Combinatorics
and
Computer Algebra 2015
(CoCoA15)

July 20-24, 2015

Abstracts of Talks

Colorado State University

Fort Collins, Colorado
<table>
<thead>
<tr>
<th>Sunday</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/19</td>
<td>7/20</td>
<td>7/21</td>
<td>7/22</td>
<td>7/23</td>
<td>7/24</td>
</tr>
<tr>
<td>Sam</td>
<td>Registration TILT Building Room 221</td>
<td>Korchmaros TILT Building Room 221</td>
<td>Soicher TILT Building Room 221</td>
<td>Egan TILT Building Room 221</td>
<td>Pawe TILT Building Room 221</td>
</tr>
<tr>
<td>8am</td>
<td>9am</td>
<td>10am</td>
<td>10:30am</td>
<td>10am</td>
<td>10am</td>
</tr>
<tr>
<td>coffee break</td>
<td>coffee break</td>
<td>coffee break</td>
<td>coffee break</td>
<td>coffee break</td>
<td>coffee break</td>
</tr>
<tr>
<td>room 221</td>
<td>room 221</td>
<td>room 221</td>
<td>room 221</td>
<td>room 221</td>
<td>room 221</td>
</tr>
<tr>
<td>11am</td>
<td>12pm</td>
<td>1pm</td>
<td>1pm</td>
<td>1pm</td>
<td>1pm</td>
</tr>
<tr>
<td>problem session</td>
<td>lunch</td>
<td>Carvalho TILT Building Room 221</td>
<td>Kelley TILT Building Room 221</td>
<td>Gavrilyuk TILT Building Room 221</td>
<td>Szilasi TILT Building Room 221</td>
</tr>
<tr>
<td>1:30pm</td>
<td>2pm</td>
<td>2:30pm</td>
<td>2:30pm</td>
<td>2:30pm</td>
<td>2:30pm</td>
</tr>
<tr>
<td>Vandenbussche TILT Building Room 221</td>
<td>problem session</td>
<td>Raithel TILT Building Room 221</td>
<td>coffee break</td>
<td>coffee break</td>
<td>coffee break</td>
</tr>
<tr>
<td>3pm</td>
<td>4pm</td>
<td>4pm</td>
<td>4pm</td>
<td>4pm</td>
<td>4pm</td>
</tr>
<tr>
<td>problem session</td>
<td>Registration TILT Building Room 221</td>
<td>problem session</td>
<td>problem session</td>
<td>problem session</td>
<td>problem session</td>
</tr>
<tr>
<td>4:30pm</td>
<td>5pm</td>
<td>6pm</td>
<td>6pm</td>
<td>6pm</td>
<td>6pm</td>
</tr>
<tr>
<td>Academic Village TILT Building Room 221</td>
<td>problem session</td>
<td>Engineering E204/5 TILT Building Room 221</td>
<td>problem session</td>
<td>problem session</td>
<td>problem session</td>
</tr>
<tr>
<td>5pm</td>
<td>6pm</td>
<td>6pm</td>
<td>6pm</td>
<td>6pm</td>
<td>6pm</td>
</tr>
</tbody>
</table>

- Registration: Lory State Park Room 302 (Longs Peak Room)
- Lunch: Great Hall

*Note: All times are in AM/PM format.*
Invited Talks

Partial difference sets in Abelian groups

**Stefaan De Winter**
Michigan Technological University

(Joint work with Ellen Kamischke and Zeying Wang)

Partial difference sets (PDS) in finite groups were defined by S.L. Ma in the early 80s. These interesting subsets of finite groups allow for the construction of strongly regular Cayley graphs. In this talk I will first review basic definitions and constructions, as well as the major results on PDS, with a focus on PDS in Abelian groups. In the second half of the talk I will present new results (in particular a technique to prove non-existence results). I will end with some directions for future research in the area of PDS in Abelian groups.

On Cameron-Liebler line classes

**Alexander Gavrilyuk**
N.N. Krasovsky Institute of Mathematics and Mechanics

A Cameron-Liebler line class of the finite projective space $PG(3, q)$ is a set of lines that shares a constant number $x$ of lines with every spread of $PG(3, q)$. The number $x$ is called the parameter of the Cameron-Liebler line class. These classes appeared in connection with an attempt by Cameron and Liebler (1982) to classify collineation groups of $PG(n, q)$, $n \geq 3$, that have equally many orbits on lines and on points.

