MATEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Tagungsbericht Nr. 21

Computational Group Theory
1.6 – 7.6.1997

This meeting was the third on Computational Group Theory held at the Mathematisches Forschungsinstitut Oberwolfach. The meeting was attended by 49 participants from 11 countries.

A considerable number of presentations were related to the continuing matrix group recognition project. This project was initiated by the question raised by J. Neubüser, at the first meeting on Computational Group Theory held at MFO in 1988, of how to recognise special linear groups giving generating matrices. From this starting point the project has now reached a stage where, for significantly large degrees over reasonable sized fields, not only can the special linear group be recognised, but also a composition series can be computed for any matrix group over a finite field. An informal session was organized on Tuesday afternoon for the people working in this area to coordinate their future activities.

Other topics covered included more traditional topics in the study of linear representations of groups, methods for studying finitely presented groups and their applications, new methods for studying groups given by polycyclic presentations and improvements for methods for studying permutation groups. Furthermore methods and developments in Lie algebras, groups and combinatorics, semigroups or monstrous moonshine were reported. Some of the talks included status reports on software packages, e.g. ELIAS, CARAT, GRAPE, SYMMETRICA, MONOID, CHEVIE and GAP.

A particular stimulus for computational group theory has always been its application to special, seemingly intractable problems. Some highlights in this area presented during the conference were the completion of the character table of the Iwahori-Hecke algebra of type E_8 and the explicit construction of generators for the Monster group. The Monster had been the only sporadic simple group for which no computer construction was known. Now explicit calculations with certain elements are possible.

In order to allow adequate time for informal discussion (sometimes at computer terminals to access implementations of algorithms), the 'formal' program included, as well as the traditional invited and offered talks, both 'posters' (in the form of extended abstracts of no more than four pages) and 'five-minute' talks. Both methods proved to be effective and the people who used them deserve special commendation for the care they put into their presentations.

Beside the talks there was a lot of discussion on possible new algorithms and implementations and on ways of improving existing algorithms and implementations.

The meeting showed there has been considerable progress since the last meeting and gave the feeling that the field is in a lively stage and good progress can be expected. We were particularly pleased that a significant number of younger mathematicians could take part in the meeting and become more closely integrated into a wider group of colleagues in the field.

Organisers:
M.F. Newman, Canberra
H. Pahlings, Aachen
This report was compiled by B. Eick

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Charles R. Leedham-Green
Recognising matrix groups

We now have a first version of the complete matrix group recognition algorithm. Let $G \leq GL(d,q)$. A famous theorem of Aschbacher implies that G lies in at least one of nine categories. (Two of these we sub-divide, so the number of categories is now eleven.) One of these eleven categories consists of the unipotent groups, one consists of classical groups in their natural representations, and one (C_q) consists of other almost simple groups (modulo scalars). These three categories are *terminal*. If G lies in any other category, there is a natural homomorphism of G onto a non-trivial group H, where H is either given as a subgroup of $GL(d',q')$ where $d > d'$ or $d = d'$ and $q > q'$, or H is given as a subgroup of the symmetric group of degree n for some $n \leq d$, or H is cyclic.

The first step in the project was to recognise an Aschbacher category in which G lies, and to construct the corresponding homomorphism, if the category is not terminal. This step has now been completed, except that the symplectic p-group case is still in an unsatisfactory state, and some other cases have no complexity analysis and may fail, through lack of resources, in bad cases. Generally speaking we hope to succeed for $d, q \leq 100$, and may succeed in much larger cases. For example the Niemeyer - Praeger non-constructive classical groups recognition algorithm runs in MAGMA for $SL(5000,2)$ in a few hours.

The second step is to use our ability to determine Aschbacher categories to analyse an arbitrary subgroup $G = \langle X \rangle$ of $GL(d,q)$, given X. We use a binary tree structure, generalizing the concept of a composition series. The leaves L in the tree correspond to classical groups, C_q-groups, p-groups, subgroups of permutation groups of modest degree, and cyclic groups. We have two fundamental problems:

FP1; given any $g \in L$ and generating set $Y \subseteq L$, write g as word in Y.

FP2; produce a presentation for L on Y.

If we can solve FP1 for each leaf of the tree we have a Monte-Carlo algorithm to construct the tree.

If we can solve FP2 for each leaf of the tree we can verify the result, thus making the whole algorithm Las Vegas.

Our fundamental data structure is in effect used also for permutation groups. The hope is that this will lead to a merging of the matrix and permutation group projects.

This is a joint work with many people. My student Anthony Pye has produced a first version of the complete algorithm. Celler, Holt, Niemeyer, O'Brien, Praeger and Pye are responsible (with myself) for most of the major ingredients. Known permutation representations of large sporadic groups, R. Wilson's standard generators, and the exciting work reported on at this conference on black box recognition of classical groups need to be added to our package.

Robert Beals
On black-box methods for matrix groups

In this talk we sketched several ideas from the theory of black-box group algorithms which may have practical significance in Charles Leedham-Green's recognition project. The task of finding elements of proper normal subgroups is of particular importance, both in theory and in practice. We gave two methods to help achieve this goal.

The first is a *normal still*. We show how to distill a list of group elements, with the property that at least one lies in a normal subgroup, down to a single element which lies in a proper normal subgroup. This uses a small number of group operations per element of the list: typically constant, and $\log |G|$ in the worst case.

The second is a very general method for finding elements of a proper normal subgroup. If we have gone to the effort of verifying that a black-box group G is not isomorphic to a particular group T, then a small amount of bookkeeping suffices to produce an element of a proper normal subgroup if T is a homomorphic image of G. The list of T for which good isomorphism tests exist includes A_n and S_n [Beals & Babai'93, Beals & Seress, Leedham-Green & Niemeyer & Praeger], as well as all classical groups over small fields [Cooperman & Finkelstein & Linton, Bratus, Kantor & Seress].

We hope that these ideas will prove useful in matrix group computations.

Gene Cooperman

Reduction of Center and Other Problems to Matrix Recognition or Matrix Group Order

This talk is motivated by a recent challenge problem of Peter Neumann. A result was recently announced that reduces the problem of finding the kernel of a matrix group homomorphism to any of: matrix group recognition, group order, or certain other decision problems [1]. Eight years earlier a result was announced reducing center, centralizer of a normal subgroup (a key ingredient in many socle algorithms) and certain other problems to that of finding a kernel [2]. The ongoing matrix recognition project promises matrix recognition, matrix group order, and certain other decision problems [3]. The composition of these results yields surprising conclusions about the ease of doing center, socle and other problems for matrix groups. I acknowledge discussions with Eugene Luks that contributed to these ideas.
[1] R. Beals, "Towards Polynomial-Time Algorithms for Matrix Groups", *Proc. of DIMACS Workshop on Groups and Computation II* **28**, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, L. Finkelstein and W.M. Kantor (eds.), AMS, Providence, RI, 1997. [2] G. Cooperman, L. Finkelstein, and E. Luks, "Reduction of Group Constructions to Point Stabilizers", *Proc. of 1989 International Symposium on Symbolic and Algebraic Computation*, ACM Press, 1989, pp. 351–356. [3] talks by F. Celler, C. Leedham-Green, E. O'Brien et al.

