MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 22/1988

COMPUTATIONAL GROUP THEORY

15.5. bis 21.5.1988

The two organizers of the conference, J. Neubüser (Aachen) and C. Sims (Rutgers) were glad to welcome 55 participants from 11 countries.
In numerous talks algorithms for computing with finitely presented groups, with solvable groups, with p-groups and finally with representations of finite groups were presented and discussed. Several speakers demonstrated how they had successfully applied some of these algorithms to various problems.
For the first time in an Oberwolfach meeting a variety of computers had been brought to the institute. The firms MASSCOMP and SUN had provided an MC 5600 and a SUN 3/60 resp. free of charge. Also the institute now owns two MacIntosh II computers, donated by APPLE. An ATARI and an HP-VEKTRA, as well as peripheral equipment, had been brought along from Lehrstuhl D für Mathematik of the RWTH Aachen.
Several persons provided software to demonstrate algorithms.

> The Sydney CAYLEY system, which includes most of the algorithms for computing with finite groups (cf. the abstract by J. Cannon) was available, as was GAP, a system for groups and programming, recently developed in Aachen, which enables the users to implement their own algorithms easily (cf. the abstracts by M. Schönert and W. Plesken).
>
> SPAS, a system originating from Canberra, St. Andrews and Aachen, includes the main coset table methods for finitely presented groups (cf. the abstract of J. Neubüser's first talk). Various programs were supplied by C. Sims for experiments with the Knuth-Bendix algorithm, coset enumeration and the low index subgroup procedures (cf. C. Sims' abstract). D. Holt from Warwick also provided an implementation of the Knuth-Bendix algorithm.
>
> The Aachen SOGOS system (cf. the abstract of J. Neubüser's second talk) computes in finite soluble groups.
>
> A nilpotent quotient program was available from Canberra which had been applied to classify p-groups (see O'Brien's abstract). L. Soicher provided his "Deep Thought" system for multiplying in nilpotent groups, which includes various experimental collectors (cf. the abstract of his talk).

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Classical character theory was represented by CAS, the Aachen system for the handling of ordinary characters. To find the modular representations of finite groups is the principal purpose of R. Parker's MEAT-AXE (cf. Parker's abstract). The MOC system, which was developed at Aachen with major contributions from R. Parker is intended to assist the user in calculating the modular characters of a finite group (cf. the abstracts of K. Lux and G. Hiß). To find 1^{st} and 2^{nd} cohomology groups and Schur multipliers of finite groups is the purpose of COHOMOLOGY, a program written by D. Holt.

As a novelty in a Computational Group Theory meeting there were also some systems available specifically oriented towards infinite groups. From CWI, Amsterdam, originated LIE, a system for Lie group computations, such as multiplicities, tensor product decompositions and Weyl group computations (cf. A. Cohen's abstract). Then there was PNCRE which tests the discreteness of a given group $\Gamma \subset SL_2(\mathbf{C})$ and if it is discrete, finds a presentation (cf. R. Riley's abstract).

Finally, some programs written in MAPLE by R. Sommeling at CWI, Amsterdam, to compute the Galois group of a polynomial over the rationals could also be used since the MAPLE system (University of Waterloo) was available.

All these programs were intensively used during the meeting.
The 43 talks given during the conference illustrated the whole range of methods and applications of Computational Group Theory. The discussion following the talks and the exchange of new implementations made very clear that this young branch of mathematics is of increasing interest to a continuously growing number of mathematicians.

Abstracts

R. Brandl: Finite varieties and a finitely presented group

It is known that there exists a sequence $w_1, w_2, \ldots$ of words in two variables with the following property: The finite group G is soluble if and only if $w_k(G) = 1$ for all but finitely many values of k. We present some explicit sequences in four variables and discuss a question whose answer would yield a satisfactory series involving two variables. This leads to the groups $G(a,b) = \langle X, Y \mid X = [X, {}_aY], Y = [Y, {}_bX] \rangle$ that have $SL(2,q)$ as a quotient for various values of q, a and b. For example, $G(5,5)$ maps onto $SL(2,5)$. Nothing is known about $G(2,3)$, however it seems that adjoining the extra relations $X^r = 1$, $Y^s = 1$ where r and s are coprime, causes the group to collapse. (Joint work with J. S. Wilson.)

C. M. Campbell: Presentations for simple groups

In a recent paper with E. F. Robertson (St. Andrews) and P. D. Williams (San Bernardino) we give presentations for the groups $PSL(2,p^n)$, p prime, which show that the deficiency of these groups is bounded below. We also give deficiency -1 presentations for direct products of $SL(2,2^{n_i})$ for coprime n_i.

In this talk we describe certain new efficient presentations given in that paper for certain cases of these groups. Further we consider the groups $PSL(2,p) \times PSL(2,p)$, giving a 2-generator 6-relation presentation for these groups. We give efficient (2-generator 4-relation) presentations in some cases.

J. Cannon: Cayley Version 4

Cayley Version 4 is a computer algebra system designed to support computation with discrete algebraic and combinatorial structures. The computational domains planned for the system include various classes of groups, algebraic number fields, modules, rings, finite geometries, graphs, designs and codes. The programming language is designed around the notions of algebraic structure, set, sequence and mapping. The use of a powerful set constructor, which permits a set to be defined in terms of properties, leads to a particularly compact method of programming.

