MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 25/1992

# Computational Group Theory

## 7. 6. bis 13. 6. 1992

The meeting which was the second of its kind in Oberwolfach - the first took place from May 15 to 21, 1988 - was organized by J. Neubüser, Aachen, and C. Sims, Rutgers. It was attended by 51 participants from 9 countries. Although in the time between the two Oberwolfach meetings further conferences on the same topic had taken place at Warwick, England, and Rutgers, New Jersey, the wealth of new material presented in this meeting showed that this field of work is in a phase of rapid development. In 41 talks reports on new algorithmic ideas and their complexity analysis, on new implementations and system developments, and on applications of these to concrete questions were given. The subjects treated could roughly be divided into 5 areas: permutation groups, matrix groups, finitely presented groups, polycyclicly presented groups, and representation theory.

The development of algorithms for permutation groups that started with C. Sims' seminal papers in the 60s, has obtained a new thrust from the complexity analysis of such algorithms that started some 10 years ago with the discovery of E. Luks that permutation group algorithms could be used for showing the existence of certain graph algorithms with polynomial complexity. Until very recently this complexity theoretic analysis of permutation group algorithms had remained rather theoretical. However in time for this meeting practical implementations had started using the introduction of some combinatorial methods by L. Babai and others. The reports that these algorithms are now practically available formed one of the highlights of the meeting.

The investigation of matrix groups given by generators had in the past been a rather neglected question. It was really prompted by a discussion that took place in the previous Oberwolfach meeting in 1988, which resulted in a paper by P. Neumann and C. Praeger. This meeting already saw several reports on new ideas, and it can be predicted that methods for the investigation of matrix groups will be a main area of activity during the next years.

In the area of finitely presented groups coset table methods have been technically improved and a new infinite nilpotent quotient program is now available, while methods for finding soluble quotients are still in the phase of discussion and only first implementations exist.

In the area of the structural analysis of polycyclicly presented groups further methods have been developed, the classification of $p$-groups has been extended.

The area of computational methods in representation theory was presented by the largest number of talks of the five areas mentioned above. Here in addition to the extension of methods some large projects for the classification of representations dominated the scene.

Since 1988 computing facilities (a SUN SPARCstation 2, some Macintoshs, and a Siemens PC W 2000) have been installed at Oberwolfach. These were supplemented by an IBM RS 6000 brought from the University of Essen with financial support by NAG, a HP 710 which was kindly provided by Hewlett Packard, and a DECstation 5120 which was brought from RWTH Aachen. At Oberwolfach in addition to the computer algebra system Maple three major group theoretical systems are now permanently installed: Cayley, GAP, and LIE. Those that are normally commercially distributed have been donated to the institute. In addition to these several further systems and stand-alones were available at the meeting. All of this software was frequently used for demonstrations and joint projects, during the breaks and until late into the night. Thursday evening saw an informal discussion about the further development of one of the systems (GAP).

The lively discussions during the meeting and the interest in the exchange and joint development of methods and programs showed that computational group theory is a most active part of group theory. (J.N.)

## Greg Butler

### Applications of homomorphisms

Homomorphisms are critical in divide-and-conquer approaches to computing in permutation groups. These include restriction to one orbit of an intransitive group, the induced action on an invariant partition of the points, and the isomorphism given by a polycyclic generating sequence of a soluble group or a $p$-group. We discuss improved algorithms for computing Sylow $p$-subgroups and the conjugacy classes of elements of a permutation group which are based on homomorphisms. Experimental results are presented.

## Colin M. Campbell

### Computing efficient presentations

At the 1988 Oberwolfach computational group theory meeting I discussed a possible theorem concerning the efficiency of $PSL(2,p) \times PSL(2,p)$, $p$ prime. In a joint paper with E. F. Robertson and P. D. Williams (J. London Math. Soc. 41 (1990), 69-77) the theorem is stated and proved.

In this talk we briefly describe the above result and, in addition, give efficient presentations for $A_5^3$ and $A_5^4$. Other efficient presentations are described as is some work in the area by two St. Andrews research students, D. M. Gill and B. Vatansever.

## Arjeh M. Cohen

### Computing with Coxeter group elements

This talk intended to announce that there are now

1. fast algorithms for computing canonical forms (in the software package LIE for Weyl groups; by Du Cloux (Lyon) for arbitrary Coxeter groups); and

2. a solution to the conjugacy problem for hyperbolic Coxeter groups, due to D. Krammer (Utrecht).

Arjeh M. Cohen

## On the solution of Kostant's conjecture

In joint work with R. L. Griess and B. Lisser, the group $G = L(2,61)$ is embedded in $E_8(1831)$ by means of a three step procedure. First the standard Borel subgroup of $G$ is embedded in a torus normalizer, in which also an element $w_0$ is found inverting the diagonal subgroup of $G$. Then, the embedded diagonal subgroup of $G$ is put in diagonal form with respect to a Chevalley basis of the adjoint module for $E_8(1831)$, the Lie algebra. Finally, an involution $w \in w_0 H$, where $H$ is the group of all diagonal elements of $E_8(1831)$, is found that generates a subgroup $\cong G$ with the embedded Borel subgroup. This third step is done by solving a system of 1984 linear equations in 240 variables. It is argued that there is a unique conjugacy class of subgroups $\cong G$ in $E_8(1831)$. A Brauer lifting argument leads us to conclude that there also is a unique conjugacy class of subgroups $\cong G$ in $E_8(\mathbb{C})$. This solves a conjecture of Kostant's.

Gene Cooperman and Larry Finkelstein

## A unified approach to membership testing for large and small base permutation groups

(Presented by Gene Cooperman)

A new approach to group membership is presented which leads to a unified treatment for both large and small base permutation groups. It is almost purely combinatorial, not even relying on the concepts of transitivity and primitivity. The algorithm appears to be simpler than algorithms described previously in joint work with Babai, Luks and Seress and has the potential for leading to superior implementations. For ease of comparison, we neglect terms involving $|S|$ and terms not involving $n$. In the large base case, the asymptotic time is $O(n^2 \log |G| \log n)$ with reliability at least $1 - 1/n$, as compared with the previous result of $O(n^3 \log^4 n)$. In the small base case, the asymptotic time is $O(nb^2 \log^2 |G| \log n)$ with reliability at least $1 - 1/n$. This is close to the previous result of $O(n \log^3 |G|)$ for small $b$, but has a higher reliability of at least $1 - 1/n$.

Gene Cooperman and Larry Finkelstein

## Cyclic base change algorithms for permutation groups

(Presented by Larry Finkelstein)

An overview of base change algorithms for permutation groups will be presented. The focus of the talk will be on two new cyclic base change algorithms. One is deterministic and the other is randomized. When $G$ is a *small* base permutation group both algorithms have worst case time complexities which are better than existing algorithms in their class. For $G$ a permutation group of degree $n$ specified by a generating set $S$, the deterministic algorithm requires $O(n \log^2 |G| + n|S| \log |G|)$ time. It outputs a Schreier vector data structure which requires $O(n \log |G|)$ space and in which every Schreier tree has depth bounded by $2 \log |G|$. The randomized algorithm returns a Schreier vector data structure for which the sum of the depths of the resulting Schreier trees is $O(\log |G|)$. It is shown that the algorithm has probability exceeding $1 - 2/n$ of using $O(nb \log^2 n)$ time for $b$ the size of a non-redundant base. As with most randomized base change algorithms, it is Las Vegas in the sense that within the same time it can be deterministically verified whether the answer is correct. In order to achieve this time bound it is necessary that random elements of $G$ be computable in time $O(n \log |G|)$. A final result is a randomized algorithm which given an arbitrary strong generating set $S$ for $G$ constructs a Schreier vector data structure which can be used to compute random elements in $O(n \log |G|)$ time. It is shown that this algorithm has probability $1 - 1/|G|$ of using $O(n \log^2 |G| + n|S|)$ time.

