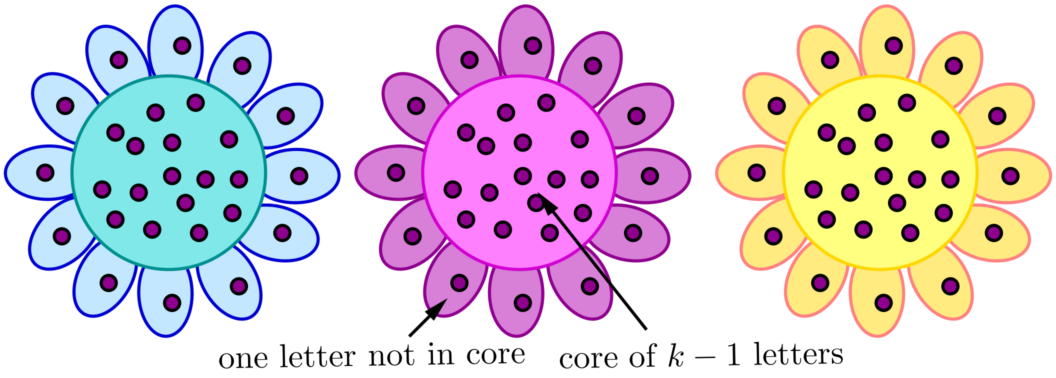
1. Algorithm **FindSystem** takes as input a set of group generators S for G acting on X and returns as output elements g and h in G and a k-set Π such that
   - g corresponds to the n-cycle $(1\,2\ldots n)$ and h to the transposition $(1\,2)$ in the natural action.
   - Π contains exactly one of 1 and 2.
2. Algorithm **BuildBouqet** takes as input the elements g and h found in (1) and computes a data-structure called a *bouquet* described below.
3. Algorithm **ImageTransposition** takes as input the elements g and h found in (1), the bouquet computed in (2), and a group element t, where t corresponds to a transposition $(a\,b)$ in the natural action. Then **ImageTransposition** returns a and b.
4. Algorithm **ImagePermutation** takes as input the elements g and h found in (1), the bouquet computed in (2) and a group element x. It returns the permutation in S_n corresponding to x in its natural action.

The algorithm **FindSystem** was inspired by the approach in [1] for the recognition of S_n as a black-box group. The strategy we employ to find group elements g and h in (1) is similar to the one employed in [1], yet the underlying theory is very different. As mentioned in [5], we aim to find an element of g which is an n-cycle in the natural action, by testing whether a small number of points in X have an orbit of length n under g. As the proportion of n-cycles in S_n is $1/n$ we proved in [4] that the the conditional probability that an element g is an n-cycle given that a small number of points in X have an orbit of length n under g is at least $1 - O(\frac{1}{n^6})$.

If **FindSystem** succeeds, we can define a map $\varphi : \langle g, h\rangle \rightarrow S_n$ via $g^\varphi = (1\,2\ldots n)$ and $h^\varphi = (1\,2)$. We need an algorithm which computes f^φ for any $f \in G$.

A collection $\mathcal{D}$ of $n-k+1$ points is called a *flower*, if, when viewed as k-sets of letters in $\{1, \ldots, n\}$ the letters in any $\mathcal{D}$ overlap pairwise in the same set of $k-1$ letters $\Gamma(\mathcal{D})$, called the *core* of $\mathcal{D}$.

A collection $D = \{\mathcal{D}_1, \ldots, \mathcal{D}_t\}$ of flowers is called a *bouquet* if for any two letters a and b, there is an $i \in \{1, \ldots, t\}$ such that neither a, nor b lies in $\Gamma(\mathcal{D}_i)$. We illustrate a bouquet in the following picture.



Algorithm **BuildBouquet** computes a bouquet and for every flower $\mathcal{D}$ in the bouquet it identifies all letters not in the core.

Algorithm **ImageTransposition** uses the flowers we have defined to find the natural action of a transposition as follows. Suppose $t = (a\,b)$ is a transposition and Π a set which contains exactly one of a and b. Then we can find a flower $\mathcal{D}$ in our bouquet whose core does not contain a and b. Then there are exactly two k-sets Δ in $\mathcal{D}$ for which $\Delta t \neq \Delta$. We identify $\{a, b\}$ as the letters in each of these two sets not in the core.

Algorithm **ImagePermutation** recovers the natural action of x from the natural actions of t_i^x, where t_i in its natural action corresponds to the transposition $(i\ i{+}1)$ for $1 \leq i \leq n-1$. Note that the natural actions of t_i^x can be determined by algorithm **ImageTransposition**.

Given a group G as described in the algorithmic situation, the above rough outline can be turned into a Las Vegas algorithm such that for a given error probability ε the cost of the algorithm is $O(\log(\varepsilon^{-1})n^3R)$ computations of images of points in X under elements of G, where R is an upper bound for the length of a random element as word in the generators of G. The algorithm has been implemented in GAP [2].

References

[1] Robert M. Beals, Charles R. Leedham-Green, Alice C. Niemeyer, Cheryl E. Praeger, and Ákos Seress. A black-box algorithm for recognizing finite symmetric and alternating groups, I. *Trans. Amer. Math. Soc.*, **355** (2003), 2097–2113.

[2] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2006, (`http://www.gap-system.org`).

[3] Maska Law, Alice C. Niemeyer, Cheryl E. Praeger and Ákos Seress, A reduction algorithm for large-base primitive permutation groups, *LMS Journal of Computational Math.*, **9**, 159–173, 2006.