P. Le Chenadec: Knuth-Bendix Algorithm and Dehn Algorithm

Assume $G = \langle \mathbf{g}, \mathcal{E} \rangle$ is a finite group presentation. In the Knuth-Bendix algorithm, restrict the computation of critical pairs to the "normal" or "group" ones:

$$k : a_1 \cdots a_n \rightarrow b_1 \cdots b_m, \; a_i, b_j \in \mathbf{g},$$

$$normal \;\; pairs : \begin{cases} (a_2 \cdots a_n, a_1^{-1} b_1 \cdots b_m) \\ (a_1 \cdots a_{n-1}^{-1}, b_1 \cdots b_m a_n^{-1}) \\ (a_n^{-1} \cdots a_1^{-1}, b_m^{-1} \cdots b_1^{-1}) \end{cases}$$

The Knuth-Bendix algorithm halts and computes a symmetrized set of defining relations $\mathcal{R}$. Ask now what are the minimal conditions that will imply the solvability of the word problem for the given presentation of G by $\mathcal{R}$. Answer: the usual condition $C'(1/4)$ of small cancellation theory plus some new condition: the non-existence of some diagrams in the Cayley graph of G. So yet another proof of the fundamental result of small cancellation theory is obtained. It sharpens the usual ones in the following way: 1) the usual metric conditions imply the new ones. 2) The group $G = \langle A, B, C \mid ABC = CBA \rangle$ becomes an s.c. group, 3) we have structural hints on the Cayley graph of s.c. groups.

M. CLAUSEN: Fast Wedderburn Transforms

Let G be a finite group. Then $L_s(G)$, the linear complexity of a suitable Wedderburn transform for $\mathbf{C}G$, is smaller than $2 \cdot |G|^2$. The FFT algorithms improve this trivial upper bound by showing that for cyclic groups G, $L_s(G) = O(|G| \cdot \log |G|)$. Motivated by applications in digital signal filtering, we are interested in extending these results to other classes of groups. Some results: If G is a dihedral or generalized quaternion group then $L_s(G) = O(|G| \cdot \log |G|)$, for symmetric groups we have $L_s(S_n) = O(|S_n| \cdot \log^3 |S_n|)$. For all groups G of order 64 we have (joint work with U. Baum and T. Beth) $L_s(G) \leq 3/2 \cdot |G| \cdot \log |G|$. In general, our investigations indicate that fast Wedderburn transforms are adapted to certain subposets of the subgroup lattice of G. CAYLEY and CAS are of great use in finding the relevant data.

A. M. COHEN: Finite subgroups of $E_8(\mathbf{C})$, and an interactive software package for Lie groups

Computer algebra aspects of embedding finite groups in exceptional Lie groups have been discussed. Also, we introduced an interactive software package, entitled LIE, to which this study has led.

J. D. DIXON: Galois Theory and Computation in Fields

Let $f(X) \in \mathbf{Z}[X]$ be a monic irreducible polynomial with roots $\Omega := \{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n\}$. Let $G = Gal(f)$, considered as a permutation group on Ω.

Then $\mathbf{Q}(\alpha)$ is the fixed field of the point stabilizer G_α, and so $\mathbf{Q}(\alpha)$ has a subfield F of index $d \iff G$ has a block of imprimitivity Δ of size d. If the latter holds then 'generically', if $\Delta = \{\alpha_1, \ldots, \alpha_d\}$, then we can take $F = \mathbf{Q}(\delta)$ with $\delta = \alpha_1 \cdots \alpha_d$.

Often we have certain information about $Gal(f)$ which suggests the existence of such a subfield. In the talk I outlined a method of calculating the roots of $f(X)$ over a p-adic field $\mathbf{Q}_p$, determining a small list of d-subsets which might form a block, and deciding whether the corresponding δ generates a subfield of F.

L. FINKELSTEIN: Computation in Permutation Groups Using Labelled Branchings

In this talk we describe new algorithms for performing fundamental group computations. The algorithms are based, in part, on a new data structure for representing permutation groups invented by M. Jerrum and referred to as complete labelled branching. This data structure allows the complete coset table for a permutation group G acting on n points to be represented using $O(n^2)$ space, and for a coset representative to be accessed in $O(n)$ time. This data stucture was used by Jerrum to give the first algorithm for computing a strong generating set for a permutation group using $O(n^5)$ time and $O(n^2)$ space. We will use labelled branchings to present a new change of basis algorithm for permutation groups (Brown, Finkelstein, Purdom) which generalizes Sims' original method and which runs in time $O(n^3)$, an improvement of two orders of magnitude. We will then describe an algorithm for testing whether a set S of generators for G is a strong generating set in $O(n^2|S| + n^4)$ time. As a consequence of this test, we are able to construct a presentation for G using at most $n-1$ generators and $(n-1)^2$ relations (Brown, Cooperman and Finkelstein). This is an improvement on the best known previous bound of $O(n^2(\log(n))^c)$ for the number of relations given by Babai, Luks and Seress. In addition, we will show how our test can be used to give an improved algorithm for constructing a complete labelled branching for G (and hence a strong generating set) which will run substantially faster in practice than Jerrum's original $O(n^5)$ algorithm.

R. GILMAN: The Knuth-Bendix Procedure

The Knuth-Bendix procedure attempts to turn an arbitrary finite presentation for a group G into a confluent one. The procedure may also be used to enumerate the cosets in G of a finitely generated subgroup H and may succeed even if it fails to converge on the presentation for G itself.