John D. Dixon

## A census of finite primitive linear groups

(Joint project with Holger Gollan, Essen)

Let $Z$ be the group of scalars in $GL(n, \mathbb{C})$. Consider the set of primitive subgroups $G$ of $GL(n, \mathbb{C})$ with $Z \leq G$ and $G/Z$ finite. Jordan (1878) showed that this set is finite (up to conjugacy) for each $n$. Since then, a number of mathematicians have enumerated these groups for various $n$. Write $S/Z := \mathrm{soc}(G/Z) = T_0/Z \times T_1/Z \times \ldots \times T_m/Z$ where $T_0/Z$ is abelian and $T_i/Z$ is nonabelian, simple for each $i > 0$. Then $S$ is irreducible and

$S \simeq \overline{T}_0 \otimes \ldots \otimes \overline{T}_m$ where $\overline{T}_i \leq GL(n_i, \mathbb{C})$ and $T_i \simeq \overline{T}_i$ with $n_0 n_1 \cdots n_m = n$. The normalizer of $S$ in $GL(n, \mathbb{C})$ is isomorphic to $(\overline{N}_0 \otimes \ldots \otimes \overline{N}_m) \cdot U$ where $\overline{N}_i$ is the normalizer of $\overline{T}_i$ in $GL(n_i, \mathbb{C})$ and $U$ is a permutation group of degree $m$ which "fuses" the isomorphic $\overline{N}_i$. It is known that $\overline{N}_0 = \overline{T}_0 \cdot \Pi_{i=1}^{s} Sp(2k_i, p_i)$ where $n_0 = p_1^{k_1} \cdots p_s^{k_s}$ and $\overline{N}_i/\overline{T}_i$ is isomorphic to a group of outer automorphisms of $T_i/Z$. Hence it is possible to construct systematically explicit matrix representations of the primitive group of degree $n$ in families according to the value of $S/Z$. This uses the known representation of $\overline{N}_0$ and the projective characters of the almost simple groups $\overline{N}_i/Z$ (from the ATLAS, for example).

Meinolf Geck

## CHEVIE – Character Tables of Hecke Algebras

CHEVIE (Chevalley & Lie) is a joint project of G.Hiß/G.Malle (Heidelberg), P.Fleischmann/I.Janiszak (Essen) and M.Geck/G.Pfeiffer (Aachen). Its purpose is to collect in a unified way information on finite groups of Lie type, and to provide tools and programs for working with these data. The parts of CHEVIE dealing with finite Weyl groups and associated Hecke algebras are developed in Aachen.

Let $W = \langle s \in S \mid s^2 = (ss')^{m_{ss'}} = 1 \rangle$ (where $m_{ss'}$ are fixed non–negative integers) be a finite Weyl group and $H$ be the associated Hecke algebra over the field of fractions of the ring $A$ of Laurent polynomials over $\mathbb{Z}$ in indeterminates $u_s^{1/2}$, $s \in S$, such that $u_s = u_{s'}$ whenever $s, s' \in S$ are conjugate in $W$. Let $\phi_j$, $j = 1, \ldots, m$, be the irreducible characters of $H$. G.Pfeiffer and the author have shown:

(1) For $w \in W$, denote by $T_w$ the corresponding basis element of $H$. Then $T_w$ and $T_{w'}$ are conjugate by a unit in $H$, if $w, w' \in W$ are of minimal length in one fixed conjugacy class of $W$.

(2) For each conjugacy class $C$ of $W$, fix an element $w_C \in C$ of minimal length. Then, for each $w \in W$, there exist uniquely determined polynomials $f_{w,C} \in A$ such that $\phi_j(T_w) = \sum_C f_{w,C} \phi_j(T_{w_C})$ for all $j$.

The character table of $H$ is then defined to be the square matrix $(\phi_j(T_{w_C}))_{j,C}$. It has been determined for $W$ of type $F_4$ and $E_6$, for example.

## Robert H. Gilman

### Applications of formal language theory

The coset table obtained by enumerating the cosets of a subgroup $H$ of finite index in a finitely presented group $G$ may be thought of as a finite automaton accepting the language of all words representing elements of $H$. From this point of view it is natural to ask what may be gained by replacing this finite automaton by one of the more powerful types studied in the theory of formal languages. There is a variant of pushdown automaton which accepts all words representing elements of a subgroup $H$ if and only if there exists $N$ of finite index in $G$ with $H$ normal in $N$ and $N/H$ isomorphic to a free group. Further there is a test which may be applied to the partial coset tables obtained during the enumeration of the cosets of a finitely generated subgroup $H$ in $G$. The tables will eventually pass the test if and only if there is a subgroup $N$ embedded as above.

## Stephen P. Glasby

### Constructing absolutely irreducible representations of a finite soluble group

This talk has two parts. Let $G$ be a finite soluble group given by a (confluent) PAG-system, and let $p$ be a prime. In part **I**, we describe an algorithm for constructing all the absolutely irreducible representations of $G$ in characteristic $p$, where each representation is written over its character field. As representations are extended or induced, the character field may become larger or smaller and the changing of fields can be done efficiently. In part **II** we discuss a convenient recursive algorithm for computing with finite fields.

Let $1 = m_1, m_2, \ldots, m_r = m$ be a sequence of divisors of $m$ where $m_i/m_{i-1}$ is a prime, for $i = 2, \ldots, r$. We compute in $\mathbf{F}_{p^m}$ via the "composition series"

$$\mathbf{F}_p = \mathbf{F}_{p^{m_1}} \subset \mathbf{F}_{p^{m_2}} \subset \cdots \subset \mathbf{F}_{p^{m_r}} = \mathbf{F}_m,$$

using polynomials $f_i(X_i)$ where $f_i(X_i) \in \mathbf{F}_{p^{m_i}}[X_i]$ is irreducible. The elements of $\mathbf{F}_{p^m}$ are viewed as polynomials in $X_1, X_2, \ldots, X_r$. Using some basic ideas such as

$$\mathbf{F}_{q^{ab}} \cong \mathbf{F}_{q^a} \otimes_{\mathbf{F}_q} \mathbf{F}_{q^b}$$

if $\gcd(a,b) = 1$, we may change easily from one composition series to another and reuse the polynomials. It is now particularly efficient to construct embeddings $\mathbf{F}_{p^d} \to \mathbf{F}_{p^n}$ and $\mathbf{F}_{p^n} \to \mathrm{Mat}(n/d, \mathbf{F}_{p^d})$ for any divisor $d$ of $n$.

In practice, we construct tables of irreducible polynomials for computing in $\mathbf{F}_{p^a}$, where $a$ is a power of a prime $r$. There are some theorems which may be used to construct infinitely many irreducible polynomials for given $p$ and $r$. The arithmetic in this recursive schema has a lower complexity than that of computing modulo one irreducible polynomial.

## George Havas

### Coset enumeration: implementation and application

New strategies for enumerating cosets in finitely presented groups are described. They are based on the observation that, when a coset enumeration completes, both the relator tables and the coset table will be filled. Thus, coset definitions are made to keep these tables in relative balance.

A stand-alone implementation of these strategies exists and they are also available in the latest version of Cayley. They show excellent performance on difficult enumerations, defining orders of magnitude fewer cosets in some cases. They do not appear to make any easy enumerations require significantly more cosets.

