Abstracts

Alexandre Borovik

Black box groups, pseudofinite groups and groups of finite Morley rank

The talk will outline an alternative proof of the Larsen-Pink Theorem (the latter says, roughly speaking, that "large" finite simple groups of matrices are Chevalley groups over finite fields). This "asymptotic" version of the classification of finite simple groups is intimately related to probabilistic recognition of "black box" finite groups. An explanation of this link is best done with the help of some model theory, but the talk will concentrate on group-theoretic rather than on logical aspects of a new emerging theory.

(Parts of the talk are joint work with Pinar Ugurly and Sucru Yalcinkaya)

Jason B. Hill

Stabilizer Chains and Backtrack in Parallel

There are several factors to consider when trying to achieve speed-up in a program as the result of parallelization. On one side, problem and algorithm dependent considerations (e.g., Amdahl's Law) can limit gains. Commonly, machine architectures place their own limitations (network topology, network latency -vs- throughput, cache size, RAM and disk space), making portability from one machine to the next challenging. In this talk, I'll discuss an architecture-dependent approach to backtrack searches in permutation groups, aimed at portability. The implementation is tested on machines ranging from a weak commodity single-core machine operating at 2 GFLOPS to a 15,648-core supercomputer capable of 175 TFLOPS.

Derek Holt

Algorithms and generator numbers for matrix groups

This talk will be in two parts. In the first part, we give a brief survey of the "Composition Tree" method for the computational analysis of potentially large matrix groups over finite fields, which has been developed and implemented over the past 20 years by Leedham-Green, O'Brien, Seress, Neunhöffer and many others. In this approach, we need to find generating sets for the kernels of homomorphisms from matrix groups, which we do by choosing a collection of random elements of the kernel.

This motivates the second part of the talk, which is joint work with Colva Roney-Dougal, in which we investigate how many random elements of a finite matrix group we need in order to generate it with high probability. There is copious literature on this topic. For example, Kovács and Robinson proved in a 1991 paper that a completely reducible finite matrix group of degree d over any field can be generated by $3d/2$ elements, and this bound is sharp. But many of the other proven results involve unspecified constants, whereas for practical applications, we need to know their values.

Adam James

Computing Mapping Class Group Orbits

The talk presents joint work with K. Magaard, S. Shpectorov, and G. Wang. The mapping class group of a compact connected surface acts naturally on the fundamental group of the given surface. Using this action and some Riemann surface theory, we can translate questions about Riemann surfaces into group theoretical questions. A particularly interesting question is: to what extent does the automorphism group of a compact Riemann surface determine its complex structure, and how are Riemann surfaces with the same automorphism group related?

In particular, when we fix the automorphism group, how many components in the moduli space of compact Riemann surfaces do we get? The aim of the talk is to discuss how mapping class group orbits are related to the problems discussed and some of the computational issues associated with computing these orbits.

Mikhail Klin, Matan Ziv-Av

Strongly regular graphs with no triangles: hidden history, challenges, computer algebra results

A strongly regular graph (briefly SRG) Γ is called primitive if both Γ and its complementary graph are connected. Only primitive SRGs are considered. The most famous SRG with no triangles, denoted by $NL_2(10)$, has parameters (100, 22, 0, 6), it was described in the paper by Higman and Sims in 1968 in the course of the discovery of a new sporadic simple group HS. Currently only 7 SRGs with no triangles are known, those on 5, 10, 16, 50, 56, 77 and 100 vertices. All of them appear as induced subgraphs of $NL_2(10)$, the (unique) SRG with no triangles on 100 vertices.

This survey talk is influenced by our recent careful investigation (jointly with A. Woldar) of two texts by Dale Marsh Mesner (1923-2009) dated 1956 and 1964. It turns out that the graph $NL_2(10)$ was discovered by Mesner as early as in his thesis (1956), while in 1964 the proof of the uniqueness of the graph was presented in his notes. Moreover, in framework of his investigation of the graph $NL_2(10)$ the elements of a general theory of SRGs with no triangles were developed, with a special emphasis on SRGs of negative Latin square type with no triangles.

We will start from a digest of the investigations by Mesner, paying a special attention to the challenges, which naturally appear from the acquaintance with his ideas and techniques. Mesner's model of the graph $NL_2(10)$ will be reconsidered in the framework of computer algebra experimentation. With the aid of GAP all isomorphism classes of the embeddings of SRG's with no triangles into the graph $NL_2(10)$ are classified. We hope that some of them may serve as patterns for the possible new lines of investigations.

Special attention will be payed to fresh ideas, which stem from recent results by M. Macaj, J. Siran and other authors.

Dimitri Leemans

Searching for Geometries with Magma

There has been a long tradition in Brussels of using Magma and other computational algebra software to search for geometric structures that can be constructed from groups. These last years, we have focused more on abstract regular and chirally regular polytopes. In this talk we will show some of the experimental and theoretical results obtained during the last five years.

