Mathematisches Forschungsinstitut Oberwolfach

Report No. 34/2001

Computational Group Theory

July 30th–August 3rd

This meeting was the fourth on Computational Group Theory held at the Mathematisches Forschungsinstitut. The meeting was attended by 49 participants. There was a good mix of nationalities, age-groups, and research communities – such as matrix group recognition, representation theory, finitely-presented groups. There were 9 people for whom this was their first meeting. (The gender balance reflected that of the community.)

We made a strong effort to provide a balance between time in the lecture room and more informal discussion – quite a bit at the terminals in the basement. We were very pleased to see the continuing progress with this facility. (Some of us recall the first meeting in 1988 when a significant effort had to be put into transporting equipment from Aachen and setting it up.) This enabled people to test ideas from discussions in familiar (and sometimes extensive) computing environments at other locations. Posters were used to good effect (they included a report on an associated meeting on *Finitely-presented groups: questions and algorithms* held in Trento, Italy, the week before). There were several invited survey talks. We also had a formal discussion on the theme: Support for software. All the newcomers were given the opportunity to make a formal presentation.

It is perhaps a sign of the increasing maturity of the field that there was more emphasis on theoretical developments – though of course these would not have been possible without significant implementational developements.

The abstracts which follow give a good indication of the range of topics that are active in the field. The matrix group recognition project continues to receive a lot of attention. There were surveys by O'Brien and Kantor. Other surveys were by Sims on the Knuth-Bendix procedure, Hiß on Representation Theory and Holt on automatic and hyperbolic groups.

The abstract of Leedham-Green's closing talk gives an indication of the very positive interactions which were made possible by a face-to-face meeting. This underlines that even in an era of “quick” communication a community needs to meet face-to-face from time-to-time.

The organisers: G. Hiß, D. Holt, M. Newman, H. Pahlings.

Abstracts

Groups acting on trees

L. Bartholdi

The class of “finite-state groups” seems to combine the best qualities of many worlds: they are describable by finite data yet can be infinite; they are simple to compute with yet can possess exotic properties; they served as a source of examples and counter-examples in group theory for the last 20 years.

Given an isometry g of the d-regular tree T, it decomposes as a permutation $\pi_g \in S_d$ of the top d branches, and isometries $(g_1, \dots, g_d)$ of the d subtrees, each isomorphic to T. These g_i can in turn be decomposed, and the set of all $g_i, g_{ij}, \dots$ obtained in this way is the *states* of g. A group G is *finite-state* if it is generated by isometries with finite set of states; equivalently, if all elements of G have a finite set of states.

As examples, all finite groups and countable abelian groups admit finite-state representations; this class is closed under wreathing with a finite group and taking direct products; and contains examples like the Grigorchuk group G, which is a finitely generated, infinite, torsion, recursively presented 2-group of finite width and intermediate growth.

I will explain how computations can be performed on such groups; they have a solvable word problem, and admit a natural family of approximating quotients obtained by restricting the action to some level of the tree T.

Its lattice of normal subgroups, and its tower of automorphism groups, have recently been determined. I hope to discuss such computations, and outline their generalization to the whole class of finite-state groups.

Extracting Generators and Relations for Matrix Algebras

J. Carlson

This is a report of work in progress. For some time I have been talking to John Cannon about methods to redesign the structures for *finite dimensional algebras* in magma. At the present time there are numerous “algebra” types in magma, each optimized for a particular type of tasks. But there is no communication between the types. One can not, for example, define a module over a matrix algebra or a structure constant algebra. The best way to solve this problem it would seem, is to introduce generators and relations for algebras in general. Then a basis for the algebra could be computed as elements in a polynomial ring with non-commuting variables and Groebner basis methods could resolve such questions as dimensions of the algebra.

The center post of such a system then would be a type of free algebra and a program for computing non-commutative Groebner bases. Some of this has been written for magma though it is not yet available in any official release. In order to make the system work it will be necessary to have the capability of obtaining generators and relations for the various types of algebras. The most difficult and also most general of the types is the matrix algebra. Currently we are working on the development of algorithms for this purpose and we have some implementations. In addition the programs being written could have numerous other uses.

Parallelizing Coset Enumeration

G. Cooperman

Coset enumeration for group presentations, like Groebner bases, is well known to be a challenging problem to parallelize. Recently, a new parallel coset enumerator was developed jointly with Victor Grinberg, which is believed to have achieved the greatest degree of parallelism (32 CPU's on an SGI Origin 2000 with an eight times speedup) to date among parallel enumerators. The method is based on a new strategy (clouds) for defining many cosets at once. In a traditional computer program (even a sequential one), the quality of the enumeration with respect to both CPU time and memory depends strongly on the ability to process coincidences and make deductions as soon as possible after they are discovered. We present a class of what we call bulk definition strategies, which avoid this restriction.

This leads to an interesting strategy for parallelization. STEP 1: Find a bulk definition strategy such that the sequential algorithm does not degrade excessively when using the strategy. STEP 2: Parallelize it. (Parallelize the relator tracing.)

We will observe that STEP 2 exhibits a nearly linear speedup over the modified sequential algorithm of STEP 1.

We also describe a sequential "prescan strategy", which is surprisingly effective during the second half of an enumeration (speeding up the sequential enumeration by a factor of about three on Lyons' group). The "prescan strategy" suffers from not maintaining Felsch consistency. Hence, the final table must be verified, but this is usually fast.

TOP-C (Task Oriented Parallel C/C++, www.ccs.neu.edu/home/gene/topc.html) was used for the parallel implementation. This allowed us to parallelize a 3,200 line sequential program by adding approximately 250 lines of parallel-specific code.

The orbit-stabiliser problem for polycyclic groups

B. Eick

(joint work with G. Ostheimer)

The general problem considered in this talk is the development of practical algorithms for (possibly infinite) polycyclic groups. A useful general approach to such methods is by induction over a normal series with elementary or free abelian factors. In the inductive step, an elementary or free abelian normal subgroup A of a group G is considered. There are two fundamental problems which often arise this setting.

- The orbit-stabilizer problem:
  (1) Given $b, c \in A$, determine $Stab_G(b)$ and an element $g \in G$ with $b^g = c$ (if g exists).
  (2) Given $B, C \leq A$, determine $Stab_G(B)$ and an element $g \in G$ with $B^g = C$ (if g exists).
- The extension problem: Determine $H^1(G/A, A)$ and $H^2(G/A, A)$.

