Titles and Abstracts

Finite Geometries Groups Computation
2004
Pingree Park
Colorado State University

Betten, Anton; Colorado State University, (Monday 10:00)
betten@math.colostate.edu

Hyperovals and Geometric Codes

In 1989, David Glynn published a criterion for hyperoval polynomials. ("A condition for the existence of ovals in $PG(2, q)$, q even", Geometriae Dedicata 32, 247-252). The purpose of this talk is to explain why this condition works. If time permits, I would also like to point out how to derive that criterion from the theory of geometric codes. This part of the talk is based on the paper by D.G. Glynn and J.W.P. Hirschfeld, "On the Classification of Geometric Codes by Polynomial Functions", Designs, Codes and Cryptography 6 (1995) 189-204.

Brooksbank, Peter; Bucknell University, (Tuesday 5:10)
brooksbank@math.ohio-state.edu

Recognising normalisers of symplectic-type groups.

A "Matrix Group Project" has been underway for ten years, whose goal is to compute a composition series for any group given by a generating set of invertible matrices with entries in a finite field. In this context, it is important to be able to recognise when some given subgroup G of $GL(r^m, p^k)$ normalises a symplectic-type r-group. Until now, only the case $m = 1$ for odd r has been adequately dealt with. In this talk I will report on some recent progress with the general problem. This is joint work with Alice Niemeyer and Ákos Seress.

Brown, Matt; University of Adelaide, Australia (Thursday 10:00)
mbrown@maths.adelaide.edu.au

Sets of ovoids of $\mathrm{PG}(3, s)$ and generalized quadrangles of order (s, s^2)

In his paper "Generalized Quadrangles of order (s, s^2), III" of 1999 J. A. Thas gave a unified geometric construction of the generalized quadrangles constructed algebraically from a flock of a quadratic cone by Kantor (s odd) and Payne (s even) in the mid 1980's. (Previously Knarr had given a geometric construction valid for s odd.) To do this Thas geometrically constructed a set of elliptic quadrics of $\mathrm{PG}(3, s)$ from a flock of a quadratic cone and showed that they were the elliptic quadrics arising from the fact that a dual flock GQ satisfies Property (G) at a line. (Property (G) in a GQ of order (s, s^2) allows the construction of a $\mathrm{PG}(3, s)$ from the GQ.)
Previously, the speaker (together with S. Barwick and T. Penttila) followed on from this work on a different tack by giving simple axioms for a set of elliptic quadrics of $\mathrm{PG}(3, s)$ called a *tetradic set* which characterises the set of elliptic quadrics associated with a dual flock GQ.
In this talk the speaker generalized these axioms to sets of any ovoids of $\mathrm{PG}(3, s)$ and shows the connection to generalized quadrangles satisfying Property (G) at a flag, thus including the GQ of Tits in the schema.

Ciobanu, Laura; Rutgers University (Sunday 4:50)
ciobanu@math.rutgers.edu

On the endomorphism problem in free groups

The endomorphism problem is solvable for a word W in a free group F if it can be decided effectively whether, given U in F, there is an endomorphism of F sending W to U. In this talk I discuss the complexity of an algorithm based on C. Edmunds' and C. Sims' approach that solves the endomorphism problem for a few classes of words. In particular I show that the algorithm runs in polynomial time when W is a two-generator word.

Dempwolf, Ulrich; Universität Kaiserslautern, Germany (Tuesday 4:30)
dempwolff@mathematik.uni-kl.de

Automorphisms of Bent Functions

Let $V = V(2n, 2)$ and $B \subseteq V$ such that $(V, \mathbf{B})$, $\mathbf{B} = \{B + v | v \in V\}$ is a symmetric design. Then B is called an elementary abelian Hadamard difference set and the characteristic function of B a bent function. The problem of computing the automorphism groups of elementary abelian Hadamard difference sets or equivalently of bent functions seems to have attracted not much interest so far. We describe some classes of such sets where the method of construction make large parts of the automorphism group visible. In such cases often the full automorphism group can be computed. For some of these series our investigations display connections between the existence of such sets and the degree 1-chohomology of certain Chevalley groups in characteristic two.

