Finite Geometry Workshop

University of Szeged

A four-day workshop that brings together experts in the fields of finite geometry, Galois fields, cryptography, coding theory, and combinatorics.

OCTOBER 23 – OCTOBER 26, 2025

Claude Carlet
University of Paris,
University of Bergen

Vedran Krcadinac
University of Zagreb

Giuseppe Marino
Università di Napoli
Federico II

Štefko Miklavič
University of Primorska

Michel Lavrauw
University of Primorska

Irene Villa
University of Trento

Szeged, Hungary

DETAILS https://www.math.u-szeged.hu/~nagyg/GeoWS25/

Foreword

Since 2013, the Bolyai Institute of the University of Szeged has regularly organized an international conference titled "Finite Geometry Workshop" in the fields of finite geometry, algebraic curves over finite fields, coding theory, and algebraic graph theory. This series of conferences has been taking place in an increasingly large circle; 2025 will be the sixth time. The recent results of the actively researched topics will inspire the approx. 60 domestic and international scientists participated and strengthened research through international cooperation. The personal conversations and joint brainstorming will later yield fruitful collaborations among conference participants.

The conference offers young researchers and PhD students a valuable opportunity to develop professionally, build professional relationships, and learn how to present their results to the public in a 15-minute presentation. All 6 invited speakers are international-level researchers or young talent. We will invite one of them, who already has high-quality YouTube content, to deliver an open online lecture. The goal is to present an area of finite geometry in a comprehensible way.

The agenda for the workshop includes a range of topics:

- Finite Fields and Galois Geometries
- Algebraic Curves over Finite Fields and Post-Quantum Cryptography
- Boolean Functions and Symmetric Cryptography
- Algebraic Graph Theory
- Independent Sets in Hypergraphs
- Arcs and Caps from Cubic Curves and Their Applications in Coding Theory

Plenary speakers

- **Claude Carlet,** University of Paris 8 (France) and University of Bergen (Norway)
  Open Lecture: *A notion on S-boxes for a partial resistance to some integral attacks*
- **Vedran Krcadinac,** University of Zagreb (Croatia)
  Open Lecture: *On three-dimensional combinatorial designs*
- **Giuseppe Marino,** Università di Napoli Federico II (Italy)
  MRD codes, shortest minimal codes, and intersecting codes from scattered subspaces
- **Štefko Miklavič,** University of Primorska (Slovenia)
  Terwilliger algebra of a graph
- **Michel Lavrauw,** University of Primorska (Slovenia)
  Nets, webs and squabs of conics over finite fields
- **Irene Villa,** University of Trento (Italy)
  Construction and cryptanalysis of a multivariate CCZ scheme

Organisers

- **Gábor P. Nagy,** Bolyai Institute of the University of Szeged
- **Tamás Szőnyi,** Department of Computer Science, Eötvös Loránd University
- **György Kiss,** Department of Geometry, Eötvös Loránd University
- **Zoltán L. Blázsik,** Bolyai Institute of the University of Szeged

Sponsors

- Grant `MEC_SZ_149263` of the National Research, Development and Innovation Fund of Hungary
- Bolyai Institute of the University of Szeged (Hungary)

Group photo

Program

Thursday, October 23

14:00 – 15:50	**Registration**
15:50 – 16:00	**Opening**
16:00 – 17:00	**OPEN LECTURE** **Claude Carlet** (University of Paris 8 & University of Bergen) *A notion on S-boxes for a partial resistance to some integral attacks*
17:00 – 17:30	**Coffee break**
17:30 – 17:55	**Francesco Ghiandoni** (University of Perugia) *Hermitian codes for Secure and Private Information Retrieval*
17:55 – 18:20	**Gioia Schulte** (University of Salento & University of Basilicata) *Evaluation codes from linear systems of conics*
18:45 – 20:45	**Wine&Cheese reception in the Bolyai Institute**

Friday, October 24, morning session

08:30 – 09:00	**Registration**
09:00 – 10:00	**OPEN LECTURE** **Vedran Krčadinac** (University of Zagreb) *On three-dimensional combinatorial designs*
10:00 – 10:25	**Lucija Relić** (University of Zagreb, Faculty of Science) *Difference sets for higher-dimensional symmetric designs*
10:25 – 10:55	**Coffee break**
10:55 – 11:20	**Gábor Gévay** (University of Szeged) *The many faces of the Möbius–Kantor configuration*
11:20 – 11:45	**Tomaž Pisanski** (University of Primorska) *Polycirculant LCF codes for cubic graphs*
11:45 – 12:10	**György Kiss** (ELTE Budapest & University of Primorska) *Balanced biregular cages*