For elementary abelian groups A, practical solutions to these problems are well-known. For free abelian groups A, practical methods to solve these problems have been developed recently. The resulting approach to solve the orbit-stabilizer problem for elements (1) is described in this talk.

Solutions to these and related problems have further been used to obtain a variety of practical algorithms for polycyclic groups. These include the following.

- Determine $C_G(g)$, $N_G(U)$ and $U \cap V$ for $g \in G$ and $U, V \leq G$.
- Compute the torsion subgroup $T(G)$ (if it exists) or the normal torsion subgroup $TN(G)$.
- Calculate the conjugacy classes of finite subgroups.
- Construct the subgroups of low index in G.
- Calculate $Fit(G)$, $Z(G)$ or the FC-centre $FC(G)$.
- Exhibit the nilpotent-by-abelian-by-finite structure of G.

Implementations for most of these methods are available in the *Polycyclic* package (joint work with W. Nickel). This package is based on GAP and Kant.

Bounds on the degree of commutativity of a p-group of maximal class

M. García-Sánchez

(joint work with A. Vera-López, J. Arregi, F. Vera-López, R. Esteban-Romero)

A group G of order p^m is said to be a p-group of maximal class if $Y_{m-1} \neq 1$, where $Y_0 = G$, $Y_i = [\overbrace{G, \dots, G}^{i}]$ for every $i \geq 2$ and Y_1 such that $Y_1/Y_4 = C_{G/Y_4}(Y_2/Y_4)$.

One of the main invariants of a p-group of maximal class is its degree of commutativity c. Another important invariant associated to such a group is defined by $v = v(G) = \min\{k \in [2, m-c-2] \mid [Y_1, Y_k] = Y_{1+k+c}\}$. It is proved that $v = v(G)$ is an even number $2l$ satisfying $v = 2l \leq p-1$ and if $v + 2 = 2l + 2 \leq m - c - 1$, then $1 \leq l \leq (p-3)/2$.

We have designed an algorithm that gives us a lower bound for the degree of commutativity of a p-group of maximal class of order p^m. Running this algorithm for primes $p \leq 43$, we have conjectured the existence of a function $g(p, l, c_0)$ such that $2c \geq m - g(p, l, c_0)$, where c_0 is the residue class of c modulo $p-1$, for all p-group of maximal class with the invariants l and c_0. In fact, we have proved the validity of $g(p, l, c_0)$ for the six regions. The union of these six regions covers almost all possible (l, c_0). Besides, the given bound is exact in three of the six regions.

Experiments in GAP and special pieces in unipotent varieties

M. Geck

(joint work with G. Malle)

This is a report on a joint work with Günter Malle which appeared in Experimental Mathematics **8** (1999), 281–290. It is the result of experiments performed using computer programs written in the GAP language. We describe an algorithm which computes a set of rational functions attached to a finite Coxeter group W. Conjecturally, these rational functions should be polynomials which have the following meaning.

Assume that W is the Weyl group of a Chevalley group G defined over the finite field $\mathbf{F}_q$. We consider the conjugacy classes of G consisting of unipotent elements. It is known that there are only finitely many such classes and that they can be classified in a uniform way if the characteristic is large enough; the classification in small characteristics is different, however.

Now, following Lusztig and Spaltenstein, one can define a partition of the variety of unipotent elements of G into so-called *special pieces*. These special pieces are unions of unipotent classes and they are classified in terms of certain irreducible characters of the finite group W (and, hence, independently of the characteristic). Lusztig showed (by an extremely elaborated counting argument) that the number of $\mathbf{F}_q$-rational points in a special piece is given by a well-defined polynomial in q. Our conjecture is that these polynomials are precisely the ones produced by our algorithm.

The algorithm is a variant of a known algorithm (due to Shoji and Lusztig) for computing the Green functions in the character theory of finite groups of Lie type. It even works for complex reflection groups. We give a number of examples which show, in particular, that our conjecture is true for all types except possibly B_n and D_n.

Computing Canonical Bases of quantum groups

W. de Graaf

Let U^- be the negative part of the quantized universal enveloping algebra of a semisimple Lie algebra. Kashiwara and Lusztig have independently constructed a basis of U^- with very favourable properties. This basis is called the canonical basis. In this talk I sketch an algorithm for computing the elements of the canonical basis of a given weight. This algorithm is based on the following two facts. Firstly, the matrix giving the base change from the canonical basis to a basis consisting of standard monomials is upper triangular with 1's on the diagonal. Secondly, the same holds for the matrix of the base change from the canonical basis to a basis of PBW-type. The algorithm based on this computes the elements of the canonical basis as linear combinations of elements of a PBW-type basis.

ACME, an Andrews-Curtis move enumerator

G. Havas

Andrews and Curtis have conjectured that every balanced presentation of the trivial group can be transformed into the standard presentation by a finite sequence of elementary transformations. Previous computational work on this problem has been based on genetic algorithms. We show that a computational attack based on a breadth-first search of the tree of equivalent presentations is also viable, and seems to outperform that based on genetic algorithms. It allows us to extract shorter proofs (in some cases, provably shortest) and to consider the length thirteen case for two generators. We prove that, up to equivalence, there is a unique minimum potential counterexample.

Computational Representation Theory

G. Hiss

In this survey talk I discussed three topics:

1. The Modular Atlas,
2. Minimal Degrees,
3. Symmetric Groups.

Ad 1. Here I summarized some recent results, in particular the completion of the Brauer trees of the Lyons simple group, accomplished by Müller, Neunhöffer, Röhr and Wilson. I also discussed the work that still needs to be done, giving some more details for three of the sporadic groups, the Fischer group Fi_{22}, the Thompson group Th and the Harada-Norton group HN.

Ad 2. Here I shortly discussed the knowledge on the smallest degrees of representations of the finite simple groups and their covering groups. More details were given in the talk by Frank Lübeck.