Gramlich, Ralf, TU Darmstadt,Germany (Wednedsay 4:30)
gramlich@mathematik.tu-darmstadt.de

On geometries on hyperbolic lines.

Geometries on the hyperbolic lines of a symplectic polar geometry have been studied and characterized by Jon Hall and by Hans Cuypers. Extending from these characterizations, one can give some sort of local characterization of these geometries, which implies a characterization of the symplectic groups by centralizers of involutions.

Similar results are possible for geometries on the hyperbolic lines of a unitary polar geometry, based on unpublished results by Hans Cuypers. In the unitary case, however, there still seems to be space for improvement.

I will report on existing results and on the joint efforts with my PhD student Kristina Altmann to improve those results.

Hall, Jonathan , Michigan State University, (Wednesday 5:00)
jhall@math.msu.edu

Imprimitive geometries

Often in the study of highly homogeneous geometries, the automorphism group acts primitively by nature or by hypothesis. We discuss some recent work on geometries for which the automorphism group is naturally or assumed to be imprimitive. Particular cases of interest are transversal designs and imprimitive distance transitive graphs.

Havas, George; The University of Queensland, Australia (Wednesday 10:30)
havas@itee.uq.edu.au

Efficient presentations for the Mathieu simple group M_{22} and its cover

(joint work with Marston Conder and Colin Ramsay)

Noting that the full covering group of the Mathieu simple group M_{22} has surprisingly short efficient presentations, we study efficient presentations for both it and M_{22} itself. We use three different methods to obtain efficient presentations for both of these groups. We produce a number of new short presentations and also presentations which have nice structure.

Hulpke Alexander, (Monday 5:00)
hulpke@math.colostate.edu

Searching for Geometries in Groups

Bill Kantor observed that permutations of the elements of a group with certain properties would lead to projective planes. I want to report about a search for such objects.

Kantor, William, University of Oregon, (Saturday 2:45)
kantor@darkwing.uoregon.edu

Finite Semifields.

I will survey the known finite semifields and discuss the question:
How many finite semifields of given order are there up to isotopism

Leedham-Green, Charles; Queen Mary, University of London, UK (Wednesday 9:00)
C.R.Leedham-Green@qmul.ac.uk

A divide and conquer strategy for the explicit recognition of special linear groups.

Despite the more general and fundamental work of W. Kantor, A. Seress and P. Brooksbank, we have persevered, in the style of [Celler and Leedham-Green] in the production of algorithms and code for the explicit recognition of $G := SL(d, q)$, with emphasis on the natural representation. Naturally we hope to deal with the other classical groups in the same style. Our objective is simply to find a canonical generating set. It is then of course easy to write any element of G as a word in these generators. To some extent the algorithm can be adapted to work in greater generality; particularly for other irreducible representations of G in the same characteristic. When working in greater generality, we would still have a problem in writing an arbitrary element of G as a word in these generators. This problem has been solved by A. Cohen and S. Murray, given the canonical generating sets that we provide.

Our algorithms are by recursion on d, the case $d = 2$ being critical. An algorithm due to M. Conder, E. O'Brien and the author reduces this to the solution of a discrete log problem in $GF(q)$. The current implementation of discrete logarithms in MAGMA is sufficiently powerful to make this reduction useful.

If the natural ordered basis of the space V on which G acts is denoted by $(e_1, \ldots, e_d)$, the chosen generating set consists of a canonical generating set for the copy of $SL(2, q)$ acting on $\langle e_1, e_2\rangle$, including the transposition (e_1, e_2); and the d-cycle $(e_1, \ldots, e_d)$ (now denoting a permutation, not an ordered basis). These two elements generate a copy of the Weyl group, namely the symmetric group S_d. The algorithm centres on finding this d-cycle.