Coset enumeration has been applied to the Burnside group B(2,5) to obtain a new result. In the restricted Burnside group R(2,5), the third term in the lower central series, $\gamma_3(\mathrm{R})$, has index 125 and may be generated by 12 elements. A 12 element generating set has been found for $\gamma_3(\mathrm{B})$.

## Derek F. Holt

### Computing in matrix groups

This talk concerns the following problem. Let $G$ be a subgroup of the general linear group $GL(n,q)$ given by explicit generating matrices. Then determine structural properties of $G$. The principal theoretical result used is the theorem of Aschbacher which states that $G$ must lie in at least one of nine classes of subgroups of $GL(n,q)$.

The first part of the talk is a description of an implementation in GAP by Holt and Rees of an algorithm by Neumann and Praeger for deciding whether $G$ contains $SL(n,q)$. This turns out to be practical for degrees $n$ up to about 60 and $q \leq 2^{16}$ (i.e. all finite fields known to GAP). This is a Monte-Carlo algorithm which has a small probability of giving the wrong answer. It involves choosing random elements from the group $G$.

The second part concerns an extension of Parker's MEATAXE algorithm for testing whether $G$ is irreducible, which works for large fields as well as small. There is also a test for absolute irreducibility. These procedures have been implemented in GAP.

The third part is a general discussion as to how to proceed with the recognition of groups from the other classes in the Aschbacher classification. In this connection it is important to be able to find elements in nonscalar normal subgroups of $G$.

Ingo Janiszczak

## The generic conjugacy class numbers of Chevalley groups of type $E_6$, $E_7$ and $E_8$

(Joint work with Peter Fleischmann)

Let $G$ denote a finite group of Lie type E. Using a computer program dealing with the poset of closed subsystems of the rootsystem of $G$ (in particular calculating the Moebius function of the poset) we determined the number of semisimple conjugacy classes of $G$ whose centralizers form a given $G$-conjugacy class in the case that $G$ is simply connected.

By Jordan decomposition of irreducible characters we got the following result

**Theorem:** *Let $G(q)$ be a finite group of adjoint Lie type E. Then the number $Cl(q)$ of conjugacy classes of $G(q)$ is given as follows:*

1.) $G = E_6(q)$ : $Cl(q) =$

$$
\begin{aligned}
&= q^6 + q^5 + 2q^4 + 2q^3 + 9q^2 + 9q + 22 \quad \textit{for} \quad q \equiv 1 \pmod 6;\\
&= q^6 + q^5 + 2q^4 + 2q^3 + 6q^2 + 4q + 4 \quad \textit{for} \quad q \equiv 2 \pmod 6;\\
&= q^6 + q^5 + 2q^4 + 2q^3 + 7q^2 + 5q + 3 \quad \textit{for} \quad q \equiv 3 \pmod 6;\\
&= q^6 + q^5 + 2q^4 + 2q^3 + 8q^2 + 8q + 20 \quad \textit{for} \quad q \equiv 4 \pmod 6;\\
&= q^6 + q^5 + 2q^4 + 2q^3 + 7q^2 + 5q + 4 \quad \textit{for} \quad q \equiv 5 \pmod 6;
\end{aligned}
$$

2.) $G = {}^2E_6(q^2)$ : $Cl(q) =$

$$
\begin{aligned}
&= q^6 + q^5 + 2q^4 + 4q^3 + 11q^2 + 11q + 16 \quad for \quad q \equiv 1 \pmod 6;\\
&= q^6 + q^5 + 2q^4 + 4q^3 + 12q^2 + 14q + 30 \quad for \quad q \equiv 2 \pmod 6;\\
&= q^6 + q^5 + 2q^4 + 4q^3 + 11q^2 + 11q + 15 \quad for \quad q \equiv 3 \pmod 6;\\
&= q^6 + q^5 + 2q^4 + 4q^3 + 10q^2 + 10q + 14 \quad for \quad q \equiv 4 \pmod 6;\\
&= q^6 + q^5 + 2q^4 + 4q^3 + 13q^2 + 15q + 34 \quad for \quad q \equiv 5 \pmod 6;
\end{aligned}
$$

3.) $G = E_7(q)$ : $Cl(q) =$

$$
\begin{aligned}
&= q^7 + q^6 + 2q^5 + 4q^4 + 10q^3 + 15q^2 + 25q + 21 \quad for \quad q = 2^n;\\
&= q^7 + q^6 + 2q^5 + 5q^4 + 13q^3 + 24q^2 + 46q + 57 \quad for \quad q = 3^n;\\
&= q^7 + q^6 + 2q^5 + 5q^4 + 13q^3 + 24q^2 + 47q + 59 \quad else;
\end{aligned}
$$

4.) $G = E_8(q)$ : $Cl(q) =$

$$
\begin{aligned}
&= q^8 + q^7 + 2q^6 + 3q^5 + 9q^4 + 14q^3 + 32q^2 + 47q + 70 \quad for \quad q = 2^n;\\
&= q^8 + q^7 + 2q^6 + 3q^5 + 10q^4 + 16q^3 + 39q^2 + 65q + 102 \quad for \quad q = 3^n;\\
&= q^8 + q^7 + 2q^6 + 3q^5 + 10q^4 + 16q^3 + 40q^2 + 67q + 111 \quad for \quad q = 5^n;\\
&= q^8 + q^7 + 2q^6 + 3q^5 + 10q^4 + 16q^3 + 40q^2 + 67q + 112 \quad else.
\end{aligned}
$$

The case $E_6$ also was obtained by Deriziotis and Holt.

William M. Kantor

## Computations in quotient groups and other aspects of Sylow subgroups of permutation groups

The talk consisted of two parts. The first outlined an efficient but complicated algorithm for finding Sylow subgroups of a group $G \leq S_n$. The algorithm has a bottleneck when $G$ is simple, primitive and small ($|G| < n^5$), when backtrack should be fairly efficient but seems overly crude.

The second part of the talk concerned algorithms (due to Luks and myself), that use Sylow subgroups: finding the core of a subgroup of $G$, and computing in quotient groups (e. g., finding $Z(G/K)$ if $K \lhd G \leq S_n$).

Adalbert Kerber

## Symmetrica

The computer algebra system mentioned in the title was introduced. The main properties of it are the following ones:

- It is devoted to the representation theory and combinatorics of finite symmetric groups and of related classes of groups like the alternating groups, the wreath products of symmetric groups,..., the genereal linear groups.
- It is a system that runs on any computer with a C-compiler.
- It mainly uses symbolic calculations in terms of sequences of natural numbers or of tableaux.
- It is written in an object oriented way to avoid the implementation of an extra language on top of the procedures and therefore keeps the usability of programming tools like optimizer, debugger, profiler and so on.
- It provides routines for
  - characters of $S_n$ (also modular), $A_n$, $S_m \wr S_n$,
  - matrix representations of $S_n$ (also modular), $GL_m(\mathbb{C})$,
  - Schur, Schubert, zonal polynomials, symmetric polynomials together with base change matrices,
  - cycle indicator polynomials for combinatorial enumeration,
  - the ordinary group algebra of the symmetric groups.