Ad 3. Here I presented some recent results on the representation theory of symmetric and alternating groups, as well as their covering groups. There exist GAP-programs for computing the ordinary character tables of $2.A_n$ and $2.S_n$, implemented by Müller and Noeske. The modular tables for the symmetric groups S_n are completely known for all $n \leq 17$. In S_{18}, only one bit of information is missing in characteristic 2. Also, the Brauer trees for $2.A_n$ and $2.S_n$ are now known for all n by the work of Müller and Noeske. Finally I mentioned the programs by Frank Lübeck for computing the Jantzen filtration of Specht modules.

Collection in polycyclic groups

B. Höfling

Given a finite polycyclic presentation $\langle g_1, \ldots, g_n \mid g_i^{e_i} = w_{i,i}, g_j^{g_i} = w_{i,j}, i < j \rangle$, multiplication of reduced words is performed by collecting, i. e., by reducing the word obtained by concatenation of the original words. Collection is usually done from the left, that is, choosing the leftmost occurrence of a left hand side of a rewriting rule. While this works well in practice, theoretical bounds on the complexity are extremely bad, usually $O(N^{n+1})$, where N is the input length, or $O(N^c)$, where c is the p-class of the p-group G.

Using a polycyclic presentation obtained from the derived series of G in a natural way, I could show that a collection can be carried out in $O(N^{3d})$ steps. This assumes that certain powers $(g_j^a)^{g_i^b}$ are pre-computed. But even this bound (which is sub-exponential in N) apparently is far from reality.

A reason for this might be that most intermediate collection steps actually take place in small exhibited subgroups H of G. These are subgroups of the form $H = \{g_1^{a_1} \ldots g_n^{a_n} \mid 0 \leq a_i < e_i,\, a_i = 0 \text{ if } i \notin I\}$, where I is a subset of $\{1, \ldots, n\}$. Using this observation, one obtains upper bounds and estimates for the average cost of a collection. The estimates thus obtained generally agree with experimental data to within an order of magnitude.

As a consequence, it seems to be advisable to choose generators $\{g_1, \ldots, g_n\}$ such that $G = HG_i$, where G_i is a small normal subgroup of G and H is exhibited, and then to recursively decompose H in the same way. There is an algorithm for obtaining such a polycyclic presentation from one refining a normal series with nilpotent factors.

Computation in automatic and hyperbolic groups

D. Holt

This was a survey talk, summarising recent progress in the art of computing efficiently in automatic and hyperbolic groups.

The definition of an automatic group is due to Thurston and dates from about 1985. Roughly speaking, a (finitely generated) group is automatic if there is a finite state automaton (FSA) recognising a unique word in the generators for each group element, and other automata that read two words in the generators simultaneously and synchronously, and accept the pair if both are in normal form and one is equal in the group to the other multiplied on the right by a group generator.

Once these FSA have been computed for a specific group, the word problem in that group can be solved in quadratic time by reducing the word to its normal form. The growth function (which is necessarily rational) and orders of elements can also be computed. Recently these programs have been used to prove that various groups are infinite that have resisted other methods of proof. For example, the Heineken group

$$H = \langle x,\ y,\ z \mid [x,[x,y]] = z,\ [y,[y,z]] = x,\ [z,[z,x]] = y\rangle$$

is automatic (indeed, it is hyperbolic), and infinite.

Hyperbolic groups form an important subclass of the automatic groups in which more problems are solvable efficiently. Presentations of certain subgroups, known as quasiconvex subgroups, can be computed, and the generalized word problem can be solved for these subgroups. Recently, my student Joe Marshall has implemented algorithms for testing elements of infinite order for conjugacy, and for testing quasiconvex subgroups for malnormality in hyperbolic groups. For example, the subgroup $\langle [x,y],\ [y,z],\ [x,z]\rangle$ of the group H defined above is free of rank three and is malnormal in H.

Algorithms for finite linear groups

W. Kantor and Á. Seress

In the first half of the talk, we survey recognition algorithms for finite simple groups. Given any quasisimple matrix representation of a finite simple group G, there is a Monte Carlo algorithm which, in time polynomial in the input length, determines the standard name of G. In slightly more time, namely polynomial in the input length and in the size q of the underlying field of definition of G if G is of Lie type, it is also possible to identify G with a standard copy C of its isomorphism type constructively. This means that there is an isomorphism $\lambda : G \to C$ such that for any $g \in G$ we can compute $\lambda(g) \in C$, and for any $c \in C$ we can compute $\lambda^{-1}(c)$. Moreover, we can express any $g \in G$ in polynomial time as a function of some fixed generating set X of G.

In the second part, we outline an algorithm which reduces the basic handling of arbitrary matrix groups G to the constructive recognition of its composition factors. The algorithm is based on structural properties of G, instead of trying to exploit the geometric properties of the action of G in the input representation. The latter approach is described in Eamonn O'Brien's talk.

A modular version of Molien's formula

G. Kemper

(joint work with I. Hughes)

Molien's formula is one of the most remarkable tools in invariant theory of finite groups. It allows the computation of the Hilbert series of an invariant ring without touching a single invariant. Unfortunately, Molien's formula breaks down in the modular case, i.e., when the characteristic p of the ground field divides the group order $|G|$.

In this work we obtain a formula for computing the Hilbert series in the "mildly" modular case, i.e., when p divides $|G|$ but p^2 does not. The main ingredients we use are:

- species and linear combinations thereof,
- symmetrization and the lambda-structure of representation rings,
- a periodicity property of symmetric powers

An extension of our formula also allows the easy computation of the depth of a mildly modular invariant ring.

Isometry classes of linear codes

A. Kerber

A brief review was given on our (i.e. mainly A. Betten, A.K., A. Kohnert and R. Laue's) activities in the field of *constructive theory of finite structures.* We are mainly after *existence proofs* (via construction) of structures for given sets of parameters (e.g. of $t-(v,k,\lambda)$-designs for given v,t,k) as well as after the development and the implementation of algorithms for the *systematic and exhaustive construction* of complete catalogs.

Our generator MOLGEN for molecular graphs corresponding to a given chemical formula and (optional) further conditions was mentioned and it was shown in which situation in molecular structure elucidation the fast generation of complete catalogs is necessary. It was also pointed to the package DISCRETA that is devoted to the systematic construction of designs with a prescribed group of automorphisms.