The problem splits into two seriously different cases, depending on the parity of q, the odd case being the easier...

Magaard, Kay; Wayne State University (Sunday 3:50)
kaym@math.wayne.edu

The action of the mapping class group on Nielsen classes

Let G be a finte group. By Riemann's Existence theorem the orbits of the mapping class group on certain classes of generating systems of G correspond to irreducible families of covers of Riemann surfaces (by Riemann surfaces). Thus, many problems on algebraic curves require the computation of mapping class group orbits. In the talk I will describe an implementation of this computation.

Maschietti, Antonio; Universita' "La Sapienza", Roma, Italy
maschiet@mat.uniroma1.it

Symplectic translation planes of even order (Wednesday 11:00)

Topics:

1. Projective planes and completely regular line–ovals.
2. Symplectic translation planes. A characterization of symplectic translation planes of even order in terms of the existence of completely regular line–ovals.
3. The group of a completely regular line–ovals. Some results on flag–transitive symplectic translation planes.
4. Symplectic translation planes of even order q^2: open problems.

Mathon, Rudi; University of Toronto, Canada (Saturday 9:10)
combin@cs.toronto.edu

Stochastic algorithms for spreads, cliques and intersection sets

We will describe algorithms based on restricted neighborhood search for finding intersesting subsets of points or blocks in various incidence systems. These can be used to generate designs, geometries and codes as well as cliques and clusters in large networks. A number of new results are highlighted which were obtained from such stochastic combinatorial searches.

Merchant, Eric; University of Oregon (Sunday 3:10)
emerchan@noether.uoregon.edu

Structural properties of Hadamard designs.

This talk will focus on structural properties of Hadamard designs, i.e. symmetric designs with parameters $2-(4n-1, 2n-1, n-1)$. The properties of interest are good blocks and good points, and how they interact. One application will be: given a Hadamard design of order n, we derive an exponential lower bound for the number of non-isomorphic Hadamard designs of order $2n$. Also, given a finite group G, we construct a Hadamard design with full automorphism group isomorphic to G.

O'Brien, Eamonn; University of Auckland, New Zealand (Saturday 10:30)
obrien@math.auckland.ac.nz

Linear groups: questions, algorithms, answers.

One of Bill Kantor's major contributions has been to computational aspects of group theory, in particular to the development and analysis of high-performance algorithms for linear groups.
I will identify some of the problems inherent in algorithm design for linear groups. I will survey a major on-going research program, which seeks to develop new paradigms for their study, reporting some of the mathematics developed by Kantor and others as part of this program, and mentioning some of the challenging problems which arise.

Payne, Stanley; University of Colorado at Denver (Monday 11:00)
spayne@math.cudenver.edu

Finite, Non-abelian Groups that Admit Kantor Families

A Kantor family in a finite group is a collection of subgroups satisfying two rather simple (but group-theoretically awkward) conditions first identified by Kantor. Such a family coexists with a certain kind of generalized quadrangle known as an elation generalized quadrangle. The number of distinct, known finite non-abelian groups admitting Kantor families is still rather small, and some of them have been studied very little. We review the construction of the known groups and mention some additional restrictions that have been discovered. We then survey some of the open questions concerning these groups.

Penttila, Tim; University of Western Australia, Australia. (Saturday 1:30)
penttila@maths.uwa.edu.au

Applications of computer algebra to finite geometry

I will survey some past successes in applying computational group theory as available in computer algebra packages to construction problems in finite geometry. I will go on to look at future prospects, with an eye towards present barriers to progress that may be overcome with improvements in algorithms in computational group theory in the near future. The overriding theme is that interesting geometrical objects can be constructed using computational group theory, even when the geometrical objects fail to have interesting groups.

It is no surprise that progress with computation with matrix groups is needed, but the emphasis will be on the advances needed to help with finite geometry problems, which is certainly a different perspective from the usual one, and involves some problems which may be easier to solve than those causing difficulties at present with computational group theory for matrix groups.