  For these procedures you can use
  - integer arithmetic, long integers, automatically and if necessary,
  - cyclotomic fields,

At present for modular purposes only prime fields of prime characteristics are used and necessary. Later on this will be extended. The program system is available by anonymous ftp from: 132.180.8.29 , the name of the file is math/SYM/SYM.tar.Z

Wolfgang Kimmerle

**Computational aspects of the isomorphism problem of group rings**

1. The modular isomorphism problem:
   Let $F_p$ be the field of $p$ elements, $G$ and $H$ finite $p$-groups. Does $F_pG \cong F_pH$ imply that $G$ and $H$ are isomorphic? The program Sisyphos (based on an algorithm due to Scott and Roggenkamp, modified and implemented by Wursthorn) is discussed. One application of Sisyphos is the proof that 2-groups of order $2^6$ have a positive answer for the modular isomorphism problem.

2. A slight modification of Sisyphos allows the computation of automorphisms of $p$-groups. The knowledge about special automorphisms not only of $p$-groups is relevant for the third topic.

3. The integral isomorphism problem:
   Let $G$ and $H$ be arbitrary groups. Does $\mathbb{Z}G \cong \mathbb{Z}H$ imply $G \cong H$? This problem has for groups of order $p^a \cdot q^b$ a positive answer, if $G/F(G)$ has the property that each conjugacy class preserving automorphism is inner.

Charles R. Leedham-Green

**Recognizing the special linear group**

(Joint work with Frank Celler, Aachen)

We have three algorithms for recognizing matrix groups. The first two have been programmed in GAP, the third is being programmed.

1. To calculate the order of a matrix $A \in GL(n,q)$.
   This runs in $O(n^3 \log q \log t)$ time, where $t$ is the number of distinct prime divisors of the order of $A$. We take the factorization of the integers $q^i - 1$, $1 \leq i \leq n$, as given.

2. To decide whether or not $\langle X \rangle$ contains $SL(n,q)$, where $X$ is a subset of $GL(n,q)$. The algorithm either returns 'YES' with a proof (depending on Aschbacher's classification of matrix groups and making strong use

of the classification of finite simple groups), or 'NO' to any required degree of confidence. The algorithm is based on the Neumann-Praeger algorithm, and has the same complexity as 1.

3. As above, but a constructive algorithm is used, in that, if the answer is 'YES', a generating set of elementary matrices is evaluated as words in $X$. This algorithm runs in $O(n^4 \log q + q)$ time, and is elementary.

Steve Linton

## A module enumeration algorithm

## "Todd-Coxeter for matrices"

In this talk I described an algorithm analogous to Coset Enumeration, but constructing matrix representations of finitely presented $k$-algebras, rather than permutation representations of finitely presented groups. The input to the algorithm is a field $k$ and a set $X$ of generators. We then write $A = A(X)$ for the free $k$-algebra generated by $X$. Further input is a set $R \subseteq A$ of *relators*. The algebra constructed is then the quotient

$$P = A/\langle ARA \rangle.$$

Further input is an integer $s$, allowing us to define the free $s$-generator left $A$-module $M = \bigoplus_{i=1}^{s} A$. This has a natural homomorphism onto the free $s$-generator $P$-module. Finally we input a set of members of $M$ (that is $s$-tuples of members of $A$) whose images will generate the left $P$-module on whose quotient we will compute the action of the generators.

This seems complex, but when each $x \in X$ is invertible $P$ will be a (quotient of a) group-algebra, and when each $r \in R$ is of the form $x_1 \cdots x_t - 1$ and each component of each $w \in W$ is of the same form then the algorithm simply reduces to coset enumeration and constructs a permutation representation (with $s$ orbits).

The talk covered the algorithm, which is quite naturally derived from coset enumeration, and various refinements which are essential for a practically fast implementation.

The algorithm has been implemented and the program is freely available, anyone wanting it should contact sl25@cus.cam.ac.uk .

Finally some areas where the algorithm has found application were mentioned. These include representation theory, Hecke algebras, the operator $p$-quotient algorithm of Alice Niemeyer and, most recently, computing homology of graphs.

## Andrea Lucchini

### Computing the minimal number of generators in finite soluble groups

The problem of determining the minimal number $d(G)$ of generators for a finite solvable group $G$ has been discussed and completely solved by Gaschütz. The work of Gaschütz also suggests a computational method to find a set of generators of minimal cardinality for a finite solvable group. The main idea is to go down along a series with abelian factors, using the following fundamental remark (Gaschütz): Let $N$ be a normal subgroup of $G$ and let $y_1, ..., y_d \in G$ be such that $G/N = \langle y_1N, ..., y_dN \rangle$. If $G$ can be generated with $d$ elements then there exist $u_1, ..., u_d \in N$ such that $G = \langle y_1u_1N, ..., y_du_dN \rangle$.

This suggests a simple algorithm to determine a set of generators of minimal cardinality for a finite solvable group $G$, given by a pc-presentation, when a chief series is available. For the case when it is difficult or too expensive to compute a chief series, a less simple algorithm, but nevertheless efficient, is also presented. Both algorithms have been implemented in Cayley and in GAP.

## Eugene Luks

### Computing in solvable linear groups

We announce methods for computing in solvable $G \leq GL(n, q)$, aiming, at this point, for guaranteed polynomial time. Given a small generating set, $S$, for $G$, testing solvability and testing nilpotence are in polynomial-time, that is, in time $O((n+\log q)^c)$. It seems unlikely that membership-testing in $G$ is in polynomial time, as even the case $n = |S| = 1$ subsumes the discrete log problem. However, letting $\mu$ denote the largest prime in $|G|$ that does not divide $q$, the following can be carried out in time $O((n + \log q + \mu)^c)$

steps: test membership in $G$; find $|G|$; find generators for the subgroup fixing a set or a subspace; find Sylow subgroups; find centralizers and normalizers of subgroups. As an application, finding normalizers in solvable permutation groups is in polynomial time.

Klaus Lux

**Peakword condensation and finite lattices of submodules**

We outline an algorithm which, given an algebra $A$ over a finite field $F$, determines the lattice of submodules of an $A$-module $V$. If $S$ is a simple constituent of the module $V$ an $S$-peakidempotent $e$ is an idempotent in $A$ with the property that $\dim_F(Se) = \dim_F(\mathrm{End}_A(S))$. An $A$-module $M$ is said to be $S$-local if $M/\mathrm{Rad}(M) \cong S$. There is a one-to-one correspondence between the $S$-local submodules of the $A$-module $V$ and the $eSe$-local submodules of the $eAe$-module $Ve$. Peakidempotents can be found systematically by looking for peakwords in $A$, i.e., elements of $A$ which have the property $\mathrm{kernel}(a_T) = 0$ if $T$ is a composition factor of $V$ with $T \not\cong S$ and $\dim_F(\mathrm{kernel}(a_S)) = \dim_F(\mathrm{kernel}(a_S^2))$ and $\dim_F(\mathrm{kernel}(a_S)) = \dim_F(\mathrm{End}_A(S))$. The Conway-Benson theorem on modular lattices tells us that the submodule lattice of $V$ can be recovered from the local submodules and certain relations amongst them. Based on this the implemented version of the algorithm proceeds as follows: It determines a composition series for $V$, then finds the peakwords and peakidempotents for the various composition factors, works out the local submodules in $V$, and the relations amongst them. Finally it recovers the lattice of submodules using the Conway-Benson theorem.

Gunter Malle

**CHEVIE and Green functions**

CHEVIE is a database and a program system for generic character tables of (small rank) groups of Lie type. At present, it contains the tables of all rank 2 groups. The handling of generic tables is possible by subdividing the set of conjugacy classes into finitely many "families of classes", and similarly subdividing the irreducible characters into "families of characters". Work

on generic character tables was begun by Hiß and Geck in Aachen, and is now continued by groups in Aachen, Essen and Heidelberg.

