

Algorithms for Linear Groups

Jon F. Carlson (University of Georgia),
Bettina Eick (University of Braunschweig),
Alexander Hulpke (Colorado State University),
Eamonn O'Brien (University of Auckland)

November 16 – 21, 2014

1 Overview of the Field

The development of algorithms for the study of matrix groups is a very active area of computational group theory. It is a rapidly growing research topic with many highly interesting recent results and challenging open problems. Its overall goal is to develop effective algorithms to investigate and classify matrix groups of various types. The research in this area has interesting links to abstract group theory, representation theory, the theory of matrix algebras as well as to computer science and the general theory of efficient algorithms. Further, it has applications in areas such as crystallography, coding theory, number theory, topology, and cryptography.

Matrix groups are subgroups of a general linear group over a field. The design of algorithms for matrix groups depends heavily on the underlying field. In the case of finite fields, the “matrix group recognition project” has made significant progress in the development of algorithms to investigate the structure of a matrix group given by generators. This meeting considered the status of this major international research project and surveyed the open problems that still need to be resolved. In the case of infinite fields, the situation is much more difficult and less well understood at the current time. This meeting had a number of talks on recent advances in different aspects on this still wide open research topic. This may be considered as an important initial step forward.

We include a brief overview on the research topic of algorithms for matrix groups below. For details on the various aspects of this research topic we refer to the surveys by O'Brien [21]; Kantor & Seress [15]; Leedham-Green [16]; Babai, Beals & Seress [4]; Neunhöffer & Seress [19]; and Detinko, Eick & Flannery [9]. We also note that the Handbook of Computational Group Theory [14] contains an introduction to the topic.

2 Developments and Open Problems

The meeting witnessed the confluence of different strands of mathematics that in the past interacted on an ad-hoc basis, but rarely, if ever, came together in a broader context.

2.1 Matrix Group Recognition

The catalyst for enabling this broad interaction has been the “matrix group recognition project”, which for the last two decades has been one of the major areas of study in computational group theory. This research project is now reaching fruition, moving from a self-motivated project towards becoming a crucial tool for the computation with groups.

It has benefited from contributions by many researchers from various different areas of mathematics. Put succinctly, the problem is this: Given a small collection of invertible $n \times n$ matrices, for some $n > 0$, defined over a finite field K , provide effective algorithms to describe the structure of the group that they generate. In other words, one wants to identify the group from the representation that is provided by the action of the matrices on the vector space of row vectors.

Aschbacher [1] described the maximal subgroups of the general linear groups and other finite classical groups. This classification of maximal subgroups underpins the matrix group recognition project: the first step of this recognition is to determine a maximal subgroup in which the considered group is contained. For example, it is easily determined if the representation fixes some proper non-trivial subspace and thus is reducible. In this case, a maximal subgroup containing the given group is determined. At the same time, this type of recognition of the matrix group gives rise to a decomposition of the group into smaller matrix groups and thus allows for a recursive application of the method.

Aschbacher’s classification of maximal subgroups shows that every subgroup of $GL(n, K)$ lies in a subgroup that is in at least one of nine classes. The first seven classes are characterized by geometric conditions such as being reducible, being definable over a smaller field or having the representation imprimitive or tensor induced. The starting point of the project was the development of algorithms that run in polynomial time to recognise membership in a specific class and exploit the natural linear action of the group on the underlying vector space.

The remaining two classes are classical groups in their natural representation and other absolutely irreducible tensor-indecomposable representation of simple groups. Here the aim is to “constructively recognise” the group: obtain an effective isomorphism between the given copy of the group and a “standard” copy of the associated simple group. If such an isomorphism is available, then it allows us to translate known data (for example, its conjugacy class representatives) from the standard copy to the input copy.

At the meeting the lecture by Charles Leedham-Green summarized the progress

on the project. The goal of constructing a chief series of the linear group is essentially now realised. At the present time, there is a nearly complete implementation of the resulting algorithms available in the computer algebra system MAGMA. Leedham-Green suggested in his lecture that it is now appropriate for a unified push to create an alternative implementation in the system GAP. The advantages of having a second implementation are significant, both from the standpoint of correctness by providing the ability to check results, and the development of new ideas and refinements. It also would provide general access to what is increasingly viewed as a central piece of infrastructure for computational group theory. A meeting of some of the participants was held one evening at the workshop for the purpose of planning this second implementation.