Topics in geometry to be touched upon include ovals, generalised quadrangles, projective planes, and ovoids and spreads of projective and polar spaces. The talk aims to be accessible to people with no prior knowledge of finite geometry, with the goal of describing some of the problems in computational group theory that it would be helpful to overcome in order to attempt to solve some important construction problems in finite geometry.

Praeger, Cheryl; University of Western Australia, Australia. (Thursday 10:40)
praeger@maths.uwa.edu.au

Limits of finite vertex-primitive graphs.

The class of all connected vertex-transitive graphs forms a metric space under a natural combinatorially defined metric. In the talk I will discuss the structure of graphs which are limit points, in this metric space, of the subset consisting of all finite graphs that admit a vertex-primitive group of automorphisms. A description of these limit graphs provides a useful description of the possible local structures of generic finite graphs that admit a vertex-primitive automorphism group. An analysis is given of the possible types of these limit graphs, which relies on the finite simple group classification. This is collaborative work with Michael Giudici, Cai Heng Li, Akos Serress, and Vladimir Trofimov.

Pralle, Harm; TU Braunschweig, Germamy (Monday 10:30)
H.Pralle@tu-bd.de

A spread of a polar space Π of rank 4 inducing a generalized quadrangle.

(Joint with Sergey Shpectorov)

Let Π be a polar space of rank 4 over a field $\mathbb{K}$ such that the generalized quadrangle $Res^+(\alpha)$ of a line α of Π which consists of the planes and 3-spaces of Π containing α, admits a spread. Let $\mathcal{L}$ be a line-spread of Π with the following property:

Let $\mathcal{D}$ be the set of 3-spaces of Π in which $\mathcal{L}$ induces spreads. For every point Σ of Π, the 3-spaces of $\mathcal{D}$ containing Σ all contain the spread line $\lambda \in \mathcal{L}$ covering Σ and form a spread of the generalized quadrangle $Res^+(\lambda)$.

Given such a spread $\mathcal{L}$, we show that $\Gamma = (\mathcal{L}, \mathcal{D})$ is a generalized quadrangle which we characterize for the classical polar spaces $\Pi \cong Sp_8(\mathbb{K})$ and $O^-_{10}(\mathbb{K})$ as $Sp_4(\mathbb{K}(\zeta))$ and $H_5(\mathbb{K}(\zeta))$, respectively, where $\mathbb{K}(\zeta)$ is a quadratic field extension of $\mathbb{K}$. For finite polar spaces, we show they are the only two admitting such a spread. We give an example of a spread $\mathcal{L}$ for the infinite hermitian polar space $H_8(\mathbb{C})$ over the complex numbers $\mathbb{C}$ where $\Gamma = (\mathcal{L}, \mathcal{D})$ is a hermitian generalized quadrangle $H_4(\mathbb{Q})$ over the quaternions.

This research is motivated by the following: Dualizing Π, the point set $\bigcup_{X \in \mathcal{D}} X^{\perp_\Delta}$ of the dual polar space Δ dual of Π is a hyperplane of Δ intersecting each symp Σ, i.e. an element of maximal type of Δ, in the neighbours of an ovoid of a quad of Σ.

Roney-Dougal, Colva; University of St. Andrews, UK (Monday 3:30)
Colva@dcs.st-and.ac.uk
The primitive groups of degree less than 2500.

I will discuss my recent classification of the primitive permutation groups of degree less than 2500.

Shult, Ernie ; Kansas State University (Sunday 2:30)
shult@math.ksu.edu
Some remarks on certain substructures of $E_(6,1)$ and $E_{7,7}$.

The talk begins by examining details regarding a construction of Cooperstein that follows from the assumed existence of an ovoid in the finite polar space $D_{5,1}(q)$ – still an outstanding problem. Special versions of this structure exist over certain infinte fields through generalizations of two basic theorems of B.. Muehlherr regarding the geometries of the title, from 15 years ago. Can this structure (a projective plane) exist in the finite case? If so, the counting consequences are extremal.