Alice Niemeyer

Recognizing the full symmetric group as a black box group

Let $G = \langle X \rangle$ be a finite group given as a black box group. We describe an algorithm which determines whether or not G is isomorphic to S_n for a given integer n. This algorithm works in two steps. In the first step we attempt to construct a homomorphism from S_n into G by finding appropriate images for the generators $(1,2)$ and $(1,2,\ldots,n)$. We seek suitable elements of G for these images by random selection. To do this we first determine for such elements defining properties which can be checked in a black box group G. We also design procedures for finding such elements and checking these properties. (For example as the proportion of transpositions in $G \cong S_n$ is small we construct a transposition from a "pretransposition" in G which we define as an element f of order $2t$ with $t > 1$ and t odd, such that $h = f^t$ has the property that $o(hh^x) \in \{1,2,3\}$ for all $x \in G$.) We give complexity analyses of these procedures: since they depend on random selection, our analyses depend on the proportions of elements of S_n with relevant properties. We give estimates of these proportions, and thereby give and estimate for the probability that the algorithm will fail to identify, for a black box group $G \cong S_n$, that G really is S_n. In a second step we decide whether the homomorphism is onto by constructing preimages for each generator $x \in X$. This method also relies on random selection and again we can estimate the probability of failure if G is isomorphic to S_n.

Peter Neumann

On tensor factorisation problems

There are several contexts in which a tensor product makes good sense: for example

(1) the tensor product of modules;

(2) the Kronecker product of matrices;

(3) if $x(t)$, $y(t)$ are monic polynomials then $(x \otimes y)(t)$ may be defined to be $\prod(t - \xi_i\eta_j)$ where $x(t) = \prod(t - \xi_i)$ and $y(t) = \prod(t - \eta_j)$;

(4) if x, y are multisets from an abelian group (or even a commutative semigroup) A then we may define $x \otimes y := \{x_i y_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s\}$, where $x = \{x_j, \ldots, x_r\}$ and $y = \{y_1, \ldots, y_s\}$;

(5) if Γ, Δ are G-sets for a given group G then $\Gamma \times \Delta$ is the ordinary cartesian product.

Similarly, there are exterior square constructions in each of these contexts.
Each tensor product has an algorithmic "Tensor Factorisation Problem" associated with it; each exterior square has an associated "Exterior Square Root Problem". The problems are connected (though in some

cases quite loosely). To tensor factorise a G-module it helps to be able to factorise matrices; to factorise a matrix it helps to be able to factorise its characteristic polynomial; to factorise a polynomial it helps to be able to factorise the multiset of its roots; factorising the multiset of its roots can be assisted by considering G-sets where G is the Galois group.

In this lecture the algorithmic problems were posed and what little I know about attempts to solve them was surveyed: the module decomposition problem has been tackled with some success for smallish dimensions or smallish groups by Leedham-Green & O'Brien [1997]; the exterior-square root problem for multisets and matrices has been treated by Catherine Greenhill in her Oxford D.Phil. dissertation [1996]; the "exterior square root problem" for G-sets (though that is perhaps not a good name in this context) has been tackled by Graham Sharp [1997] and his preprint will form part of his Oxford D.Phil. thesis; work in progress by Cheryl Praeger and me gives a very promising approach to the tensor factorisation problem for multisets, with applications to polynomials, to matrices and to modules. The final part of the lecture contained a sketch of our ideas.

Eamonn A. O'Brien

Implementing matrix group algorithms

The matrix group recognition project seeks to recognise matrix groups defined over finite fields. In my lecture, I reported on the contents of a new share package for the GAP system, which seeks to provide comprehensive and integrated access to implementations of algorithms developed as part of the project.

I then discussed the SMASH algorithm, which decides whether a given matrix group preserves certain decompositions of the underlying vector space with respect to a normal subgroup, and discussed finding elements of a normal subgroup.

I described the Product Replacement algorithm for constructing random elements of a group.

Finally I presented two algorithms for constructing "large" p-local subgroups of a matrix group.

Jon F. Carlson

Homological Algebra and Computers

This lecture is a survey of some of the efforts to construct module theory applications of computer technology for finite dimensional algebras. The main problems that must be solved in any such system are the lifting of homomorphisms from projective modules and the creation of the kernel of a homomorphism. Earlier work on these problems was aimed at the calculation of the mod-p cohomology of p-groups. The methods have now been extended to work on more general local algebras.

It seems possible that the same techniques can be adapted to work on any algebra which is expressed as a basic algebra. The main idea is that such an algebra should be expressed as the collection of its nonisomorphic projective modules. Each projective module should come equiped with a tree which associates a basis for the module with monomials in the generators of the radical. That is, an algorithm for the solution to the homomorphism lifting problem should be encoded in the definition of the algebra. The package for handling the algebras needs only a function for reading the tree. This technique would provide a matrix theoretic implementation which would be alternative to the noncommutative Groebner basis approach that has been suggested by others.

Jean Michel

Application of the CHEVIE package of GAP: Determination of the character table of the Hecke-Iwahori algebra of type E_8

(Joint work with M. Geck)

The determination of the character table of the Iwahori-Hecke algebra of type E_8 (an algebra of dimension 696729600) was considered an untractable problem. In the talk I explained how this problem was solved using some theoretical advances prompted by experimentation using the GAP package CHEVIE (Co-authored by M. Geck, G. Hiss, F. Lübeck, G. Malle, G. Pfeiffer and myself).

The main new tool is a property of elements of minimal length in a conjugacy class, lifted to the braid group. Let W be a Coxeter group, let B be the corresponding Artin-Tits braid group. The natural projection $p : B \to W$ has a section B^+_{red} consisting of those elements of the braid monoid which have same length as their image in W. For $w \in W$ let $\mathbf{w}$ be its lift in B^+_{red}; let S be the Coxeter generating set of W and for $I \subset S$ let W_I be the corresponding parabolic subgroup of W, and let w_I be the longest element of W_I (in particular we denote by w_S the longest element of W). Then

Theorem. *In any conjugacy class C of W, there exists an element w of minimal length in C such that the equality $\mathbf{w}^d = \mathbf{w}_{I_1}^{n_1} \dots \mathbf{w}_{I_k}^{n_k}$ holds in B, where d is the order of w, where n_i are even natural integers and where $I_1 \supset \dots \supset I_k$ is a strictly decreasing sequence of subsets of S.*

As a corollary, when w is of minimal length in its class, we can compute the absolute value of the eigenvalues of the basis element T_w of the Hecke algebra $H(W, q)$ in any irreducible representation; these absolute values turn out to be fractional powers of q, which answers a long-standing conjecture in the particular case of elements of minimal length in their class. Using this, we reduce the problem of computing character values to that of solving a system of linear equations. To get enough equations so that the system becomes determined, we need to appeal to quite a few properties of Hecke algebras, in particular to the work of M.Geck on modular representations of Hecke algebras.

Frank Lübeck

Parameterization of semisimple conjugacy classes in finite groups of Lie type

This talk addressed a part of a bigger project of computing generic character tables for series of finite groups of Lie type. Examples for such series are sets of groups like $\{\mathrm{GL}_4(q)\}$ or $\{\mathrm{E}_7(q)_{sc}\}$, where q runs over all prime powers.