Friday, October 24, afternoon session

14:00 – 15:00	**PLENARY LECTURE** **Stefko Miklavic** (University of Primorska) *Terwilliger algebra of a graph*
15:00 – 15:25	**Nino Bašić** (University of Primorska & IMFM) *Nut graphs with a prescribed automorphism group*
15:25 – 15:50	**Giusy Monzillo** (University of Primorska) *On the (weakly) uniform structure of bipartite graphs which admit a dual adjacency matrix (candidate)*
15:50 – 16:20	**Coffee break**
16:20 – 16:45	**Safet Penjić** (University of Primorska) *On combinatorial structure of imprimitive graphs, part I*
16:45 – 17:10	**Luka Šinkovec** (University of Primorska) *On edge-transitive dihedrants*
17:10 – 17:35	**Ágnes Szalai** (University of Primorska) *Classifying vertex-transitive graphs of order a product of two distinct primes*
17:35 – 18:00	**Sanja Rukavina** (University of Rijeka) *On the construction of extremal Type II codes over* $\mathbb{Z}_{2^k}$

Saturday, October 25, morning session

09:00 – 10:00	**PLENARY LECTURE** **Michel Lavrauw** (University of Primorska) *Nets, webs and squabs of conics over finite fields*
10:00 – 10:25	**Martin Macaj** (Comenius University Bratislava) *How to decompose the affine plane into parabolas*
10:25 – 10:55	**Coffee break**
10:55 – 11:20	**Bence Csajbók** (Eötvös Loránd University, Budapest) *On the graph and the set of determined directions of functions over* GF(q)
11:20 – 11:45	**Dávid R Szabó** (Rényi Institute) *Blocking s-spaces by t-spaces in* $\mathbb{F}_q^n$
11:45 – 12:10	**Alessandro Giannoni** (University Federico II of Naples) *Connection between t-packings and QMDS codes*

Saturday, October 25, afternoon session

14:00 – 15:00	**PLENARY LECTURE** **Giuseppe Marino** (University of Naples Federico II) *MRD codes, shortest minimal codes, and intersecting codes from scattered subspaces*
15:00 – 15:25	**Giovanni Giuseppe Grimaldi** (University of Perugia) *Generalizing two families of scattered quadrinomials in* $\mathbb{F}_{q^{2t}}[X]$
15:25 – 15:55	**Coffee break**
15:55 – 16:20	**Giovanni Longobardi** (University of Naples Federico II) *A lower bound on the minimum weight of some geometric codes*
16:20 – 16:45	**Arianna Dionigi** (University of Florence) *Curves with a large automorphism group admitting a cyclic subgroup of index 2*
16:45 – 17:10	**Marco Timpanella** (University of Perugia) *On automorphism groups and p-rank of algebraic curves in positive characteristic*
18:30 – 19:15	**Guitar concert at the Fricsay Hall, Faculty of Arts**
19:15 – 22:30	**Conference dinner in the Mojo Club**

Sunday, October 26

09:00 – 10:00	**PLENARY LECTURE** **Irene Villa** (University of Trento) *Construction and cryptanalysis of a multivariate CCZ scheme*
10:00 – 10:25	**Bojan Bašić** (University of Novi Sad) *On finite florets in Hilbert's (geo-)garden*
10:25 – 10:55	**Coffee break**
10:55 – 11:20	**Fariha Iftikhar** (Budapest University of Technology and Economics) *The random generation of Latin rectangles based on the assignment problem*
11:20 – 11:45	**Valentino Smaldore** (Università degli Studi di Padova) *Strongly regular graphs with 2-transitive two-graphs*
11:45 – 12:10	**Gábor Nagy** (University of Szeged) *On linear codes with random multiplier vectors and the maximum trace dimension property*
12:10 – 12:20	**Closing**

Plenary lectures

A Notion on S-boxes for a Partial Resistance to Some Integral Attacks

Claude Carlet

University of Bergen (Norway)
University of Paris 8 (France)