2.2 Maximal subgroups of Classical Groups

To utilize the reduction process of matrix group recognition to simple composition factors, one needs to understand the ninth class in Aschbacher's classification, consisting of maximal subgroups of classical groups that are not identifiable by some geometric property. Understanding this class would have widespread applications, for example to matrix group recognition and, more generally, broadening the range of applicability of many algorithms for the structural investigations of matrix groups. It would also allow an explicit determination of maximal subgroups of the classical groups, which has been a long-standing problem of intense interest in finite group theory. The recent monograph by Bray, Holt and Roney-Dougal [7] is a first step in this direction by offering a complete classification of the maximal subgroups of classical groups of degree at most 12; the results of this are already being exploited in many algorithms.

A non-geometric maximal subgroup of a classical group must satisfy certain conditions on its generalized Fitting subgroup and the action of that Fitting subgroup on the natural module of the classical group. The generalized Fitting subgroup is generated by the largest nilpotent subgroup and the maximal normal semisimple subgroup. Recent developments in the field have put a premium on finding the maximal subgroups in this class. Kay Magaard reported on progress in this direction.

His latest work has taken the form of looking for obstructions to maximality, that is, subgroups lying between a given subgroup and a classical group. The focus of his work has been on obstructions that are sporadic simple groups.

The pervasive presence of classical groups, and matrix representations of simple groups, was seen in the work of several other participants.

2.3 Isomorphism testing

The constructive isomorphism test required for simple composition factors is a special case of the more general problem of algorithmic determination of an isomorphism between two finite groups.

Efficient algorithms to test if two groups are isomorphic or to reduce a collection of groups to isomorphism type representatives have a wide range of applications in group theory. For example, such methods provide a basis for the classification of groups of small order, see [6]. The currently available algorithms to test isomorphism for finite p -groups [13] and finite groups in general [8] make significant use of algorithms for matrix groups over finite fields and hence are an important application of such algorithms.

At the workshop two talks addressed aspects of the isomorphism problem directly. Peter Brooksbank

spoke on a new algorithm for testing isomorphism of p -groups of genus 2. These are groups of small nilpotency class. Any effort at a solution immediately encounters difficult problems in the area of algorithms for matrix groups.

Alice Niemeyer

spoke on a closely related problem. She considered

the question of how to construct finite p -groups whose automorphism groups map onto prescribed matrix groups and presented an interesting solution to this problem.

The problem of solving the isomorphism problem for matrix groups is still wide open even for finite matrix groups; this can be considered as a major challenge in this area.

2.4 Infinite Fields

Over infinite fields the analysis

of matrix groups by computational methods is far more difficult than it is over finite fields.

Generically, such a

task may be intractable and it is known that some fundamental problems, such as the membership problem, may be undecidable in general for arbitrary infinite matrix groups.

On the other hand such groups play an important role in many applications, and even solutions for particular classes of groups are therefore highly welcome. Several participants reported on progress for particular classes.

The Tits alternative and applications. A dividing line between the possible and impossible here appears to be given by the Tits Alternative [22], a theorem which asserts that a finitely generated matrix group is either has a solvable normal subgroup of finite index or has a non-abelian free subgroup. The Tits Alternative has been shown to be algorithmically verifiable; see [10, 5]. Its solution relies on the outcome of the “matrix group recognition project” to study finite images. The class of solvable-by-finite matrix groups seems to be accessible for algorithmic methods. For example, an algorithm of Assmann & Eick [2] decides if a rational virtually solvable group is also

virtually polycyclic.

The class of matrix groups that contain a non-abelian free subgroup is significantly harder to investigate. Even deciding if a matrix group with two generators is free on these two generators is an open problem. In the meeting a first step towards computations with free matrix groups was reported by Markus Kirschmer, see [12].

Arithmetic groups. Arithmetic groups are matrix groups which are defined as a variety of a polynomial ideal. It is known that each integral arithmetic group is finitely generated.

A first main goal in the algorithmic investigation of such groups is to find generators of such a group. Willem de Graff discussed

how to solve this problem if the considered group is unipotent or abelian.

Dane Flannery

extended these solutions to consider solvable matrix groups.

Alla Detinko

presented a survey

on recent advances on arithmetic subgroups that have the congruence subgroup property. Here again finite images, treated by matrix group recognition, are a crucial component.

Lattices and unit groups. Crystallographic groups are rational matrix groups that preserve a lattice.