S. P. GLASBY: Algorithms for Finite Soluble Groups

Algorithms are presented here for calculating normalizers and intersections in a finite soluble group G. Most attention will be given to algorithms for computing the normalizer in G of Hall π-subgroups and for computing the intersection of two subgroups whose indices in G are coprime. An algorithm for conjugating one given Hall π-subgroup to another is used to construct Hall π-subgroups, and is also used by the normalizer algorithm. The above algorithms may be used to construct system normalizers, Carter subgroups and Sylow bases. Details of algorithms for computing normalizers of arbitrary subgroups and for computing the intersection of two arbitrary subgroups will be described in a forthcoming joint paper with M. Slattery.

G. HAVAS: Supercomputer Applications

Some applications of supercomputers to group theory were considered. Specific examples were a nilpotent quotient algorithm for Lie rings, CAYLEY, and integer matrix diagonalization.

The nilpotent quotient algorithm for Lie rings (as distinct to that for groups) is particularly well suited for vectorization of the Lie product operation (whereas collection in groups is much more difficult). Some results on Lie algebras related to Burnside groups were presented.

A FORTRAN version of CAYLEY has been installed on a FACOM VP100 supercomputer. A C version on a Cray machine is planned.

The integer matrix diagonalization algorithm is ideal for vectorization. Vectorization ratios exceeding 90% are readily achieved. Use of a vector supercomputer effectively cuts the calculation time, which is polynomial in the matrix rank, by reducing the polynomial degree by 1.

G. HISS: MOC: a modular character system—theoretical background

MOC is a computer system for dealing with modular characters. It was developed in Aachen in joint work with R. Parker and K. Lux. Some theory behind this system is described in my talk.

Certain bases for the ring of generalized Brauer characters and projective characters are introduced. Firstly, basic sets of Brauer characters resp. projective characters are defined and secondly, in duality to these, bases of Brauer atoms and projective atoms. The problem of finding all possible decomposition matrices for a finite group, which are consistent with a given set of information, can be reduced to the following problem.

Let A, B, U be integral matrices such that U is square, has determinant 1 and non-negative entries. Find all integral square matrices U_1, U_2 with $U = U_1 \cdot U_2$ such that U_1, U_2, $A \cdot U_1$ and $B \cdot U_2$ have non-negative entries.

D. F. Holt: Computing with infinite finitely presented groups

Certain infinite groups defined by finite presentations that arise naturally from geometry and topology (the Von Dyck groups, for example) can be shown to have very regular properties, in a precise sense. This means that a normal form can be found for the group elements (which will consist of shortest words for the elements), and efficient algorithms exist for putting arbitrary words into normal form. These algorithms involve computations using finite state automata, and they are expected to have applications to the underlying geometrical or topological structure. Practical methods for constructing these automata will be discussed. Methods that have been attempted to date include Todd-Coxeter coset enumeration and Knuth-Bendix reduction.

D. Johnson: Power-Series Groups

Iain York (research student) has made use of REDUCE (Nottingham) and CAYLEY (Manchester) packages to find invariants of power-series groups $G_n(p)$ = {integer polynomials under substitution}/(x^{n+1}, p). ($G_n(p)$ has order p^{n-1}.) As a result, several conjectures have been formulated, and some of them have been proved. For example, the class and exponent of $G_n(p)$ are now known explicitly in all cases.

W. Kantor: Short Presentations

Define the length of a presentations $\langle X \mid R \rangle$ to be $|X| + \sum_{r \in R} l(r)$, where $l(r)$ is the length of r as a word in $X \cup X^{-1}$. The following have been proved by Babai-Kantor-Luks-Pálfy.

Theorem 1. *Every finite group G has a presentation of length $O((\log|G|)^3)$; the exponent 3 is best possible.*

Theorem 2. *Every finite simple group G has a presentation of length $O((\log|G|)^2)$—and even one of length $O(\log|G|)$ if G is neither an odd-dimensional unitary group nor a rank 1 group of Lie type.*

Conjecture. *Every finite simple group has a presentation of length $O(\log|G|)$.*

A. Kerber: Algebraic Combiantorics: The Use of Finite Group Actions

Combinatorial applications of the Cauchy-Frobenius lemma and Burnside's lemma (both in their constant and weighted form) were shown in this review talk, together with constructive methods (direct, probabilistic and recursive ones).

C. R. LEEDHAM-GREEN: Computing in p-groups

A number of remarks about computing in groups of prime power order were made. For example

(i) An important source of examples comes from linear groups over local fields. We have programs to compute in such groups, including a program for arithmetic in local fields of characteristic 0 written by a Ph.D. student C. Murgatroid.

(ii) The dramatic improvement in our collection algorithm over the traditional method has a theoretic explanation. Theory and praxis show that the time required for our method increases exponentially in the derived length rather than the class of the group.

(iii) Our symbolic method of multiplying elements of a p-group, called 'deep thought', as an alternative to collection, allows us to perform calculations very rapidly that are completely out of range for collection. The method requires further development, and we would welcome collaboration.

This is joint work with L. Soicher.

R. J. LIST: Certain Groups Associated with Finite Projective Geometries

The abelian groups determined by the point-hyperplane incidence matrix and its complement are determined for the projective spaces derived from the vector spaces $V_n(p)$, where p is prime, and $n > 1$.

E. M. LUKS: Parallel Computation in Permutation Groups

We show that basic polynomial-time methods for manipulating permutation groups have fast parallel speedups. In particular, the following problems are in NC (solvable in $O(\log^{c_1} n)$ time using $O(n^{c_2})$ processors): testing membership, finding orders, finding composition series, finding presentations, finding pointwise set stabilizers. Two striking observations: **1** all these problems use deep structural information and the correctness proofs appeal to the classification of finite simple groups; **2** the techniques have led to an order of magnitude speedup in the sequential complexity, all the above problems are now solvable in $O(n^4 \log^c n)$ time. This work is joint with L. Babai and Á. Seress.

