Mohammed Ayad
COMPOSITION, ITERATION AND IRREDUCIBILITY OF POLYNOMIALS

Nigel Boston
COMBINING GROUP THEORY AND NUMBER THEORY COMPUTATIONS

A few years ago, Charles Leedham-Green and I introduced a pruned version of p-group generation that computes certain Galois groups of interest to number theorists. This was adapted by Michael Bush and Harris Nover to perform massive computations of Galois groups of p-class towers. Refinements of this method with Jordan Ellenberg yield heuristics, some proven, for counting such extensions. We thereby obtain some of the first results in a large program to produce computational data, analogous to our now deep understanding and application of Frobenius actions in the abelian case, in anabelian geometry.

Peter Brooksbank
POLYNOMIAL-TIME ALGORITHMS FOR ALGEBRAS WITH INVOLUTION

Building on results of Rónyai, Ivanyos, and Eberly and Geisbrecht for matrix algebras, I present a polynomial-time theory for algebras of matrices that possess an involutory anti-automorphism. Such $*$-*algebras* have a structure theory analogous to the classical theory of ordinary matrix algebras. In particular, the usual Jacobson radical of a $*$-algebra is a $*$-*ideal*, and the quotient of the $*$-algebra by its radical is isomorphic to a direct sum of $*$-*simple* algebras whose structure is well-understood.

Algorithms for matrix $*$-algebras can be used to study the structure of group algebras, and they also underpin an algorithm to construct the group preserving a collection of reflexive forms on a finite vector space. In the talk I will describe the latter application – and its importance to computational group theory – in some detail.

This is a report on joint work with James Wilson at The Ohio State University.

Arjeh Cohen
BIRMAN-MURAKAMI-WENZL ALGEBRAS OF DYNKIN TYPE

Alla Detinko
ALGORITHMS FOR MATRIX GROUPS OVER INFINITE FIELDS

We present new techniques for computing with matrix groups over infinite domains, based on the theory of finitely generated linear groups. We use those techniques to develop efficient algorithms for a number of computational problems, some of which will be discussed in the talk. We will also discuss the state-of-the-art in the area.

This is joint research with Dane Flannery and Eamonn O'Brien.

Carlo Di Franco
INFORMATION FLUX APPROACH: FROM QUANTUM STATE TRANSFER TO MATRYOSHKA STATES

In this talk, I introduce and formalise the concept of information flux in a quantum many-body register as the influence that the dynamics of a specific element receive from any other element of the system. By quantifying the information flux in a protocol, one can design the most appropriate initial state of the register and, noticeably, the distribution of coupling strengths among the parts of the system itself. The intuitive nature of this tool and its flexibility, which allow easily manageable numerical approaches when analytic expressions are not straightforward, are greatly useful in interacting many-body systems

such as quantum spin chains. In order to clarify how the method works, I present two interesting examples. In the former, by means of a map between the temporal behaviour of the information flux in two different systems, I propose a protocol for perfect quantum state transfer in a finite, open chain of spins that does not preserve the number of excitations. In the latter, I find a coupling-strength configuration which gives rise to simultaneous multiple Bell states and suggest a way such an interesting entanglement pattern can be used in order to distribute maximally entangled channels to remote locations.

Carlo Di Franco

INFORMATION FLUX APPROACH: QUANTUM INFORMATION PROTOCOLS WITHOUT STATE INITIALISATION

In this talk, the concept of information flux is exploited in order to propose two interesting quantum information protocols on chains of interacting spins. Both the schemes do not require state initialisation of the medium, considerably relaxing their prerequisites. In the first part, I present a protocol to achieve perfect quantum state transfer by using an engineered spin chain and clean local end-chain operations. This allows us to shed light on the interplay among purity, entanglement and operations on a class of many-body systems potentially useful for quantum information processing tasks.

In the second part, I propose a scheme for the determination of the coupling parameters in a spin chain. This requires only time-resolved measurements over a single particle, simple data post-processing and no prior knowledge of the state of the chain. The protocol fits well into the context of quantum-dynamics characterisation and is efficient even when the spin-chain is affected by general dissipative and dephasing channels.