Then it was described what we did for the systematic evaluation of representatives of isometry classes of linear codes. Isometry classes were introduced and it was shown how the calculation of transversals of such classes amounts to a consideration of orbit sets of the following form:

$$GL_k(q)\backslash\!\!\backslash\big(S_n\backslash\!\!\backslash P_{k-1}(q)^n\big),$$

where $P_{k-1}(q)$ means a projective geometry. (This shows perfectly why there is such a close connection between projective geometry and the theory of linear codes!) Numerical results on the number of (indecomposable) isometry classes were shown, and it was mentioned that the corresponding generator matrices are available and that the corresponding minimal distances are known. Details can be found in the book *A. Betten, H. Fripertinger, A. Kerber, A. Wasserman, K.-H. Zimmermann: Codierungstheorie, Springer-Verlag 1998.*

Matrix groups recognition: The seven last transparencies

C. Leedham-Green

My lecture was a post-script to O'Brien's lecture. His lecture (at the start of the conference) showed how, after many years work, and with the collaboration of a large proportion of the participants at the conference, the matrix recognition project was beginning to come to fruition. This provoked a collection of challenge problems, constructed by Parker and Wilson, and I mentioned at the end of my lecture that the first five had already been solved, which provoked a supply of some 'harder' problems by Müller and Lübeck.

Small degree projective irreducible representations of finite simple groups

F. Lübeck

Let G be a finite simple group and $F = \bar{F}$ an algebraically closed field of characteristic l.

In my talk I considered the following two problems:

(a) What are the (few) smallest degrees $d > 1$ of irreducible projective representations of G over F?

(b) Given F and (a reasonably small) d: Which simple G have a projective irreducible representation of degree d over F?

Such questions arise in various classification and identification problems. For example it is of relevance in the matrix recognition project which was a major topic during this meeting.

In my talk I gave an overview on five papers concerning these questions. I tried to give an idea how the results look like (using some transparencies) and about the methods used to obtain the results.

In some more detail:

1. Landázuri-Seitz-Zalesskii (1974/93): gave lower bounds for the smallest degree d for $G = G(q), q = p^f$ of Lie type and $l \neq p$. These are given as 'polynomial in q'.
2. Tiep-Zalesskii (1996): Considered the case $l = 0$ and $G = G(q)$ a classical group of Lie type. Gave the smallest d (in some cases also the second and third smallest) and its multiplicity.
3. Lübeck (2001): Considered the case $l = 0$ and $G = G(q)$ an exceptional group of Lie type. Gave the seven smallest degrees and their multiplicities. Also the (few) known results for these G and primes $l \neq p$ are collected.
4. Hiß-Malle (2001): Considered l a prime and $d \leq 250$. Determined all G which occur, except the $G = G(q)$ groups of Lie type in defining characteristic $l = p$.
5. Lübeck (2001): $G = G(q)$, $q = p^f$ group of Lie type and $l = p$: Gave for $r = \text{rank}(G) \geq 12$ all representations of degree $\leq r^3/8$ for type A_r and of degree $\leq r^3$ for the other types of classical groups. Furthermore for $r < 12$ there are longer lists of all such representations of degree smaller some bound, which depends on the type.

The 5-modular character table of the sporadic simple Harada-Norton group

K. Lux

I report on joint work with R. Borcherds, UC Berkeley, and A. Ryba, Queen's College, New York. We have determined all but two of the 5-modular irreducible characters for the Harada-Norton group using theoretical and computational methods. From our results it follows that the degrees of the first 14 Brauer characters, $b_1, \ldots, b_{14}$ in the principal block are

$$1 \quad 133 \quad 626 \quad 2451 \quad 6326 \quad 8152 \quad 9271 \quad 54473 \quad 69255 \quad 84798 \quad 131747$$

$$145275 \quad 170258 \quad 335293.$$

For the last two irreducible Brauer characters in the principal block we get the following explicit bounds, where $a_{15} = 638571$ and $a_{16} = 784379$,

$$a_{15} \leq b_{15} \leq a_{15} + b_7 + b_8$$

and

$$a_{16} \leq b_{16} \leq a_{16} + 2b_2 + b_3 + 2b_7 + b_8.$$

Our method of proof uses the following techniques.

1) Modular character theory.
2) Vertex operator algebras.
3) Condensations of symmetrized powers and direct condensations.

For 3) we used a package for determining condensations of symmetrized powers developed by A. Ryba and a package for calculating direct condensations by F. Lübeck and M. Neunhöffer, both at Lehrstuhl D für Mathematik, RWTH Aachen. We are particularly thankful to M. Neunhöffer, who constructed two direct condensations using the St.Andrews cluster of PCs. For other relevant computations we also relied upon the following software packages: GAP 3 and 4, the C-Meataxe 2.4, and MOC.

Computations arising from Monstrous Moonshine

J. McKay

The objects of interest are the monstrous moonshine functions, $\{f\}$ and their discrete invariance groups, G_f. There is a fascinating interplay between the functions, their groups, analysis, and number theory.

P1 and P2 each characterize the elliptic modular function, $j(z)$, with invariance group $G_j = PSL(2, Z)$, and monstrous normalization

$$j(z) = 1/q + 0 + \sum c_k q^k, \quad k > 0,$$

with $q = e^{2\pi iz}$, $\Im(z) > 0$, ($z \in H$, the upper 1/2-plane).

Replicable functions generalise the j-function:

P1. Under the Hecke operator:

$$\forall n \geq 1,\ n \times T_n(j) = \sum j((az+b)/d) = F_{n,j}(j),$$

where F_n is the Faber polynomial of degree n with coefficients dependent on its argument, thus $F_{2,j}(j) = j^2 - 2c_1$, with $c_1 = 196884$. We characterize the Faber polynomial, and define the Grunsky coefficients, $\{h_{m,n}\}$, by

$$F_{n,f}(f) = 1/q^n + \sum h_{m,n} q^m, \quad m \geq 1.$$

P1 generalizes to replicable functions (Norton) by requiring that $h_{m,n} = h_{r,s}$ if $\gcd(m,n) = \gcd(r,s)$ and $\mathrm{lcm}(m,n) = \mathrm{lcm}(r,s)$. (This is equivalent to the introduction of replication power maps into the Hecke sum.)