Seress, Ákos; Ohio State University (Thursday 9:00)
akos@math.ohio-state.edu
Quasiprimitive s-arc transitive graphs of product action type

(joint work with Cai Heng Li)
An s-arc in a graph Γ is a sequence of vertices $(v_0, ..., v_s)$ such that $\{v_i, v_{i+1}\}$ is an edge for all $i \le s-1$ and $v_i \ne v_{i+2}$ for all $i \le s-2$. The graph Γ is called s-arc transitive if an s-arc can be mapped to any other s-arc by a graph automorphism. A permutation group is called quasiprimitive if all nontrivial normal subgroups are transitive.
C. Praeger proved that any non-bipartite s-arc transitive graph is a cover of one that has a quasiprimitive group of automorphisms, and so a first step of classification of s-arc transitive graphs may be the study of quasiprimitive ones. Praeger's "O'Nan–Scott type" classification of quasiprimitive groups divides them into eight classes; it was known that four of these classes cannot contain automorphism groups of 2-arc transitive graphs, three of them could, and the status of the product action type was unknown.
In this talk, we provide examples of quasiprimitive 2-arc transitive graphs of product action type, and report progress toward the classification of all such graphs.

Slattery, Michael; Marquette University (Wednesday 3:30)
mikes@studsys.mscs.mu.edu
Producing Groups of Square-free Order

An algorithm is described for the enumeration and recognition of groups whose order is a product of distinct primes. The focus is providing access to isomorphism classes of such groups by computing representatives as needed rather than storing a large database.

Suetake, Chihiro; Fukushima National College of Technology, Japan (Sunday 5:20)
suetake@fukushima-nct.ac.jp
The Classification of Symmetric Transversal Designs $STD_4[12;3]$'s

In this article we prove that there is only one symmetric transversal design $STD_4[12;3]$ up to isomorphism. We also show that the order of the full automorphism group of $STD_4[12;3]$ is $25 \cdot 33$ and Aut $STD_4[12;3]$ has a regular subgroup as a permutation group on the point set. We used a computer for our research.

Thas Joseph, Ghent University, Belgium (Monday 9:00)
jat@cage.rug.ac.be

Finite Translation Generalized Quadrangles: old results, new results, open problems

In $PG(2n+m-1,q)$ consider a set $O(n,m,q)$ of q^m+1 $(n-1)$-dimensional subspaces $\mathrm{PG}^{(0)}(n-1,q)$, $\mathrm{PG}^{(1)}(n-1,q),\cdots,\mathrm{PG}^{(q^m)}(n-1,q)$, every three of which generate a $\mathrm{PG}(3n-1,q)$ and such that each element $\mathrm{PG}^{(i)}(n-1,q)$ of $O(n,m,q)$ is contained in a $\mathrm{PG}^{(i)}(n+m-1,q)$ having no point in common with any $\mathrm{PG}^{(j)}(n-1,q)$, for $j \neq i$. For $n=m$ such a set $O(n,n,q)$ is called a *pseudo-oval* or a *generalized oval* or an $[n-1]$-*oval* of $\mathrm{PG}(3n-1,q)$; a generalized oval of $\mathrm{PG}(2,q)$ is just an oval of $\mathrm{PG}(2,q)$. For $n \neq m$ such a set $O(n,m,q)$ is called a *pseudo-ovoid* or a *generalized ovoid* or an $[n-1]$-*ovoid* or an *egg* of $\mathrm{PG}(2n+m-1,q)$. It appears that the theory of the sets $O(n,m,q)$ is equivalent to the theory of the finite translation generalized quadrangles; see the monograph *Finite Generalized Quadrangles* by S.E. Payne and J. A. Thas (Pitman, Boston, 1984). In the talk old results will be surveyed, new results will be given, and open problems will be mentioned.

Thas Koen , Ghent University, Belgium (Monday 4:30)
kthas@cage.ugent.be

Elation generalized quadrangles of order $(qq2)$, q even, with a classical subGQ of order q containing the elation point are classical.