[4] Steve Linton, Alice C. Niemeyer, Cheryl E. Praeger and Sven Reichard, Finding n-cycles in the symmetric group of degree n acting on subsets. *preprint.*

[5] Cheryl E. Praeger. Permutations of order a multiple of the degree. *Oberwolfach*, (to appear) (2006).

Enumeration of big orbits

Jürgen Müller

(joint work with Max Neunhöffer and Rob Wilson)

1. Introduction.

In recent years there has been increasing interest in dealing with 'large' permutation representations, in particular of the 'large' sporadic finite simple groups. Actually, the first steps in this direction have been taken as early as 1980, for the Baby Monster group [16]. Since then all sporadic groups have been under intense computational study, in particular to find revised existence and uniqueness proofs, e.g. [5, 6], as well as in the framework of the 'Modular Atlas project' [8, 18], aiming at the determination of the decomposition numbers of the 'Atlas' [3] groups, e.g. [4, 13, 15].

We present a novel technique to handle 'big' permutation domains for 'large' groups. It is based on the idea of using 'small' helper subgroups, which ultimately goes back to unpublished work of R. Parker from 1995. The latter has taken place in the context of 'condensation' techniques, which originally have been invented for the explicit computation of decomposition numbers [17], but now have found different applications as well [11]. The basic idea has independently been made explicit in [9], where a parallelised version of the 'direct condensation' technique has been developed. Based on practical experience [11], we have been led to elaborate on this idea by using a whole chain of helper subgroups instead of a single helper subgroup [14].

2. Enumerating orbits.

Given a finite group G acting on a finite set X and $x_1 \in X$, the aim is to enumerate the G-orbit $x_1G \subseteq X$. This can be achieved efficiently with the well-known Schreier-Sims orbit-stabiliser algorithm, which not only determines x_1G but also finds the stabiliser $\mathrm{Stab}_G(x_1) \leq G$ of x_1 in G. However, to do this in practice all points in x_1G have to be kept in memory at the same time, to be able to recognise whether a point in the orbit has already been found or not; this can of course be done using hashing techniques, such that only a nearly constant amount of time is needed to look up a point, regardless of how many points have already been found.

But if x_1G is 'too large' to be stored completely, this methods fails. We are going to remedy this, allowing to enumerate G-orbits being much 'too large' in this sense, at the expense that we have to assume the group order $|G|$ and some additional structural information about G to be known in advance: The basic idea is not to store single points in x_1G, but to archive the x_1G-orbit in bigger chunks. To this end, we use a 'helper' subgroup $U < G$, and enumerate the set of U-orbits contained in x_1G. We store appropriate pieces xU, such that we are able to decide whether or not a given point $x \in X$ is in one of the U-orbits already stored. This is achieved as follows:

Let Y be finite 'small' helper U-set and let $\overline{}\colon X \to Y$ be a homomorphism of U-sets. We first enumerate Y completely, then in every U-orbit in Y we pick a 'U-minimal' point arbitrarily. For each such U-minimal point y we store generators for $\mathrm{Stab}_U(y)$, while for the remaining points $y \in Y$ we store an element $u_y \in U$ such that $yu_y \in Y$ is U-minimal. Now, given a U-orbit $xU \subseteq X$, we only store its U-minimal points, where a point $x \in X$ is called U-minimal, if $\overline{x} \in Y$ is U-minimal. Hence the U-minimal points in xU are precisely given as $x\mathrm{Stab}_U(\overline{x})$, where generators for $\mathrm{Stab}_U(\overline{x})$ have been stored before. Given any $x \in X$, we find a U-minimal point in xU by applying the group element $u_{\overline{x}} \in U$ also stored before.

Note that to archive U-orbits as just described we have to assume that U and Y are 'small enough' to enumerate Y completely. For 'large' groups G this tends to imply that U is 'too small' to be helpful. Hence instead of using a single helper subgroup we use a chain $U_1 < U_2 < \cdots < U_k < U_{k+1} := G$ of helper subgroups, together with U_i-sets X_i and homomorphisms $\pi_i\colon X_{i+1} \to X_i$ of U_i-sets, for $1 \leq i \leq k$, where we let $X_{k+1} := X$. Thus we enumerate $x_1G \subseteq X$ by U_k-orbits, while iterating the above technique the U_i-orbits in X_i, for $k \geq i \geq 2$, in turn are enumerated by U_{i-1}-orbits.

3. Applications.

The above technique has been implemented in GAP [7]. The implementation of the various orbit enumeration algorithms and hashing techniques, and of some heuristics to find appropriate helper subgroups U_i and helper U_i-sets, needs some 3000 lines of code, and will be published, including explicit input data for several examples, in the GAP package ORB [12].

We have compiled a database [2] of character tables of endomorphism rings of multiplicity-free permutation modules of the sporadic simple groups and their cyclic and bicyclic extensions. In particular this data encodes information on spectral properties of the orbital graphs associated to these actions, such as distance-regularity and the Ramanujan property. The computations necessary [1, 11] involved heavy use of the above technique, and actually have been part of the original motivation for its development.

In particular, we have dealt with the two largest multiplicity-free actions of the sporadic simple Baby Monster group, namely with its action on the $\sim 10^{13}$ cosets of $2_+^{1+22}.Co_2$ [11], and on the $\sim 10^{15}$ cosets of Fi_{23} [14]. Moreover, for the action of the sporadic simple Conway group Co_1 on the reduction of its Leech lattice representation over $\mathbb{F}_5$, we have found all orbits in the associated projective space $\mathbb{P}(\mathbb{F}_5^{24})$, having $\sim 10^{16}$ elements, answering a question in [10].