Clearly the first steps are to find parameterizations of the conjugacy classes and the irreducible characters. For both there is a ***Jordan decomposition*** which divides the problem into two parts: First find the classes of ***semisimple elements*** of the group, respectively dual group, and then parameterize the classes of ***unipotent elements***, respectively the ***unipotent characters***, of the centralizers of semisimple elements. It turns out that finding the semisimple conjugacy classes is a computationally challenging part of the project.

This talk wanted to give an idea how this problem can be reformulated in a combinatorial setting using the ***root datum*** describing a connected reductive algebraic group, the associated Weyl group and the operation of a Frobenius morphism on these structures. In this reformulation it can be solved by computer programs. It was pointed out that general algorithms for permutation groups are a very useful tool in these programs.

An implementation of the algorithm and some examples were mentioned.

Klaus Lux

Group Algebras and Morita Equivalence

Let F be a field and let A be a finite-dimensional F-algebra. If $e \in A$ is a nontrivial idempotent, then multiplication by e induces a functor from the module category of right A-modules RMod(A) to the category RMod(eAe). This functor defines a categorical equivalence also called a **Morita equivalence** if and only if Se is nonzero for all simple A-modules S. The functor can be used for reducing certain properties of a module V in RMod(A) to the corresponding properties of Ve. For example, it preserves the property of a module being projective, simple etc., and hence can be used to determine the socle series of a projective indecomposable A-module.

Even though it is difficult to find a suitable idempotent for a given algebra A, in case of the group algebra FG of a finite group G we can proceed as follows. Let H be a subgroup of G whose order is coprime to the characteristic of F, then $e_H = \frac{1}{|H|}\sum_{h \in H} h$ is a nontrivial idempotent.

For the sporadic simple groups of order at most 10^9 and small primes p, I have determined a suitable subgroup H of largest order such that the principal blocks of F_pG and $e_H F_p G e_H$ are Morita equivalent. This has been achieved using a character theoretic reformulation of the condition above and the computer algebra system GAP, especially its library of tables of marks for simple groups.

For most of the cases above I have also determined a generating system for the algebra $e_H F_p G e_H$. As a consequence one can now use the above functor explicitly in studying modules in the principal block

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

of FG. For example, in case of the sporadic simple group J_3 and $p = 3$ it was possible to determine the socle series of all projective indecomposable modules in the principal block, the largest module being of dimension 67554. Furthermore, a student in Aachen, S. Weiss, has applied the functor in order to determine a presentation of the basic algebra of the principal block as a quotient of a quiver with relations for some sporadic simple groups.

It is well known that there is an even more general functorial relationship between algebras which runs as follows. If M is an A-module then we can define the functor $\mathrm{Hom}(M,-)\colon \mathrm{RMod}(A) \to \mathrm{RMod}(\mathrm{End}_A(M))$ which takes $V \in \mathrm{RMod}(A)$ to $\mathrm{Hom}_A(M,V)$. Setting M to be eA we can in principle recover the above situation. Given a subgroup $H \leq G$ and the transitive $\mathbb{Z}G$-permutation module $(\sum_{h\in H} h)\mathbb{Z}G$, we can explicitly determine the action of the elements $|H|_p e_H g e_H \in \mathrm{End}_{\mathbb{Z}G}((\sum_{h\in H} h)\mathbb{Z}G)$ on $\mathrm{Hom}_{\mathbb{Z}G}((\sum_{h\in H} h)\mathbb{Z}G, V)$ for a given $\mathbb{Z}G$-permutation module V. The reduction modulo p of these elements then contains at least the ideal of the projective endomorphisms of the F_pG-permutation module $(\sum_{h\in H} h)F_pG$. This can be used to find explicit Morita equivalences for nonprincipal blocks of F_pG even in the case where the order of H is divisible by p.

Wilhelm Plesken
Algorithms for crystallographic groups

Together with J. Opgenorth and T. Schulz I am setting up a package handling crystallographic groups of degrees ≤ 6. The system is called CARAT and contains implementations of various algorithms and a library of Bravais groups. There are three basic algorithms: computing sublattices, automorphism groups of lattices with quadratic forms, and extension groups. The talk concentrates on Opgenorth's normalizer algorithm which is based on the Voronoi algorithm for perfect quadratic forms. With the machinery available one can decide conjugacy of finite unimodular groups in $GL_n(\mathbb{Q})$ and $GL_n(\mathbb{Z})$, can split $\mathbb{Q}$-classes in $\mathbb{Z}$-classes, compute isomorphism classes of space groups, and perform various related tasks.

Gabriele Nebe
Some arithmetic in definite quaternion algebras

Let G be a finite group. Then $\mathbb{Q}G = \oplus D_i^{n_i \times n_i}$ is a direct sum of simple $\mathbb{Q}$-algebras. One might ask which division algebras $D := D_i$ do occur. Clearly $Z(D) =: K$ is the character field of the corresponding character hence an abelian numberfield. If the character is real, then the involution $\mathbb{Q}G \to \mathbb{Q}G \; g \mapsto g^{-1}$ for all $g \in G$ induces an involution $^{-}$ on D that is the identity on K whence one has the
Theorem (Brauer,Speiser) If K is totally real then either $D = K$ or D is a quaternion algebra over K.
I determined the totally definite quaternion algebras D with $D^{n\times n} \mid \mathbb{Q}G$ for some finite group G and $[K : \mathbb{Q}]n \leq 10$ by classifying the absolutely irreducible maximal finite subgroups G of $GL_n(D)$. The representation theoretic methods to build up the groups are the same as for fields, though one has to build up fairly large groups before one may calculate the maximal finite supergroups as automorphism groups of invariant lattices, because one does not know D in advance. The groups yield many interesting rational lattices up to dimension 40. E.g. I found 11 structures of the Leech lattice as a Hermitian lattice over a maximal order of a definite quaternion algebra. The key problem to find the isomorphism classes of G-invariant lattices is to find all conjugacy classes of maximal orders in D. There are some tricks [illegible] get enough maximal orders and one has a mass formula to check completeness. The conjugacy test can be performed very efficiently using the normform $N : D \to K, x \mapsto x\bar{x}$, which is a totally positive definite quadratic form over K. Two maximal orders M, M' in D are conjugate, if and only if the lattices (M, N) and (M', N) are isometric.

George Havas
Integral Gaussian elimination

Gaussian elimination is the basis for classical algorithms for computing canonical forms of integer matrices. Experimental results have shown that integer Gaussian elimination may lead to rapid growth of

intermediate entries. On the other hand various polynomial time algorithms do exist for such computations, but these algorithms are relatively complicated to describe and understand. Gaussian elimination provides the simplest descriptions of algorithms for this purpose. These algorithms have a nice polynomial number of steps, but the steps deal with long operands. We prove that there is an exponential length lower bound on the operands for a well-defined variant of Gaussian elimination when applied to Smith and Hermite normal form calculation. We present explicit matrices for which this variant produces exponential length entries. Thus, Gaussian elimination has worst-case exponential space and time complexity for such applications. The analysis provides guidance as to how integer matrix algorithms based on Gaussian elimination may be further developed for better performance, which is important since many practical algorithms for computing canonical forms are so based.
(Joint work with Xin Gui Fan, to appear in Proc. ISSAC'97, ACM Press)