By the theory of Deligne-Lusztig, the main ingredient for the computation of a character table of a group of Lie type are the Green functions. This is a set of functions on the unipotent classes, indexed by $F$-conjugacy classes of the Weyl group. Algorithms for the computation of these functions in good characteristic are known. In bad characteristic it is possible to determine these functions from their formal properties, like orthogonality relations, at least in special cases. So the characteristic 2 Green functions of $F_4$, $E_6$, ${}^2E_6$, $E_6.2$, and ${}^2E_6.2$ can be computed. They have also been fed into the CHEVIE system.

## Victor Mazurov

### Computations with character tables

(Joint work with N. Mazurova and S. Zharov)

A permutation character of a finite group is an integral linear combination of irreducible characters with some restrictions on coefficients. Most of these restrictions are in the form of linear inequalities. This makes possible to use linear optimization algorithms for the finding of permutation characters of bounded degree. For example, by this method were calculated the permutation characters of the least degree for sporadic simple groups $F_2$, $F_3$, and $F_5$.

In the second part of the talk an algorithm for the distributing of characters in $p$-blocks based on new results of V. Belonogov is discussed.

## John McKay

### Imprimitivity of Galois groups

(Joint work with David Casperson)

For irreducible $f = \Pi_{i=1}^{n}(x - \alpha_i) \in \mathbb{Q}[x]$ we have the

Proposition

(1) $f \mid g \circ h$, $g, h \in \mathbb{Z}[x]$, $\deg g, \deg h < \deg f$.

(2) $\exists$ an intermediate field $\mathbb{Q}(\beta)$, $\mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$.

(3) $\mathrm{Gal}_{\mathbb{Q}} f$ acts imprimitively on $\{\alpha_i\}$.

(1) $\leftrightarrow$ (2) $\leftrightarrow$ (3).

Computationally, given approximations to $\{\alpha_i\}$ then, for $\alpha_i \neq \alpha_j$ in the same block, we have

$$h(\alpha_i) = h(\alpha_j) \rightarrow \sum_k h_k(\alpha_i^k - \alpha_j^k) = 0$$

from which $\{h_k\}_{k>0}$ can be deduced from a $\mathbb{Z}$-linear depend-ence program (Ferguson/Bailey or $L^3$). The constant term of $h$ may be absorbed into $g = \mathrm{minpoly}(\sum_{k>0} h_k(\alpha_i^k))$ which may be found using a $\mathbb{Z}$-linear depend-ence algorithm, Gröbner basis, or resultants. Note that $\deg g = \#$ of blocks.

## Michael F. Newman

### The use of $p$-quotient programs

The basic purpose of $p$-quotient programs is to take groups of $p$-power order described as quotients of finitely presented groups and produce consistent power-commutator presentations for them. Some more or less routine uses of such programs were mentioned, in particular the computation of some $p$-quotients of presentations of interest in the context of the Golod-Šafarevič Theorem (see my talk - Some computations - at the recent meeting here on $p$-groups). In some contexts the finite presentation may only be *implicit*. For example the underlying group description may include an exponent law. In a $p$-quotient a finite set of instances suffices to ensure the law holds. Another example is when the set of relations of the underlying group is the closure of a finite set of words under a set of endomorphisms of the relevant free group. This way of giving a group is useful when handling large groups of finite exponent. Two examples were given. The computation of consistent power-commutator presentations for the largest class 14 quotient of the 2-generator Burnside group of exponent 8 (which turns out to have order $2^{2240}$) and, with E. A. O'Brien, for the 3-generator restricted Burnside group of exponent 5 (which has order $5^{2282}$). These computations were done with a new $p$-quotient program written in C by E. A. O'Brien.

## Werner Nickel

### Schur multiplier and representation groups

The Schur multiplicator $M(G)$ of a finite group $G$ given by a finite presentation $\langle a_1, \ldots, a_n \mid r_1, \ldots, r_m \rangle$ can be described as the torsion part of $R/[R,F]$, where $F$ is the free group on $\{a_1, \ldots, a_n\}$ and $R$ the normal closure of $\{r_1, \ldots, r_m\}$ in $F$. Any $C < F$ such that $C > [R,F]$ and $C/[R,F]$ is a complement for $M(G)$ in $R/[R,F]$ gives rise to a representation group $F/C$ of $G$.

In the case of a finite soluble group $G$ this description can be used to compute $M(G)$ and a set of groups which contains a representative for each isomorphism class of representation groups. The procedure uses a consistent polycyclic presentation for $G$ to obtain a consistent polycyclic presentation for $F/[R,F]$. Furthermore, it allows to determine a set of representatives for the isomorphism classes of representation groups using the action of $\mathrm{Aut}(G/Z^*)$ on the complements of $M(G)$ in order to form orbits which correspond to the isomorphism classes of representation groups. $Z^*$ is the image of the center of any representation group of $G$ under the natural projection.

The last third of the talk was used to describe an implementation of a nilpotent quotient algorithm written by the speaker in the programming language C.

## Alice C. Niemeyer

### An operator $p$-quotient algorithm

Let $G$ be a group given by a finite presentation with a finite soluble homomorphic image $K$. It is assumed that $P = O_p(K)$ is non-trivial and that $K$ is given by a power-commutator presentation using a composition series through $P$. An algorithm, called the *operator $p$-quotient algorithm*, is outlined which computes a power-commutator presentation for an extension $H$ of $K$ by an elementary abelian $p$-group, such that $H$ is a homomorphic image of $G$ and $O_p(H)$ is an 'immediate descendant' of $P$. The method used has similarities with the $p$-quotient algorithm, which computes power-commutator presentations for quotients of prime power order of finitely presented groups.

## Eamonn A. O'Brien

### Isomorphism testing for $p$-groups

In this talk, I describe an algorithm which can be used to determine whether two given $p$-groups are isomorphic. The technique used is to define a canonical or standard presentation of a finite $p$-group and to provide an algorithm to construct it. Under this scheme, given two finite presentations, in order to establish that the two presented groups are isomorphic, it is sufficient to generate the standard presentations for each of these groups and to compare the presentations obtained.

One view of the $p$-group generation algorithm is that it is a method to construct a power-commutator presentation for a given $p$-group. The presentation obtained by constructing the group using this algorithm is designated as the standard presentation of the group.

The standard presentation algorithm proceeds class by class of the lower exponent-$p$ central series. At the $k$th iteration, it takes as input a set of defining relations and the standard presentation for the class $k$ $p$-quotient of $G$ and produces as output a (possibly) modified set of defining relations for $G$ and the standard presentation for the class $k+1$ $p$-quotient of $G$.

An implementation of this algorithm has been developed as part of the ANU $p$-Quotient Program. A number of examples of its performance were presented.

## Herbert Pahlings

### Characters in GAP

The programs for computing with character tables of finite groups, which are now contained in the computer algebra system GAP are surveyed. As examples of its use the following problems were considered:

Question 1: Is every multiple of a primitive character of a finite group primitive too?

Question 2: Is it true, that for every irreducible character $\chi$ of a finite group G there is a character $\phi$ of a proper subgroup such that $(\chi, \phi^G)_G = 1$?

Question 1 has a positive answer for solvable groups, as was shown by Ferguson and Isaacs, who also raised the question for general groups. A search, using the character table library of GAP quickly produces the

following examples of primitive characters multiples (in fact, doubles) of which are imprimitive: $J_2$ ($\chi_{20}$), $Ru$ ($\chi_{33}$), and $Suz$ ($\chi_{36}$).