References

[1] T. Breuer, J. Müller, A database of character tables of endomorphism rings of multiplicity-free permutation modules, Preprint, 2006.

[2] T. Breuer, J. Müller, Character tables of endomorphism rings of multiplicity-free permutation modules of the sporadic simple groups and their cyclic and bicyclic extensions, 2005, http://www.math.rwth-aachen.de/ ~Juergen.Mueller/mferctbl/mferctbl.html.

[3] J. Conway, R. Curtis, S. Norton, R. Parker, R. Wilson, Atlas of finite groups, Clarendon Press, 1985.

[4] G. Cooperman, G. Hiss, K. Lux, J. Müller, The Brauer tree of the principal 19-block of the sporadic simple Thompson group, Experiment. Math. 6 (4), 1997, 293–300.

[5] G. Cooperman, W. Lempken, G. Michler, M Weller, A new existence proof of Janko's simple group J_4, in: Computational methods for representations of groups and algebras, Essen, 1997, 161–175, Progr. Math. 173, Birkhäuser, 1999.

[6] H. Gollan, A new existence proof for *Ly*, the sporadic simple group of R. Lyons, Computational algebra and number theory, Milwaukee, 1996, J. Symbolic Comput. 31 (1-2), 2001, 203–209.

[7] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4, 2006, http://www.gap-system.org.

[8] C. Jansen, K. Lux, R. Parker, R. Wilson, An atlas of Brauer characters, Clarendon Press, 1995.

[9] F. Lübeck, M. Neunhöffer, Enumerating large orbits and direct condensation, Experiment. Math. 10, 2001, 197–205.

[10] G. Malle, Private communication.

[11] J. Müller, On endomorphism rings and character tables, Habilitationsschrift, RWTH Aachen, 2003.

[12] J. Müller, M. Neunhöffer, F. Noeske, GAP-4 package ORB, 2006,
http://www.math.rwth-aachen.de/ ~Max.Neunhoeffer/Computer/Software/Gap/orb.html.

[13] J. Müller, M. Neunhöffer, F. Röhr, R. Wilson, Completing the Brauer trees for the sporadic simple Lyons group, LMS J. Comput. Math. 5, 2002, 18–33.

[14] J. Müller, M. Neunhöffer, R. Wilson, Enumerating big orbits and an application: B acting on the cosets of Fi_{23}, in preparation.

[15] G. Hiss, M. Neunhöffer, F. Noeske, The 2-modular characters of the Fischer group Fi_{23}, to appear in J. Algebra.

[16] C. Sims, How to construct a baby monster, in: M. Collins (ed.), Finite simple groups II, Durham, 1978, 339–345, Academic Press, 1980.

[17] J. Thackray, Modular representations of some finite groups, Ph.D. Thesis, Univ. of Cambridge, 1981.

[18] R. Wilson (et al.), The Modular Atlas homepage,
http://www.math.rwth-aachen.de/homes/MOC/.

Maximal subgroups of finite groups: new developments

Colva M. Roney-Dougal
(joint work with John N. Bray, Derek Holt)

Work by Cannon and Holt [3] reduces the problem of computing the maximal subgroups of arbitrary finite permutation and matrix groups to that of computing the maximal subgroups of the almost simple groups.

For the sporadic groups, a database is used which stores algorithms to compute standard generators, along with words in the standard generators for the generators of each maximal subgroup, as provided by [11]. The same approach is currently used for the exceptional groups.

The alternating and classical groups have many low-degree permutation and matrix representations, so a more generic approach for constructing maximal subgroups has been developed by Holt and the author. Constructive recognition yields computable isomorphisms between the socle of the almost simple group G and the natural representation of the simple group S, reducing the problem to that of finding the maximal subgroups of the almost simple group in its natural representation.

For the alternating and symmetric groups we use the recognition algorithm of Bratus and Pak [2]. The intransitive and imprimitive maximal subgroups are then constructed in the natural representation. The database of primitive groups (complete up to degree 2499 [10]) has an entry, for each group, which stores whether that group is maximal in the alternating or the symmetric group. If the group is maximal in A_n then the number of A_n-conjugacy classes of such maximals is also stored. The computable isomorphism then maps each of these maximal subgroups back into the input group.

Holt and the author have developed a similar approach for the classical groups, using the recognition algorithms of Kantor and Seress [6]. An *AS-maximal* geometric subgroup of a classical group is the largest subgroup to preserve one of the geometries given in Aschbacher's theorem [1]. We have proved that one can write down representatives of the AS-maximal geometric subgroups of the linear, symplectic and unitary groups in dimension d over $\mathrm{GF}(q)$ in time $O(d^{3+\epsilon}\log^3 q)$ for any real $\epsilon > 0$ [5]. This is extremely close to best possible, as there are $O(d)$ groups, each of which is generated by explicit $d \times d$ matrices over $\mathrm{GF}(q)$. Similar algorithms for the orthogonal groups have now been implemented by Holt. The only remaining groups that could possibly be maximal subgroups of a classical group are almost simple modulo scalars: see the extended abstract by Holt for more details of our approach in this case.

When dealing with the alternating and symmetric groups, work by Liebeck, Praeger and Saxl [8] can be used to determine which of the possibly maximal groups are in fact maximal in S_n or A_n, given a list of the almost simple primitive groups of degree n. Our recent work has highlighted the absence of similar classifications in low dimensions for the classical groups. For dimension at least 13, Kleidman and Liebeck [7] have determined when a geometric AS-maximal group is in fact maximal, leaving open the case of the groups that are almost simple modulo scalars, but far less is known about dimension less than 13.