K. LUX: MOC-Algorithms

I describe a program system, MOC 2/3, written by R. Parker, G. Hiß and myself, which tries to find the Brauer character table of a finite group. It was successfully applied to the following cases: Brauer trees of sporadic simple groups and covering groups, $2 \cdot Sp_6(2)$ for primes 3, 5, $2 \cdot G_2(4)$ for $p = 3, 5$, He for $p = 7$ (A. Ryba) and ${}^3D_4(2)$ for $p = 3, 7$. The program system generates projective and Brauer characters first. Then it will find **Z**-bases for the projective and the Brauer characters. It tries to prove indecomposability of some projective characters and tries to subtract them from other projectives. This process can be iterated and finally leads to (ideally one) a few possible Brauer character tables.

B. H. MATZAT: Braid Orbits on Classes of Generators of Finite Groups

In the first section a report is given on the realizations of finite simple groups as Galois groups of regular field extensions over $\mathbf{Q}^{ab}(t)$ and $\mathbf{Q}(t)$.

In the second section the braid orbit theorems are applied to prove that the groups $PSL_2(5^2)$, $PSL_2(7^2)$ and M_{24} are Galois groups of regular field extensions over $\mathbf{Q}(t)$. Therefore, by Hilbert's irreducibility theorem, there exist infinitely many Galois extensions over $\mathbf{Q}$ with these groups as Galois groups.

J. MCKAY: The Computation of Galois Groups from Polynomials over Q

Degree shapes of f mod p give a lower bound on $G = Gal(f)$ and the integrality of polynomial invariants gives upper bounds. These techniques suffice to compute $Gal_{\mathbf{Q}}(f)$ for degree $f \leq 7$. A Galois group finder for these small degrees is implemented on MAPLE (by Ron Sommeling of Nijmegen). Open problems: Give 'explicit' expressions for the zeros of a solvable polynomial. Use ramified primes. An example of Matzat for the Mathieu group M_{11} as $Gal(f_{11})$ has been verified using p-adic approximation (on ALGEB - David Ford, Concordia U., Montreal) by Henri Darmon.

F. MENEGAZZO: An Application of SOGOS

If groups G, G_1 are given, and $\sigma : L(G) \to L(G_1)$ is an isomorphism of their subgroup lattices, it is well known that the image N^σ of a normal subgroup N of G needs not to be normal in G^σ. In the critical case where G/N is cyclic, N^σ is core-free in G_1, and both G and G_1 are finite p-groups, then N is abelian if $p \neq 2$. An example (Busetto-Stonehewer) shows that if $p = 2$ N may be non-abelian.

A. Luccini and myself, using SOGOS to do part of the checking, found one more example:

$$G = \langle a,h,k \mid a^{2^7} = h^{2^4} = k^{2^4} = 1,\ h^k = h^9,\ h^a = h^{-1},\ k^a = hk^{-1}\rangle$$

$$G_1 = \langle a_1,h_1,k_1 \mid a_1^{2^7} = h_1^{2^4} = k_1^{2^4} = 1,\ h_1^{k_1} = h_1^5,\ h_1^{a_1} = a_1^{-8}h_1^{-1},\ k_1^{a_1} = h_1^{-1}k_1^{-1}\rangle$$

where $N = \langle h,k\rangle$ has $|N'| = 2$, $N \lhd G$, $N^\sigma = \langle h_1,k_1\rangle$ is core-free in G_1. The computations ran on a VAX/VMS; CPU time is approximately 2^{h}.

J. NEUBÜSER: Subgroup Presentations Revisited

Let a group G be given by the finite presentation

$$G = \langle g_1,\ldots,g_n | r_1(g_i) = 1,\ldots,r_m(g_i) = 1\rangle.$$

For computational purposes a subgroup $U < G$ of finite index can be given in three ways:

1) by a set $S = \{s_1(g_i),\ldots,s_r(g_i)\}$, which generates U;

2) if $U \lhd G$ by a set $S = \{s_1(g_i),\ldots,s_r(g_i)\}$ such that the normal closure of S is U;

3) by a coset table of U in G.

By the Todd-Coxeter method 3) can be obtained from 1) or 2); from 3) by Reidemeisters's theorem as implemented by G. Havas, a presentation of U in terms of the $(n-1)(G:U)+1$ Schreier generators of U can be obtained, while from 1) a "modified coset table" can be constructed that allows to read off a presentation of U in terms of $s_1,\ldots,s_r$. This is advantageous, since the number of Schreier generators in the Reidemeister presentation has usually to be reduced by a sequence of Tietze transformations before it can be put to further use. In the talk a new mixture of the two methods was presented, which allows an a priori reduction of the number of Schreier generators in case U is given in one of the forms 2) or 3), and thereby also improves computing times.

A brief report on the system SPAS was also given that combines the new with some of the old methods. (Joint work with V. Felsch and A. Luchini.)

J. NEUBÜSER: Computation of the Conjugacy Classes of Soluble Groups

By recursion over a series of normal subgroups with elementary abelian factors, finding the classes of a finite soluble group G reduces to the following task:

Let N be an elementary abelian normal subgroup of G, let $g_1N,\ldots,g_rN$ be representatives of the conjugacy classes of G/N and $C_i/N := C_{G/N}(g_iN)$.