In this talk, I will survey some recent results on Cameron-Liebler line classes such as a new necessary existence condition; new examples, non-existence or uniqueness of line classes for some $x$ and $q$.

On non–bipartite distance-regular graphs with very small smallest eigenvalue

**Jack Koolen**
University of Science and Technology of China

(Joint work with Zhi Qiao (USTC))

We study distance-regular graphs with valency $k \geq 3$ and smallest $-k/2 \geq \theta > -k$. Examples are the dual polar graphs with $a_1 = 1$, the Odd graphs, and the folded $2D + 1$-cubes. We show that for fixed diameter there are only finitely many of them and we classify them for diameter at most 3. As a consequence we can determine the distance-regular graphs with chromatic number 3 and diameter three.

Automorphism groups of algebraic curves

**Gábor Korchmáros**
Dipartimento di Matematica ed Informatica, Università della Basilicata, Campus Universitario di Macchia Romana
85100 Potenza, Italy
gabor.korchmaros@unibas.it

(Joint work with Massimo Giulietti)
Let $\mathcal{X}$ be a (projective, geometrically irreducible, non-singular) algebraic curve defined over an algebraically closed field $K$ of characteristic $p \geq 0$. We mainly focus on positive characteristic, and in particular on the case where $K$ is the algebraic closure of a finite field. Let $K(\mathcal{X})$ be the field of rational functions (the function field of transcendency degree one over $K$) of $\mathcal{X}$. The $K$-automorphism group $\text{Aut}(\mathcal{X})$ of $\mathcal{X}$ is defined to be the automorphism group $\text{Aut}(K(\mathcal{X}))$ consisting of those automorphisms of $K(\mathcal{X})$ which fix each element of $K$. $\text{Aut}(\mathcal{X})$ has a faithful action on the set of points of $\mathcal{X}$.

By a classical result, $\text{Aut}(\mathcal{X})$ is finite if the genus $g$ of $\mathcal{X}$ is at least two.

It has been known for a long time that every finite group occurs in this way, since for any ground field $K$ and any finite group $G$, there exists $\mathcal{X}$ such that $\text{Aut}(\mathcal{X}) \cong G$.

This result raised a general problem for groups and curves: Determine the finite groups that can be realized as the $K$-automorphism group of some curve with a given invariant. The most important such invariant is the genus $g$ of the curve, and there is a long history of results on the interaction between the automorphism group of a curve and its genus.

In positive characteristic, another important invariant is the $p$-rank of the curve (also called the Hasse-Witt invariant), which is the integer $\gamma$ so that the Jacobian of $\mathcal{X}$ has $p^\gamma$ points of order $p$. It is known that $0 \leq \gamma \leq g$.

In this survey we focus on the following issues:

(i) Upper bounds on the size of $G$ depending on $g$.
(ii) Examples of curves defined over a finite field with very large automorphism groups.
(iii) The possibilities for $G$ when the $p$-rank is 0.
(iv) Upper bounds on the size of the $p$-subgroups of $G$ depending on the $p$-rank.

The study of the automorphism group of an algebraic curve is mostly carried out by using Galois Theory, via the fundamental group of the curve. Here, we adopt a different approach in order to exploit the potential of Finite Group Theory.

References


On the constructions of optimal linear codes

Tatsuya Maruta
Osaka Prefecture University

(Joint work with Yuuki Kageyama)

An \([n, k, d]_q\) code is a linear code of length \(n\), dimension \(k\) and minimum Hamming weight \(d\) over the field of \(q\) elements \(\mathbb{F}_q\). A fundamental problem in coding theory is to find \(n_q(k, d)\), the minimum length \(n\) for which an \([n, k, d]_q\) code exists for given \(q, k\) and \(d\). A natural lower bound on \(n_q(k, d)\) is the Griesmer bound:

\[
\begin{align*}
n_q(k, d) \geq g_q(k, d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,
\end{align*}
\]

where \(\lceil x \rceil\) denotes the smallest integer \(\geq x\). In this talk, we construct linear codes over \(\mathbb{F}_q\) whose lengths are close to the Griesmer bound, using the geometric methods such as geometric puncturing and projective dual.