Sarah Rees

Hairdressing in groups

Let $X = \{x_1, \dots, x_k\}$ be a finite set, $G = \langle X \rangle$ a group, Γ its Cayley graph. A language for G is a set L of words over X (alternatively, paths from the identity vertex of Γ), which maps onto G under the natural map.
Two paths in Γ synchronously (resp. asynchronously) fellow travel if 'travellers' moving with equal (resp. appropriate) speeds on the two paths remain a bounded distance apart. A language L for G is a synchronous (resp. asynchronous) combing for G if the paths in Γ corresponding to words $v, w \in L$ for $v =_G w$ or $v =_G wx$ $(x \in X)$ synchronously (resp. asynchronously) fellow travel; we shall use the word combing to mean asynchronous combing.
G is automatic if it has a combing which is a regular language, asynchronously automatic if it has an asynchronous combing with that property. Many topologically interesting groups are automatic (or asynchronously automatic), including the fundamental groups of many compact manifolds; but the list of non-examples includes the fundamental groups of some compact, geometrisable 3-manifolds and all nilpotent groups which are not virtually abelian. We aim to capture these examples by dropping the regularity condition of automatic groups and looking at more general combings.
Any combable group is finitely presented (Bridson), and has soluble word problem (Gersten).
We let $\mathcal{F}$ be a family of formal languages, and look at groups which are $\mathcal{F}$-combable, that is have combings in $\mathcal{F}$.
Bridson & Gilman proved that all compact geometrisable 3-manifolds M have $\pi_1(M)$ which is an indexed language; in fact real time languages work too.
Which other non-automatic groups have real time combings? The following answers come from joint work with Gilman and Holt.

- Any class 2 nilpotent group with 2 or 3 generators or cyclic G' has a real time combing.
- Any metabelian, polycyclic, torsion-free group with $G' \cap Z(G)$ trivial has a real time combing.
- Any f.g. nilpotent or even polycyclic by finite group embeds in a real time combable group.

Derek Holt

Automatic Groups and Subgroups

Automatic groups form a class of finitely presented groups that have been studied extensively during the past ten years, defined by a collection of finite state automata. They have a normal form for group elements, which enables one (after constructing the automata) to solve the word problem in quadratic time, enumerate group elements, and sometimes to calculate the growth series of the group. Finiteness can also be decided, and usually whether given elements are torsion or not.
Many groups arising from topology and geometry are automatic, including fundamental groups of negatively curved manifolds, most knot groups, word-hyperbolic groups, Euclidean groups, Coxeter groups and braid groups.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

The author's package kbmag (freely available by anonymous ftp from ftp.maths.warwick.ac.uk in the directory people/dfh/kbmag2, or as a GAP share library) can be used to carry out these calculations on a shortlex automatic group. For example, it has been used to prove that the Fibonacci group $F(2,9)$, $F(4,8)$, $F(9,6)$ and $F(15,6)$ are infinite, as is the Heineken group

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

The concept of an automatic group can be generalised to a group G being automatic with respect to a finitely generated subgroup H. In that case there is a normal form for a system of coset representatives of H in G. For example, this is the case for a quasiconvex subgroup of a word-hyperbolic group, but there are many other situations in which it applies. There are some facilities in the standalone version of kbmag for computing the associated automata and, when successful, the finiteness of $|G : H|$ can be decided. It is also possible to compute a presentation for H (which is always finite). For example, it was used to show that the subgroup $\langle [x,y],[x,z],[y,z] \rangle$ of the Heineken group (defined above) is free of rank 3.

Werner Nickel
Polynomials for nilpotent groups

A generating set $\{a_1, \ldots, a_n\}$ for a finitely generated torsionfree nilpotent group can be chosen such that each element of the group has a unique form

$$\underline{a}^{\underline{x}} = a_1^{x_1} \ldots a_n^{x_n}, \qquad x_i \in \mathbb{Z}.$$

P. Hall (Edmonton Notes, 1957) proved that in the product $\underline{a}^{\underline{z}} = \underline{a}^{\underline{x}}\underline{a}^{\underline{y}}$ of two elements z_k is a polynomial in x_i and y_j. These polynomials can be computed by Deep Thought (Leedham-Green & Soicher, OW 1988) from a commutator presentation on these generators and used to perform symbolic multiplications and inversions in the group.
This 5-minute talk explained how these polynomials can be used to check if the group satisfies an (Engel) identity and reported recent computations in the free 2-generator 5-Engel group with GAP 4. The polynomials involved have 104 indeterminates and total degree at most 9.

William Kantor and Akos Seress
Black box classical groups, with an application to permutation group algorithms

1. There is a Las Vegas algorithm which, when given a black box group known to be isomorphic to a simple classical group over a field of given size q, produces an explicit isomorphism.

2. There are nearly linear Las Vegas algorithms which, when given $G = \langle S \rangle \leq S_n$ with no composition factor an exceptional group of Lie type or a 3-dimensional unitary group, determine membership in G, $|G|$, a composition series for G, a Sylow subgroup for each prime factor of $|G|$, and everything else that previously could be found only by Monte Carlo algorithms.

Alexander Hulpke
Algorithms for permutation groups based on homomorphisms

We have nice algorithms for element test, size, composition series, centralizer &c. for permutation groups; theoretically as well as practically. Some other things are harder to compute like conjugacy classes, maximal subgroups, complements. In PC-Groups, on the other hand, we can compute such things rather fast by using the homomorphism principle. We compute a normal series with elementary factors and lift the results over the factors. As each factor is isomorphic to a vector space, all to do is linear algebra.
To extend this approach to general permutation groups, one needs to generalize such lifting procedures to nonabelian elementary groups.
Suppose $N \lhd G$ is an elementary nonabelian normal subgroup, $N \cong T_1 \times \ldots \times T_d$, $T_i \cong T$ simple. Then $C_G(N) \cap N = 1$, thus G is a subdirect product of G/N with $F = G\varphi \leq \mathrm{Aut}(N)$, denoting by

φ the operation homomorphism of G in $Aut(N)$. As $\{T_1, \dots, T_d\}$ is a characteristic class, furthermore $\mathrm{Aut}(T) \cong \mathrm{Aut}(T) \wr S_d$, yielding a small degree permutation representation for F. Let $\psi : F \to S_d$, then $M := \ker \psi$ is an iterated subdirect product of A, $T \leq A \leq Aut(T)$.
Example:Conjugacy Classes. Strategy: A: Classes of G as classes of subdirect product, B: Classes of M as classes of subdirect product and further fusion by F, C: Classes of F outside M.
Ideas: A: Component-wise representative construction. B: "minimal" class arrangement in each representative tuple. C: Instead F-classes of $F \setminus M$ only M-classes on $F \setminus M$, together with further F-fusion. (As we have only few classes in $F \setminus M$, this is no problem.) Then the action of M on M, $z \mapsto (m \mapsto [r, z]m^z)$ splits into components and can be regarded as such.
The algorithm is still in the process of implementation, so it is too early to do comparisons with other approaches.

Bettina Eick
Construction of finite soluble groups

In this talk a method to construct all soluble groups of given order is introduced. The underlying idea of the algorithm is due to W. Gaschütz: in the first step we construct a list of candidates for the Frattini factors of the desired groups (up to isomorphism) and in the second step we compute Frattini extensions of each candidate. The method can be restricted to compute certain classes of soluble groups only, such as non-nilpotent groups or groups without normal Sylow subgroup.
We used a GAP implementation of this method to construct all soluble, non-nilpotent groups of order at most 1000 except for the orders divided by 2^7. This shows in particular, that the method is practical.
In combination with two other methods to construct certain finite groups and the p-group generation method of E. A. O'Brien we obtained a list of all groups of order at most 1000 except for 512 and 768 up to isomorphism.
(Joint work with H. U. Besche.)