Question 2 apparently was first raised by Janusz in 1966; it came up again in various contexts, e.g. recently in a paper of Ritter and Sehgal on units of integral group rings. O. Bonten (Aachen) has shown, that $J_4$ provides a counterexample. Another such example is given by the sporadic simple group $Ly$ ($\chi_{37}$). Since not all of the character tables of the maximal subgroups of $Ly$ are known at present, a proof required the construction of permutation characters using a new algorithm due to T. Breuer (Aachen).

## Götz Pfeiffer

### Tables of marks in GAP

Let the group $G$ act on a set $\Omega$ and define the *mark* $\beta_\Omega(G)$ to be the number of fixed points of $G$. Burnside considered all transitive actions of $G$ on the cosets $G/A$ of its subgroups $A$ and defined the *table of marks* of $G$ as the matrix $(\beta_{G/A}(B))_{A,B}$ where both $A$ and $B$ run through a list of representatives of conjugacy classes of subgroups of $G$. The table of marks provides a compact description of the subgroup lattice of $G$, since $\beta_{G/A}(B) = |\{A^x \geq B | x \in G\}||N_G(A) : A|$. The number of conjugates of a subgroup $B$ which are contained in a subgroup $A$ of $G$ can be expressed in terms of marks, in particular the total number of subgroups of $G$ can be computed from the table of marks. A Mackey decomposition of tensor products informs about intersections of subgroups. The table of marks describes the Burnside ring of $G$ and can be used to investigate its structure (idempotents, units).

Let $\mu$ denote the Möbius function of the subgroup lattice of $G$ and $\lambda$ that of the poset of conjugacy classes of subgroups of $G$. Hawkes, Isaacs, Özaydin, and Pahlings compared these functions and proved the following

**Theorem.** If $G$ is solvable and $a \leq G$ then

$$\mu(A, G) = |N_{G'}(A) : G' \cap A| \, \lambda(A, G).$$

These values of $\mu$ and $\lambda$ can be computed from the table of marks and provide counterexamples for non-solvable $G$: the simple groups $M_{12}$ and $McL$ don't have the stated property for $A = 1$.

The table of marks can be constructed from the subgroup lattice of $G$ by counting conjugates. Alternatively it can be computed by inducing marks from (maximal) subgroups of $G$.

**Theorem.** Let $A, B \leq U \leq G$. Then

$$\beta_{G/A}(B) = |N_G(B)| \sum_{B' \sim B} \frac{1}{|N_U(B')|} \beta_{U/A}(B')$$

where the sum ranges over all representatives $B'$ of conjugacy classes of subgroups of $U$ which are conjugate to $B$ in $G$.

It remains to determine the fusion of the conjugacy classes of subgroups of the maximal subgroups into $G$. For that purpose two equivalence relations $\star$ and $\equiv$ are introduced on the disjoint union of the sets of conjugacy classes of subgroups of all representatives of maximal subgroups of $G$, such that always $[A] \star [B] \Rightarrow A \sim B \Rightarrow [A] \equiv [B]$.

Now the relation $\equiv$ has to be refined, $\star$ has to be made more coarse until both coincide. Then they will both describe conjugation of subgroups in $G$.

A future release of GAP will contain a library of tables of marks including those of all simple groups of order less than a million, $J_3$, $M_{23}$, $M_{24}$, and $McL$, together with a library of functions that deal with tables of marks.

Wilhelm Plesken

## Constructing rational representations of finite groups

Recently B. Souvignier has computed the irreducible maximal finite subgroups of $GL(10, \mathbb{Z})$ and the irreducible Bravais groups of degree 8. G. Nebe and myself have determined the irreducible maximal finite subgroups of $GL(n, \mathbb{Q})$ for $n \leq 23$. For these applications it is important to have algorithms to construct irreducible rational representations of finite groups. These can be extracted from reducible representations, once the centralizer algebra is known. The latter can be obtained by a summation process over the group, which however is not practical. By using the Perron-Frobenius theorem for positive matrices it is shown that the summation process can be approximated by iterating the summation only over a set of generators.

Sarah Rees

## Computing quotients of finitely presented groups

In collaboration with Derek Holt I have implemented in C an interactive graphics program QUOTPIC which, given a finitely presented group $G$, constructs and displays finite quotients of $G$ in a lattice, thus allowing the user to gain very quickly a general overview of the group. Standard permutation group algorithms are called by QUOTPIC via UNIX system calls. The main group theoretic techniques currently consist of

(i) a C program PERMIM, which enumerates maps from $G$ onto given finite permutation groups,

(ii) various variations of the Reidemeister-Schreier procedure, and

(iii) the MEATAXE program for computing the lattice of submodules over a finite group ring.

The design of QUOTPIC has made it easy to import code from elsewhere, for example the MEATAXE is the Aachen implementation and the $p$-Quotient from the ANU. We have plans to extend our repertoire of programs, thus substantially increasing the versatility of the system (for example, we shall soon be incorporating a low index subgroup program, and a general nilpotent quotient).

QUOTPIC is available via anonymous ftp from tuda.ncl.ac.uk, where it sits in pub/local/nser in tar files isomtar1.Z etc.

Edmund F. Robertson

## Programs to enumerate semigroups and using these programs to study semigroup presentations

Two programs to enumerate semigroups have been developed in St. Andrews. Using these programs to investigate semigroup presentations has led to many interesting results and conjectures. This talk will describe results about the semigroups

$$\langle a_1, a_2, \ldots, a_n \mid a_i^{m+1} = a_i,\ a_i a_j^2 = a_j a_j^2\ (1 \leq i \leq j \leq n) \rangle$$

and the semigroups

$$\langle r, s \mid r^3 = r,\ s^{a+1} = s,\ w_1(r,s) = w_2(r,s) \rangle.$$

Interesting questions about groups related to the second class of semigroups arise.

## Derek J. S. Robinson

### Theoretical algorithms for finitely generated soluble groups

It is known that the word problem and the isomorphism problem are insoluble for finitely presented soluble groups of derived length 3. Despite this, the prospects for a successful algorithmic theory of suitable classes of finitely generated soluble groups remain favourable. In particular a large number of algorithms have been constructed for polycyclic groups and for finitely generated metabelian groups. For plycyclic groups these are due to G. Baumslag, F. B. Cannonito, D. Segal, and the author (J. Algebra 142 (1991), 118-149); the results for finitely generated metabelian groups are contained in a preprint by Baumslag, Cannonito, and the author.

As a result of this work, it is in principle possible to carry out many standard group theoretic constructions. For example, there are algorithms to find the centre, Fitting subgroup, centralizers and normalizers, limit of the lower central series, and Frattini subgroup. It remains to be seen whether any of these algorithms is implementable.

## Gerhard Schneider

### Computing Loewy-series and projective resolutions

An algorithm for computing the endomorphism ring of a $KG$-module can be modified to compute the homomorphisms between two $KG$-modules. This can be used to determine the Loewy-series of a $KG$-module by computing maps from the $KG$-module onto the various simple $KG$-modules. Several examples will be given, such as the series for the projective indecomposable modules of $M_{12}$ in characteristic 2 and 3 and $Sz(8)$ in characteristic 2.

Furthermore, the algorithm can be used to determine maps between projective covers $P_M, P_N$ of simple $KG$-modules $M, N$ and to determine

the quiver with relations for the group algebra. Non-commutative Gröbner-basis methods are employed to determine the projective resolutions for simple $KG$-modules; as an example $U_3(3)$ was discussed. The second part of the talk is joint work with Ed Green, Virginia Tech.

It is always assumed, that char$K$ divides the group order.