Parity-check codes and their representations

Gretchen Matthews
Clemson University

A linear code is often represented as the null space of a matrix; equivalently, it may be represented as a bipartite graph, called a Tanner graph. The performance of the code when coupled with an iterative decoding algorithm depends on its graphical representation. Low-density parity-check (LDPC) codes, which are defined by sparse graphs, have received much attention over the past decade due to the fact that they are capacity achieving when paired with iterative message-passing decoding algorithms. One drawback of these decoding algorithms is that they may produce noncodeword outputs, loosely called pseudocodewords. In this talk, we discuss combinatorial and algebraic tools for studying pseudocodewords.

Combinatorics, Modular Functions, and Computer Algebra

Peter Paule
Research Institute for Symbolic Computation (RISC),
Johannes Kepler University Linz

The talk reports on recent computer algebra developments related to problems in enumerative combinatorics, number theory, and special functions. A major case study concerns the algorithmic revitalization of partition analysis, a method developed by MacMahon more than a hundred years ago in connection with the problem to solve linear systems of Diophantine inequalities over non-negative integers. In a project with George Andrews, an implementation of partition analysis has been used to construct a new class of combinatorial objects, partition diamonds, which are partially ordered sets having modular forms as generating functions. This in turn led to variety of number theoretic observations which again can be proved with computer algebra. To this end, Radu set up an algebraic framework to enable an algorithmic treatment of modular functions. This part concerns joint work with George Andrews and Silviu Radu.

In a separate part of the talk, I will present a survey of other software packages developed by members of the algorithmic combinatorics group at RISC. Such packages found applications also outside combinatorics, for instance, in collaborations with particle physicists from DESY (Deutsches Elektronen-Synchrotron) or in industrial projects with partners from numerical analysis.
More About Venn Diagrams

Frank Ruskey
University of Victoria

An n-Venn diagram is a collection of n simple closed curves in the plane that divide it into $2^n$ non-empty regions, one unique region per possible intersection of the interiors/exteriors of the curves. If the curves lie in general position; e.g., so that no 3 curves intersect at a point then it is unknown whether rotationally symmetric diagrams exist for every prime n (the primality of n being an easily proved necessary condition). However, if curves can intersect at 3 or more curves, rotationally symmetric diagrams exist for prime n, and the proof relies on a modification of the classic symmetric chain decomposition of the Boolean lattice. In this talk this proof will be discussed along with other open problems in the area of Venn diagrams (e.g., can a new curve always be added to a Venn diagram to get a new Venn diagram?).

Applying block intersection polynomials to study graphs and designs

Leonard Soicher
Queen Mary University of London

About eight years ago, block intersection polynomials were introduced by Peter Cameron and myself [1] to derive information about block intersections from the parameters of a $t$-$(v, k, \lambda)$ design, and in particular, to provide an upper bound on the number of times a block may be repeated in such a design.

I later realised [2] that block intersection polynomials really apply more generally to the study of graphs, and for the applications to a $t$-design, the graph to use is simply the incidence graph of that design.

My aim in this talk is to give a simplified introduction to block intersection polynomials and to survey some of their applications, both theoretical and computational, over the last eight years, in the hope that you can apply these polynomials in your research.

References


Contributed Talks

Switched symplectic graphs and their 2-ranks

Aida Abiad

Tilburg University, The Netherlands

(Joint work with W.H. Haemers)

We apply Godsil-McKay switching to the symplectic graphs over $\mathbb{F}_2$ with at least 63 vertices and prove that the 2-rank of (the adjacency matrix of) the graph increases after switching. This shows that the switched graph is a new strongly regular graph with parameters $(2^{2\nu - 1}, 2^{2\nu - 2}, 2^{2\nu - 2})$ and 2-rank $2\nu + 2$ when $\nu \geq 3$. For the symplectic graph on 63 vertices we investigate repeated switching by computer and find many new strongly regular graphs with the above parameters for $\nu = 3$ with various 2-ranks. Using these results and a recursive construction method for the symplectic graph from Hadamard matrices, we obtain several graphs with the above parameters, but different 2-ranks for every $\nu \geq 3$.

Computing Hyperplanes of Near Polygons

Anurag Bishnoi

Ghent University

(Joint work with Bart De Bruyn)

A (geometric) hyperplane of a point-line geometry is a subset $H$ of points with the property that for every line $l$ either $l \cap H$ is a singleton or $l$ is completely contained in $H$. For certain classes of point-line geometries hyperplanes appear naturally when one geometry is isometrically embedded inside the other. In this talk, I will discuss some algorithmic and mathematical techniques that we have used for computing hyperplanes in near polygons. Some of the motivation for these computations is as follows.