Then one has to find representatives $g_{i,j}$ of the orbits of the action of C_i on g_iN by conjugation and $Stab_{C_i}(g_{i,j})$ for all $g_{i,j}$. This can be done by the "soluble orbit algorithm," using that the orbit of a normal subgroup of C_i is a block for C_i (cf. Laue, Neubüser, Schoenwaelder; in M. Atkinson, ed., Computational group theory, (1984)). Improvements of this were given that are based on the following observation of H. Pahlings and W. Plesken, (Journ. f. d. r. u. a. Math. 380 (1987)): via the mapping $g_in \mapsto n$ of $g_iN \to N$ the operation of $c \in C_i$ by conjugation on g_iN can be replaced by the "affine" operation of C_i on N defined by $\alpha_c : n \to n^c[g_i, c]$. Since then elements $m \in N$ act by "translation" by $[g_i, m]$, it further suffices to consider the action of C_i on $N/[g_i, N]$. Compared with earlier implementations in SOGOS (1986) and CAYLEY (1987) computing times for the determination of the 181 classes of a group of order $2^{11} \cdot 3^{13}$ dropped from 41.5 minutes to 1.5 minutes. Improvement of data structure e.g. allows computation of the 52195 classes of a group of order $2^{31} \cdot 3^{13}$ in 6 hours 38 minutes on a Masscomp 5400. (Joint work with M. Mecky.)

M. F. NEWMAN: Computing in Groups of Exponent Four

The study of groups of exponent four continues to throw up interesting computational challenge. Some additions and improvements to the nilpotent quotient algorithm were described which should allow to determine the order of the 5-generator (relatively) free group B of exponent four with reasonable resources. These improvements are based primarily on a more careful analysis of the structure of an appropriate system of linear equations over $GF(2)$. From this work so far it follows that an upper bound for the order of B is 2^{2728} and it seems very likely that this is the order of B.

E. O'BRIEN: Algorithms for the Dermination of Finite p-Groups

The groups of order 256 have been determined by computer. The algorithms used in the determination are extensions of the p-group generation algorithm described by Newman (1977). The basic algorithm will be reviewed briefly and the extensions will be described in some detail. Implementation and performance details will be provided together with a summary of results.

M. F. Newman (1977), "Determination of groups of prime-power order", Group Theory (Canberra, 1975), pp. 73–84. Lecture Notes in Math. 573. Springer-Verlag.

R. PARKER: The MEAT-AXE and Related Topics

A. Pritchard has some work on low index algorithm. S. Linton has a succesful implementation of double coset enumeration. Using lexicography instead of Zorn's lemma, one can actually choose a map from the roots of 1 in fields of order p^n to complex roots of 1. This gives Brauer characters a sharper definition.

The MEAT-AXE and its development are briefly described, and the programs (in FORTRAN) are freely available to anyone who may want them.

W. PLESKEN: A Soluble Quotient Algorithm

The algorithm can compute the biggest finite soluble factorgroup of a finitely presented group in case it exists. The basic idea, which is not restricted to finite or soluble groups, is as follows: Deciding whether an epimorphism ϵ of a finitely presented group G onto a group H can be lifted to an epimorphism of G onto an extension $\tilde{H}$ of an irreducible H-module by H leads to a system of linear equations. In the situation of finite soluble images the construction of the relevant modules and extensions is also largely a matter of linear algebra. Finding the relevant new prime divisors for $|\tilde{H}|$ can be approached by using the rational representations of H.

C. E. PRAEGER: Algorithms for Finite Soluble Groups and Permutation Groups

I reported on the results of discussions with Charles Leedham-Green and Leonard Soicher aimed at developing algorithms for groups which could be implemented in a short period of time in a high level language such as CAYLEY. We concentrated on the problem of finding the kernel of a group homomorphism. We developed three algorithms: Let $G = \langle X \rangle$ and H be groups and $\Phi : G \to H$.

Algorithm 1: assumes that G and H are permutation groups for which bases are known, tests whether Φ determines a homomorphism, and if so finds the kernel.

Algorithm 2: assumes that G and H are soluble groups for which power commutator generators are known and assumes that Φ is a homomorphism; it finds power commutator presentations for the kernel and image.

Algorithm 3: is a "random algorithm." It assumes that G and H are permutation groups or soluble groups, that Φ is a homomorphism, and that $|G|$ is known. It finds the kernel and image.

S. REES: Constructing Machines for Automatic Groups

Basically a group is automatic if a finite state automaton can be used to recognize a well structured normal form for its elements (a more precise definition is given in D. Holt's talk). For many automatic groups (e.g. groups of hyperbolic isometries) such a normal form is provided by the set of all words which are a) of minimal length and b) lexicographically least according to an ordering of the generators for the group.

In this talk an algorithm (due to David Epstein) for the construction of such a machine is outlined. The machine is constructed in terms of a finite set of word differences found within a partial CAYLEY graph. The construction of the graph is weighted heavily towards the development of those areas which seem to lead to the most rapid increase in the growing set of word differences.

R. F. RILEY: Presentations of Discrete f.g. Subgroups of $SL_2(\mathbf{C})$

$\Gamma \subset SL_2(\mathbf{C})$ generated by $\vec{X} = \{X_1, \ldots, X_m\}$ is algorithmically defined if algorithms are provided to solve the word problem on $\vec{X}$ and to compute the entries of each X_k to any requested accuracy. If Γ is both alg. defined and discrete in $SL_2(\mathbf{C})$ we can get a presentation for Γ on the side-pairing transformations of an H-polyhedral fundamental domain $\mathcal{D} \subset \mathbf{H}^3$ for Γ, although if Γ is geometrically infinite the presentation is finite. My file PNCRE of FORTRAN programs decides whether Γ is discrete or not, and in favourable cases produces a presentation of Γ. It is a rather general system which has been used to compute hyperbolic structures on 3-manifolds and to give presentations of Bianchi groups, et al.