## Martin Schönert

### Domains in GAP

The concept of **domains** is the most important difference between GAP 2.4 and the new release GAP 3.1. A domain in GAP is simply a structured set. Examples of domains are the ring of integers, permutation groups, or even conjugacy classes of subgroups.

Some domains such as `GaussianIntegers` are predefined in the GAP library. Most domains are created by **domain constructors** such as `Group` or `GaloisField`. Also many library functions such as `Stabilizer` return domains.

Domains can be handled just like other objects, e.g., they can be assigned to variables, put into lists or records, and passed to functions. **Set theoretic functions** such as `Size` or `Intersection` accept domains of any type. Other functions are only applicable to domains that belong to a certain **category**. For example the function `Centre` is only applicable to groups, i.e., domains that belong to the category of groups.

Domains are represented in GAP by **domain records**. Initially such a domain record only holds enough information to identify this domain. As more knowledge is computed for a domain this knowledge is stored in the domain record. It is important to note that all knowledge GAP has about a certain domain is contained in the domain record, and is therefore accessible.

A special component in the domain record, the so called **operations record**, contains a special **method** for every function applicable to this domain. Thus one function is implemented by different methods for different domains. For example, for permutation groups the function `Size` is implemented by a method which uses a Schreier–Sims algorithm to compute a stabilizer chain.

Ákos Seress

**Almost linear time algorithms for small base permutation groups**

In the last couple of years, there was significant progress in the development of almost linear time algorithms for small base permutation groups. These are (mostly random) algorithms with worst case running time $O(n \log^c |G|)$ for $G \leq S_n$; in particular, for the important class of groups of polylogarithmic base size, the running time is $O(n \log^{c'} n)$. We review algorithms for constructing a composition series, centralizers of normal subgroups, Fitting subgroup, and the maximal solvable normal subgroup.

These algorithms are implemented in the GAP system.

Charles C. Sims

**Computation with finitely presented groups**

The first part of the talk presented a brief report on the status of computing with finitely presented groups. Many of the algorithms used in such computations have wider applications and provide natural bridges to other parts of computational algebra. There is a need to reconsider terminology as we begin to compute in infinite polycyclic groups. The literature in the field is of widely varying quality with the weakest papers related to calculations of Hermite and Smith normal forms of integer matrices. A great deal of powerful software has been developed, but there is so far no single package which incorporates all the available tools. There is a need for implementations of the basic operations in infinite polycyclic groups, of the Baumslag-Cannonito-Miller polycyclic quotient algorithm, and the solution to the word problem for one-relator groups. Since complexity analyses are generally lacking, we must rely heavily on experimental evidence. Carefully designed experimentation is difficult but much more needs to be done. Makanin's result on the decidability of existence of solutions to equations over free groups could in principle have applications to the study of Burnside groups, but the algorithm as stated is not practical.

The second part of the talk reported on some experiments with $R = R(2,5)$. If $R = \langle a, b \rangle$ and $x = ab$ and $y = ba$, then

$$yx^2y^2xy^3xy^2x^2y = x^3yxyx^3yxyx^3$$

holds in $R$. This, and the relation obtained by interchanging $x$ and $y$, are now known for the shortest monoid relations in $a$ and $b$ which hold in $R$ but may not hold in $B(2,5)$. Confluent sets of rewriting rules with respect to the length-plus-lexicographic ordering save roughly a factor of 9 in space compared to coset tables for the quotients $R/\gamma_{c+1}(R)$, $c = 1, ..., 5$.

## Michael C. Slattery

### Double cosets and transversals in finite soluble groups

Using the homomorphism principle and orbit-stabilizer one can compute a set of $H, K$ double coset representatives in a finite soluble group $G$. An improvement can be obtained by using techniques similar to the Generalized Covering Lemma in the Intersection Algorithm described by Slattery and Glasby. This reduces the orbit sizes.

While this leads to a possible method for working with right transversals of subgroups in soluble groups, it turns out that the standard approach to transversals in $p$-groups provides a correct method for *left* cosets in arbitrary soluble groups. Right cosets can then be handled by taking inverses.

## Geoff Smith

### Solving infinitely many linear equations in infinitely many unknowns

Let $P$ be a finite $p$-group. Except in degenerate circumstances, a linear recurrence will define a periodic bi-infinite sequence in $P$, the fundamental period of the sequence being called the Wall number of the sequence.

This talk concerned the relationship between this Wall number, and the period of the recurrence in $GF(p)$ with initial data $0, 0, ..., 0, 1$ (say $k$). In general the length of a sequence in $P$ will divide $kp^t$ where $t$ can be described in terms of the structure of $P$.

In special circumstances, $t$ can be chosen to be 0. In order to prove this fact (for a given recurrence, for all but finitely many primes $p$), one can study sums and multiple sums, over a fundamental period, of periodic functions $f : \mathbb{Z} \to GF(p)$.

The evaluation of these sums or integrals can be accomplished by a linearizing device, which leads to systems of infinitely many linear equations

in infinitely many unknowns. These equations exhibit such a high degree of symmetry that if one can force any specified unknown to vanish, all must vanish.

The argument is completed by taking a sufficiently large subset of the equations and solving them on a Computer Algebra system (AXIOM, née SCRATCHPAD).

Leonard H. Soicher

**GRAPE (GRaph Algorithms using PErmutation groups)**

GRAPE is a computer system, based on GAP 3.1, for constructing and analysing graphs related to permutation groups and finite geometries. Each graph $\Gamma$ in GRAPE comes with an associated $G \leq \mathrm{Aut}\Gamma$, and this $G$ is used to reduce the time and store requirements for calculations with $\Gamma$. GRAPE is available free of charge from the author.

Zusammengestellt von V. Felsch (Aachen)

## Tagungsteilnehmer


Dr. Greg Butler
Concordia University
Depart. of Computer Science
1455, de Maisonneuve,
Blvd. West

Montreal Quebec H3G 1M8
CANADA

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

Boston , MA 02115
USA

Dr. Colin M. Campbell
The Mathematical Institute
University of St. Andrews
North Haugh

GB- St. Andrews Fife, KY16 9SS

Prof.Dr. John D. Dixon
Dept. of Mathematics and Statistics
Carleton University

Ottawa, Ontario , K1S 5B6
CANADA

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

I-38050 Povo (Trento)

Dr. Volkmar Felsch
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

W-5100 Aachen
GERMANY

Frank Celler
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

W-5100 Aachen
GERMANY

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

Boston , MA 02115
USA

Dr. Arjeh M. Cohen
Stichting Mathematisch Centrum
Centrum voor Wiskunde en
Informatica
Kruislaan 413

NL-1098 SJ Amsterdam

Dr. Meinolf Geck
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

W-5100 Aachen
GERMANY

Prof.Dr. Robert Gilman
School of Mathematics
Institute for Advanced Study

Princeton , NJ 08540
USA

Prof.Dr. I. Martin Isaacs
Department of Mathematics
University of Wisconsin-Madison
Van Vleck Hall
480 Lincoln Drive

Madison WI, 53706
USA

Dr. Stephen P. Glasby
School of Mathematics & Statistics
University of Sydney

Sydney N.S.W. 2006
AUSTRALIA

Dr. Ingo Janisczak
Institut für Experimentelle
Mathematik
Universität-Gesamthochschule Essen
Ellernstr. 29

W-4300 Essen 12
GERMANY

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

Queensland 4072
AUSTRALIA

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

Eugene , OR 97403-1222
USA

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

W-6900 Heidelberg 1
GERMANY

Prof.Dr. Adalbert Kerber
Fakultät für Mathematik und Physik
Universität Bayreuth
Postfach 10 12 51