To remedy this defect, Bray, Holt and the author are currently classifying the maximal subgroups of the almost simple classical groups in dimension at most 12. We have finished dimensions $2, 3, 4, 5, 6$ and 7, and are currently working on dimensions 8 and 9. We are using Aschbacher's theorem [1], along with papers by Lübeck, Hiss and Malle [4, 9] as our starting point, and are deliberately redoing the maximality calculations from scratch, comparing with previous classifications only once we have finished our work. At this point, it appears that our results will reveal many errors in the previous best-known similar classification, which is in the PhD thesis of Peter Kleidman, and describes the maximal subgroups of the simple classical groups in dimension up to 11.

References

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

[2] S. Bratus and I. Pak, *Fast constructive recognition of a black box group isomorphic to S_n or A_n using Goldbach's conjecture*, J. Symbolic Comput. **29** (2000), no. 1, 33–57.

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

[4] G. Hiss and G. Malle. *Low dimensional representations of quasi-simple groups*, LMS J. Comput. Math., **4** (2001), 22–63.

[5] D.F. Holt and C.M. Roney-Dougal. *Constructing maximal subgroups of classical groups*, L.M.S. J. Comput. Math., **8** (2005), 46–79.

[6] W.M. Kantor and Á. Seress. *Black box classical groups*, Mem. Amer. Math. Soc., **149**, 2001.

[7] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups.* Cambridge University Press: Cambridge, 1990.

[8] M.W. Liebeck, C.E. Praeger, J. Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups*, J. Algebra, **111** (1987), 365–383.

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

[10] C.M. Roney-Dougal, *The primitive groups of degree less than 2500* J.Algebra, **292**, (2005), 154-183.

[11] R. Wilson, P. Walsh, J. Tripp, I. Suleiman, R. Parker, S. Norton, S. Nickerson, S. Linton, J. Bray and R. Abbott. *ATLAS of Finite Group Representations*, `<http://brauer.maths.qmul.ac.uk/Atlas/v3/>`

Computing maximal subgroups of finite groups

Derek Holt

(joint work with John N. Bray and Colva M. Roney-Dougal)

In [1], results of Kovács, Aschbacher and Scott dating from the mid 1980's are used to reduce the computation of the maximal subgroups of a general finite group G to the case when G is *almost simple*; that is, when the socle of G is a nonabelian simple group. For such a group, a suitable *Black box recognition algorithm* [4] can be used to define a computable isomorphism between the group as given and a standard copy of the group. It remains then to develop and implement methods to write down the maximal subgroups within the standard copies of the almost simple groups.

Smaller almost simple groups can be handled on an individual basis, using information in the ATLAS of finite simple groups. In [5], Kleidman and Liebeck have used a classification theorem of Aschbacher to give a very detailed description of the geometric-type maximal subgroups of the finite classical groups. In [3], the author and C.M. Roney-Dougal converted these descriptions into practical algorithms in the non-orthogonal cases.

Significant progress has been made by Liebeck, Seitz and others on finding a corresponding description of the maximal subgroups of the almost simple groups of exceptional Lie type, but most of these are sufficiently large that they are not an immediate concern from the viewpoint of practical computation, and the few smaller examples can be treated as sporadic.

Handling the non-geometric almost simple subgroups of the classical groups in low dimensions is more urgent, and this is currently being undertaken by the author, C.M. Roney-Dougal, and J.N. Bray. Complete lists of representations of quasisimple groups up to dimension 250 due to Hiss, Malle [2] and Lübeck [6] are available, but practical constructions of the groups on these lists are still required.

It is most useful to construct these representations in characteristic zero wherever possible; they can then be reduced over finite fields as required. Indeed, the availability of explicit representations in all characteristics of simple groups and their decorations has numerous applications both inside and outside of mathematics, and so it is highly desirable to construct databases of such representations and to make them available both directly on the web, and via computer algebra systems such as GAP and Magma. A facility of this type [7] has been under construction and continuous development for several years now. In particular, as part of the work for his PhD thesis, Simon Nickerson constructed most of the characteristic zero representations of the simple groups in the Hiss-Malle tables.

The various methods that have been used to construct such representations were summarized in the talk. To achieve minimal degree, the representations should be defined over suitable algebraic extensions of the rationals. A problem with this is that the rational coefficients occurring in the entries in the matrices often turn out to be unpleasantly large, and no suitable methods are currently known for reducing their size. An alternative is to construct representations over the integers, and then to use the LLL algorithm to reduce the size of the entries. This works well, but has the disadvantage that the degree of the representation will often be significantly larger than that of the corresponding absolutely irreducible representation.

As a final point, the observant reader may have noticed that the tables of Hiss, Malle and Lübeck list representations of quasisimple groups, whereas we are trying to construct the maximal subgroups of almost simple groups. Our strategy is to construct the characteristic zero representation of the appropriate quasisimple group, to reduce it over the required finite field, and then to extend it by any group automorphisms involved by calculating the associated module isomorphisms.

References

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

[2] G. Hiss and G. Malle. *Low dimensional representations of quasi-simple groups*, LMS J. Comput. Math., **4** (2001), 22–63.

[3] D.F. Holt and C.M. Roney-Dougal. *Constructing maximal subgroups of classical groups*, L.M.S. electronic journal of computation and mathematics **8** (2005), 46–79.