E. F. ROBERTSON: Simplifying Presentations

Joint work with K. Rutherford has resulted in a system containing many small primitive functions which can be combined to give Todd-Coxeter, Reidemeister-Schreier and Tietze transformation facilities. Considerable flexibility allows easy experimenting with different strategies. The talk reports on results obtained from this system and other programs, showing the effects of adding extra relations to the modified Todd-Coxeter obtained from early closing rows and from coincidences and the effects of different simplification strategies in applying Tietze transformations.

In particular weight functions can be used to allow substring searching with length functions on words different from the length in the free group. The user can choose weights to improve the chances of finding relators of a particular type in the final presentation.

A. RYBA: Construction of Representations of Hecke Algebras

We describe a computational technique called condensation which turns representations of a finite group into representations of a related Hecke algebra. Under certain circumstances condensation sets up a Morita equivalence between modules of the group algebra and the very much smaller modules for the Hecke algebra; this allows us to use condensation to obtain otherwise inaccessible information about the groups. We describe the use of the condensation programs in the calculation of the 2-modular characters of $G_2(3)$.

G. J. A. SCHNEIDER: Vertices and Sources

Let F be a (finite) field of characteristic p, G a finite group (such that p divides $|G|$) and let M be an indecomposable FG-module. A vertex is a subgroup P of G of smallest possible order which has an indecomposable FP-module N (a source) such that M is a direct summand of the induced module $N\uparrow^G$.

We present methods that automatically determine vertex and source for an indecomposable FG-module M. In particular we describe how to compute the ring of FG-endomorphisms of a module M and how to prove the indecomposability of M or to find an explicit decomposition.

The methods have been implemented as part of the CAYLEY system and have been used to compute a number of examples.

MARTIN SCHÖNERT: GAP, Groups and Programming

GAP is a new programming system designed for computational group theory. It tries to reduce the time spent to program new algorithms, thereby increasing the programmers and users productivity, in the following ways:

GAP has a PASCAL like programming language with special data types like permutations, finite field elements, vectors and matrices. The programming language allows to write algorithms in their most general setting, e.g. the same piece of code could be used to compute the orbit of a point in a permutation group, of a vector in a matrix group or the conjugacy class of an element in any kind of groups.

An interactive programming environment eases writing, debugging and improving programs. It allows for example to trace program execution, inspect the situation after an error occurred in great detail or time the execution to identify the time critical parts.

GAP comes with a library of group theoretical algorithms for computing with groups, for example to find the centralizer of an element in a permutation group. All this algorithms are written in the GAP programming language, and thus can be easily modified by the user if necessary.

GAP is available for a large number of different computers, ranging from the Apple MacIntosh to UNIX superminis. It is distributed from Aachen for a small amount of money used to cover our expenses.

S. SIDKI: A generalization of the Alternating Groups

The author introduced in 1982 (J. Algbra vol. 75) the class of groups

$$Y(m,n) = \{a_i\ (1 \le i \le m) \mid a_i^n = 1,\ (a_i^k a_j^k)^2 = 1\ \ (1 \le i < j \le m,\ 1 \le k \le n/2)\}.$$

Extensive computational investigation done together with J. Neubüser in Aachen during January - March 1987, and independently by E. Robertson and C. Campbell in St. Andrews confirm a conjecture that this series is formed by orthogonal and symplectic groups defined over certain fields of characteristic two.

We propose to discuss our recent work on the infinite variant $Y(m)$ of the above series where the relations $a_i^n = 1$ are deleted. This involves the study of presentations of linear groups defined over Laurent polynomial rings.

C. SIMS: The Knuth-Bendix Procedure and Coset Enumeration

The Knuth-Bendix procedure for strings is outlined. Two examples are presented. In these examples, the Knuth-Bendix procedure is able to provide more information than coset enumeration. A family of orderings on free monoids is defined. The orderings have proven to be useful in computations with polycyclic groups. Four implementation issues associated with the Knuth-Bendix procedure are discussed: rewriting strategy, indexing the rules, overlap strategy, and provision for lenght increasing rules.

M. C. SLATTERY: Computation in Finite Solvable Groups

In a finite solvable group, one can compute normalizers and intersections using traditional orbit-stabilizer techniques. Well-known orbit reduction tricks reduce the amount of work by working down a normal series in G with elementary abelian factors. Further speedups are achieved for these algorithms by using S. Glasby's fast algorithms (developed for normalizers of Hall subgroups and intersection of subgroups with coprime indices) when appropriate. In this way, orbit calculations are replaced by integer or linear algebra calculations, thus permitting reasonable computation in some situations with very large orbits.

G. C. SMITH: Dirichlet Series Associated with Groups

If G is a finitely generated group let

$$\zeta_G(s) = \sum_{H \le G, |G:H|\ finite} |G:H|^{-s}$$

a Dirichlet series. $\zeta_{\mathbb{Z}}(s) = \zeta(s)$, the Riemann zeta function. If G is a torsion-free, f.g. nilpotent group then this series enjoys an Euler product; if

$$\zeta_G^p(s) = \sum_{H \leq G, |G:H| \ p-power} |G:H|^{-s},$$

then $\zeta_G(s) = \prod_{p \in \mathcal{P}} \zeta_G^p(s)$ ($\mathcal{P}$ denotes the set of rational primes).