Karel Dekimpe

reported on the problem of

determining a small, or even a minimal, generating set for a crystallographic group, utilizing methods from computational group theory. This intriguing problem still has no general algorithmic solution.

Gabriele Nebe

showed how the classical algorithm of

Voronoi can be used in a new application to determine normalizers of finite matrix groups and unit groups of orders.

The structure of unit groups of integral group rings was discussed by Eric Jespers.

2.5 Open problems.

John Dixon (Ottawa, Canada) presented a very interesting lecture on “Some open problems in linear groups”. We list some of his suggested problems in the following.

(1) Given elements x, y of prime order p in the general linear group $GL(n, \mathbb{C})$, what can be said about the subgroup $\langle x, y \rangle$ which they generate.

It is known that if $\langle x, y \rangle$ is finite then it is abelian.

Does this give any information about the infinite case?

(2)

A matrix $x \in GL(n, F)$ is cyclic if its minimal polynomial has degree n . Cyclic matrices play a role

in computational questions in linear

groups. An open problem due to Thompson asks whether there is always a

permutation matrix u such that ux is cyclic.

(3)

Determining whether a linear group is free is an important problem in computational study of infinite linear groups. Is there some sense in which almost all pairs of elements of $\mathrm{GL}(n, \mathbb{Q})$ generate a free group? Is the set of such pairs Zariski-dense in $\mathrm{GL}(n, \mathbb{Q}) \times \mathrm{GL}(n, \mathbb{Q})$?

(4)

Is it possible to generate (approximately) uniformly random conjugacy classes in a finite group without generating random elements? In other words is the former problem easier than the latter?

(5)

Let $s: G \rightarrow \mathrm{GL}(n, \mathbb{C})$ be a representation of a finite group.

There are cases when it would be useful to find c in the group ring $\mathbb{C}G$ such that c is easily computed from a given set of generators of G and $s(c)$ has rank 1 (or nullity 1). How can we do this?

3 A summary of presentations

The following is a summary of the broad themes covered by the individual lectures at the meeting.

Matrix Group Recognition. Charles Leedham-Green (London, UK) presented a major lecture on “The matrix group recognition project; where do we go from here?” This was the first lecture of the Ákos Seress day.

The speaker noted that the matrix group recognition is (with small gaps that are being filled) fully functional and available in MAGMA, see [3]. Some theoretical problems, such as reliance on integer factorisation and discrete logarithms, remain but only cause problems in extreme cases.

He presented five directions for future work: improve performance; increase functionality; incorporate modular representation theory; use the software; produce a version in GAP.

The talk, as well as an evening discussion, focused on the last of these objectives.

Alex Ryba (New York, US) presented a lecture on “Tensor Decompositions”.

It is related to one of the more difficult issues of the matrix group recognition project. He introduced an algorithm to determine all decompositions of a matrix as a tensor product of smaller representations. The method involves a polynomial reduction to the Pure Tensor Problem:

Given a subspace of a tensor product determine all pure tensors in the subspace. He discussed some issues with the running time of the algorithm; it currently relies on use of Gröbner basis techniques

and so does not run in polynomial time.

He concluded by raising the following intriguing questions:

Is “matrix recognition” in the NP complexity class?

An answer to this latter question seems tantalizingly close.

If so, is “matrix recognition” NP complete? This is not implausible, given some of the characteristics it shares with known NP complete problems, and would make it an interesting problem from a computer science point of view.

Bill Kantor (Eugene, US) introduced new results obtained with another participant, Martin

Kassabov (Cornell, US) which allow for efficient constructive recognition of a black box group isomorphic to $\text{PSL}(2, q)$ where q is even. There is related work by Borovik and Yalçinkaya for q odd.

This is a critically important base case for many algorithms.

Arithmetic Groups. Willem de Graaf (Trento, Italy) lectured on “Generators of arithmetic groups”.

Let G be an algebraic matrix group defined over \mathbb{Q} and let $G(\mathbb{Z})$ denote the subgroup consisting of the elements with coefficients in \mathbb{Z} . This group, and subgroups of $G(\mathbb{Q})$ commensurable with it, are arithmetic subgroups of G . A major problem in algorithmic matrix group theory is to determine a finite set of generators for $G(\mathbb{Z})$.

While a finite generating set exists, it remains a difficult problem to construct one. The speaker discussed some examples where such is known: unit groups of number fields

(an algorithm of Buchmann (1990) solves the problem);

unit groups of quaternion algebras (algorithms go back to Ford (1925));

the unit groups of group rings (there are several constructions of subgroups of finite index of the unit group, starting with work of Bass (1966)). He presented a solution to the problem where

G is unipotent or diagonalizable. The first part is joint work with Pavan, and the second with Faccin and Plesken.