[4] W,M. Kantor and A. Seress. *Black box classical groups*, Mem. Amer. Math. Soc., **149**, 2001.

[5] P. Kleidman, M. Liebeck. *The subgroup structure of the finite classical groups.* 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.

[7] R. Wilson, P. Walsh, J. Tripp, I. Suleiman, R. Parker, S. Norton, S. Nickerson, S. Linton, J. Bray, and R. Abbott. *ATLAS of Finite Group Representations*, <http://brauer.maths.qmul.ac.uk/Atlas/v3/>

Integral group ring of the first Mathieu simple group

Alexander Konovalov

(joint work with Victor Bovdi)

Let $V(\mathbb{Z}G)$ be the normalized unit group of the integral group ring $\mathbb{Z}G$ of a finite group G. The following famous conjecture was formulated in [10] by H. Zassenhaus:

(ZC) Every torsion unit $u \in V(\mathbb{Z}G)$ is conjugate within the rational group algebra $\mathbb{Q}G$ to an element of G.

This conjecture is already confirmed for several classes of groups but, in general, the problem remains open, and a counterexample is not known.

Various methods have been developed to deal with this conjecture. One of the original ones was suggested by I.S. Luthar and I.B.S. Passi [8, 9], and it was improved further by M.Hertweck [5]. Using this method, the conjecture was proved for several new classes of groups, in particular for S_5 and for some finite simple groups (see [2, 5, 6, 8, 9]).

The Zassenhaus conjecture appeared to be very hard, and several weakened variations of it were formulated (see, for example, [1]). One of the most interesting modifications was suggested by W. Kimmerle [7]. Let us briefly introduce it now.

Let G be a finite group. Denote by $\#(G)$ the set of all primes dividing the order of G. Then the *Gruenberg-Kegel graph* (or the *prime graph*) of G is a graph $\pi(G)$ with vertices labelled by primes from $\#(G)$, such that vertices p and q are adjacent if and only if there is an element of order pq in the group G. Then the conjecture by Kimmerle can be formulated in the following way:

(KC) If G is a finite group, then $\pi(G) = \pi(V(\mathbb{Z}G))$.

For Frobenius groups and solvable groups this conjecture was confirmed in [7]. In the reported research we continued the investigation of **(KC)**, and confirmed it for the first simple Mathieu group M_{11}, using the Luthar-Passi method. Moreover, this allows us to give a partial solution of **(ZC)** for M_{11}. Our main results are the following:

Theorem 4. *Let $V(\mathbb{Z}G)$ be the normalized unit group of the integral group ring $\mathbb{Z}G$, where G is the simple Mathieu group M_{11}. Let u be a torsion unit of $V(\mathbb{Z}G)$ of order $|u|$. We have:*

(i) *if $|u| \neq 12$, then $|u|$ coincides with the order of some element $g \in G$;*

(ii) *if $|u| \in \{2, 3, 5, 11\}$, then u is rationally conjugate to some $g \in G$;*

(iii) *if $|u| = 4$, then the tuple of partial augmentations of u belongs to the set*

$$\{ \ (\nu_{2a}, \nu_{3a}, \nu_{4a}, \nu_{6a}, \nu_{5a}, \nu_{8a}, \nu_{8b}, \nu_{11a}, \nu_{11b}) \in \mathbb{Z}^9 \quad | \ \nu_{kx} = 0, \\ kx \notin \{2a, 4a\}, \quad (\nu_{2a}, \nu_{4a}) \in \{ \ (0, 1), \ (2, -1) \ \} \ \};$$

(iv) *if $|u| = 6$, then the tuple of partial augmentations of u belongs to the set*

$$\{ \ (\nu_{2a}, \nu_{3a}, \nu_{4a}, \nu_{6a}, \nu_{5a}, \nu_{8a}, \nu_{8b}, \nu_{11a}, \nu_{11b}) \in \mathbb{Z}^9 \quad | \ \nu_{kx} = 0, \\ kx \notin \{2a, 3a, 6a\}, \quad (\nu_{2a}, \nu_{3a}, \nu_{6a}) \in \{ \ (-2, 3, 0), (0, 0, 1), \\ (0, 3, -2), (2, -3, 2), \ (2, 0, -1) \ \} \quad \};$$

(v) *if $|u| = 8$, then the tuple of partial augmentations of u belongs to the set*

$$\{ \ (\nu_{2a}, \nu_{3a}, \nu_{4a}, \nu_{6a}, \nu_{5a}, \nu_{8a}, \nu_{8b}, \nu_{11a}, \nu_{11b}) \in \mathbb{Z}^9 \quad | \ \nu_{kx} = 0, \\ kx \notin \{4a, 8a, 8b\}, \quad (\nu_{4a}, \nu_{8a}, \nu_{8b}) \in \{ \ (0, 0, 1), \ (0, 1, 0), \\ (2, -1, 0), \ (2, 0, -1) \ \} \quad \};$$

(vi) *if $|u| = 12$, then the tuple of partial augmentations of u cannot belong to the set*

$$\mathbb{Z}^9 \setminus \{ \ (\nu_{2a}, \nu_{3a}, \nu_{4a}, \nu_{6a}, \nu_{5a}, \nu_{8a}, \nu_{8b}, \nu_{11a}, \nu_{11b}) \in \mathbb{Z}^9 \quad | \quad \nu_{kx} = 0, \\ kx \notin \{2a, 4a, 6a\}, \quad (\nu_{2a}, \nu_{4a}, \nu_{6a}) \in \{ \ (-1, 1, 1), \ (1, 1, -1) \ \} \quad \}.$$

Corollary 1. *Let $V(\mathbb{Z}G)$ be the normalized unit group of the integral group ring $\mathbb{Z}G$, where G is the simple Mathieu group M_{11}. Then $\pi(G) = \pi(V(\mathbb{Z}G))$, where $\pi(G)$ and $\pi(V(\mathbb{Z}G))$ are prime graphs of G and $V(\mathbb{Z}G)$, respectively. Thus, for M_{11} the conjecture by Kimmerle is true.*

We used the computational algebra system GAP [4] and its character table library to obtain the ordinary and Brauer character tables of M_{11}, and to implement required algorithms, which we plan to include in the next version of our package LAGUNA [3].