Ayan Mahalanobis

The MOR cryptosystem and extra-special p-groups

The MOR cryptosystem is a generalization of the ElGamal cryptosystem. In a MOR cryptosystem, the security depends on the *discrete logarithm problem* in the automorphism group of a group G, not G itself.

In this talk, we describe the MOR cryptosystem as presented by Paeng et. al. at Crypto2001. We propose to build a MOR cryptosystem using the automorphism group of the extra-special group of exponent p, p being an odd prime. We discuss the security and speed of this cryptosystem.

Mark Mixer

Algorithms for classifying abstract regular polytopes

In 2006, D. Leemans and L. Vauthier published "An atlas of abstract regular polytopes for small groups", where polytopes were classified up to isomorphism and duality for small almost simple groups. Also in 2006, M. I. Hartley published "An atlas of small regular abstract polytopes", where polytopes are classified up to isomorphism for all almost all groups with fewer than 2000 elements. In this talk we will describe a new isomorphism test for abstract polytopes, which uses CPR graphs, and discuss the progress of new algorithms, which use this new test for finding and classifying all regular polytopes in a fixed group.

Padraig Ó Catháin

Doubly transitive group actions on Hadamard matrices and skew difference sets

A *Hadamard matrix* of order $4n$ is a matrix with entries in $\{\pm 1\}$ which satisfies $HH^\top = 4nI_{4n}$. A Hadamard matrix of order $4n$ determines a 2-$(4n-1, 2n-1, n-1)$ design and a 3-$(4n, 2n, n-1)$ design, called Hadamard 2- and 3-designs respectively. An old paper of Ito considers actions of non-affine doubly transitive groups on Hadamard 3-designs, and concludes that such a group must be $PSL_2(q)$, M_{12} or $Sp_6(2)$. By consideration of the Hadamard 2-designs, we show that each group has a doubly transitive action on a unique equivalence class of Hadamard matrices.

We say that $D \subseteq G$ is a *difference set* in G if every non-identity element of G has a fixed number, λ, of distinct representations $d_i d_j^{-1}$ where $d_i, d_j \in D$. A difference set corresponds naturally to a regular subgroup of the automorphism group of a 2-design. We say that D is a *Hadamard difference set* if $|G| = 4n-1$, $|D| = 2n-1$ and $\lambda = n-1$. A difference set is *skew* if $G = \{1_G\} \cup D \cup D^{(-1)}$, where $D^{(-1)} = \left\{d^{-1} \mid d \in D\right\}$. A skew difference set is necessarily Hadamard. Classical examples are given by the Paley difference sets, and for many years it was conjectured that there are no others. Other examples have been found in groups of order q^3 over the past 5 years or so. We describe a new family of skew-Hadamard difference sets. This provides examples at infinitely many new orders.

Felix Rehren

Majorana Calculations

Majorana algebras are an axiomatisation due to Ivanov of Griess-type algebras, involved in the celebrated construction of the sporadic simple Monster group and well-known in the context of Vertex Operator Algebras. Recent work by Ivanov and Pasechnik, Seress, Shpectorov has been in the theory of Majorana representations of finite groups. We will exhibit a construction of the universal Majorana algebra with n generators, which is an initial object in the category of such algebras, based on a slightly different axiomatisation. In this context a theorem of Sakuma becomes a classification of Majorana algebras with 2 generators. We will look at some of the computational methods featuring in the classification of such algebras. This is being carried out in GAP. The work has been done jointly with S. Shpectorov.

Csaba Schneider

Six-dimensional nilpotent Lie algebras

I will present a classification of six-dimensional nilpotent Lie algebras that is valid over an arbitrary field including fields that are not algebraically closed and fields of characteristic 2. This work can be considered as a revision and extension of earlier research by Willem de Graaf

who solved this problem using computational tools for fields of characteristic different from 2. We extended de Graaf's classification to all fields and in the process we discovered interesting connections between the class of nilpotent Lie algebras with dimension 6 and the theory of quadratic forms. Namely, some isomorphism classes of such Lie algebras can be characterized by the equivalence classes of certain quadratic forms using the Gram determinant, if the characteristic is different from 2, or the Arf invariant, if the characteristic is equal to 2. The research presented in this talk was carried out in collaboration with Willem de Graaf and Serena Cicalo.

Sergey Shpectorov

The uniqueness of the generalized octagon of order (2,4) under additional group theoretic assumptions

This is a joint project with A.M. Cohen and E. O'Brien. We prove the uniqueness of the octagon in the title under the additional assumption that its automorphism group contains a subgroup Q of order 2^{10} fixing a point a and acting regularly on the points far away from a. This problem was posed by Cohen just over twenty years ago. The solution achieved recently involves massive computer enumeration. The project naturally splits into two parts depending on whether a particular set of five involutions in Q generates an index 2 subgroup in Q, or it generates the entire Q. In the first case, a set of condition was checked on all groups of order 2^9 eliminating all but the one known example. This computation was run by O'Brien in MAGMA. In the second case a certain factorization of the group Q arises (similar to the factorizations as the product of the root subgroups). A full list ($\sim$ 3.1 million) of such factorizations has been constructed and then a set of conditions was checked for all of them, eliminating all of them. This was run by Shpectorov in GAP.