The algorithm for the problem in the diagonalizable case can be used to find generators of units groups of integral abelian group rings.

Alla Detinko (Galway, Ireland) lectured on

“Algorithms for arithmetic groups: a practical approach”. She presented a survey of recent results in joint work with Flannery and Hulpke on computing with arithmetic subgroups which have the congruence subgroup property,

giving most consideration to arithmetic subgroups of the special linear group. She discussed decidability of fundamental algorithmic problems, and presented a general technique to handle algorithmically this class of groups. Applying that technique, it is possible to solve a number of computational problems such as membership testing, the orbit-stabilizer problem, and finding algorithms to investigate subnormal structure of arithmetic subgroups.

Dane Flannery (Galway, Ireland)

lectured on “Integrality and arithmeticity of solvable linear groups”.

He described an

algorithm to decide whether a finitely generated

subgroup H of a solvable algebraic group G is arithmetic. The algorithm incorporates procedures by de Graaf *et al.* to compute a generating set of an arithmetic subgroup of G . He introduced a simple new algorithm for integrality testing of finitely generated solvable-by-finite linear groups over \mathbb{Q} . This enables one to decide whether the index $|H : H_{\mathbb{Z}}|$ is finite. Another component of the main algorithm requires the determination of torsion-free ranks of solvable finitely generated subgroups of $GL(n, \mathbb{Q})$, which uses an algorithm developed by Detinko, Flannery, and O'Brien.

Structure and characters for finite groups. A number of lectures were given on various aspects of finite group

theory and group representation theory that use computational methods. The work on these problems has contributed significantly to other areas of computational group theory.

Robert Wilson's (London, UK) lecture, entitled "Black box groups and the Monster", considered how methods developed initially for solving hard problems for sporadic groups have migrated into general-purpose software. Examples are Sims' machinery of base and strong generating set for permutation groups (applied by Sims to groups such as the Baby Monster, in which one cannot even write down permutations), or the Meataxe, originally designed by Parker and Thackeray for constructing the sporadic group J_4 .

The speaker discussed how methods developed by him and several collaborators for computing in the Monster, of order approximately 10^{53} and probably the single most interesting matrix group, but whose matrices were too big to write down, are now used in other situations. One example is the use of involution centralizer methods in the matrix group recognition project.

Kay Magaard (Birmingham, UK) lectured on "Quasisimple overgroups of quasisimple irreducible subgroups of classical groups". He discussed finding maximal subgroup of finite classical groups. This is a problem that has implications for many areas of computational group theory.

Suppose that X is a finite classical group with natural module $V = k^m$.

In 1984 Aschbacher defines eight families of "geometric" subgroups of X . The maximal subgroups of X that are not in a geometric family are distinguished by the structure and action on V of their generalized Fitting subgroups.

Building on the earlier work of Kleidman and Liebeck and the 2012 work of Bray, Holt and Roney-Dougal, a full classification of the maximal subgroups of the finite classical groups can be achieved by answering the very challenging question: When is a non-geometric subgroup H maximal in X ?

The possible obstructions to the maximality of non-geometric

H in X , that is subgroups G where $H < G < X$, must lie in one of the geometric classes and the group H must be sporadic, alternating, or of Lie type.

Magaard surveyed research on obstructions to maximality as well as introducing some new results, mainly concerning cases where $H = J_1$ or where H is of Lie type.

Rebecca Waldecker (Halle, Germany) reported on joint work with Magaard on “Permutation groups where non-trivial elements have few fixed points”.

The motivation for the work is a better understanding of the automorphism groups of Riemann surfaces.

It is known that the automorphism group of a compact Riemann surface X of genus at least 2 is finite, and one way to prove this uses the so-called Weierstrass points, a finite set of geometrically significant points on X on which the automorphism group acts.

To identify nontrivial automorphisms fixing at least 5 such points they investigate permutation groups where all non-trivial elements have at least two, three, or four fixed points, aiming to describe precisely those finite simple groups which occur in these cases. Waldecker sketched some typical arguments, and discussed other related questions needing resolution.

A lecture by Klaus Lux (Tucson, US) discussed “Character tables of trivial source modules”.