In [1] we prove the non-existence of semi-finite generalized hexagons of order $(2, t)$ that contain a sub-hexagon of order 2, and our first step in the proof was to compute all the hyperplanes of the (completely classified) hexagons of order 2. In [2] we construct a new near octagon as an involution geometry of the finite simple group $G_2(4)$. We first discovered this octagon in a computer as a geometry that contains the Hall-Janko near octagon, and computing all the hyperplanes (up-to isomorphism) of the Hall-Janko near octagon was crucial for our discovery.

Hyperplanes which do not contain any line are called 1-ovoids. It was an open problem to determine if the dual split Cayley hexagon of order 4 contains any 1-ovoids. We have recently settled this problem by giving a computer assisted proof of non-existence, which as a corollary implies the non-existence of semi-finite generalized hexagons of order $(4, t)$ containing $H(4)^D$. We will discuss the techniques used in this proof and their other possible applications.

References


Gröbner bases methods in affine and projective variety codes

Cícero Carvalho

Universidade Federal de Uberlândia, Brasil

(Joint work with Victor G.L. Neumann)

Let $X := \{P_1, \ldots, P_m\}$ be a subset of $\mathbb{A}^n$, the affine space of dimension $n$ over a finite field with $q$ elements $\mathbb{F}_q$ and let $I_X \subset \mathbb{F}_q[X_1, \ldots, X_n] =: \mathbb{F}_q[X]$ be the ideal of $X$. Then $I_X$ is a zero-dimensional ideal, hence $\mathbb{F}_q[X]/I_X$ is a finite dimensional $\mathbb{F}_q$-vector space, and the evaluation morphism $\varphi : \mathbb{F}_q[X]/I_X \to \mathbb{F}_q^m$ given by $\varphi(f + I_X) = (f(P_1), \ldots, f(P_m))$ is an isomorphism. Let $L \subset \mathbb{F}_q[X]/I_X$ be an $\mathbb{F}_q$-vector subspace, the image $C_L := \varphi(L)$ is called the affine variety code defined over $X$ and associated to $L$ (see [1]). When $L = \{f + I_X \mid f = 0 \text{ or } \deg(f) \leq d\}$ for some nonnegative integer $d$ the code $C_L$ is said to be of Reed-Muller type.

One can do a similar construction for a subset $Y := \{Q_1, \ldots, Q_m\} \subset \mathbb{P}^n(\mathbb{F}_q)$. We denote by $I_Y \subset \mathbb{F}_q[Y_0, \ldots, Y_n] =: \mathbb{F}_q[Y]$ the homogeneous ideal of $Y$, and consider $\mathbb{F}_q[Y]/I_Y$ as a graded algebra $\mathbb{F}_q[Y]/I_Y = \bigoplus_{d=0}^{\infty} \mathbb{F}_q[Y]/I_Y(d)$. Writing the coordinates of the points of $Y$ such that the first nonzero entry from the left is one we define the evaluation morphism $\phi : \mathbb{F}_q[Y]/I_Y(d) \to \mathbb{F}_q^m$ by $\phi(f + I_Y) = (f(Q_1), \ldots, f(Q_m))$. Unlike the affine case $\phi$ is not an isomorphism, but it is injective and if $L \subset \mathbb{F}_q[Y]/I_Y(d)$ is a vector space we call the image $C_L := \phi(L)$ a projective variety code. We say that $C_L$ is of Reed-Muller type when $L = \mathbb{F}_q[Y]/I_Y(d)$.

In this talk we intend to show how one can use data from a Gröbner basis for $I_X$ or $I_Y$ to find information about the parameters of Reed-Muller type codes $C_L$ in both the affine and projective cases. In the affine case we will focus on codes defined over the cartesian product of $n$ nonzero subsets of $\mathbb{F}_q$, for which we gave a new proof for the minimum distance formula (originally found in [4]) and also found some of the higher Hamming weights of $C_L$ (see [2]). In the projective case we will take $Y$ to be the projective surface known as rational normal scroll. For this case we have determined the dimension, a bound for the minimum distance and the exact value of the minimum distance for some instances of these codes.