References

[1] F. M. Bleher and W. Kimmerle, *On the structure of integral group rings of sporadic groups*, LMS J. Comput. Math. **3** (2000), 274–306 (electronic). MR1783414 (2001i:20006)

[2] V. Bovdi, C. Höfert and W. Kimmerle, *On the first Zassenhaus conjecture for integral group rings*, Publ. Math. Debrecen **65** (2004), no. 3-4, 291–303. MR2107948 (2006f:20009)

[3] V. Bovdi, A. Konovalov, R. Rossmanith, C. Schneider, *LAGUNA – Lie AlGebras and UNits of group Algebras*, v.3.3.3; 2006 (http://ukrgap.exponenta.ru/laguna.htm).

[4] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*; 2006 (http://www.gap-system.org).

[5] M. Hertweck, *Partial augmentations and Brauer character values of torsion units in group rings*, to appear (2005), 26 pages

[6] M. Hertweck, *On the torsion units of some integral group rings*, Algebra Colloq. **13** (2006), no. 2, 329–348. MR2208368

[7] W. Kimmerle, *On the prime graph of the unit group of integral group rings of finite groups*, in *Groups, rings and algebras*, Contemporary Mathematics, AMS, to appear

[8] I. S. Luthar and I. B. S. Passi, *Zassenhaus conjecture for A_5*, Proc. Indian Acad. Sci. Math. Sci. **99** (1989), no. 1, 1–5. MR1004634 (90g:20007)

[9] I. S. Luthar and P. Trama, *Zassenhaus conjecture for S_5*, Comm. Algebra **19** (1991), no. 8, 2353–2362. MR1123128 (92g:20003)

[10] H. Zassenhaus, *On the torsion units of finite group rings*, in *Studies in mathematics (in honor of A. Almeida Costa) (Portuguese)*, 119–126, Inst. Alta Cultura, Lisbon. MR0376747 (51 #12922)

Computing Character Tables of Parabolic Subgroups

Frank Himstedt

Characters of parabolic subgroups are used to obtain information on the structure and the representation theory of finite groups of Lie type. For example: In [6], character tables of parabolic subgroups led to new information on modular characters of the Chevalley groups $G_2(2^n)$, and in [4], irreducible characters of maximal parabolic subgroups were used to determine degrees of modular irreducible representations of Steinberg's triality groups ${}^3D_4(q)$ in non-defining characteristic.

In my talk, I described techniques and computer programs which are helpful in computing generic character tables of parabolic subgroups of finite groups of Lie type.

The computation of these generic character tables is usually done in the following way: In a first step, one determines the conjugacy classes of elements of the parabolic subgroups. The necessary calculations like computing centralizers and tests for conjugacy can be done computer-assisted using GAP-programs written by Christoph Köhler and myself in CHEVIE [1].

In particular, we have written programs for computing in connected reductive linear algebraic groups based on the Steinberg presentation and Bruhat normal form. Additionally, I have implemented a polynomial arithmetic for multivariate polynomials where the exponents are polynomials in an indeterminate q. Such polynomials occur when calculating centralizers in parabolic subgroups of twisted groups of Lie type generically. The parametrization of the semisimple conjugacy classes of parabolic subgroups can be done automatically using an algorithm due to C. Köhler [5] (assuming that the centralizers of semisimple elements in an underlying algebraic group are connected).

In the next step, one constructs the irreducible characters of the parabolic subgroups using the Levi decomposition, Clifford theory and induction of characters from proper subgroups. The MAPLE-part of CHEVIE provides an environment for storing and processing generic character tables of parabolic subgroups. Built-in CHEVIE functions for computing scalar products and tensor products of characters and MAPLE-programs written by C. Köhler and myself for inducing and restricting class functions between generic character tables can be used to construct irreducible characters of parabolic subgroups.

The abovementioned tools were successfully applied to compute

- the generic character tables of all parabolic subgroups of Steinberg's triality groups ${}^3D_4(q)$ [2], [3],
- the conjugacy classes of the Borel and two maximal parabolic subgroups of $F_4(q)$, q a power of a prime $\neq 2, 3$ [5],
- the conjugacy classes of all parabolic subgroups of ${}^2F_4(2^{2n+1})$, joint work with Shih-chang Huang, in preparation.

References

[1] M. Geck, G. Hiss, F. Lübeck, G. Malle, G. Pfeiffer, *CHEVIE – A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), 175–210.

[2] F. Himstedt, *Character tables of parabolic subgroups of Steinberg's triality groups*, J. Algebra **281** (2004), 774–822.

[3] F. Himstedt, *Character tables of parabolic subgroups of Steinberg's triality groups* ${}^3D_4(2^n)$, in preparation.