P2. Under the Schwarzian (Dedekind 1878):

$$\{z, j\} = R(j) = N(j)/(D(j))^2, \quad \text{with} \quad R(j) = (36j^2 - 41j + 32)/36(j(j-1))^2$$

where Dedekind uses the analytic normalization for j: $1728j(z) = 1/q + 744 + 196884q + \cdots$, for which j takes the values $s_\infty = \infty$, $s_\omega = 0$, $s_i = 1$ at its critical points ($j'(z_i) = 0$, $j(z_i) = s_i$), $\omega = e(\pi i/3)$.

The partial fraction expansion of $R(j)$ makes its choice more apparent. This Schwarzian equation is available for all Hauptmodules. The Hecke and the Schwarzian approach are related.

It is conjectured that replicable functions are either

a) modular functions $f(z) = 1/q + cq$ (including exp, cos, sin) or
b) Normalized Hauptmodules, f, with $\Gamma_0(N) < G_f$, with $\Gamma_0(N) =$ upper-triangular matrices mod N.

We have: McKay-Sebbar (Math. Annalen 2000):

$$\{f, z\}/(4\pi^2) = 1 + 12 \sum m \cdot n \cdot h_{m,n} q^{m+n}, \quad m,\ n \geq 1.$$

When is $\{f, z\}$ holomorphic? Just when G_f has no elliptic fixed points which is when G_f is free and of finite index in $PSL(2, Z)$. Such free, finite index, genus zero, congruence subgroups have been classified (McKay-Sebbar):

There are 33 of these, each described by a dessin d'enfant (which is a coset graph of $PSL(2, Z)$ over G_f).

References: URL: http://www-cicma.concordia.ca/ and follow "Moonshine".

Multiplicity-free permutation representations of the sporadic groups

J. Müller

(joint work with T. Breuer, I. Höhler and M. Neunhöffer)

For the sporadic finite simple groups and their automorphism groups, there are 253 multiplicity-free transitive permutation representations [Breuer-Lux, 1996]. For 249 of them, i. e., currently 4 are missing, we have compiled a database containing: the collapsed adjacency matrices, the character tables of their endomorphism rings, the bijection from these characters to the constituents of the permutation character, and data on the orbital graphs, e. g., the number of the connected components and their diameters.

Hereby, we have built upon earlier work of [Praeger-Soicher, 1997], [Ivanov-Linton-Lux-Saxl-Soicher, 1995], [Norton, 1985], and other people. The database will be made public on the Aachen HomePage http://www.math.rwth-aachen.de/LDfM. The data will be provided in human readable form as well as in GAP-readable form.

The techniques employed encompass a few of the modern powerful tools of computational group and representation theory, e. g., the various condensation techniques. Besides their own interest, one possible application of these data is in algebraic combinatorics. Indeed, quite a few of these orbital graphs are so-called Ramanujan graphs.

Computing in groups of Lie type

S. Murray

(joint work with A. Cohen and D. Taylor)

The groups of Lie type are a vital part of modern mathematics. Examples include reductive Lie groups, reductive algebraic groups and finite groups of Lie type. In this talk I describe a new package within the Magma computer algebra system for computing within these groups. This package uses the Steinberg presentation to represent elements, and uses the Bruhat decomposition to compute a useful normal form for the elements.

I will demonstrate the use of this package for a couple of nontrivial problems. I will also describe new algorithms for converting from a matrix representation for the group to the Steinberg presentation – this algorithm is a generalisation of the LUP algorithm. I will also discuss applications to matrix group recognition.

Orthogonal representations of finite groups

G. Nebe

Let G be a finite group and V a $\mathbb{Q}G$-module. Then V is uniquely determined by its character χ_V. On the other hand, given V, one can easily calculate the G-invariant quadratic forms

$$\mathcal{F} = \{F : V \times V \to \mathbb{Q} \mid F \text{ symmetric, bilinear, and } G\text{-invariant}\}.$$

So in principle χ_V also determines $\mathcal{F}(V)$.

I present a character theoretic trick, that uses Clifford algebras to calculate rational invariants of the elements in $\mathcal{F}(V)$.

To a pair $\varphi = (V, F)$ with $F \in \mathcal{F}(V)$ non-degenerate, one can functorially attach a central simple $\mathbb{Q}$-algebra $c(\varphi)$. Since G acts on φ as isometries, it acts on $c(\varphi)$ as $\mathbb{Q}$-algebra automorphisms. Therefore the simple $c(\varphi)$-module W becomes a projective $\mathbb{Q}G$-module of which the character $\chi_W = \sqrt{\chi_{c(\varphi)}}$ is a certain square root of the character $\chi_{c(\varphi)}$.

Each constituent of χ_W with odd multiplicity can be used to determine either the Hasse invariant (i.e. the class of $c(\varphi)$ in $\mathrm{Br}(\mathbb{Q})$ of φ if n is odd, or the determinant of φ if n is even).

Statistical studies of standard structures

P. Neumann

The standard structures of this lecture were classical groups defined over a finite field F; that is, groups G such that $SL(n,q) \leq G \leq GL(n,q)$, $SU(n,q) \leq G \leq GU(n,q)$, $Sp(2m,q) \leq G \leq GSp(2m,q)$, $SO(2m+1,q) \leq G \leq GO(2m+1,q)$, or $\Omega^{\pm}(2m,q) \leq G \leq GO^{\pm}(2m,q)$. The study-worthy statistics were of the form $Prob[X \in G$ has property $\mathcal{P}]$, where $\mathcal{P}$ was any of being eigenvalue-free (in the sense that there are no eigenvalues in the field F), having eigenvalue-free exterior square, being cyclic, having cyclic exterior square, being regular, being semisimple. Here probability is simply the notion of frequency, that is, the proportion of elements of the group with the given property. Many of the studies of these statistics were originally motivated by applications to the design and analysis of matrix-group algorithms.

Recent results by Neumann & Praeger [1996], G E Wall [2000], Fulman [2000], Fulman & Neumann & Praeger [200x], Guralnick & Lübeck [2001], Brydon [200y], Britnell [200z] were surveyed. Mention was made of the methods – some of the theorems were proved in combinatorial/geometric ways, others by use of cycle indices and/or generating functions.

The lecture ended with two mysterious problems (which have little to do with computational group theory).