A method for calculating $\zeta_G(s)$ was explained and some examples given. The zeta function of the free nilpotent group of class 2 on 2 generators is $\zeta(s)\zeta(s-1)\zeta(2s-2)\zeta(2s-3)/\zeta(3s-3)$. A class of more complex class 2 groups were introduced, and it was explained how the system REDUCE could be used to aid the substantial algebraic manipulation involved.

Attention was drawn to the relevance of the Tauberian theorem to studying the function

$$s(x) = \sum_{H \leq G, |G:H| < x} 1.$$

L. H. SOICHER: Collection

Given a finite soluble group G described by a power-conjugate presentation, the elements of G can be multiplied by a collection process. We give strong experimental evidence that collection from the left (always collecting the leftmost minimal non-normal subword) is vastly more efficient than collection from the right, which had been the most commonly used collection method. (We coded the first implementation of collection from the left for soluble groups at the meeting, and on a group with composition length 53, it outperformed the existing implementation by a factor of about 100.)

We also describe the "deep thought" method for obtaining a multiplication formula for elements of a polycyclic nilpotent group (joint work with C. Leedham-Green).

M. R. VAUGHAN-LEE: Collection from the Left

I describe an implementation of collection from the left which can be substituted for the Havas-Nicholson algorithm for collection from the right in the Canberra nilpotent quotient algorithm. This algorithm has also been incorporated in a version of CAYLEY, and time savings by a factor of up to 14 have been observed. The algorithm incorporates combinatorial collection.

V. ZAYCHENKO: Computations in Algebras of Invariant Relations

Computer algorithms are designed for the study of invariant relations algebras. Given a group (G, W), the orbits of action of G on W^k are represented by the k-paths in a tree T_G, constructed by the algorithms. The complexity of sub-algebras study is $O(2^{\mathrm{rank}\, G})$ for V-rings and it can't be reduced. Applications for the study of distance-regular graphs, Hamming association schemes, transitive extensions of permutation groups are given.

Berichterstatter: Gerhard Hiß

Tagungsteilnehmer

Prof. Dr. M. D. Atkinson
School of Computer Science
Carleton University
Herzberg Building

Ottawa K1S 5B6
CANADA

Dr. M. Clausen
Fakultät für Informatik
Institut für Algorithmen und
Kognitive Systeme
Postfach 6980

7500 Karlsruhe 1

Dr. R. Brandl
Mathematisches Institut
der Universität Würzburg
Am Hubland 12

8700 Würzburg

Dr. A. M. Cohen
Mathematisch Centrum
Centrum voor Wiskunde en
Informatica
Postbus 4079

NL-1009 AB Amsterdam

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

GB- St. Andrews Fife, KY16 9SS

Prof. Dr. L. Di Martino
Dipartimento di Matematica
"Federigo Enriques"
Universita di Milano
Via Saldini 50

I-20133 Milano

Dr. J. R. Cannon
Department of Pure Mathematics
The University of Sydney

Sydney N.S.W. 2006
AUSTRALIA

Prof. Dr. J.D. Dixon
Dept. of Mathematics and Statisti
Carleton University

Ottawa, Ontario , K1S 5B6
CANADA

Prof. Dr. A. Caranti
Dipartimento di Matematica
Universita di Trento

I-38050 Povo (Trento)

Dr. V. Felsch
Lehrstuhl D für Mathematik
der RWTH Aachen
Templergraben 64

5100 Aachen

Prof. Dr. L. Finkelstein
College of Computer Science
Northeastern University

Boston , MA 02115
USA

Dr. G. Havas
Department of Mathematics
IAS
Australian National University
GPO Box 4

Canberra ACT 2601
AUSTRALIA

Prof. Dr. B. Fischer
Fakultät für Mathematik
der Universität Bielefeld
Postfach 8640

4800 Bielefeld 1

Dr. G. Hiß
Lehrstuhl D für Mathematik
der RWTH Aachen
Templergraben 64

5100 Aachen

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

Hoboken , NJ 07030
USA

Dr. D.F. Holt
Mathematics Institute
University of Warwick

GB- Coventry , CV4 7AL

Dr. S. P. Glasby
Department of Pure Mathematics
The University of Sydney

Sydney N.S.W. 2006
AUSTRALIA

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

Madison WI, 53706
USA

Prof. Dr. P. Hauck
Mathematisches Institut
der Universität Freiburg
Albertstr. 23b

7800 Freiburg

Dr. D. L. Johnson
Dept. of Mathematics
The University of Nottingham
University Park

GB- Nottingham , NG7 2RD

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

Eugene , OR 97403-1222
USA

Dr. R. J. List
Dept. of Mathematics
The University of Birmingham
P. O. Box 363

GB- Birmingham , B15 2TT

Prof. Dr. O.H. Kegel
Mathematisches Institut
der Universität Freiburg
Albertstr. 23b

7800 Freiburg

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

Eugene , OR 97403
USA

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

8580 Bayreuth

K. Lux
Lehrstuhl D für Mathematik
der RWTH Aachen
Templergraben 64

5100 Aachen

Dr. Ph. Le Chenadec
INRIA
Domaine de Voluceau - Rocquencourt
B. P. 105

F-78153 Le Chesnay Cedex

Prof. Dr. S.S. Magliveras
Department of Computer Science
University of Nebraska, Lincoln