[4] F. Himstedt, *On the 2-decomposition numbers of Steinberg's Triality Groups* ${}^3D_4(q)$*, q odd*, to appear in J. Algebra.

[5] C. Köhler, *Unipotente Charaktere und Zerlegungszahlen der endlichen Chevalleygruppen vom Typ* F_4, Ph.D. thesis, RWTH Aachen University (2006).

[6] K. Waki, *A note on decomposition numbers of* $G_2(2^n)$, J. Algebra **274** (2004), 602–606.

Character Tables in Magma

William R. Unger

The table of ordinary characters of a finite group is one of the important algebraic objects associated with the group. It is of interest in its own right, as well as being the start of much representation theory. Computer algorithms to get the character table of a group have been both investigated and heavily used since the 1960's. In this talk I describe an algorithm I have recently devised and implemented in Magma V2.12 [1]. A full description of the algorithm is given in [6].

As an example, take $U_5(4)$, a simple group with character table considered beyond straightforward computation until now. Using the implementation of this new algorithm in Magma V2.12, its character table is found within half an hour on a 750MHz machine using a permutation representation of degree 17425. The Dixon-Schneider algorithm [3, 5], which depends on the sizes of the conjugacy classes of the group, fails to complete within a day, as it is forced to consider a conjugacy class of size $\approx 6.8 \times 10^{10}$.

The new algorithm follows the "generate and split" paradigm for computing ordinary character tables, where we find whatever ordinary characters we are able to and then add and subtract to find characters of norm 1. The characters used by the new algorithm are those induced from elementary subgroups. By a theorem Brauer, all characters of our group G arise as integer linear combinations of such induced characters. An elementary group is a direct product of a p-group and a cyclic group, and the characters of the p-group are found using Conlon's algorithm [2]. The characters of the full elementary group are then easily found and induced to characters of G.

The "split" part of the method is achieved using LLL lattice reduction. This means we work with generalised characters, not true characters, but no problems arise from this. To keep the arithmetic of computing inner products and updating the reduced basis of characters fast, the implementation borrows from Dixon [3] and works over a prime field. The prime is taken to be $> 2|G|$ so that inner products can be computed without ambiguity.

When the computation is nearing completion, techniques such as factorising a Gram matrix have been found to be very useful. See [4] for an algorithm achieving this. The implementation uses a restricted form, where the factors sought are invertible.

The new algorithm has performed very well in computing character tables of groups that are nearly simple, as well as maximal and local subgroups of such groups. The article [6] gives examples including local subgroups of Fi_{24} and the Monster. For many of these examples it is completely impractical to compute the character tables with the Dixon-Schneider algorithm, but the new algorithm succeeds using quite modest resources of time and space.

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symbolic Comp. **24** (1997), 235–265.

[2] S.B. Conlon, *Calculating characters of p-groups*, J. Symbolic Comp. **9** (1990), 551–570.

[3] J.D. Dixon, *High speed computation of group characters*, Numer. Math. **10** (1967), 446–450.

[4] W. Plesken, *Solving $XX^{\mathrm{tr}} = A$ over the integers*, Linear Algebra Appl. **226/228** (1995), 331–344.

[5] G.J.A. Schneider, *Dixon's character table algorithm revisited*, J. Symbolic Comp. **9** (1990), 601–606.

[6] W.R. Unger, *Computing the character table of a finite group*, J. Symbolic Comp. **41** (2006), 847–862.

Computing in linear algebraic groups

Scott H. Murray

(joint work with Arjeh Cohen, Willem de Graaf, Sergei Haller, and Don Taylor)

Linear algebraic groups are subgroups of $\mathrm{GL}_n(k)$ defined by polynomial equations, where k is a field. Examples include $\mathrm{GL}_n(k)$, $\mathrm{SL}_n(k)$, the classical groups, the group of lower triangular matrices, and the group of lower unitriangular matrices.

A linear algebraic group can also be viewed as a functor:

$$\{\text{commutative associative algebras over } k\} \to \{\text{groups}\},$$

satisfying certain additional conditions. For example, $\mathbb{G}_a(K) = K^+$, $\mathbb{G}_m(K) = K^\times$ This scheme-theoretic approach is useful for computation because the fundamental objects are the groups, rather than the polynomials.

Groups over k that become isomorphic over $\bar{k}$ are called forms. For example, $\mathrm{O}_n^+(q)$ and $\mathrm{O}_n^-(q)$ are forms of $\mathrm{O}_n(\bar{\mathbb{F}}_q)$. Such forms are classified using Galois cohomology – the computation of Galois cohomology was studied in [3].

We wish to do structural computations with linear algebraic groups, similar to those currently possible for permutation and matrix groups. Every linear algebraic group G contains subgroups $R_u(G) \le G^\circ \le G$ where G/G° is finite, $G^\circ/R_u(G)$ is reductive, and $R_u(G)$ is unipotent. So we start by considering unipotent and reductive groups

1. Unipotent groups

Let U be k-unipotent. Such groups are known to be nilpotent. We have adapted PC-group theory to deal with these groups.

Theorem. *We can choose parameters $x_r : \mathbb{G}_a \to G$ such that, for every extension K of k, $U(K)$ has the presentation*

$$x_r(a)x_r(b) = x_r(a+b)\prod_{t=r+1}^{N} x_t(f_{rt}(a,b)),$$

$$x_r(a)^{-1} = x_r(-a)\prod_{t=r+1}^{N} x_t(g_{rt}(a)),$$

$$x_s(b)x_r(a) = x_r(a)x_s(b)\prod_{t=s+1}^{N} x_t(h_{rst}(a,b))$$

The standard techniques of collection can be now be used for these groups. If k has characteristic zero, then we can also take $f_{rt} = g_{rt} = 0$. We hope to find similar presentations for soluble algebraic groups, but there are many more forms to consider in this case.