Problem 1. Define $c_G(\infty,q) := \lim_{n\to\infty} \mathrm{Prob}[X \in G \text{ is cyclic}]$. Are $c_U(\infty,q)$, $c_{Sp}(\infty,q)$, $c_O(\infty,q)$, and $c_{O^{\pm}}(\infty,q)$ rational functions of q?

This is motivated by the remarkable observation made independently by Wall and Fulman that $c_{GL}(\infty,q) = (1-q^{-5})/(1+q^{-3})$.

Problem 2. One of the Rogers-Ramanujan identities can be cast in the form

$$1 + \sum_{n=1}^{\infty} |GL(n,q)|^{-1} = \prod_{r \equiv \pm 1 \pmod 5} (1-q^{-r})^{-1}.$$

Are there analogous product expansions for

$$1 + \sum_{n=1}^{\infty} |U(n,q)|^{-1}, \quad 1 + \sum_{m=1}^{\infty} |Sp(2m,q)|^{-1}$$

and

$$1 + \sum_{m=1}^{\infty} (|O^{+}(2m,q)|^{-1} + |O^{-}(2m,q)|^{-1})|\,?$$

This is motivated by an observation of Fulman, who uses the quoted Rogers-Ramanujan identity to prove a product formula for $\lim_{n\to\infty} \mathrm{Prob}[X \in GL(n,q) \text{ is semisimple}]$.

Enumerating very large orbits

M. Neunhöffer

Let G be a finite group, F a field, FG the group algebra, $K < G$ a subgroup such that the characteristic of F does not divide $|K|$, and $e := 1/|K| \cdot \sum_{k \in K} k \in FG$. Then e is an idempotent. Therefore $P \mapsto Pe$ is an exact functor from the category of right FG-modules to the category of right $eFGe$-modules. We call this **fixed point condensation**, because $Pe = \{x \in P \mid xk = x \ \forall k \in K\}$.

In the case where Ω is a transitive G-set and $P := F\Omega$ is the permutation module with basis Ω one can describe the action of an element $ege \in eFGe$ on Pe explicitly in terms of the numbers $|\omega K \cap \omega' Kg|$ for any two K-orbits ωK and $\omega' K$ in Ω. Therefore we want to enumerate very large orbits and count the elements in these intersections.

In this talk I present an idea of F. Lübeck and me ([1]) which helps to condense very large permutation modules. J. Müller, F. Röhr, R. Wilson and I for example used this for an orbit Ω of the sporadic simple Lyons group which consists of 1,113,229,656 subspaces of dimension 10 within a simple module of dimension 111 over $GF(5)$ ([2]). In our case the condensation group K had 362,880 elements and the condensed module had dimension 3,207. This computation was done on a workstation cluster in St. Andrews with 50 machines in 13 hours of wallclock time. The result was used to complete the information in [3] on the Brauer trees for the Lyons group in characteristics 37 and 67.

References:

[1] Frank Lübeck and Max Neunhöffer. Enumerating Large Orbits and Direct Condensation. *Experimental Mathematics*, **10:2** (2001), p. 197–205.

[2] Jürgen Müller, Max Neunhöffer, Frank Röhr, and Robert Wilson. Completing the Brauer Trees for the Sporadic Simple Lyons Group. Submitted.

[3] Gerhard Hiß and Klaus Lux. *Brauer trees of Sporadic Groups.* Clarendon Press, Oxford, 1989.

Matrix representations for polycyclic groups

W. Nickel

A well known theorem conjectured by P. Hall and proved by L. Auslander asserts that every polycyclic group can be embedded into $GL(n, \mathbb{Z})$ for some n. In the lecture, an algorithm for the more special case of constructing such an embedding for a finitely generated torsion-free nilpotent group H was explained. A computer implementation of this algorithm exists in the GAP 4 package *polycyclic*.

The algorithm works upwards along a central poly-C_∞ series of H. Each element of H can be written as a normal word in a generating sequence arising from the series. The exponents in the product of two normal words are polynomials in the exponents of the two factors by a result of P. Hall's. These polynomials are used to construct a faithful $\mathbb{Z}H$-submodule of $\mathbb{Z}H^*$ of finite $\mathbb{Z}$-rank consisting of polynomials.

The approach can be extended to the construction of faithful matrix representations over $\mathbb{Z}$ for polycyclic nilpotent-by-free-abelian groups.

Recognising finite alternating and symmetric groups

A. Niemeyer and C. Praeger

(joint work with R. Beals, C. Leedham-Green and Á. Seress)

Given a generating set X for a (black-box or matrix) group G we address the problem of deciding whether G is isomorphic to A_n or S_n, and if it is, we further address the problem of constructing an isomorphism for efficient computation in G. Polynomial-time Las Vegas algorithms were constructed for doing this by Beals and Babai (1993) and Morje in his PhD thesis (1995; student of Kantor and Seress). A faster Las Vegas algorithm that runs in time $O(n \log^2 n(\xi + n\mu))$ was given by Bratus and Pak in 2000. (Here ξ is the cost of one random element and μ is the cost of one group operation.) However the Bratus/Pak algorithm relies on the Extended Goldbach Conjecture or a variant of it.

A new Las Vegas algorithm was constructed by the speakers and colleagues for black-box groups that runs in $O(n \log n(\xi + \mu))$ time. It relies heavily on the statistical distribution of certain elements of S_n to construct an n-cycle. We also explore algorithms for recognising constructively A_n and S_n as matrix groups in their smallest dimensional faithful matrix representation which avoid the construction of n-cycles and more quickly find a 3-cycle in A_n. The cost is reduced to $O(n^{1/3} \log n(\xi + \mu))$. This work was initiated by intense discussions of the speakers and their colleagues at the Computational Groups Week at Oberwolfach in 1997.

Matrix group recognition following Aschbacher

E. O'Brien

The matrix group "recognition" project was initially motivated by the desire to develop useful algorithms to study the structure of matrix groups defined over finite fields.

One strand of it relies heavily on Aschbacher's theorem about the (maximal) subgroup structure of $\mathrm{GL}(d, q)$: either the group G has a normal subgroup N which reflects the geometry of the group, or G is almost simple modulo scalars.

In this talk I surveyed the status of recognition following Aschbacher. Considerable progress has been made on the first 8 categories of Aschbacher. We are currently able to "name" the composition factors of many groups in the final category. This ability relies on work of Babai et al. and many others.