Trivial source modules are direct summands of permutation modules and play a central role in several conjectures in representation theory, for example the celebrated Alperin weight conjecture. Conveniently, there are only finitely many indecomposable trivial source modules.

The speaker discussed methods to determine a trivial source character table (as introduced by Benson and Parker)

computationally and demonstrated these for the Mathieu groups and the Higman-Sims group.

The computational techniques use a variety of GAP packages, for example the `basic` package for basic algebras.

Groups of Lie Type. Several lectures at the workshop concentrated on structure and representations of these finite simple groups.

Arjeh Cohen (Eindhoven, Netherlands) reported on joint work with Don Taylor (Sydney, Australia) on “Row Reduction for Twisted Groups of Lie type”. This represented an extension of earlier work (also with Murray) on an algorithm for a finite group G of untwisted Lie type and an irreducible G -module M over a field of the same characteristic as G .

Given a linear transformation A on M , and the coefficients of the highest weight λ of the representation, it decides whether

A is in the image of G ; if so, it finds a preimage of A in polynomial time in $\log q$, subject to the existence of a discrete log oracle for $GF(q)$.

Gerhard Hiss (Aachen, Germany) lectured on “Imprimitive representations for quasisimple classical groups”. He reported on a joint project with Magaard. In previous work with Husen, they

classified the imprimitive (not induced from smaller subgroups) ordinary irreducible representations of finite groups of Lie type arising from algebraic groups with connected centers. This excludes some quasisimple classical groups such as the special linear groups or the spin groups. The new project applies results of the former, Clifford theory and Lusztig's generalized Jordan decomposition of characters to the classification of the imprimitive representations for quasisimple classical groups.

Free Groups as Matrix Groups. Markus Kirschmer (Aachen, Germany) lectured on “The explicit membership problem for discrete free subgroups of $\mathrm{PSL}(2, \mathbb{R})$ ”, joint work with Eick and Leedham-Green. Computing with matrix groups over infinite rings is much more complicated than working with matrix groups over finite fields. For example, the membership problem is undecidable in general. However, for subgroups of $\mathrm{PSL}(2, \mathbb{R})$ the situation is much better since there are powerful geometric methods available. Kirschmer presented a practical method which uses the Ping-Pong Lemma to solve the membership problem in this case.

Classical Groups. Cheryl Praeger (Perth, Australia) lectured on “Generating finite classical groups by elements with large fixed point spaces”. She discussed a body of work, comprising her collaboration with Seress and others over the past decade. It relates to work of many other researchers in the discipline. She discussed problems arising in the analysis of the constructive recognition algorithm of Leedham-Green and O'Brien [17] for classical groups in odd characteristic and natural representation, specifically in finding balanced involutions and constructing their centralizers. This work was followed by several papers on generation of such classical groups by a sequence of balanced involutions. Constructive recognition for finite classical groups in even characteristic is more difficult. Innovative new procedures developed by Neunhöffer and Seress, and by Dietrich, Leedham-Green, Lübeck & O'Brien [11] have solved the problem with two rather different approaches. Justifying either of these new methods requires proof that the groups can be generated efficiently by elements with large fixed point spaces. A fundamental problem involved the generation of a classical group in dimension $2n$ over a field of order q by so-called ‘good elements’, namely elements with an n -dimensional fixed point space, and with order divisible by a primitive prime divisor of $q^n - 1$. The lecture described estimates, obtained in her work with Seress and Yalçınkaya, for the probability that two random conjugates of a good element generate the classical group, and how this result is employed in the design of the algorithms.

Discrete groups and unit groups. Several lectures presented advances in techniques for studying discrete groups and unit groups of algebras.

Gabriele Nebe (Aachen, Germany) lectured on “Computing unit groups of orders”.

Let Λ be an order in some semisimple rational algebra A .

Its unit group Λ^\times is a finitely presented group.

In joint work with Braun,

Coulangeon, and Schönnenbeck,

she applied an algorithm first developed by Voronoi in 1900 in the context of reduction theory of integral lattices to compute generators and relations of Λ^\times .

Additional data obtained from Voronoi’s algorithm can be used to solve the word problem in these generators.

The algorithm has applications in many contexts. For example,

it can be used to determine generators for the normalizer of a finite integral matrix group as shown by Opgenorth (2001); it also can be employed to calculate the automorphism group of a lattice of signature $n, 1$ as described by Mertens (2009).

Nebe reported on a recent implementation to handle certain unit

groups of orders including all orders in rational division algebras. For quaternion algebras it improves substantially the existing implementation in MAGMA.