References


Classifying cocyclic Butson Hadamard matrices

Ronan Egan

National University of Ireland, Galway

(Joint work with Dane Flannery and Padraig Ó Catháin)
An $n \times n$ matrix $H$ with entries in $\langle \zeta_k \rangle$, the $k$th roots of unity, is Butson Hadamard if and only if $HH^* = nI_n$, where $H^*$ denotes the Hermitian transpose of $H$. For a group $G$ of order $n$, $\psi : G \times G \to \langle \zeta_k \rangle$ is a cocycle if and only if $\psi(g, h)\psi(gh, k) = \psi(g, h)\psi(h, k)$ for all $g, h, k \in G$. A matrix $H$ is cocyclic with indexing group $G$ if $H \approx H' = [\psi(g, h)]_{g, h \in G}$ where $\approx$ denotes equivalence, i.e., $H$ and $H'$ are equivalent if $H' = PHQ^*$ for $(P, Q) \in \text{Mon}(n, \langle \zeta_k \rangle)^2$.

We classify all the cocyclic Butson Hadamard matrices $\text{BH}(n, p)$ of order $n$ over the $p$th roots of unity for an odd prime $p$ and $np \leq 100$ up to equivalence [2]. That is, we compile a list of matrices such that any cocyclic $\text{BH}(n, p)$ for these $n$, $p$ is equivalent to exactly one element in the list. Our approach encompasses non-existence results and computational machinery for Butson and generalized Hadamard matrices that are of independent interest.

Butson Hadamard matrices have applications in disparate areas such as quantum physics and error-correcting codes. So lists of these objects have value beyond design theory. We were motivated to undertake the classification in this paper as a first step towards augmenting the available data on complex Hadamard matrices and we found several matrices not equivalent to any of those in the catalog [1].

References


Graphs with second largest eigenvalue at most 1

**Gary Greaves**

Tohoku University

(Joint work with Xi-Ming Cheng and Jack Koolen)

I will describe recent progress on the problem of classifying graphs whose second largest eigenvalue is at most 1. In particular, I will present a classification of such graphs having at most three distinct eigenvalues.

Symmetric coverings and the Bruck-Ryser-Chowla theorem

**Daniel Horsley**

Monash University, Australia

(Joint work with Nevena Francetić and Sarada Herke)

The Bruck-Ryser-Chowla theorem famously establishes the nonexistence of various symmetric block designs, including projective planes. In this talk I will discuss attempts to generalise this result from the setting of designs, where each pair of points must appear together in exactly some fixed number of blocks, to the setting of coverings, where each pair of points need only appear together in at least some fixed number of blocks.
Graph-based codes for distributed storage systems

Christine Kelley

University of Nebraska-Lincoln

(Joint work with Allison Beemer and Carolyn Mayer)

Coding for distributed storage systems has become an area of active interest as increasingly large amounts of data are being stored. Batch codes [1] address how to store \( n \) items in \( m \) servers so that any \( k \) of the \( n \) items can be retrieved by reading at most \( t \) items from each server, with consideration given to minimizing the total number of items, \( N \), stored across all servers. Combinatorial batch codes are replication-based and most constructions rely on discrete structures, such as designs, cage graphs, generalized quadrangles, and finite geometries. Graph-based constructions have recently been presented for multiset batch codes that store linear combinations of items in the database and allow for multiple users accessing data from the same devices [2, 3]. Alternatively, codes are analyzed for DSS with respect to a variety of metrics such as locality, which is the number of nodes that participate in the repair process of a failed node [4]. In this talk we will summarize some of these approaches and present a new construction of graph-based codes.

References


Algebraically defined graphs and generalized quadrangles

Brian Kronenthal

Kutztown University of Pennsylvania

(Joint work with Felix Lazebnik and Jason Williford)

In this talk, we will study generalized quadrangles from the perspective of their point-line incidence graphs. The incidence graphs of classical generalized quadrangles of odd prime power order \( q \) contain induced bipartite subgraphs that may be defined algebraically; indeed, defining partite sets \( P = \mathbb{F}_q^3 = L \), we say vertices \((a_1, a_2, a_3) \in P \) and \([x_1, x_2, x_3] \in L \) are adjacent if and only if \( a_2 + x_2 = a_1 x_1 \) and \( a_3 + x_3 = a_1 x_1^2 \). This subgraph has girth eight. Of particular interest is whether it is possible to alter these equations, by replacing \( a_1 x_1 \) and \( a_1 x_1^2 \) with other bivariate polynomials, to create a nonisomorphic girth eight graph. Success could illuminate a strategy for constructing new generalized quadrangles. We will also discuss similar questions about algebraically defined graphs over the complex numbers.
Group Symmetries of Complementary Code Matrices

Brooke Logan
Rowan University
Professor Hieu D. Nguyen

A complementary code matrix (CCM) is a generalization of a Golay code pair. Both types of codes have useful applications in radar and communication. This talk will demonstrate a way to characterize known symmetries of poly-phase CCMs in terms of group generators and relations, extending the results of Coxson for Barker sequences. As an application, the corresponding symmetry group is used to classify CCMs in terms of their equivalence classes. Classification results for $N \times 4$ quad-phase CCMs where $N = 2, 3, 4, 5, 6$ will be presented, as well as a new construction method involving ternary CCM dual pairs.