Stephen Glasby

A RECURSIVE MEAT-AXE ALGORITHM

The MEAT-AXE is a fundamental tool in computational representation theory which takes as input a finitely generated subalgebra $A = \langle X_1, \ldots, X_k \rangle_F$ of the algebra $F^{d\times d}$ of all $d \times d$ matrices over F, and outputs one of: a proof of irreducibility, a proper non-zero invariant submodule, an endomorphism algebra, an invariant form, etc. The algebra A need not be an epimorphic image of $F[G]$ for some finite group G, and the field F is arbitrary. (Our examples, F is an algebraic extension of a function field $\mathbb{Q}(t_1, \ldots, t_n)$.)

One useful tool for proving irreducibility is Norton's Irreducibility Criterion, which involves both the natural module $V := F^{1\times d}$ and its dual module $V^* := F^{d\times 1}$. Another useful tool involves algebraically conjugate modules and the Galois group $\mathrm{Gal}(E/F)$ of certain finite extensions of F. This leads naturally to writing modules over proper subfields which in turn leads to solving norm equations. The former problem is related to 1-cohomology via Hilbert's Satz 90, and the latter is related to 2-cohomology via the Brauer-Hasse-Noether theorem.

We shall give explicit familiar examples which illustrate the main problems and their solutions. Some of the ideas, particularly in the inhomogeneous case, date back to work of Plesken and Souvignier (1996).

Rod Gow
MATRIX SUBSPACE PROBLEMS RELATING TO RANK

Gábor Ivanyos
SYSTEM SOLVING IN QUANTUM ALGORITHMS

In this talk we discuss certain systems of polynomial equations, efficient solutions of which lead or would lead to polynomial quantum algorithms. These systems arise in quantum algorithms which are among the currently best results regarding the noncommutative Hidden Subgroup Problem, HSP. (The HSP is a paradigm which includes computational problems such as finding orders of group elements and computing discrete logarithm as commutative instances; and the Graph Isomorphism Problem as a noncommutative instance. While hidden subgroups of abelian groups can be found in quantum polynomial time, very little is known about the quantum complexity of the noncommutative case.)

Natalia Iyudu
EXPERIMENTS WITH HILBERT SERIES COMPUTATIONS AND THE ANICK CONJECTURE

We study the question on whether the famous Golod-Shafarevich estimate, which gives a lower bound for the Hilbert series of a (noncommutative) algebra, is attained. This question was considered by Anick in his 1983 paper 'Generic algebras and CW-complexes', Princeton Univ. Press., where he proved that the estimate is attained for the number of quadratic relations $\frac{n^2}{4} \leq d$ and $d \geq \frac{n^2}{2}$, and conjectured that it is the case for any number of quadratic relations. After this, no progress have been made on this question so far. In [N.Iyudu,P.Cameron, J.Symb.Comp., 2007] we, on the basis of computational experiments, made with the GRAAL package for the Gröbner bases and Hilbert series computations (A.Verevkin, Uljanovsk, A.Kondratiev, Linz), showed that the conjecture is true for the number of relations $d = \frac{n(n-1)}{2}$, when $n \leq 7$. The conjecture for this particular number of relations, which is the number of relations in the algebra of commutative polynomials, or in an arbitrary PBW algebra, was formulated by Vershik. Recently we moved the known since Anick's paper as a white zone frame $(\frac{n^2}{4}, \frac{n^2}{2})$ and proved the Vershik conjecture over any field of characteristic 0.

Ekatherina Karatsuba
THE COMPLEXITY OF COMPUTATION OF TRANSCENDENTAL FUNCTIONS

Devoted to the memory of my father A.A.Karatsuba whose method of fast multiplication was the first fast method of computational mathematics.

The evaluation of the values of the functions with a given accuracy in an appropriate time of computer work is one of the central problems in computational mathematics. The first nontrivial problem of such kind was formulated by A.N. Kolmogorov the problem of the study of the complexity M(n) of calculation of the product of two n-digit integers. A solution was found in 1960 by a student A.A. Karatsuba who invented the first method of fast multiplication. From the moment of the invention of "fast multiplication", different fast algorithms were constructed (e.g. the Schnhage-Strassen, the FFT, the AGM etc. algorithms) and implemented in the programs and the program libraries.