A lecture by Eric Jespers (Brussels, Belgium)

surveyed methods to determine the unit group of an integral group ring of a finite group. In many circumstances, it is possible to determine a

subgroup of finite index in such a unit group, but the full group of units is known in comparatively few cases only. He also

discussed a structure theorem for the unit group for some classes of finite groups.

Crystallographic Groups. Karel Dekimpe (Leuven, Belgium) lectured “On the number of generators of a crystallographic group”.

A Bieberbach group is a torsion-free

crystallographic group and these groups are the fundamental groups of the compact flat Riemannian manifolds.

Each such

group has a natural matrix representation and this is usually used to compute with such a group.

There exist upper bounds on the rank of an n -dimensional crystallographic group Γ in case the holonomy group is a p -group.

In a joint paper with Penninckx (2009), the speaker proved that if the holonomy of Γ is elementary abelian,

then Γ can be generated by n elements

The result raises the question whether every

n -dimensional Bieberbach group (or even every

torsion-free polycyclic-by-finite group of Hirsch length n) can be generated by n elements. In this direction, the speaker together

with Adem, Petrosyan and Putrycz proved (2012) that such a group

Γ can be generated by $a(n - \beta_1)/(p - 1) + \beta_1$

elements, where $a = 2$ if $p \leq 19$ otherwise $a = 3$, and

β_1 is the rank of $Z(\Gamma)$, which equals the torsion-free

rank of $\Gamma/[\Gamma, \Gamma]$.

Abstract Groups and Algebras. Gretchen Ostheimer (New York, US) lectured on “Recognizing torsion-free nilpotent groups as direct products”, joint work with Baumslag and Miller.

She described an algorithm to decide if a given finitely generated torsion-free nilpotent group is decomposable as the direct product of two non-trivial subgroups, and, if so, to compute such a decomposition.

Alice Niemeyer (Perth, Australia) lectured on “Symmetric p -groups”.

In 1978, Bryant and Kovács showed that for every subgroup H of $\text{GL}(d, p)$ for a prime p there is a finite p -group P such that the automorphism group of P induces a subgroup on the Frattini quotient $P/\Phi(P)$ which is isomorphic to H .

Their proof demonstrates the existence of such a p -group by considering sufficiently large quotients to terms of the exponent- p lower central series of the free group F on d generators.

In joint work with Bamberg, Glasby and Morgan, the speaker has considered maximal subgroups of $\text{GL}(d, p)$ for odd primes p and $d \geq 4$ and they show that in many cases it is only necessary to consider exponent- p class 3 quotients of F to find such a p -group.

Alastair Litterick (Auckland, New Zealand) lectured on “Non-Completely Reducible Subgroups of Exceptional Algebraic Groups”.

The subgroup structure of algebraic groups has been heavily studied recently, with applications to finite groups of Lie type and elsewhere. An approach due to Serre generalizes concepts from representation theory by replacing $\text{GL}(V)$ by another reductive algebraic group G . This leads naturally to the concept of a subgroup being ‘ G -completely reducible’.

Litterick presented recent joint work with Thomas, which classifies connected, reductive, non- G -completely reducible subgroups when G is of exceptional type and the ambient characteristic is good for G . Techniques employed vary from standard Lie theory and representation theory of reductive groups to non-abelian cohomology and computational methods.

Tobias Moede (Braunschweig, Germany) lectured on “Coclass theory for nilpotent associative algebras”.

The talk concerned joint work with Eick.

Coclass theory is a highly successful tool in the classification of finite p -groups. For a finite-dimensional nilpotent associative algebra A of class c , its coclass is defined as $\dim(A) - c$.

One can visualize the algebras of a given coclass r by a coclass graph $\mathcal{G}_{\mathbb{F}}(r)$. The

vertices in this graph correspond one-to-one to isomorphism types of finite-dimensional nilpotent associative \mathbb{F} -algebras of coclass

r and there is a directed edge $A \rightarrow B$ if $A \cong B/B^{cl(B)}$. Moede presented an algorithm to determine finite parts of the associated coclass graphs and exhibited some examples.

He gave a structural description for the infinite paths in these graphs and used this to determine which coclass graphs have finitely many maximal infinite paths.

Automorphisms and isomorphisms of finite groups. The problems of constructing the automorphism group of a finite group

and of testing for isomorphism between two finite groups are both important and difficult. Indeed, the problems seem most difficult for very restricted classes of groups.