Götz Pfeiffer
Computing the Size of a Semigroup

MONOID is a package of GAP functions that allows calculations in and a structural analysis of a finite transformation monoid, i.e, a submonoid M of the full transformation monoid T_n of all maps from $\{1, \dots, n\}$ to itself. The basic theoretical tool is the concept of a generalized (right) Schützenberger group of an element $s \in M$, a permutation group on the set of images of the map s which stands in bijection to a certain subset of M containing s. The whole monoid M is partitioned into such sets where many of the associated permutation groups are isomorphic. Thus a task like, e.g, the computation of the size of M can take much advantage of existing (and powerful) algorithms for permutation groups. The development of the algorithms in MONOID is joint work with S. Linton, E. Robertson, and N. Ruskuc.

Steve Linton
GAP: Status Report and Some Possible Directions

Over the next months, the GAP system will undergo two dramatic changes: firstly, version 4 of the system will be released; secondly, GAP headquarters will move from Aachen to St Andrews.
Already, the final release of GAP 3, version 3.4.4, has been released from St Andrews, incorporating bug fixes, some new developments from the GAP team, and many contributions from users. The formal handover will take place soon, and the e-mail addresses for the GAP forum, the "gap-trouble" helpline, and so forth will move to St Andrews.
We evisage "A move from an Aachen-based project with international involvement to an international project coordinated at St Andrews", and will depend on user contributions, for which we will try to provide support and recognition.
GAP version 4 will provide a number of new features, improving both the system itself, and its collection of mathematical algorithms. Alpha test versions are available now, a beta version will be released soon.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Among the new features in GAP 4 will be: workspace saving and loading; compact storage and fast arithmetic for vectors and matrices over small fields; better access to files and external programs; a compiler; p-adic numbers; much improved code for vector spaces; multi-variate polynomials; infinite polycyclic groups; Lie algebras and much improved permutation group code.
Three especially interesting features are immutability, enabling faster handling of sets of sets and the like, enumerators, which are virtual lists and iterators, which allow one to run through the elements of a set without listing them all at once.
The biggest change in GAP 4 is the new scheme for organising the library. Most user-visible functions are actually Operations: place-holders for multiple Methods, applicable in various circumstances. The system chooses which method to apply, based on the Types of the arguments.
Some Possible Future directions for GAP include: broadening the algebraic range to algebras, semigroups, quantum groups, etc.; links to other systems; improved modularity in the library; support for parallel or distributed processing and user interface improvements. The overall aim remains to help people do research, teach and learn in algebra and discrete mathematics.
Finally, an increasing amount of data about known groups is being accumulated and made available in GAP, but it is not yet stored and presented uniformly, nor is the best possible use made of it in computation. Many interesting questions arise.

Marston Conder

Recent applications and adaptations of the low index subgroups process

The low index subgroups process may be used to find subgroups of small index in a finitely-presented group G, and hence to determine all transitive permutation representations of G of small degree. As well as generating homomorphic images — with application for example to the construction of graphs and surfaces with large automorphism group — this can also help provide answers to questions about the finiteness (or more generally the structure) of G. Two useful adaptations of the process are described: one which ignores prescribed branches of the search tree (and is thus capable of finding all *complements* of a given subgroup of finite index), and one which finds all *normal* subgroups of small index in the group G. Recent applications of these are also mentioned: the construction of combinatorially regular maps with large or trivial automorphism groups, hyperbolic 3-manifolds of minimal volume and/or tessellated by regular solids, classification of trivalent symmetric graphs of small order, and the search for cages (small graphs of large girth).

Adalbert Kerber

Applied Finite Group Actions

It was reported on joint work with R. Laue, K.-H. Zimmermann, A. Betten, H. Fripertinger and A. Wassermann. The joint work is devoted to the enumeration, construction and randomly generation of unlabelled finite structures. We studied in particular graphs, linear codes and combinatorial designs. Unlabelled structures of that kind are usually introduced as equivalence classes of labelled structures and therefore they can be defined as orbits of finite groups on finite sets, and so the well developed theory of finite group actions can be applied.
i) *A flexible Ansatz* is to choose suitable actions ${}_GX$ and ${}_HY$ and to consider the set

$$Y^X := \{f\colon X \to Y\},$$

together with an induced action of $G, H, H \times G$ or $H \wr G$ on Y^X. Here is an easy example: The labelled graphs on V, a set of vertices, can easily be identified with the set of mappings from the set $\binom{V}{2}$ (of pairs of vertices) into the set $\{0,1\}$, i.e. the set of these labelled graphs is equal to

$$Y^X = 2^{\binom{V}{2}}.$$

Correspondingly, the set of unlabelled graphs on this set of vertices is the following set of orbits of the symmetric group S_V :

$$S_V\backslash\backslash 2^{\binom{V}{2}}.$$

ii) In *coding theory* we are after isometry classes of $(n,k)-$codes, i.e. we consider the following set of orbits of the isometry group $H\wr G := GF(q)^*\wr S_n$ on the set of subspaces of dimension k in the finite vector space $GF(q)^n$:

$$GF(q)^*\wr S_n\backslash\backslash U(n,k).$$

But $U(n,k)$ is too abstract to be handled, and so we need to consider generator matrices which consist of k rows and n columns, and so they are contained in $Y^X := (GF(q)^k)^n$. For obvious reasons we may restrict attention to matrices without zero columns, i.e. we will in fact consider the following set of orbits ($GL_k(q)$ comes in since a subspace has usually many bases):

$$GL_k(q)\backslash\backslash GF(q)^*\wr S_n\backslash\backslash(GF(q)^k\backslash\{0\})^n.$$

According to Lehmann's Lemma the inner set of orbits can be replaced by

$$S_n\backslash\backslash(GF(q)^*\backslash\backslash GF(q)^k\backslash\{0\})^n = S_n\backslash\backslash P_{k-1}(q)^n,$$

where $P_{k-1}(q)$ denotes the projective space. This result is quite interesting since it clearly shows two things: First of all it demonstrates why projective geometry plays such an important role in coding theory, and, moreover, it shows why the Hamming codes are so prominent: A particular orbit is formed by the injective mappings, these matrices generate *simplex codes*, the dual of *Hamming codes*.
iii) In design theory we are faced with existence problems, e.g. the existence of 7-designs with small parameters (there is a well-known theorem that assures the existence of 7-designs, but the parameters which guarantee the existence are astronomical). Designs can be considered as 0-1-solutions of a big systems of linear equations. Such problems become tractable *by prescribing a group of automorphisms*. We found, as first 7-design with small parameters, one with parameters 7-(33,8,10) (the prescribed group of automorphisms was $P\Gamma L_2(32)$) and as first 8-design with small parameters an 8-(31,10,93)-design (with $PSL(3,5)$). In both cases the prescription of an automorphism group reduced the number of matrix entries by *a factor* of about 10^{10}.