A vectorial function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called *kth-order sum-free* [1] if, for every k-dimensional affine subspace A of $\mathbb{F}_2^n$ (or of $\mathbb{F}_{2^n}$), we have $\sum_{x\in A} F(x) \neq 0$. This notion generalizes that of almost perfect nonlinearity [5] (which corresponds to $k = 2$) and it has some relation with the resistance to integral attacks (in cryptanalysis) of those block ciphers using F as a substitution box (S-box), by preventing the propagation of the division property [6] of k-dimensional affine spaces. In this talk, we shall show that this notion, which is rarely satisfied by vectorial functions, can be weakened while retaining the property that the S-boxes do not propagate the division property of k-dimensional affine spaces. This will lead us to the property of *kth-order t-degree-sum-freedom*, whose strength decreases when t increases, and which coincides with kth-order sum-freedom when $t = 1$. The condition for kth-order t-degree-sum-freedom is that, for every k-dimensional affine space A, there exists a non-negative integer j of 2-weight (i.e. Hamming weight of the binary expansion) at most t such that $\sum_{x\in A}(F(x))^j \neq 0$. We shall show, for a general kth-order t-degree-sum-free function F, that t can always be taken smaller than or equal to $\min(k, m)$ under some reasonable condition on F, and that it is larger than or equal to $\frac{k}{\deg(F)}$, where $\deg(F)$ is the algebraic degree of F (i.e. the degree of its multivariate representation over $\mathbb{F}_2$ called algebraic normal form). We shall also show two other lower bounds: one, that is often tighter, by means of the algebraic degree of the compositional inverse of F when F is a permutation, and another (valid for every vectorial function) by means of the algebraic degree of the indicator of the graph $\{(x, F(x))\ ;\ x \in \mathbb{F}_2^n\}$ of the function. We shall study power functions $F(x) = x^d$; $x \in \mathbb{F}_{2^n}$, for which we shall prove upper bounds. We shall study in particular the multiplicative inverse function (used as an S-box in the AES), for which we shall characterize the kth-order t-degree-sum-freedom by the coefficients of the subspace polynomials of k-dimensional vector subspaces (deducing the exact value of t when k divides n) and we shall extend to kth-order t-degree-sum-freedom the result that it is kth-order sum-free if and only if it is $(n - k)$th-order sum-free.

References

[1] C. Carlet. Two generalizations of almost perfect nonlinearity. To appear in the *Journal of Cryptology* 38(2) (Topical Collection on Advances in Boolean Functions with Applications in Cryptography). Available at Cryptology ePrint Archive 2024/841.

[2] C. Carlet. On the vector subspaces of $\mathbb{F}_{2^n}$ over which the multiplicative inverse function sums to zero. Special issue in memory of Kai-Uwe Schmidt of *Designs, Codes and Cryptography* 93, no. 4, pp. 1237–1254, 2025. Available at Cryptology ePrint Archive 2024/1007.

[3] C. Carlet and X.-D. Hou. More on the sum-freedom of the multiplicative inverse function. Preprint, 2024.

[4] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, North Holland, 1977.

[5] K. Nyberg. Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT 1993, Lecture Notes in Computer Science* 765, pp. 55–64, 1994.

[6] Y. Todo. Structural evaluation by generalized integral property. *Proceedings of EUROCRYPT 2015, Lecture Notes in Computer Science* 9056, pp. 287–314, 2015.

Nets, Webs and Squabs of Conics over Finite Fields

Michel Lavrauw

University of Primorska (Slovenia)

The classification of "inequivalent" objects satisfying a given set of axioms, typically up to a "natural" action of some group on the set of such objects, has long fascinated mathematicians. Throughout history such problems have led to elegant results, sometimes requiring centuries to resolve.

In combinatorics these questions lie at the heart of enumeration problems. In finite geometry they appear in the study of ovals, hyperovals, unitals, arcs, ovoids, etc.; topics that have intrigued researchers for more than half a century, with origins in Dickson's work in the early 1900s. Beniamino Segre's seminal contributions and Jacques Tits' profound structural insights into incidence geometries provided a unifying framework that continues to shape the field today.

Besides incidence geometries, algebraic varieties over finite fields, such as algebraic curves, quadrics, cubic surfaces, and Veronese varieties, play a central role in understanding and classifying geometric objects, with important applications in coding theory and cryptography.

Some of these classification problems can be rephrased in terms of multilinear algebra, where tensors capture the essence of geometric configurations and equivalence is governed by group actions. This viewpoint sheds new light on classical problems and leads to surprising connections between geometry, algebra, and combinatorics.