I also discussed the construction of a composition tree which allows us to obtain the composition factors of a matrix group. It relies on the use of Schreier-Todd-Coxeter-Sims to provide a useful description for the almost simple groups. This can later to be modified to use other "constructive" or sporadic group recognition techniques.

I also discussed the construction of a finite presentation for the matrix group, which allows confirmation of the composition tree.

Finally I highlighted the significant outstanding problem: constructive recognition for groups of Lie type.

Conjugacy Graphs of Finite Coxeter Groups

G. Pfeiffer

Let W be a finite Coxeter group, generated by a set $S \subseteq W$ of simple reflections, and assume that W acts on a set X. Then this action gives rise to a graph with vertices $x, y \in X$ and labeled edges $x \overset{s}{—} y$ whenever $x.s = y$ $(s \in S)$. Sometimes this graph can be viewed in a natural way as a directed graph with respect to the length function on W. In this talk I discussed the graph that arises from the action of W on itself by conjugation, where the edges are chosen to point to the shorter of their end points. This graph plays an important role in the computation of character values for the Iwahori-Hecke algebra associated to W. Results were presented for classes of involutions and cuspidal classes (i.e., classes that don't intersect with proper parabolic subgroups of W). Examples of interesting graphs were displayed.

A graphical Reidemeister-Schreier method

S. Rees

A graphical interpretation of the Todd-Coxeter algorithm has been described by John Stallings. In a recent preprint, Jon McCammond and Dani Wise extend Stallings' viewpoint from graphs to 2-dimensional cell complexes and develop a theory which proves the existence of finite presentations for some finitely generated subgroups of finitely presented groups, and in special cases gives a terminating algorithm to construct them. My student Oliver Payne is developing this theory into a procedure which can be applied to a wider range of groups.

Some questions about the derived series of p-groups

C. Schneider

It was known already to Burnside that a non-abelian p-group has order at least p^3, while a non-metabelian group has order at least p^6. Generally, however, we do not know what is the smallest among the orders of finite p-groups with a given soluble length. This problem has recently been settled for soluble length 4, but we still do not know the answer for soluble length 5. A related problem is to find a sharp lower bound for the index of a term of the derived series of a finite p-group in the preceding one. This problem is unsettled even for the third derived subgroup.

I briefly discussed these problems pointing out the relevance of computational group theory to their solution.

The Knuth-Bendix Procedure for Strings and Large Rewriting Systems

C. Sims

The Knuth-Bendix procedure for strings is an important tool for studying finitely presented groups. It has recently been used to reduce dramatically the upper bound on the number of sixth powers needed to define the Burnside group $B(2, 6)$. The author has rewritten his implementation of the Knuth-Bendix procedure to take advantage of large memory, both internal and external. New index structures to facilitate the formation of overlaps of left sides of rewriting rules have greatly improved the program's efficiency.

Soluble Radicals in Permutation and Matrix Groups

W. Unger

A number of effective permutation group algorithms follow the plan: (1) find $O_\infty(G)$ and a representation of the quotient $Q = G/O_\infty(G)$; (2) solve "the problem" in Q; (3) extend to all of G. In this talk I presented an algorithm to find $O_\infty(G)$ and Q for a permutation group. This is based on the lemma: if f and g are two homomorphisms with domain G and $\ker f \cap \ker g$ is soluble then $O_\infty(G) = g^{-1}(O_\infty(f^{-1}(O_\infty(f(G)))))$. This lemma may also be used to find the soluble radical of a low degree matrix group with a given base and strong generating set.

Computing p-cores in black box groups

R. Wilson

Black box groups are a useful abstraction for investigating complexity of algorithms for computing (especially) with finite groups of matrices. Many computations can be done in Monte Carlo polynomial time, including recognising (i.e. naming) a simple group if it is known in advance to be simple. The main obstruction to recognising simple groups among all black box groups is the difficulty in distinguishing (in Monte Carlo polynomial time) between a simple group S, of Lie type in characteristic p, and a non-simple group G with $G/O_p(G) \cong S$. In joint work with Chris Parker (in progress), we solve this problem for p odd, by a recursive procedure involving computing involution centralizers. The case $p = 2$ remains intractable, as there is no known Monte Carlo polynomial time algorithm for finding an involution in a black box Lie type group over a large field of characteristic 2.

Edited by Csaba Schneider

Participants

Laurent Bartholdi
Department of Mathematics
Evans Hall
Berkeley, CA 94720-3840, USA
Email: laurent@math.berkeley.edu

Gilbert Baumslag
Department of Mathematics
The City College of New York
Convent Avenue at 138th Street
New York, NY 10031, USA
Email: gilbert@
groups.sci.ccny.cuny.edu

Anton Betten
Department of Mathematics and Statistics
The University of Western Australia
35 Stirling Highway, Crawley 6009
Western Australia
Email: anton@maths.uwa.edu.au

Peter A. Brooksbank
Department of Mathematics
University of Oregon
Eugene, OR 97403-1222, USA
Email: brooks@geometry.uoregon.edu

Andrea Caranti
Dipartimento di Matematica
Universita di Trento
Via Sommarive 14
38050 Povo (Trento), Italy
Email: caranti@science.unitn.it

Jon F. Carlson
Department of Mathematics
University of Georgia
Athens, GA 30602-7403, USA
Email: jfc@sloth.math.uga.edu

Gene Cooperman
College of Computer Science
Northeastern University
215 Cullinane Hall
Boston, MA 02115, USA
Email: gene@ccs.neu.edu

Bettina Eick
Institut für Geometrie
TU Braunschweig
Pockelstraße 14
38106 Braunschweig, Germany
Email: beick@tu-bs.de

Maria Asun García-Sánchez
Departamento de Matemáticas-Matematika Saila
Facultad de Ciencias-Zientzi Fakultatea
Universidad del País Vasco-Euskal Herriko Unibertsitatea
Apdo. 644, 48080-Bilbao, Spain
Email: mtpgasam@lg.ehu.es

Meinolf Geck
Departement de Mathematiques
Universite Claude Bernard de Lyon I
LAN Bat. 101
43, Bd. du 11 Novembre 1918
69622 Villeurbanne Cedex, France
Email: geck@desargues.univ-lyon1.fr