Mike Slattery

Computing commutator structure in some maximal class p-groups

In their book "The Structure of Groups of Prime Power Order", C.R. Leedham-Green and S. McKay describe an approach to constructing certain types of maximal class p-groups using the ring of integers in a local cyclotomic number field. By implementing these computations (in Magma), I've been able to explore possible commutator structures, especially as they relate to some character degree questions. This talk will look at the computations and some of the results.

Evgeny Vdovin [1]

On the base size of a transitive finite group with solvable point stabilizer

Assume that G acts on Ω. An element $x \in \Omega$ is called a *G-regular point* if $|xG| = |G|$, i.e., if the G-orbit of x is regular. Define an action of G on Ω^k by

$$g : (i_1, \dots, i_k) \mapsto (i_1 g, \dots, i_k g).$$

If G acts faithfully and transitively on Ω, then the minimal k such that Ω^k possesses a G-regular point is called the *base size* of G and is denoted by $\mathrm{Base}(G)$. For every natural m the number of G-regular orbits in Ω^m is denoted by $\mathrm{Reg}(G, m)$ (this number equals 0 if $m < \mathrm{Base}(G)$). If H is a subgroup of G and G acts on the set Ω of right cosets of H by right multiplication, then G/H_G acts faithfully and transitively on Ω. In this case we denote $\mathrm{Base}(G/H_G)$ and $\mathrm{Reg}(G/H_G, m)$ by $\mathrm{Base}_H(G)$ and $\mathrm{Reg}_H(G, m)$ respectively. We also say that $\mathrm{Base}_H(G)$ is the

[1]The work is supported by RFBR, projects 10-01-00391, and 10-01-90007, Deligne 2004 Balzan prize in mathematics, and the Lavrent'ev Young Scientists Competition (No 43 on 04.02.2010)

base size of G with respect to H. Clearly, $\mathrm{Base}_H(G)$ is the minimal k such that there exist $x_1, \ldots, x_k \in G$ with $H^{x_1} \cap \cdots \cap H^{x_k} = H_G$.

In the last twenty years, good progress has been achieved in finding the base sizes of almost simple groups acting primitively and non-standard. On the other hand in the series of papers of distinct authors (D. S. Passman, V. I. Zenkov, S. Dolfi, etc.) the following theorem was proven:

Theorem 0.1. *If H is a π-Hall subgroup of a π-solvable group G, then there exists $x, y \in G$ with $H \cap H^x \cap H^y = O_\pi(G) = H_G$, i.e., $\mathrm{Base}_H(G) \leq 3$.*

In the "Kourovka notebook" the author inserted the following problems:

(1) (Problem 17.40) Is $\mathrm{Base}_N(G) \leq 3$, where N is a nilpotent subgroup of a finite group G and $F(G) = 1$?
(2) (Problem 17.41):
   (a) is $\mathrm{Base}_S(G) \leq 7$,
   (b) is $\mathrm{Base}_S(G) \leq 5$,
   where S is a solvable subgroup of a finite group G and the solvable radical of G is trivial?

Our main result is the following theorem:

Theorem 0.2. *Let G be a group and let*

$$\{e\} = G_0 < G_1 < G_2 < \ldots < G_n = G \tag{1}$$

be a composition series of G that is a refinement of a chief series. Assume that for some k the following condition holds: If G_i/G_{i-1} is nonabelian, then for every solvable subgroup T of $\mathrm{Aut}_G(G_i/G_{i-1})$ we have

$$\mathrm{Base}_T(\mathrm{Aut}_G(G_i/G_{i-1})) \leq k \text{ and } \mathrm{Reg}_T(\mathrm{Aut}_G(G_i/G_{i-1}), k) \geq 5.$$

Then, for every maximal solvable subgroup S of G, we have $\mathrm{Base}_S(G) \leq k$.

Thus this theorem reduced Problem 17.41 from the "Kourovka notebook" to the investigation of finite almost simple groups.

Petr Vojtěchovský

Primitive groups and simple automorphic loops

Roughly speaking, loops are groups without associativity. More precisely, (finite) loops are the algebraic objects whose multiplication tables are normalized latin squares. I am interested in varieties of loops close to groups where computational methods of group theory are helpful.

A loop is *automorphic* if all its inner mappings are automorphisms. Groups are therefore automorphic loops, but there are plenty of nonassociative examples. A loop is simple if and only if the permutation group generated by all its left and right translations is primitive. We used the GAP libraries of primitive groups and our package LOOPS to search for simple automorphic loops. The surprising result so far: there are no nonassociative simple automorphic loops of order less than 2500.

I will describe the search and also translate the existence problem of simple automorphic loops entirely into group theory. The resulting group-theoretical problem appears difficult but not hopeless. Time permitting, I will say a bit about the deep structural results we have obtained for commutative automorphic loops (for instance the Odd Order Theorem), some with the aid of automated deduction.

This is joint work with Kenneth Johnson, Gábor P. Nagy and Michael Kinyon.