A Checker-board Tiling Problem

Curtis G Nelson
University of Wyoming

(Joint work with Bryan L. Shader)

Given nonnegative integral vectors $R = (r_1, r_2, \ldots, r_m)$ and $S = (s_1, s_2, \ldots, s_n)$, can a $m \times n$ checkerboard be tiled with vertical dimers (vertical $2 \times 1$ blocks) and monomers ($1 \times 1$ blocks) so that there are exactly $r_i$ dimers with the top half of the dimer in row $i$ and $s_j$ dimers in column $j$? This question can be thought of as an extension of the problem solved by the Gale-Ryser Theorem. I will present an answer to this question in terms of $R$ and $S$ and discuss some other properties of this combinatorial object.

On the Covering Number of Small Symmetric Groups and Some Sporadic Simple Groups

Daniela Nikolova-Popova
Florida Atlantic University (FAU), Boca Raton, USA

(Joint work with Luise-Charlotte Kappe, Eric Swartz)

We say that a group $G$ has a finite covering if $G$ is a set theoretical union of finitely many proper subgroups. The minimal number of subgroups needed for such a covering is called the covering number of $G$ denoted by $\sigma(G)$.

Let $S_n$ be the symmetric group on $n$ letters. For odd $n$ Maroti determined $\sigma(S_n)$ with the exception of $n = 9$, and gave estimates for $n$ even showing that $\sigma(S_n) \leq 2n - 2$. Using GAP calculations, as well as incidence matrices and linear programming, we show that $\sigma(S_8) = 64$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$. We also show that Maroti’s result for odd $n$ holds without exception proving that $\sigma(S_9) = 256$. We establish in addition that the Mathieu group $M_{12}$ has covering number 208, and improve the estimate for the Janko group $J_1$ given by P.E. Holmes.

References


Rank 3 permutation groups and partial linear spaces

David Raithel

The University of Western Australia

(Joint work with John Bamberg, Alice Devillers and Cheryl Praeger)

The studies of permutation groups and finite geometries have always been intricately linked – the strength of this link embodied with the classification of flag-transitive linear spaces back in 1990. This classification would not have been possible without the O’Nan-Scott Theorem, a characterisation theorem for finite primitive permutation groups.

Classification and characterisation theorems in permutation groups have allowed for deeper exploration and understanding of finite geometries. In this talk, I will discuss some of the classification and characterisation theorems of permutation groups, how they have contributed to the classifications of classes of finite geometries, current research being done in this area, and potential avenues of future research. Of particular focus will be partial linear spaces, and what rank 3 permutation groups have done and can do for them.

Decomposition algorithms in Clifford algebras

G. Stacey Staples

Southern Illinois University Edwardsville

(Joint work with David Wylie)

Beginning with a finite-dimensional vector space $V$ equipped with a nondegenerate quadratic form $Q$, we consider the decompositions of elements of the conformal orthogonal group $CO_Q(V)$, defined as the direct product of the orthogonal group $O_Q(V)$ with dilations. Utilizing the correspondence between conformal orthogonal group elements and “decomposable” elements of the associated Clifford algebra, $CL_Q(V)$, a decomposition algorithm is developed based on group actions in the conformal orthogonal group. Preliminary results on complexity reductions that can be realized passing from additive to multiplicative representations of invertible elements are also presented with examples. Algorithms are implemented in \textit{Mathematica} using the \texttt{CliffMath} package, which takes a combinatorial/set-theoretic approach to geometric computations.