Leonhard H. Soicher

Application of computational group theory to the study of finite geometries

I spoke about some new and future features of the GRAPE package for computing with groups, graphs and finite geometries.
One new function in GRAPE is for classifying (up to isomorphism) the partial linear spaces with given point graph and parameters. A modification of this algorithm has been used to classify and discover new "Bailey squares". A *Bailey square* is an $(n\times n)/k$ semi-Latin square with the property that any two distinct blocks have at most one point in common. Bailey squares are a generalization of mutually orthogonal Latin squares, and are used in the Design of Experiments.
I also spoke briefly about joint work with Sarah Rees on practical algorithms to compute fundamental groups and covers of finite simplicial complexes.

Gretchen Ostheimer

Algorithms for Polycyclic Matrix Groups

This is a report on work in progress concerning practical algorithms for studying infinite matrix groups. I restrict my attention to polycyclic-by-finite groups as this is the setting in which (most of) the interesting questions are actually decidable. I have developed algorithms for testing membership, finding presentations, and computing normal closures and kernels of homomorphisms. For some of these algorithms I have completed experiments which show that they are efficient enough to be useful in studying some moderately complicated examples; for others I have heuristic arguments that the algorithms are practical.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Eddie H. Lo

Enumerate Finite Index Subgroups of Polycyclic Groups

In this report, an efficient algorithm to enumerate finite index subgroups of polycyclic groups given by consistent polycyclic presentations is presented. This algorithm makes use of the wreath-product ordering of coset tables defined by Sims. The algorithm enumerates all the subgroups of finite index less than or equal to n using $O(nm)$ memory, where m is the number of polycyclic generators, and it seems to be efficient in terms of time.

Anton Betten

Construction of Solvable Groups

B. HUPPERT discusses the situation of a normal subgroup N of prime index in a group G (B. HUPPERT, Endliche Gruppen I, 14.8). We reverse the situation to define groups G with prescribed normal subgroup N of index p. Each solvable group G can be obtained by a sequence of extensions of this kind. One can reduce the number of necessary extensions by considering the action of Aut(N) and Aut(G/N) one the set of extensions. Nevertheless, one may still get isomorphic copies of the same group. To reduce the set of groups up to isomorphism one looks at invariants like Sylow-type, conjugacy classes, power maps, characteristic series and so on. Finally, an isomorphism test for groups is realized via canonical presentations of solvable groups. A systematic computation of the canonical form will also compute a base and strong generating set for the automorphism group of the group in question.

Eugene Luks

Symmetry-breaking predicates

There have been very successful uses of symmetries to limit the search space in combinatorial optimization problems. Typically, customised search engines are built with this in mind. To researchers in automated reasoning, a drawback of the approach is the difficulty in coordinating with the complex search control techniques that have been developed in recent years. In collaboration with the Computational Intelligence Research Laboratory (Eugene, Oregon), we investigated ways to pre-process the input problem so that it targets only a canonical element in each orbit of a group of symmetries, whereupon it can be sent to any existing and future search engines. Specifically, the objective is to design a Boolean predicate that is satisfied only by a canonical (say, lex-least) element. In general, this problem is NP-hard. However, we have provably-efficient solutions in cases corresponding to polynomial-time solvable instances of problems such as finding centralizers in permutation groups. Notably, even for these tractable instances, we show that "natural" approaches to the problem would have led to exponential-length predicates. This work is joint with Amitabha Roy.

Arjeh M. Cohen

Algorithms for Lie algebras

In GAP a suite of functions for Lie algebras called ELIAS (for Einhoven Lie Algebra System) has been implemented by Willem de Graaf. In the talk, I discussed work of de Graaf, Rónyai, Ivanyos, Wales and myself on algorithms developed for this purpose. The main goal was to be able to analyse a finite-dimensional Lie algebra given by a multiplication table. The algorithms highlighted in the talk were the detection of the solvable and the nilpotent radicals, finding a non-nilpotent element and a Cartan subalgebra (if any), finding a Levi-complement to the solvable radical (in characteristic 0), finding the decomposition of a semisimple algebra, determining the type of a simple Lie algebra with nondegenerate Killing form, and an effective version of Ado's theorem.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Michael R. Vaughan-Lee

Lie relators in varieties of groups

Mike Newman and I have used the theory of Lie relators to compute the orders of the free groups in the variety of Engel-4 groups of exponent 5.
We used Wall's theory of multilinear Lie relators to obtain a full description of the Lie relators which hold in the associated Lie rings of Engel-4 groups of exponent 5. We then used the nilpotent quotient algorithm for graded Lie rings to compute the orders of the associated Lie rings of free Engel-4 groups of exponent 5. From this we obtained the following result.
The free rank m group of the variety of Engel-4 groups of exponent 5 has order

$$5^{m+\sum_{k=2}^{m}\binom{m}{k}(g_k+c_k)},$$

where $g_k = (k-1)f_{2k} + (k+1)f_{2k-2}$, and where $c_k = 0$ for $k > 10$, and c_k has the value given in the following table for $2 \leq k \leq 10$.

c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}
3	87	595	1851	2996	2562	1094	224	35

(Here f_k is the k-th Fibonacci number.)

Mike Atkinson

Descent algebras

Descent algebras are subalgebras of the group algebra of a finite Coxeter group and have a natural basis with integer structure constants. Therefore they have a p-modular version. Solomon first proved the existence of the algebras in 1976 and gave a result about the radical in characteristic zero. We have extended this result to characteristic p and given an explicit basis for the radical.
The irreducible representations in all characteristics have been found and are closely connected with the table of marks of the Coxeter group.
The algebras are not semi-simple even in characteristic zero and so an understanding of their representation theory requires a study of their projective indecomposable modules whose composition factors are given by a Cartan matrix. The relationship between the Cartan matrices in characteristics zero and p has been found and this result is valid in a much more general setting which generalises a famous result in group representation theory (also found by Geck and Rouquier). Applying the result demands a knowledge of the decomposition matrix (which gives the modular composition factors of each irreducible representation when reduced modulo p). These decomposition matrices can also be read from the table of marks.
The lecture surveyed these theorems and used a small descent algebra (that corresponding to the Coxeter group A_3) as a running example to illustrate how they were used.

Robert A. Wilson

Taming the Monster

The Monster is the largest of the 26 sporadic simple groups, and up till now has been the only one for which no computer construction exists. This has now been remedied, by effectively constructing the 196882-dimensional representation over $GF(2)$.
Rather than storing such matrices explicitly, which would require about 5 GB each, we adopt a very compact notation, occupying about 250 KB for each generator. Rather than multiplying matrices together, which would take months on a modern workstation, we apply them to a vector, which takes seconds.
We hope to avoid consequent word-length explosion by exploiting the available fast calculations in the subgroup $3^{1+12} \cdot 2Suz$, whose action is close to being tensor product ⊕ monomial ⊕ small.
The general strategy of the construction is familiar:

1. Make the correct representation of the correct group $3^{1+12} \cdot 2Suz : 2$.
2. Find standard generators of the subgroup $3^{2+5+10}(M_{11} \times 2^2)$.