W-8580 Bayreuth
GERMANY

Dr. Derek F. Holt
Mathematics Institute
University of Warwick

GB- Coventry , CV4 7AL

Dr. Wolfgang Kimmerle
Mathematisches Institut B
Universität Stuttgart
Pfaffenwaldring 57
Postfach 80 11 40

W-7000 Stuttgart 80
GERMANY

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

W-6900 Heidelberg 1
GERMANY

Dr. Stephen Linton
111 Ross Street

GB- Cambridge CB1 3BS

Prof.Dr. Victor D. Mazurov
Institute of Mathematics
Siberian Branch of the Academy of Sciences
Universitetskiy Prospect N4

Novosibirsk 630090
RUSSIA

Dr. Andrea Lucchini
Dipartimento di Matematica
Universita di Padova
Via Belzoni, 7

I-35131 Padova

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

Montreal Quebec H3G 1M8
CANADA

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

Eugene , OR 97403
USA

Prof.Dr. Joachim Neubüser
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

W-5100 Aachen
GERMANY

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

W-5100 Aachen
GERMANY

Dr. Peter M. Neumann
Queen's College
High Street

GB- Oxford OX1 4AW

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

Canberra ACT, 2601
AUSTRALIA

Werner Nickel
Mathematics, I.A.S.
Australian National University
G.P.O. Box 4

Canberra , A.C.T. 2601
AUSTRALIA

Alice Niemeyer
Mathematics Research Section
IAS
Australian National University
GPO Box 4

Canberra ACT 2601
AUSTRALIA

Prof.Dr. Eamonn A. O'Brien
Mathematics Research Section
IAS
Australian National University
GPO Box 4

Canberra ACT 2601
AUSTRALIA

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

W-5100 Aachen
GERMANY

Richard A. Parker
Springfields
Froglane

GB- Shepton Mallet, Somerset

Götz Pfeiffer
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

W-5100 Aachen
GERMANY

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

W-5100 Aachen
GERMANY

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

Nedlands , WA 6009
AUSTRALIA

Dr. Sarah Rees
Department of Mathematics
and Statistics
University of Newcastle

GB- Newcastle Upon Tyne NE1 7RU

Dr. Edmund F. Robertson
The Mathematical Institute
University of St. Andrews
North Haugh

GB- St. Andrews Fife, KY16 9SS

Prof.Dr. Derek J.S. Robinson
Department of Mathematics
University of Illinois
273 Altgeld Hall MC-382
1409, West Green Street

Urbana , IL 61801-2975
USA

Prof.Dr. Aleksander I. Skopin
St. Petersburg Branch of
Mathematics Institute
of the Academy of Sciences
Nab. Fontanka 27

St. Petersburg 191011
RUSSIA

Dr. Gerhard J.A. Schneider
RZ Karlsruhe
Zirkel 2

W-7500 Karlsruhe
GERMANY

Prof.Dr. Michael C. Slattery
Dept. of Mathematics, Statistics
and Computer Science
Marquette University

Milwaukee , WI 53233
USA

Martin Schönert
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64

W-5100 Aachen
GERMANY

Dr. Geoffrey C. Smith
School of Mathematical Sciences
University of Bath
Claverton Down

GB- Bath , Avon , BA2 7AY

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

Columbus Ohio 43210-1174
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. Charles C. Sims
Dept. of Mathematics
Rutgers University
Busch Campus, Hill Center

New Brunswick , NJ 08903
USA

Beate Thielcke
Institut für Experimentelle
Mathematik
Universität - GH Essen
Ellernstraße 29

W-4300 Essen 12
GERMANY

E-mail addresses
---

| | |
|---|---|
| Butler, Greg | gregb@cs.concordia.ca |
| Campbell, Colin M. | cmc@maths.st-andrews.ac.uk |
| Caranti, Andrea | caranti@itnvax.cineca.it |
| Celler, Frank | fceller@bert.math.rwth-aachen.de |
| Cohen, Arjeh M. | marc@cwi.nl |
| Cooperman, Gene | gene@corwin.ccs.northeastern.edu |
| Dixon, John D. | jdixon@carleton.ca |
| Felsch, Volkmar | felsch@math.rwth-aachen.de |
| Finkelstein, Larry A. | laf@corwin.ccs.northeastern.edu |
| Geck, Meinolf | geck@kalliope.iwr.uni-heidelberg.de |
| Gilman, Robert H. | rgilman@sitvxc.stevens-tech.edu |
| Glasby, Stephen P. | glasby_s@maths.su.oz.au |
| Havas, George | havas@cs.uq.oz.au |
| Hiss, Gerhard | hiss@kalliope.iwr.uni-heidelberg.de |
| Holt, Derek F. | dfh@maths.warwick.ac.uk |
| Isaacs, I. Martin | isaacs@math.wisc.edu |
| Janiszczak, Ingo | mat480@de0hrz1a.bitnet |
| Kantor, William M. | kantor@bright.math.uoregon.edu |
| Kerber, Adalbert | kerber@btm2x2.mat.uni-bayreuth.de |
| Kimmerle, Wofgang | kimmerle@phoebus.mathematik.uni-stuttgart.de |
| Leedham-Green, Charles R. | crlg@maths.qmw.ac.uk |
| Linton, Steve | sl25@phx.cam.ac.uk |
| Lucchini, Andrea | lucchini@pdmat1.unipd.it |
| Luks, Eugene M. | luks@cs.uoregon.edu |
| Lux, Klaus | lux@math.rwth-aachen.de |
| Malle, Gunter | malle@kalliope.iwr.uni-heidelberg.de |
| Mazurov, Victor D. | mazurov@math.nsk.su |
| McKay, John | mckay@vax2.concordia.ca |
| Neubueser, Joachim | neubueser@math.rwth-aachen.de |
| Neumann, Peter M. | neumann@vax.ox.ac.uk |
| Newman, Michael F. | newman@pell.anu.edu.au |
| Nickel, Werner | werner@pell.anu.edu.au |
| Niemeyer, Alice C. | alice@pell.anu.edu.au |
| O'Brien, Eamonn A. | obrien@pell.anu.edu.au |
| Pahlings, Herbert | pahlings@math.rwth-aachen.de |
| Parker, Richard | rap1@phx.cam.ac.uk |
| Pfeiffer, Goetz | goetz@math.rwth-aachen.de |
| Plesken, Wilhelm | plesken@willi.math.rwth-aachen.de |
| Praeger, Cheryl E. | praeger@maths.uwa.edu.au |
| Rees, Sarah | sarah.rees@newcastle.ac.uk |
| Robertson, Edmund F. | efr@maths.st-andrews.ac.uk |
| Robinson, Derek J. S. | robinson@symcom.math.uiuc.edu |
| Schneider, Gerhard | mat420@de0hrz1a.bitnet |
| | schneider@dkauni2.bitnet |
| Schoenert, Martin | martin@math.rwth-aachen.de |
| Seress, Akos | akos@function.mps.ohio-state.edu |
| Sims, Charles C. | sims@math.rutgers.edu |
| Skopin, Alexander | root@lek.spb.su |
| Slattery, Michael C. | mikes@sylow.mscs.mu.edu |
| Smith, Geoffrey C. | masgcs@maths.bath.ac.uk |
| Soicher, Leonard H. | l.h.soicher@qmw.ac.uk |
| Thielke, Beate | mem310@de0hrz1a.bitnet |
| Wursthorn, Martin | pluto@phoebus.mathematik.uni-stuttgart.de |