In this talk, I will focus on recent advances on challenges involving nets, webs, and squabs of conics, based on joint work with John Sheekey, Tomasz Popiel, and Nour Alnajjarine.

MRD Codes, Shortest Minimal Codes, and Intersecting Codes from Scattered Subspaces

Giuseppe Marino

University of Naples Federico II (Italy)

Let $\Lambda = \mathrm{PG}(V, \mathbb{F}_{q^n}) = \mathrm{PG}(r-1, q^n)$, where V is a vector space of dimension r over $\mathbb{F}_{q^n}$, and let L be a subset of points of Λ. The set L is called an $\mathbb{F}_q$-*linear* set of rank k if it is defined by the nonzero vectors of an $\mathbb{F}_q$-subspace U of V of dimension k. Such a linear set is said to be *scattered* (and U is called $\mathbb{F}_q$-*scattered subspace*) if it has maximum possible size, namely $q^{k-1} + q^{k-2} + \cdots + q + 1$. Scattered subspaces are of central interest in Galois Geometry due to their strong connections with rank-metric codes.

In this talk, I will present recent constructions of scattered subspaces that give rise to new families of maximum rank distance (MRD) codes [2] and to shortest minimal rank-metric codes [3]. Furthermore, taking inspiration from intersecting codes in the Hamming metric, I will introduce the notion of rank-metric intersecting codes [1]. These are codes in which any two nonzero codewords have nontrivially intersecting supports. We will explore their structure from both geometric and coding-theoretic viewpoints, establishing connections with MRD codes, minimal codes, and 2-spannable q-systems. Structural properties, parameter bounds, and explicit constructions will also be discussed. The talk will conclude with a selection of open problems and directions for future research.

References

[1] D. Bartoli, M. Borello, G. Marino and M. Scotti: Linear rank-metric intersecting codes, arXiv:2507.00569.

[2] D. Bartoli, G. Marino and A. Neri: New MRD codes from linear cutting blocking sets, *Annali di Matematica Pura ed Applicata* **202** (2023), 115–142.

[3] S. Lia, G. Longobardi, G. Marino and R. Trombetti: Short rank-metric codes and scattered subspaces, *SIAM Journal on Discrete Mathematics*, **38(4)** (2024), 2578–2598.

Terwilliger Algebra of a Graph

Štefko Miklavič

University of Primorska (Slovenia)

In algebraic combinatorics, the following situation occurs often. Let Γ be a combinatorial object and let H be a certain algebraic object, associated with Γ. In this case, one of the main motivations in our research is the following question: what could we say about the combinatorial properties of Γ, if we know that H has certain algebraic properties? And vice-versa: what could we say about the algebraic properties of H, if we know that Γ has certain combinatorial properties?

Perhaps the most well-known example of this interplay between combinatorics and algebra is obtained if H is the automorphism group of a graph Γ. In this case there are many relations between combinatorial properties of Γ and algebraic properties of H. For example, if H acts transitively on the set of vertices of Γ, then Γ is regular (in a sense that every vertex of Γ has the same number of neighbours). If we further know that the stabilizer H_x of a vertex x has exactly three orbits, then Γ is strongly regular. There are other examples of this interplay available in the literature.

In this talk the algebraic object, associated with Γ, will not be its automorphism group, but rather a certain matrix algebra, called a *Terwilliger algebra of a graph* Γ. The main motivation, however, remains the same: what could we say about the combinatorial properties of Γ, if we know that its Terwilliger algebra has certain algebraic properties? And vice-versa: what could we say about the algebraic properties of the Terwilliger algebra of Γ, if we know that Γ has certain combinatorial properties?