3. Change to standard basis and find the 16 extensions to $3^{2+5+10}(M_{11} \times D_8)$.
4. Eliminate 14 cases and show the other two are conjugate.
There are many technical and mathematical problems, many of which required writing new programs, or at least extending or customizing old ones. Step 1 was largely done by Peter Walsh in his Ph.D. thesis (Birmingham, 1996). The rest was done in collaboration with Richard Parker and Steve Linton.
The next step is obviously to optimize the implementation of the vector-matrix multiplications, and hopefully bring the CPU time requirement down to a small fraction of a second. Then we may be able to think about tackling some problems:
1. Is the Monster a Hurwitz group?
2. Does the Monster contain subgroups isomorphic to $L_2(11)$ and/or $L_2(59)$?
Nevertheless these problems are still very hard, even if, as I expect, the answers are affirmative. A complete determination of the maximal subgroups still seems unattainable.

Larry Finkelstein

Constructive recognition of black box groups isomorphic to $SL(n,q)$, $PSL(n,q)$, $PGL(n,q)$

joint work with Sergey Bratus, Gene Cooperman and Steve Linton

A polynomial time Las Vegas algorithm is presented for constructing an isomorphism between a black box group G known to be isomorphic to one of $SL(n,q)$, $PSL(n,q)$, $PGL(n,q)$, with known n and q, and its natural projective matrix presentation. The algorithm takes time $O(nqp + n^2\mu + n^3\epsilon)$ where μ is the time required for black box multiplication, ρ is the time required to produce a (nearly) uniformly distributed random element of G, and ϵ is the time required for a field operation. The algorithm is based on an approach developed for the case $q = 2$ by Gene Cooperman, Larry Finkelstein and Steve Linton with new ideas contributed by Sergey Bratus for the general case. The algorithm uses only elementary properties of transvections and standard linear algebra. The authors believe that the simplicity and efficiency of the method will lead to a practical implementation.

John McKay

Developments in Monstrous Moonshine

joint work with Mihai Cipu

Let $f(z) = 1/q + \sum_{k>0} a_k q^k$, $q = e^{2\pi i z}$, $Im(z) > 0$, with $a_k \in \mathbb{C}$ be a universal function. We shall further assume that $a_k \in \mathbb{Z}$ to avoid questions of Galois action.
We have Newton relations between elementary symmetric functions (a_k) and the power sums $P_n(f)$. The P_n are the Faber polynomials (see Curtiss Amer. Math. Monthly, 1971) described by Faber in 1903 in Crelle. They are characterized by the property that $P_n(f) - 1/q^n \in qC[[q]]$. For us they arise from the action of a (generalized) Hecke operator, T_n, on modular functions of the form of f.
The Grunsky coefficient, $h_{m,n}$ is defined by

$$P_n(f) = 1/q^n + n * \sum_{m \geq 1} h_{m,n} * q^m,$$

and is the coefficient of q^m in $T_n(f)$.
Norton defines replicable functions by the additional property that $h_{m,n} = h_{r,s}$ when $gcd(m,n) = gcd(r,s)$ and $lcm(m,n) = lcm(r,s)$.
The equations derived from the Newton relations together with the above property enable one to tackle the problem of finding all replicable functions. Gröbner bases have been used for this purpose. Ad hoc methods have been more successful leading to 619 replicable functions so far.
Dedekind, in 1878, derives the elliptic modular function, $j(z)$, from the Schwarz differential equation. This has the form $S(f) + f'^2 * R(f) = 0$, where the differential resolvent, $R(f)$, has the form $N(f)/D(f)^2$. Roughly $D(f)$ describes the critical points of f, and $N(f)$ describes the ramification (or the internal angles between the bounding arcs of circles of a natural fundamental domain for G_f, the invariance group of f). The polynomials, D, and N, have been computed for all 619 known functions. It is hoped, that edge identifications will enable us to find presentations for all reflection groups generated by hyperbolic reflections

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

in the arcs, and hence, eventually, presentations for the groups G_f appearing as conformal subgroups of the reflection groups.

Charles C. Sims

Subgroups of automorphism groups and other topics

This talk had four parts.
The first part described a solution to the following problem: Let G be a finite group and let X be a subset of $Aut(G)$. Find the order of the subgroup generated by X.
The solution assumes that G has a series $G = S_1 \geq S_2 \geq \ldots \geq S_{n+1} = 1$ of characteristic subgroups such that the quotients $|S_i/S_{i+1}|$ are "small". The algorithm has been given a prototype implementation in GAP and used to study the automorphism group of the Burnside group $B(2,5)$.
The second part discussed the problem of deciding membership in the ring of $n \times n$ rational matrices generated by a given finite subset of $M_n(\mathbb{Q})$.
The third part raised a question about the running time of a computer program implementing multiplication in a (large) finite group as the amount of memory available to the program is varied.
The last part illustrated similarities and differences between the recent solution to the "15-puzzle" and attempts to determine the diameters of large Cayley graphs.

Robert Gilman

Computation with finite PREES

Every finite presentation may be changed by Tietze transformations into a multiplication table presentation, i.e. the relators are the defined products $ac = d$ etc. (Usually the table will have blanks in it.) By imposing various axioms we obtain different classes of groups. For example word hyperbolic groups can be characterized by twelve or so axioms, and virtually free groups by an axiom scheme. Another axiom gives a generalized small cancellation condition suitable for computation.

Mike Newman

Groups with exponent six

This is a report on some computational aspects of work in progress on presentations for groups with exponent six. It is a part of joint work with George Havas, Alice Niemeyer and Charlie Sims.
It shows how implementations of various algorithms can be used. These include: coset enumeration, string rewriting, subgroup presentation calculations and soluble quotient calculations. These were done in various contexts - Magma, GAP and Quotpic. In particular the question of how many sixth powers are needed to define the group $\langle a, b \mid a^3, b^3, \text{ exponent6} \rangle$ is discussed.

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Tagungsteilnehmer

Prof.Dr. Michael D. Atkinson
Dept. of Pure Mathematics
University of St. Andrews
The North Haugh

St. Andrews , KY16 9SS
SCOTLAND

Prof.Dr. Robert Beals
Dept. of Mathematics
University of Arizona

Tucson , AZ 85721
USA

Dr. Anton Betten
Lehrstuhl II für Mathematik
Universität Bayreuth

95440 Bayreuth

Prof.Dr. Andre Caranti
Dipartimento di Matematica
Universita di Trento
Via Sommarive 14

I-38050 Povo (Trento)

Prof.Dr. Jon F. Carlson
Department of Mathematics
University of Georgia

Athens , GA 30602
USA

Frank Celler
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

52062 Aachen

Prof.Dr. Arjeh M. Cohen
Dept. of Mathematics and
Computing Science
Eindhoven University of Technology
Postbus 513

NL-5600 MB Eindhoven

Prof.Dr. Marston Conder
Department of Mathematics
The University of Auckland
Private Bag 92019

Auckland
NEW ZEALAND

Prof.Dr. Gene Cooperman
College of Computer Science
Northeastern University
215 Cullinane Hall

Boston , MA 02115
USA

Dr. Bettina Eick
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

52062 Aachen

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Prof.Dr. Larry A. Finkelstein
College of Computer Science
Northeastern University
215 Cullinane Hall

Boston , MA 02115
USA

Dr. Meinolf Geck
U. F. R. de Mathematiques
Case 7012
Universite de Paris VII
2, Place Jussieu

F-75251 Paris Cedex 05

Prof.Dr. Robert Gilman
Dept. of Mathematics
Stevens Institute of Technology
Castle Point Station