2. Reductive groups

For reductive groups, we do computations with the Steinberg presentation [2]. Take GL_n as an example. Every invertible matrix can be decomposed:

$$ut\dot{w}u'$$

where:

- u and u' are lower unitriangular,
- w is a permutation, and $\dot{w}$ is the permutation matrix,
- t is diagonal.

This leads to a presentation with three kinds of generators:

- unipotent (lower unitriangular),
- discrete (permutation), and
- toral (diagonal).

Lie algebras are a vital tool for structural computation with algebraic groups. Although the Lie correspondence breaks down in characterstic p, it is still possible to gain significant information from it. This was the approach taken in [1].

3. Magma functionality

Current functionality (2.12)

- Root systems and root data
- Coxeter groups (presentation, permutation and matrices)
- Untwisted reductive groups (Steinberg presentation)
- Highest weight representations
- Galois cohomology
- Lie algebras

New functionality (2.13)

- Much faster multiplication
- Twisted and nonreduced root data
- Twisted reductive groups
- LiE: Combinatorics of highest weight representations

References

[1] Arjeh M. Cohen and Scott H. Murray, *Algorithm for Lang's Theorem*, Preprint, 2005.

[2] Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor, *Computing in groups of Lie type*, Math. Comp. **73** (2004), 1477–1498.

[3] Sergei Haller, *Computing Galois cohomology and forms of linear algebraic groups*, Ph.D. thesis, Technical University of Eindhoven, 2005.

Reporter: Felix Noeske

Participants

Dipl. Math. Björn Aßmann
School of Mathematics & Statistics
University of St. Andrews
North Haugh
GB-St. Andrews Fife KY16 9SS

Henrik Bäärnhielm
School of Mathematical Sciences
Queen Mary
University of London
Mile End Road
GB-London E1 4NS

Prof. Dr. Laurent Bartholdi
IMB, Batiment MA, Station 8
Ecole Polytechnique Federale
CH-1015 Lausanne

Prof. Dr. Gilbert Baumslag
Department of Mathematics
The City College of New York, CUNY
North Academic Center 8/133
Convent Avenue at 138th Street
New York, NY 10031
USA

Dr. Anton Betten
Dept. 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
Dept. of Mathematics
Bucknell University
Lewisburg, PA 17837
USA

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

Heiko Dietrich
Fachbereich für Mathematik und
Informatik
TU Braunschweig
Pockelsstr. 14
38106 Braunschweig

Prof. Dr. Bettina Eick
Fachbereich für Mathematik und
Informatik
TU Braunschweig
Pockelsstr. 14
38106 Braunschweig

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

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

Prof. Dr. David J. Green
Mathematisches Institut
Friedrich-Schiller-Universität
Ernst-Abbe-Platz 1-4
07743 Jena

Prof. Dr. George Havas
ARC Centre for Complex Systems
School of ITEE
The University of Queensland
Queensland 4072
AUSTRALIA

Dr. Anne E. Henke
Mathematical Institute
Oxford University
24-29 St. Giles
GB-Oxford OX1 3LB

Dr. Frank Himstedt
Zentrum Mathematik
TU München
Boltzmannstr. 3
85748 Garching bei München

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

Jia-Lun Huang
Dept. of Mathematics
Queen's College
Oxford University
GB-Oxford OX1 4AW

Prof. Dr. Alexander Hulpke
Dept. 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 bei München

Prof. Dr. Alexander B. Konovalov
Departement Wiskunde
Fakulteit der Wetenschappen
Vrije Universiteit Brussel
Pleinlaan 2
B-1050 Bruxelles

Dr. Matthias Künzer
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

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

Prof. Steve Linton
School of Computer Science
University of St. Andrews
North Haugh
GB-St. Andrews, Fife KY16 9SS

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. Gunter Malle
Fachbereich Mathematik
T.U. Kaiserslautern
67653 Kaiserslautern

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

Dr. Scott Murray
School of Mathematics & Statistics
The University of Sydney
Sydney NSW 2006
AUSTRALIA

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

Dr. Max Neunhöffer
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

Prof. Michael F. Newman
Centre for Mathematics and its
Applications
Mathematical Sciences Institute
ANU
Canberra, ACT 0200
Australia

Dr. Werner Nickel
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt

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

Dr. Götz Pfeiffer
Mathematics Department
National University of Ireland
Galway
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 6009 WA
Australia

Prof. Dr. Edmund F. Robertson
School of Mathematics & Statistics
University of St. Andrews
North Haugh
GB-St. Andrews Fife KY16 9SS

Daniel Robertz
Lehrstuhl B für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen

Andreas Röscheisen
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg

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

Dr. Csaba Schneider
Informatics Laboratory
Computer&Automation Research Inst.
The Hungarian Academy of Sciences
Lagymanyosi u.11.
H-1111 Budapest

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
Department of Mathematics
RUTGERS University
Hill Center, Busch Campus
110 Frelinghuysen Road
Piscataway, NJ 08854-8019
USA

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

Mark Stather
Mathematics Institute
University of Warwick
GB-Coventry CV4 7AL

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

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

Sükrü Yalcinkaya
Department of Mathematics
Middle East Technical University
06531 Ankara
TURKEY