Self-complementary strongly regular graphs revisited

Ferenc Szöllösi

Aalto University

(Joint work in progress with Patric Östergård)

We revisit the classification problem of self-complementary strongly regular graphs [1] via computer aided methods along the lines of Mathon [2]. Preliminary results regarding the existence of such graphs on fewer than 57 vertices will be presented. We speculate that the combination of these methods with sufficient computing power have the potential to settle the existence of conference graphs on 65 and/or 85 vertices.
References


Classifying KM-arcs in PG(2, q), q ≤ 32

Peter Vandendriessche
Ghent University (Belgium)

Definition: [3] A KM-arc is a set of $q + t$ points in PG(2, q) for which every line $\ell$ meets it in either 0, 2 or $t$ points.

We assume $1 < t < q$ to avoid triviality. Definition is a natural generalization of hyperovals: for $t = 2$, we obtain the hyperovals, and for $t > 2$, strong structural properties hold, which yield a very similar structure.

Theorem: [3] If KM-arcs with $1 < t < q$ exist, then $q = 2^h$ and $t = 2^r$.

Theorem: [1] Any KM$_{q,t}$-arc $S$ with $1 < t < q$ has $\frac{q}{t} + 1$ concurrent lines containing $t$ points of $S$, and all other lines contain 0 or 2 points of $S$.

The converse of Theorem is a long standing open problem. All progress so far suggests that the converse should hold, but no proof has yet been given.

Infinite families of examples have been given in [1, 3, 5], covering all cases with $q ≤ 16$. In [2, 4], further examples with $q = 32$ have been randomly constructed, extending the converse to $q ≤ 32$.

A natural question is whether or not we have found all examples. In an unpublished note, I provided a full classification of the KM-arcs for $q ≤ 32$.

\[
\begin{array}{c|cccccc}
q \setminus t & 2 & 4 & 8 & 16 & 32 \\
\hline
2 & 1 & - & - & - & - \\
4 & 1 & 1 & - & - & - \\
8 & 1 & 1 & 1 & - & - \\
16 & 2 & 3 & 1 & 1 & - \\
32 & 6 & 8 & 3 & 1 & 1 \\
\end{array}
\]

Table 1: Number of inequivalent KM-arcs for $q ≤ 32$

The orbit counts of the classification can be found in Table 1. In this talk, I will discuss the computational techniques I used, as well as the remaining computational challenges to handle the next case, $q = 64$.

References

[1] A. Gács and Zs. Weiner, On $(q + t, t)$-arcs of type $(0, 2, t)$, Des. Codes Cryptogr. 29 (2003), 131–139.


Location Maps
List of Participants

Aida Abiad, University of Tilburg, The Netherlands
Abdullah AlAzemi, Kuwait University, Kuwait
Allison Beemer, University of Nebraska - Lincoln
Anton Betten, Colorado State University
Anurag Bishnoi, Ghent University, Belgium
Saul Blanco, Indiana University
Jessalyn Bolkema, University of Nebraska - Lincoln
Cicero Carvalho, Universidade Federal de Uberlandia, Brasil
Niccolò Castronuovo, University of Ferrara, Italy
Ethan Coldren, Colorado State University
Stefaan De Winter, Michigan Technological University
Brian Diamond, Loveland, Colorado
Ronan Egan, National University of Ireland, Galway, Ireland
Alexander Gavrilyuk, Krasovsky Institute of Mathematics and Mechanics, Russian Federation
Gary Greaves, Tohoku University, Japan
Ghodratollah Aalipour Hafshejani, University of Colorado Denver
Daniel Horsley, Monash University, Australia
Sogol Jahanbekam, University of Colorado Denver
Andrew Kelley, Binghamton University
Christine Kelley, University of Nebraska - Lincoln
Jack Koolen, University of Science and Technology of China, China
Gabor Korhmaros, University of Basilicata, Italy
Brian Kronenthal, Kutztown University
Liz Lane-Harvard, University of Central Oklahoma
Brooke Logan, Rowan University
Tatsuya Maruta, Osaka Prefecture University, Japan
Gretchen Matthews, Clemson University
Carolyn Mayer, University of Nebraska - Lincoln
Curtis Nelson, University of Wyoming
Peter Paule, RISC – Johannes Kepler University, Linz, Austria
Stan Payne, University of Colorado Denver
Tim Penttila, Colorado State University
Daniela Popova, Florida Atlantic University
David Raithel, University of Western Australia, Australia
Frank Ruskey, University of Victoria, Canada
Katherine Sieviec, Colorado State University
Leonard Soicher, Queen Mary University of London, UK
Stacey Staples, Southern Illinois University Edwardsville
Ferenc Szöllösi, Aalto University, Finland
Peter Vandendriessche, Ghent University, Belgium