Willem A. de Graaf
Mathematisch Instituut
Universiteit Utrecht
PO Box 80010
3508 TA Utrecht, The Netherlands
Email: graaf@math.uu.nl

George Havas
Centre for Discrete Mathematics and Computing
School of Computer Science and Electrical Engineering
The University of Queensland
Queensland 4072, Australia
Email: havas@csee.uq.edu.au

Gerhard Hiß
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen, Germany
Email: Gerhard.Hiss@math.rwth-aachen.de

Burkhard Höfling
Mathematisches Institut
Universität Jena
Ernst-Abbe-Platz 1-4
07740 Jena, Germany
Email: burkhard.hoefling@minet.uni-jena.de

Derek F. Holt
Mathematics Institute
University of Warwick
Gibbet Hill Road
Coventry, CV4 7AL, United Kingdom
Email: dfh@maths.warwick.ac.uk

William M. Kantor
Deptartment of Mathematics
University of Oregon
Eugene, OR 97403-1222, USA
Email: kantor@math.uoregon.edu

Gregor Kemper
IWR
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg, Germany
Email: Gregor.Kemper@iwr.uni-heidelberg.de

Adalbert Kerber
Fakultät für Mathematik und Physik
Universität Bayreuth
95440 Bayreuth, Germany
Email: kerber@uni-bayreuth.de

Charles R. Leedham-Green
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London, E1 4NS United Kingdom
Email: crlg@maths.qmul.ac.uk

Stephen Linton
School of Computer Science
University of St. Andrews
North Haugh
St. Andrews, Fife, KY16 9SS United Kingdom
Email: sal@dcs.st-and.ac.uk

Frank Lübeck
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen, Germany
Email: frank.luebeck@math.rwth-aachen.de

Eugene M. Luks
Deptartment of Computer and Information Science
University of Oregon
Eugene, OR 97403, USA
Email: luks@cs.uoregon.edu

Klaus Lux
Deptartment of Mathematics
University of Arizona
Tucson, AZ 85721, USA
Email: klux@math.arizona.edu

John McKay
Department of Computer Science
Concordia University
1455 de Maisonneuve Blvd. West
Montreal, Quebec H3G 1M8, Canada
Email: mckay@cs.concordia.ca

Jürgen Müller
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52056 Aachen, Germany
Email: `mueller@math.rwth-aachen.de`

Scott Murray
Faculteit Wiskunde en Informatica
Technische Universiteit Eindhoven
Postbus 513, 5600 MB Eindhoven
The Netherlands
Email: `murray@maths.usyd.edu.au`

Gabriele Nebe
Abteilung Reine Mathematik
Universität Ulm
89069 Ulm, Germany
Email: `gabi@mathematik.uni-ulm.de`

Joachim Neubüser
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen, Germany
Email: `neubueser@math.rwth-aachen.de`

Peter M. Neumann
Queen's College
Oxford OX1 4AW, United Kingdom
Email: `peter.neumann@queens.ox.ac.uk`

Max Neunhöffer
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen, Germany
Email: `max.neunhoeffer@math.rwth-aachen.de`

M. F. Newman
School of Mathematical Sciences
The Australian National University
Canberra, ACT 0200, Australia
Email: `newman@maths.anu.edu.au`

Werner Nickel
Fachbereich Mathematik
TU Darmstadt
Schlogartenstr. 7
64289 Darmstadt, Germany
Email: `nickel@mathematik.tu-darmstadt.de`

Alice Niemeyer
Deptartment of Mathematics and Statistics
The University of Western Australia
35 Stirling Highway, Crawley 6009
Western Australia
Email: `alice@maths.uwa.edu.au`

Eamonn A. O'Brien
Department of Mathematics
The University of Auckland
Private Bag 92019
Auckland, New Zealand
Email: `obrien@math.auckland.ac.nz`

Gretchen Ostheimer
Department of Computer Science
Hofstra University
207 B Adams Hall
Hempstead, NY 11549, USA
Email: `cscgzo@magic.hofstra.edu`

Herbert Pahlings
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen, Germany
Email: `pahlings@math.rwth-aachen.de`

Richard A. Parker
39 Harvey Goodwin Avenue
Cambridge CB4 3EX, United Kingdom
Email: `richard@ukonline.co.uk`

Götz Pfeiffer
Department of Mathematics
NUI Galway
Galway, Ireland
Email: `goetz.pfeiffer@nuigalway.ie`

Wilhelm Plesken
Lehrstuhl B für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen Germany
Email: plesken@willi.math.rwth-aachen.de

Cheryl E. Praeger
Department of Mathematics and Statistics
The University of Western Australia
35 Stirling Highway, Crawley 6009
Western Australia
Email: praeger@maths.uwa.edu.au

Sarah Rees
Deptartment of Mathematics and Statistics
The University of Newcastle
Newcastle-upon-Tyne,
NE1 7RU United Kingdom
Email: sarah.rees@ncl.ac.uk

Edmund F. Robertson
Deptartment of Pure Mathematics
University of St. Andrews
North Haugh
St. Andrews, Fife, KY16 9SS United Kingdom
Email: edmund@dcs.st-and.ac.uk

Csaba Schneider
Department of Mathematics and Statistics
University of Western Australia
35 Stirling Highway, Crawley 6009
Western Australia
Email: csaba@maths.uwa.edu.au

Ákos Seress
Department of Mathematics
Ohio State University
231 West 18th Avenue
Columbus, OH 43210-1174, USA
Email: akos@math.ohio-state.edu

Charles C. Sims
Deptartment of Mathematics
Rutgers University
110 Frelinghuysen Rd
Piscataway, NJ 08854-8019, USA
Email: sims@math.rutgers.edu

Leonard H. Soicher
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London, E1 4NS United Kingdom
Email: L.H.Soicher@qmul.ac.uk

William R. Unger
School of Mathematics and Statistics
The University of Sydney
Sydney, NSW 2006, Australia
Email: billu@maths.usyd.edu.au

Robert A. Wilson
School of Mathematics and Statistics
The University of Birmingham
Edgbaston
Birmingham B15 2TT, United Kingdom
Email: R.A.Wilson@bham.ac.uk

Charles R. B. Wright
Deptartment of Mathematics
University of Oregon
Eugene, OR 97403-1222, USA
Email: wright@math.uoregon.edu