Hoboken , NJ 07030
USA

Prof.Dr. George Havas
Key Centre for Software Technology
Dept. of Computer Science
University of Queensland

Queensland 4072
AUSTRALIA

Dr. Gerhard Hiß
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368

69120 Heidelberg

Dr. Derek F. Holt
Mathematics Institute
University of Warwick
Gibbert Hill Road

GB-Coventry , CV4 7AL

Dr. Alexander Hulpke
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

52062 Aachen

Prof.Dr. William M. Kantor
Dept. of Mathematics
University of Oregon

Eugene , OR 97403-1222
USA

Prof.Dr. Adalbert Kerber
Fakultät für Mathematik und Physi
Universität Bayreuth

95440 Bayreuth

Prof.Dr. Charles R. Leedham-Green
School of Mathematical Sciences
Queen Mary and Westfield College
University of London
Mile End Road

GB-London , E1 4NS

Dr. Stephen Linton
Division of Computer Sciences
University of St. Andrews
The North Haugh

St. Andrews , KY16 9SS
SCOTLAND

Prof.Dr. Eddie H. Lo
Dept. of Mathematics
Rutgers University
Busch Campus, Hill Center

New Brunswick , NJ 08903
USA

Dr. Frank Lübeck
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368

69120 Heidelberg

Prof.Dr. Eugene M. Luks
Dept. of Computer and
Information Science
University of Oregon

Eugene , OR 97403
USA

Dr. Klaus Lux
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

52062 Aachen

Dr. Gunter Martin Malle
Interdisziplinäres Zentrum
für Wissenschaftliches Rechnen
Universität Heidelberg
Im Neuenheimer Feld 368

69120 Heidelberg

Prof.Dr. John McKay
Department of Computer Science
Concordia University
1455 de Maisonneuve Blvd. West

Montreal Quebec H3G 1M8
CANADA

Prof.Dr. Jean Michel
U. F. R. de Mathematiques
Case 7012
Universite de Paris VII
2, Place Jussieu

F-75251 Paris Cedex 05

Dr. Gabriele Nebe
Lehrstuhl B für Mathematik
RWTH Aachen
Templergraben 64

52062 Aachen

Dr. Peter M. Neumann
Dept. of Mathematics
Queen's College
Oxford University

GB-Oxford OX1 4AW

Prof.Dr. Michael F. Newman
Mathematics, IAS
Australian National University
GPO Box 4

Canberra ACT, 2601
AUSTRALIA

Werner Nickel
Dept. of Pure Mathematics
University of St. Andrews
The North Haugh

St. Andrews , KY16 9SS
SCOTLAND

Alice Niemeyer
Department of Mathematics
University of Western Australia

Nedlands , WA 6907
AUSTRALIA

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

Auckland
NEW ZEALAND

Gretchen Ostheimer
Dept. of Mathematics
Tufts University

Medford , MA 02155
USA

Prof.Dr. Herbert Pahlings
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

52062 Aachen

Dr. Götz Pfeiffer
Faculty of Mathematics
University College

Galway
IRELAND

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

52062 Aachen

Prof.Dr. Cheryl E. Praeger
Department of Mathematics
University of Western Australia

Nedlands , WA 6907
AUSTRALIA

Prof.Dr. Ferenc Rakoczi
Dept. of Mathematics
University of Oregon

Eugene , OR 97403-1222
USA

Dr. Sarah Rees
Dept. of Mathematics and Statistics
The University of Newcastle

GB-Newcastle-upon-Tyne , NE1 7RU

Prof.Dr. Edmund F. Robertson
Dept. of Pure Mathematics
University of St. Andrews
The North Haugh

St. Andrews , KY16 9SS
SCOTLAND

Prof.Dr. Akos Seress
Department of Mathematics
Ohio State University
231 West 18th Avenue

Columbus , OH 43210-1174
USA

Dr. Graham Sharp
Dept. of Mathematics
Queen's College
Oxford University

GB-Oxford OX1 4AW

Prof.Dr. Charles C. Sims
Dept. of Mathematics
Rutgers University
Busch Campus, Hill Center

New Brunswick , NJ 08903
USA

Dr. Leonard H. Soicher
School of Mathematical Sciences
Queen Mary and Westfield College
University of London
Mile End Road

GB-London , E1 4NS

Prof.Dr. Michael R. Vaughan-Le
Department of Mathematics
Christ Church

GB-Oxford OX1 1DP

Dr. Robert A. Wilson
School of Maths and Statistics
The University of Birmingham
Edgbaston

GB-Birmingham B15 2TT

Prof.Dr. Charles R.B. Wright
Dept. of Mathematics
University of Oregon

Eugene , OR 97403-1222
USA

E-mail addresses:

Atkinson	mda@dcs.st-and.ac.uk
Beals	beals@math.arizona.edu
Betten	anton@btm2x4.mat.uni-bayreuth.de
Caranti	caranti@science.unitn.it
Carlson	jfc@sloth.math.uga.edu
Celler	Frank.Celler@math.rwth-aachen.de
Cohen	amc@win.tue.nl
Conder	conder@math.auckland.ac.nz
Cooperman	gene@ccs.neu.edu
Eick	Bettina.Eick@math.rwth-aachen.de
Finkelstein	laf@ccs.neu.edu
Geck	geck@mathp7.jussieu.fr
Gilman	rgilman@stevens-tech.edu
Havas	havas@cs.uq.edu.au
Hiss	hiss@euterpe.iwr.uni-heidelberg.de
Holt	dfh@maths.warwick.ac.uk
Hulpke	ahulpke@dcs.st-and.ac.uk
Kantor	kantor@math.uoregon.edu
Kerber	kerber@btm2x4.mat.uni-bayreuth.de
Leedham-Green	C.R.Leedham-Green@qmw.ac.uk
Linton	sal@dcs.st-and.ac.uk
Lo	ehlo@afterlife.ncsc.mil
Luebeck	Frank.Luebeck@iwr.uni-heidelberg.de
Luks	luks@cs.uoregon.edu
Lux	Klaus.Lux@math.rwth-aachen.de
Malle	malle@euterpe.iwr.uni-heidelberg.de
McKay	mckay@cs.concordia.ca
Michel	jmichel@mathp7.jussieu.fr
Nebe	gabi@willi.math.rwth-aachen.de
Neumann	neumann@maths.ox.ac.uk
Newman	newman@maths.anu.edu.au
Nickel	werner@dcs.st-and.ac.uk
Niemeyer	alice@maths.uwa.edu.au
O'Brien	obrien@math.auckland.ac.nz
Ostheimer	gostheim@emerald.tufts.edu
Pahlings	Herbert.Pahlings@Math.RWTH-Aachen.DE
Pfeiffer	goetz@schmidt.ucg.ie
Plesken	plesken@willi.math.rwth-aachen.de
Praeger	praeger@maths.uwa.edu.au
Rakoczi	ferenc@cs.uoregon.edu
Rees	Sarah.Rees@ncl.ac.uk
Robertson	edmund@dcs.st-and.ac.uk
Seress	akos@math.ohio-state.edu
Sharp	sharp@maths.ox.ac.uk
Sims	sims@math.rutgers.edu
Soicher	L.H.Soicher@qmw.ac.uk
Vaughan-Lee	vlee@vax.ox.ac.uk
Wilson	r.a.wilson@bham.ac.uk
Wright	wright@math.uoregon.edu