One of the famous open problems in Finite Geometry is the classification of ovoids in a projective 3-space $PG(3,q)$ over the finite field with q elements, q even. For q odd, this classification was obtained in 1955 by A. Barlotti and G. Panella. A breakthrough result was recently obtained by M. R. Brown, who showed that when such an ovoid has a conic plane section, the ovoid must be an elliptic quadric. Even more recently, M. R. Brown and M. Lavrauw generalized this theorem by obtaining a similar result for higher dimensions. Both results have equivalent statements in the theory of (translation) generalized quadrangles.

In my talk, I will speak about a generalization of these results which shows that an elation generalized quadrangle of order $(q,q2)$, q even, with a $\mathcal{Q}(4,q)$ subGQ containing the elation point, arises from a non-singular elliptic quadric in $PG(5,q)$.

The theorem itself arises as a corollary of a more general observation which works for all characteristics. There is a wealth of consequences.

Tonchev, Vladimir; Michigan Tech. (Monday 3:00)
tonchev@mtu.edu

Hyperplane line spreads and code synchronization.

A difference system of sets (DSS) is a generalization of a cyclic difference set that arises from an application to code synchronization. A method for the construction of DSS from partitions of cyclic difference sets is presented. In particular, the existence of partitions of a hyperplane in an even dimensional projective space into disjoint lines that belong to different Singer cycles are discussed.

van Maldghem, Hendrik; Ghent University, Belgium (Wednesday 3:00)
Hendrik.VanMaldeghem@rug.ac.be

Metric recognition of buildings.

We discuss under which conditions a building (in particular its type!) is determined by its set of chambers and all pairs (C,D) of chambers with the Weyl distance from C to D fixed (but unknown). In this setting, even the Weyl group of the building is not given. It will turn out that in many cases, a building is determined by very limited information on its set of chambers. The problem we deal with can be stated as a riddle, and the explanation of how the riddle works provides the main ideas of the proof of the corresponding theorem. In the talk, we start with defining a building as a metric space, and then state the riddle, followed by the explanation why it works.

Yoshiara, Satoshi; Tokyo Woman's Christian University, Japan (Wednesday 10:00)
yoshiara@lab.twcu.ac.jp

Dimensional dual hyperovals – a survey

The concept of dimensional dual hyperovals was given by C.Huybrechts, A.Pasini and I around 1997 during our attempts to generalize the concept of hyperovals in a projective plane. It is formalized as follows.

Let $PG(n, q)$ be an n-dimensional Desarguesian projective space with underlying vector space $V(n+1, q)$ over a finite field $GF(q)$. A family $\mathcal{S}$ of d-dimensional subspaces of $PG(n, q)$ is called a *d-dimensional dual arc* in $PG(n, q)$ if the following conditions are satisfied:

(1) any two distinct members of $\mathcal{S}$ intersect in a projective point,

(2) any three mutually distinct members of $\mathcal{S}$ intersect trivially,

(3) all members of $\mathcal{S}$ span the space $PG(n, q)$, and

It is easy to see that $|\mathcal{S}| \leq (q^{d+1} - 1)/(q - 1) + 1$. If the upper bound is attained, $\mathcal{S}$ is called a *d-dimensional dual hyperoval*.

Observe that 1-dimensional dual hyperovals are nothing more than dual hyperovals in a projective plane. The remarkable example is a set of 22 totally isotropic planes in $PG(5, 4)$ with a unitary form, on which the Mathieu group M_{22} acts doubly transitively. Several families of examples are constructed, using the Veronesean map, caps, almost perfect nonlinear functions etc.

Recent works by the above-mentioned researchers and A. Del Fra, B.Cooperstein, J.Thas and H. van Maldeghem reveal interesting connections of this concept with the other area of combinatorial geometries and group theory. In my talk I will try to give a survey on this promissing object to study, showing main examples, principal results and several open problems.