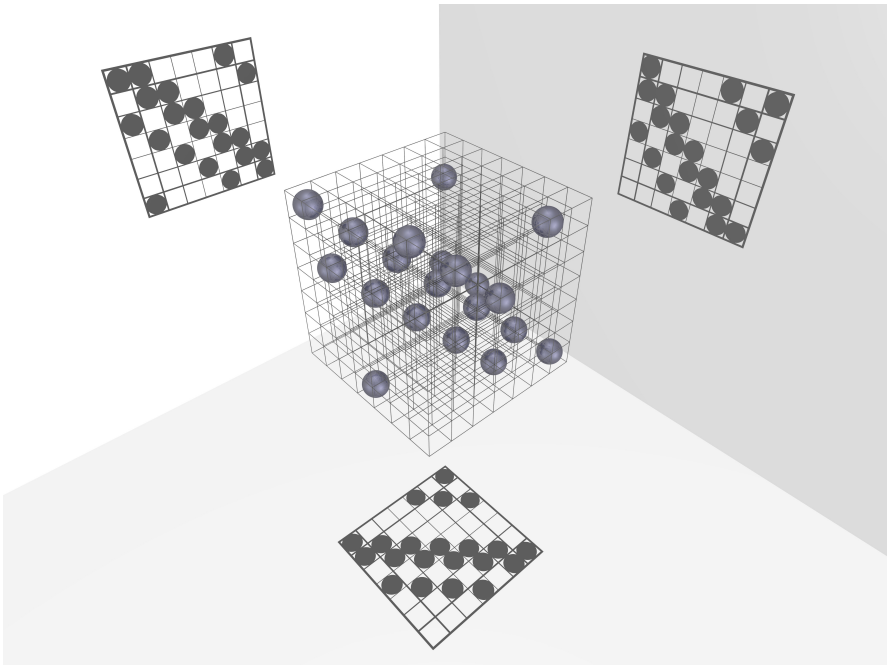
On Three-dimensional combinatorial designs

Vedran Krčadinac

University of Zagreb (Croatia)

Many classes of combinatorial designs can be defined as matrices over a finite set of elements that satisfy certain balance conditions. For example, symmetric block designs with parameters (v, k, λ) are $v \times v$ matrices over $\{0, 1\}$ with row and column sums equal to k, and pairwise scalar products equal to λ. These definitions are extended to higher-dimensional arrays of elements by imposing conditions on its subarrays or by applying other types of constraints.

Recently, there have been a number of works about higher-dimensional Hadamard matrices [1, 3] and symmetric block designs [2, 4, 5]. In this talk, I will give a brief historical overview and survey recent results. I will focus on the three-dimensional case and show pictures rendered using ray tracing software [6].



References

[1] A. Bahmanian, S. Suda, *Hadamard hypercubes*, preprint (2025).

[2] V. Krčadinac, M. O. Pavčević, *On higher-dimensional symmetric designs*, to appear in Exp. Math. (2025).

[3] V. Krčadinac, M. O. Pavčević, K. Tabak, *Three-dimensional Hadamard matrices of Paley type*, Finite Fields Appl. **92** (2023), 102306.

[4] V. Krčadinac, M. O. Pavčević, K. Tabak, *Cubes of symmetric designs*, Ars Math. Contemp. **25** (2025), no. 1, Paper No. 10, 16 pp.

[5] V. Krčadinac, L. Relić, *Projection cubes of symmetric designs*, to appear in Math. Comput. Sci. (2025).

[6] Persistence of Vision Raytracer, Version 3.7, 2013. Persistence of Vision Pty. Ltd., Williamstown, Victoria, Australia. `http://www.povray.org/`

Construction and Cryptanalysis of a Multivariate CCZ Scheme

Irene Villa

University of Trento (Italy)

Multivariate cryptography is one of the main candidates for post-quantum cryptography. Consider a finite field $\mathbb{F}_q$, and two positive integers n and m; traditional multivariate schemes are typically constructed by applying two secret affine invertible transformations S, T (of $\mathbb{F}_q^m$ and $\mathbb{F}_q^n$ respectively) to a set of m secret multivariate polynomials $\mathcal{F}$ (in n variables, defined over $\mathbb{F}_q$), often quadratic. These secret polynomials $\mathcal{F}$ contain a trapdoor that enables the legitimate user to solve the corresponding system efficiently, while the public polynomials $\mathcal{G} = S \circ \mathcal{F} \circ T$ appear indistinguishable from random ones. In this context, the secret and public key polynomials ($\mathcal{F}$ and $\mathcal{G}$) are said to be *affine equivalent*.

In an effort to generalize this construction, we propose a new approach to construct a multivariate scheme by considering *CCZ equivalence*, a concept introduced and studied in the theory of vectorial Boolean functions. Given two functions $F, G : \mathbb{F}_q^n \to \mathbb{F}_q^m$, we say that they are *CCZ equivalent* if there exists an affine invertible transformation $\mathcal{A}$ of $\mathbb{F}_q^{n+m}$ such that $\mathcal{A}(\Gamma_F) = \Gamma_G$, where $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_q^n\}$ is the graph of F. We explore the potential advantages and disadvantages of this construction. In particular, we present a cryptanalysis attempt aimed at assessing whether this approach indeed provides stronger or more general security guarantees compared to affine equivalence. The talk is based on joint works with Marco Calderini, Alessio Caminata, Elisa Gorla, Madison Mabe, and Martina Vigorito.