Lincoln , NE 68588
USA

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

GB- London , E1 4NS

Prof. Dr. B.H. Matzat
Fachbereich Mathematik / FB 3
der Technischen Universität Berlin
Straße des 17. Juni 135

1000 Berlin 12

Prof. Dr. J. McKay
Department of Computer Science
Concordia University
1455, Maisonneuve W# 961

Montreal Quebec H3G 1M8
CANADA

Prof. Dr. E. A. O'Brien
Department of Mathematics
IAS
Australian National University
GPO Box 4

Canberra ACT 2601
AUSTRALIA

Prof. Dr. F. Menegazzo
Dipartimento di Matematica
Universita di Padova
Via Belzoni, 7

I-35131 Padova

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

5100 Aachen

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

5100 Aachen

R. Parker
Mathematical Institute
University of Cambridge
16, Mill Lane

GB- Cambridge CB2 1SB

Dr. P.M. Neumann
Queen's College

GB- Oxford OX1 4AW

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

5100 Aachen

Prof. Dr. M.F. Newman
Department of Mathematics
IAS
Australian National University
GPO Box 4

Canberra ACT 2601
AUSTRALIA

Prof. Dr. M. Pohst
Mathematisches Institut
der Universität Düsseldorf
Universitätsstraße 1

4000 Düsseldorf 1

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

Nedlends , WA 6009
AUSTRALIA

Prof. Dr. R. Sandling
Dept. of Matheamtics
The University
Oxford Road

GB- Manchester M13 9PL

Dr. S. Rees
Mathematics Institute
University of Warwick

GB- Coventry , CV4 7AL

Dr. G. J. A. Schneider
FB 6 - Mathematik
Universität-GH Essen
Universitätsstr. 3
Postfach 103 764

4300 Essen 1

Dr. R. Riley
Dept. of Mathematical Sciences
State University of New York
at Binghamton

Binghamton , NY 13901
USA

M. Schönert
Lehrstuhl D für Mathematik
der RWTH Aachen
Templergraben 64

5100 Aachen

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

GB- St. Andrews Fife, KY16 9SS

Prof. Dr. S. Sidki
Departamento de Matematica
Instituto de Ciencias Exatas
Universidade de Brasilia

70 910 Brasilia DF
BRAZIL

Dr. A. Ryba
Dept. of Mathematics
University of Michigan
3220 Angell Hall

Ann Arbor , MI 48109-1003
USA

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

New Brunswick , NJ 08903
USA

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

Milwaukee , WI 53233
USA

Dr. M. R. Vaughan-Lee
Dept. of Mathematics
Christ Church
24 - 26 St. Giles

GB- Oxford OX1 1DP

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

GB- Bath , BA2 7AY

Dr. V. Zaychenko
Institute for System Studies
Academy of Sciences of the USSR
9, Prospect 60 Let Oktyabrya

117312 Moscow
USSR

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

GB- London , E1 4NS

List of E-Mail Addresses

Name	E-mail addres
M. D. Atkinson	atkinsonmd@carleton.bitnet
R. Brandl	math006@dwuuni21.bitnet
C. M. Campbell	pmscc@savb.st-andrews.ac.uk (janet)
J. Cannon	cannon_j@summer.australia.csnet
A. Caranti	caranti@itnusca.bitnet
P. Le Chenadec	lechenad@inria.inria.fr
M. Clausen	clausen@ira.uka.de
A. M. Cohen	marc@cwi.nl
J. D. Dixon	jdixon@carleton.bitnet
L. Finkelstein	iaf@corwin.ccs.northeastern.edu
B. Fischer	umatf106@dbiuni11
R. H. Gilman	rgilman@sitvxc.bitnet
S. Glasby	glasby_s@summer.su@munnari.oz
G. Havas	gzh102@phys0.anu.oz@munnari.oz
G. Hiß	*see J. Neubüser*
D. Holt	dfh@maths.warwick.ac.uk (janet)
I. M. Isaacs	isaacs@vanvleck.math.wisc.edu
W. Kantor	kantor@uoregon.bitnet *or* kantor@mist.math.uoregon.edu
C. Leedham-Green	crlg@maths.qmc.ac.uk (janet)
E. Luks	luks@cs.uoregon.edu
K. Lux	*see J. Neubüser*
S. S. Magliveras	spyros@fergvax.unl.edu
J. McKay	mckay@conu1.bitnet
F. Menegazzo	mat04@ipduniv.bitnet
J. Neubüser	fm@dacth51.bitnet
M. F. Newman	mfn102@phys0.anu@munnari.oz
E. O'Brien	ano102@phys0.anu@munnari.oz
H. Pahlings	*see J. Neubüser*
R. Parker	rap1@phx.cam.ac.uk (janet)
W. Plesken	*see J. Neubüser*
S. Rees	ser@maths.warwick.ac.uk (janet)
R. Riley	bob@phyllis.math.binghampton.edu
E. F. Robertson	pmser@savb.st-andrews.ac.uk (janet)
A. Ryba	usergdz0@ub.cc.umich.edu
R. Sandling	mbbgsrs@cms.umrcc.ac.uk (janet)
G. J. A. Schneider	mat420@de0hrz1a.bitnet
M. Schönert	*see J. Neubüser*
C. Sims	csims@zodiac.bitnet
M. Slattery	mikes@marque.mu.edu
G. C. Smith	gcs@maths.bath.ac.uk (janet)
L. Soicher	leonard@maths.qmc.ac.uk (janet)