Assuming certain complexity of such a fast multiplication of two n-bit integers we can ask about the complexity of evaluation of basic transcendental functions at given points with prescribe precision. For instance, assuming Schönhage-Strassen $O(n\,log\,n\,loglog\,n)$

complexity of multiplication R.P. Brent, J. and P. Borweins constructed the AGM-algorithms for computation of elementary transcendental functions and the constant pi with the complexity bounds which are close to optimal that is $O(n\ log^3\ n\ loglog\ n)$
(for pi — $O(n\ log^2\ n\ loglog\ n)$).

We present a general method for fast evaluation of the functions of type of the Siegel E-function, the so-called FEE method, developed by the author, and some other different fast algorithms constructed for computation of both elementary transcendental functions and higher transcendental functions with the complexity bounds which are close to optimal, that is $O(n\ log^3\ n\ loglog\ n)$ and $O(n\ log^2\ n\ loglog\ n)$.

We discuss the ways of the further development of the field of fast algorithms.

Stephen Linton
COMBINING COMPUTATIONAL ALGEBRA SYSTEMS

Mathematicians increasingly need to combine multiple software systems to solve complex problems. These may be different specialist systems whose different mathematical capabilities they wish to exploit, or multiple instances of the same system running on different computers to exploit the increasing parallelism of modern hardware. In this talk I will survey a range of techniques which have been used for these purposes, and their various strengths and weaknesses, demonstrate some new tools that have been developed in the recent European SCIEnce project to make these connections simple, and look forward to some the challenges and opportunities that face us as we try to use ever more parallel hardware to do ever more sophisticated and demanding mathematical computations.

Frank Lübeck
SMALL DEGREES OF REPRESENTATIONS OF FINITE GROUPS OF LIE TYPE

An important tool for studying a (finite) group G is to consider its representations, i.e., homomorphisms $G \to GL(n, F)$ from G into groups of invertible $(n \times n)$-matrices over various fields F. The n is called the *degree* of the representation.

In this talk we consider as groups G *finite groups of Lie type*–these will be introduced informally. They are closely related to many of the finite simple groups which were classified in the 1980's. Examples are classical (linear, unitary, symplectic or orthogonal) groups over finite fields, like $SL(n, q)$, and exceptional groups associated to root systems of exceptional type, denoted $G_2(q)$ or $E_8(q)$.

We will consider the following question: For a given such group G and a given (algebraically closed) field F, what are the smallest degrees of non-trivial (irreducible) representations of G over F?

The known answers to this question rely on quite deep mathematics, and the theoretical background is very different depending on the characteristic of the field F: F is the complex numbers, or of prime characteristic l dividing the order of G, in the latter case the *defining characteristic* (l divides q in the examples above) and *non-defining characteristic* must be considered separately.

Some of the results I will mention were obtained by computations in computer algebra systems.

Gabriele Nebe
AUTOMORPHISM GROUPS OF TYPE II CODES

A Type II code is a linear binary self-dual code for which the weight (the number of non-zero entries) of any codeword is a multiple of 4. The automorphism group of a code is its set stabilizer in the full symmetric group.

We give necessary and sufficient conditions for a permutation group G to be contained in the automorphism group of a Type II code.

This is joint work with Dr. Annika Günther.

Eamonn O'Brien
THE ORE CONJECTURE

The Ore conjecture, posed in 1951, states that every element of every finite non-abelian simple group is a commutator. Despite considerable effort, it remained open for various infinite families of simple groups. Recently, in a joint project with Liebeck, Shalev and Tiep, we developed new strategies, combining character theoretic methods with other ingredients, and used them to establish the conjecture.

Igor Pak
PROBLEMS: NEW, OLD AND UNUSUAL

The problem of generating random group elements both benefited from and led to a number of interesting problems in combinatorics and probability on finite groups. In this talk I intend to review some recent progress, put it in historical perspective, and make certain prediction on where this all is going. I will make a special effort to formulate some new problems and state some new conjectures, which are, hopefully, correct and not outrageously difficult.