References

[1] Marco Calderini, Alessio Caminata, and Irene Villa. A new multivariate primitive from CCZ equivalence. *Journal of Cryptology*, 38, 2025.

[2] Alessio Caminata, Elisa Gorla, Madison Mabe, Martina Vigorito, and Irene Villa. Cryptanalysis of a multivariate CCZ scheme. *Cryptology ePrint Archive*, Paper 2025/1329, 2025.

Contributed talks

On finite florets in Hilbert's (geo-)garden

Bojan Bašić

University of Novi Sad (Serbia)

(Joint work with K. Ago and N. Miholjčić)

Finite projective geometries constitute a well-established research topic, with applications in many different areas. However, it could be said that (arguably) the most "basic" geometry is Euclidean geometry. It is founded upon the axiom set established by David Hilbert at the end of the 19$^{\text{th}}$ century, consisting of five groups of axioms, the first of which (named "incidence axioms") introduces the primitive notions: points, lines and planes, and the primitive relation called incidence (hence the naming). Incidence axioms allow some finite models, but in stark contrast to projective geometries, in the literature there are practically no results on such models (more or less the only thing that is mentioned here and there is that the minimum number of points needed to model these axioms is 4); a very recent exception is an article [1] from 2024, where the complete catalog of such finite models with up to 12 points was exhibited. In that article, a connection between such finite models and projective planes and spaces, combinatorial designs, as well as matroid theory, has been brought to light.

How can we push the present frontier of this enumeration further? Unfortunately, 12 points is indeed an unbreakable limit for the approach employed in [1]. To overcome this barrier, we discuss the creation of a new axiom system—which is supposed to be equivalent to Hilbert's incidence axioms, but crafted in such a way as to make it amenable to attack by specialized solvers for Boolean satisfiability problems (SAT in short). Because, although the SAT problem is hard in *theory* (which means that a polynomial algorithm does not exist, unless P = NP), in *practice* the situation is not so dire. Namely, various heuristic SAT algorithms exist that perform quite well in problems that arise from practice (either from real-world or from research in other areas), even if they involve thousands or more of variables and/or logical constraints. The idea is to use such state-of-the-art algorithms on our newly constructed axiomatic system, and thereby solve our enumeration problem for larger models.

Along the way, we aim to construct several new families of finite models—which gives a lower bound for the number of models with n points (without any caps on n), but not less importantly, also showcases just how varied these "mini-Euclidean worlds" can be. In doing so, we hope to place finite incidence geometries more firmly on the research map—a century and a quarter after Hilbert first laid down the rules of the game.

References

[1] K. Ago, B. Bašić, M. Maksimović, M. Šobot, On finite models of Hilbert's incidence geometry, *Discrete Math.* **347** (2024), Article No. 114159, 15 pp.

Nut graphs with a prescribed automorphism group

Nino Bašić

University of Primorska (Slovenia) and IMFM (Slovenia)

A core graph is a simple graph whose adjacency matrix has a kernel eigenvector with no zero entries (i.e. a full eigenvector). A *nut graph* is a core graph of order at least 2 whose nullity is 1. We show that every finite group can be represented as the automorphism group of infinitely many nut graphs. Moreover, we show that such nut graphs exist even within the class of regular graphs.

This is joint work with Patrick W. Fowler (University of Sheffield, UK).

References

[1] N. Bašić, P. W. Fowler, Nut graphs with a given automorphism group, *J. Algebr. Comb.* **61** (2025) Art. no. 17, doi:10.1007/s10801-025-01389-4.

On the graph and the set of determined directions of functions over GF(q)

Bence Csajbók

ELTE Eötvös Loránt University (Hungary)

Let q be a power of a prime p, and let f be a function from GF(q) to GF(q). The graph of f is the set of points in the affine plane AG$(2,q)$ of the form $(x, f(x))$, where x ranges over GF(q). We will denote this point set by U_f. The directions determined by the graph of f are the points at infinity corresponding to the slopes of lines connecting pairs of points of the graph. We will denote this point set by D_f.