Three lectures at the workshop introduced new methods for dealing with these and related problems.

Peter Brooksbank (Lewisburg, US) lectured on “Testing isomorphism of p -groups of genus 2”.

He began by noting that testing isomorphism of p -groups of class 2 and exponent p is widely believed to be no less difficult than the general problem.

Such a group has genus 1 if its center has order p ; these are the extraspecial groups and it is elementary to decide isomorphism for this class. The speaker and collaborators considered the genus 2 case, where centers have order p^2 . While only a modest step away from extraspecial groups, testing isomorphism for this class requires dramatically different ideas.

Brooksbank

presented two approaches towards computing the automorphism groups of such groups, the critical step toward solving the isomorphism problem.

The first is based on methods of Vishnevetskii and is particular to genus 2 groups. The second uses the more general adjoint-tensor method.

Using a combination of

the two algorithms, they test isomorphism of genus 2 groups of order N in time (almost) polynomial in $\log(N)$.

A lecture on “A new isomorphism test for groups” was presented by James Wilson (Fort Collins, US).

He introduced new structures that highlight properties of automorphism groups of finite groups. A subset of the techniques already reveals new characteristic subgroups in about 80% of the groups order at most 2000 in the Small Groups Library of Besche-Eick-O’Brien.

The first idea is to introduce a more relaxed notion of a filter for groups, one that can be updated when new characteristic subgroups are found.

The speaker defined a filter over an

arbitrary pre-ordered commutative monoid. Each

filter determines an associated graded Lie algebra. Furthermore every characteristic filter induces a filter on the automorphism group. Finally, the Lie algebra of the filter on the automorphism group maps canonically to the derivations of the associated graded algebra of the original group.

At this point the problem of group automorphisms is reduced to understanding the autotopisms between the homogeneous components of a graded algebra.

Exact sequences are determined that explain the structure of the autotopism group in relation to class groups.

On a related subject, Josh Maglione (Fort Collins, US)

lectured on “Finding chief series in large unipotent groups of Lie type”. The nilpotent groups, $T(r, q)$ of

Lie type T and rank r , have a

canonical characteristic series of length $O(r^2)$ with q -bounded factors, and this applies also to almost all quotients. Compared to the standard

lower central series of length $O(r)$, these new series give strong computational speedups on problems such as constructive recognition and isomorphism testing, and answer a long-standing demand for practical improvements for calculating automorphism groups.

An implementation of these ideas using machinery from the “matrix group recognition project” computes this structure in one minute of CPU time for groups of order about 2^{80} .

4 Some notes about the meeting

The workshop had forty-one participants. There were twenty-five lectures. Many of the lectures were short, each approximately 15 minutes. The lecture schedule was kept purposefully light in order to allow for discussions among the participants which were lively and fruitful. The meeting was diverse geographically: eleven participants from North America; two from South America; twenty-three from Europe; and five from Australia and New Zealand. There were eight women among the participants, six of whom were speakers. Four participants were graduate students or had received their degree within the last year, three of these spoke. The weather was wonderful and the scenery in Banff was spectacular.

The workshop featured a special day in memory of Ákos Seress who was one of the original applicants to organize the meeting. Unfortunately, Ákos passed away a year before the meeting. There were four lectures on the special day given by Peter Brooksbank, Bill Kantor, Charles Leedham-Green, and Cheryl Praeger. All four distinguished speakers had close associations with Ákos.

At the meeting, a volume of the *Journal of Algebra*, edited by Bill Kantor and Charles Leedham-Green, dedicated to the memory of Ákos and published just in time for the meeting was displayed.

5 Discussions and future directions

In addition to the lectures, there were a variety of discussions held at the meeting. A major working session was devoted to the organization of a GAP implementation of the matrix group recognition algorithms. A problem session was held at the meeting in which additional interesting open problems were discussed.

Moreover, there were many discussions and meetings of small groups held at the meeting. In these, many interesting new research avenues were discussed and new collaborations on joint research interests were created. These will, without doubt, lead to many new and interesting research projects and new publications, thus enhancing the research in computations with matrix groups significantly.

We gratefully acknowledge the wonderful facilities offered

by the Banff Center to host meetings of this kind. It is the mixture of highly stimulating lectures and many associated informal discussions that take place in such an environment that makes a meeting of this kind such a success and a memorable experience.