Michel Planat (joint work with Metod Saniga and Peter Levay)
BALANCED TRIPARTITE ENTANGLEMENT, THE ALTERNATING GROUP A_4 AND THE LIE ALGEBRA $su(2,\mathbb{C}) \oplus u(1)$

I feature three important classes of three-qubit entangled states and their encoding into quantum gates, discrete groups and Lie algebras. States of the GHZ and W-type correspond to pure tripartite and bipartite entanglement, respectively. I introduce another generic class B of three-qubit states, that are equally balanced over two and three parties. I show how to realize the largest cristallographic group W(E8) in terms of three-qubit gates (with real entries) encoding states of type GHZ or W [M. Planat, Clifford group dipoles and the enactment of Weyl/Coxeter group $W(E_8)$ by entangling gates, Preprint 0904.3691 (quant-ph)]. Then, I describe a peculiar condensation of W(E8) to the four-letter alternating group A_4, obtained from a chain of maximal subgroups. Group A_4 is realized from two B-type generators corresponding to the Lie algebra $su(2,\mathbb{C}) \oplus u(1)$.

Applications are to particle physics and to the genetic code.

Lajos Rónyai
GROEBNER BASES AND COMBINATORICS

There are several interesting applications of Groebner bases to combinatorics along the following general line: take a finite point set X in an affine space, which describes a combinatorial object. For example, X can be the collection of characteristic vectors of a finite set family. Compute Groebner bases and related structures, such as standard

monomials, Hilbert function, for the vanishing ideal of X, and use the results to derive combinatorial consequences.

Applications of this kind will be discussed in the talk, including uniquely vertex colourable graphs (Hillar-Windfeldt), applications of Alon's Nullstellensatz, and some results from extremal combinatorics.

In the reverse direction, combinatorial methods to compute lexicographic Groebner normal sets (standard monomials) will be considered

Csaba Schneider

CONSTRUCTIVE MEMBERSHIP TESTING IN BLACK-BOX CLASSICAL GROUPS

Suppose that G is a group given by generators and x is an element possibly in an overgroup of G. In the constructive membership problem, we are required to determine if x is an element of G, and, if it is, we are required to construct a straight-line program from the given generating set of G to x. In an earlier work we proposed a solution for this problem in the context of black-box sporadic simple groups. Our solution relied on the generalized sifting procedure which is a generalization of Sims' sifting algorithm for permutation groups. Subsequently we adapted the procedure for several classes of black-box classical groups, using the standard generating sets described by O'Brien and Leedham-Green. The complexity of the algorithms is determined, and they are implemented in Magma for the classes of black-box special linear groups, symplectic groups, and special unitary groups. The results presented in this talk were obtained in collaboration with Sophie Ambrose, Scott Murray, and Cheryl Praeger.

Ákos Seress

POLYNOMIAL-TIME THEORY OF MATRIX GROUPS

There is a Monte Carlo algorithm that given $G \leq GL(n, p^e)$ with odd p, computes $|G|$ and a composition series in G. The algorithm can also test membership in G constructively, which means that it constructs a straight-line program from the input generators to any given $g \in G$. If G has no composition factors of exceptional Lie type then the algorithm can be upgraded to Las Vegas.

If $p = 2$ then we can do all the tasks above in groups with no exceptional factors.

The running time is polynomial in the input length, using number theory oracles for factorization and discrete logarithm.

The algorithm is based on the black-box group approach of Babai and Beals, but it also uses recent results utilizing centralizer of involution computations.

The talk is based on the paper

László Babai, Robert Beals, Ákos Seress: Polynomial-time theory of matrix groups, Proc. 41st STOC (2009), pp. 55–64.

Sergey Shpectorov

COMPUTING VERY LARGE ORBITS OF THE MAPPING CLASS GROUPS (JOINT WITH K. MAGAARD)

It is well known that the Hurwitz loci of curves X of fixed genus, admitting a finite groups of automorphisms G, are classified by the orbits of the suitable mapping class group on the generating tuples in G. Jointly with H. Voelklein, we wrote a collection of GAP programs that compute those orbits and determine the inclusion between the corresponding Hurwitz loci. Using the programs, the complete structure of Hurwitz loci for genera $g \leq 16$ were determined. Another application is the ongoing computation of the complete list of

the genus zero systems in the framework of the Guralnick-Thompson conjecture proven several years ago. The completion of the latter project and also the possibility to increase the bound on the genus, for which the Hurwitz loci can be determined, depends on our ability to handle very large orbits. At the moment, we can only compute orbits with lengths up to several hundreds of thousands. In the talk we will discuss some ideas and results leading, hopefully, to the dramatic increase in the orbit length.