References

- [1] M. Aschbacher,
On the maximal subgroups of the finite classical groups,
Invent. Math. **76** (1984), 469–514.
- [2] B. Assmann and B. Eick,
Testing polycyclicity of finitely generated rational matrix groups,
Math. Comp.
76 (2007), 1169–1682.
- [3] H. Bäärnhielm, D. Holt, C.R. Leedham-Green, E. A. O’Brien,
A practical model for computation with matrix groups, *J. Symb. Comp.*,
68 (2015), 27–60.
- [4] L. Babai, R. Beals, Á. Seress, Polynomial-time theory of matrix groups,
STOC’09 – Proceedings of the 2009 ACM International Symposium on Theory of
Computing, 55–64, ACM, New York, 2009.
- [5] R. Beals,
Improved algorithms for the Tits alternative,
In *Groups and Computation III (Columbus OH, 1999)*,
(A. Seress and W. M. Kantor, eds.),
Ohio State Univ. Math. Res. Inst. Publ. **8**, 63–67,
de Gruyter, Berlin, 2001.
- [6] H. U. Besche, B. Eick and E. A. O’Brien,
A millenium project: constructing small groups,
Internat. J. Algebra Comput.,
12 (2002), 623–644.
- [7] J. N. Bray, D. F. Holt, C. M. Roney-Dougal.
The maximal subgroups of the low-dimensional finite classical groups.
London Mathematical Society Lecture Note Series, 407.
Cambridge University Press, Cambridge, 2013.
- [8] J. J. Cannon and D. F. Holt,
Automorphism group computation and isomorphism testing in finite groups,
J. Symb. Comput.,
35 (2003), 241–267.

- [9] A. S. Detinko, B. Eick and D. L. Flannery,
Computing with matrix groups over infinite fields,
In *Groups St. Andrews 2009 in Bath. Volume 1*,
London Math. Soc. Lecture Note Ser.,
387, 256–270,
Cambridge Univ. Press, Cambridge, 2011.
- [10] A. Detinko, D. F. Flannery and E. A. O’Brien,
Algorithms for the Tits alternative and related problems,
J. Algebra,
344 (2011), 397–406.
- [11] H. Dietrich, C. R. Leedham-Green, F. Lübeck and E. A. O’Brien,
Constructive recognition of classical groups in even characteristic,
J. Algebra
391 (2013), 227–255.
- [12] B. Eick, M. Kirschmer and C. R. Leedham-Green,
The constructive membership problem for discrete free
subgroups of rank 2 of $SL_2(\mathbb{R})$,
London Math. Soc. J. Comput. Math.,
17 (2014), 345–359.
- [13] B. Eick, C. R. Leedham-Green and E. A. O’Brien,
Constructing automorphism groups of p -groups,
Comm. Alg.,
30 (2002), 2271–1195.
- [14] D. F. Holt, B. Eick and E. A. O’Brien,
Handbook of computational group theory,
Discrete Mathematics and its Applications (Boca Raton),
Chapman & Hall/CRC, Boca Raton, FL, 2005.
- [15] W. M. Kantor and A. Seress,
Black box classical groups
Memoirs of the Amer. Math. Soc.,
708,
American Mathematical Society, 2001.
- [16] C. R. Leedham-Green,
The computational matrix group project,
In *Groups and Computation III (Columbus OH, 1999)*,
(A. Seress and W. M. Kantor, eds.),
Ohio State Univ. Math. Res. Inst. Publ. **8**, 229–247,
de Gruyter, Berlin, 2001.

- [17] C. R. Leedham-Green and E. A. O'Brien,
Constructive recognition of classical groups in odd characteristic,
J. Algebra,
322 (2009), 833–881.
- [18] G. Nebe and W. Plesken,
Finite rational matrix groups,
Memoirs of the Amer. Math. Soc.,
116,
American Mathematical Society, 1995.
- [19] M. Neunhöffer and Á. Seress,
A data structure for a uniform approach to computations with finite groups.
ISSAC 2006, 254261, ACM, New York, 2006.
- [20] E. A. O'Brien, Isomorphism testing for p -groups,
J. Symb. Comput.,
17 (1994), 133–147,
- [21] E. A. O'Brien,
Algorithms for matrix groups,
Groups St Andrews 2009 in Bath, Volume 2, 297323,
London Math. Soc. Lecture Note Ser., **388**,
Cambridge Univ. Press, Cambridge, 2011.
- [22] J. Tits, Free subgroups in linear groups, *J. Algebra*
20 (1972), 250-270.