In this talk, we will show how properties of D_f yield information about f. To be more precise, we will use some new ideas and some old results (due to Carlitz, McConnel; Ball, Blokhuis, Brouwer, Storme, Szőnyi) to prove the following conjecture of Sziklai (which extends a result of McGuire and Göloğlu):

Theorem 1. *Let M denote a multiplicative subgroup of* GF(q) *and let f denote a function from* GF(q) *to* GF(q). *If $f(0) = 0$, $f(1) = 1$ and $D_f \subseteq M \cup \{0\}$, then f is an automorphism of* GF(q).

Then we will explain how U_f and D_f can be used to construct the smallest (known) t-fold blocking sets ($t = 1, 2, 3$) of PG$(2,q)$, that is, point sets meeting every line in at least t points. During the 2025 Budapest Research Experience for Undergraduates (REU) Math Program, together with M.R. Kepes, E. Robin, B. Sógor, S. Wang, E. Williams, we proved the following:

Theorem 2. *In* PG$(2,q^h)$, *$h > 1$, there exist t-fold blocking sets of size $t(q^h + q^{h-1} + 1)$ for $t = 2, 3$.*

References

[1] B. Csajbók: Extending a result of Carlitz and McConnel to polynomials which are not permutations, Finite Fields Appl. 108 (2025) 102683.

Curves with a large automorphism group admitting a cyclic subgroup of index 2

Arianna Dionigi

University of Florence (Italy)

(Joint work with Massimo Giulietti and Marco Timpanella)

The Hurwitz bound on the order of the $\mathbb{K}$-automorphism group $\mathrm{Aut}(\mathcal{X})$ of an algebraic curve $\mathcal{X}$ of genus $g(\mathcal{X}) \geqslant 2$ defined over a field $\mathbb{K}$ of zero characteristic states that $|\mathrm{Aut}(\mathcal{X})| \leqslant 84(g(\mathcal{X}) - 1)$. Improved bounds are available for the order of certain types of subgroups within automorphism groups. For instance, if a subgroup G of $\mathrm{Aut}(\mathcal{X})$ is dihedral, then in the complex case, $|G| \leqslant 4g(\mathcal{X}) + 4$. More recently it has been shown that a tighter bound holds for G a generalized quasi-dihedral group. In this paper we explore the more general setting of a curve defined of field of any characteristic, and G a group admitting a cyclic subgroup of index two and order coprime to the characteristic of the ground field. We first prove that many classical results about dihedral groups extend from the complex case to the case of any characteristic p. Then we provide some new results about non-dihedral groups admitting a cyclic subgroup of index 2.

References

[1] A. Dionigi, M. Giulietti and M. Timpanella *Algebraic curves with a large cyclic automorphism group*, submitted, arXiv:2410.13590.

The many faces of the Möbius–Kantor configuration

Gábor Gévay

University of Szeged (Hungary)

(Joint work with Tomaž Pisanski)

The Möbius–Kantor configuration is a unique (8_3) combinatorial configuration that was described by Möbius in 1828; he proved that it cannot be realized geometrically with points and lines in the real Euclidean plane; Kantor described it in 1881 as a geometric point-line configuration in the complex plane [4].

Based on a simple elementary geometry theorem, we have proven that it has a geometric realization in the real Euclidean plane such that its blocks are equilateral triangles. Moreover, the realization with triangles expresses a configuration theorem which states that if any seven triangles are equilateral, then the last, eighth triangle is also equilateral; thus, this theorem follows the logical pattern of the classical configuration theorems (like e.g. the Pappus or Desargues thereom).

We found that several consequences make this realization particularly interesting. To mention some of them, it can be lifted to the real Euclidean 3-space, which leads to a novel, highly self-intersecting polyhedron which is topologically equivalent to the double torus. Moreover, this polyhedron is homeomorphic to a semiregular map which can be obtained by a specific truncation from the dual of the regular map R2.1 (using Conder's notation [1]). This is consistent with the fact that the Möbius–Kantor graph (the incidence graph of the configuration) can be embedded in the double torus [2, 3].

Our new realization of the configuration $\mathrm{MK}(8_3)$ also leads to an interesting geometric representation of the Möbius–Kantor graph. This representation may serve as a starting example for defining a novel family of geometric graphs.

References

[1] M. D. E. Conder, All regular orientable maps on surfaces of genus 2 to 101, `http://www.math.auckland.ac.nz/~conder`

[2] H. S. M. Coxeter and W. O. J. Moser, Generators and Relations for Discrete Groups, Springer-Verlag, Berlin - Heidelberg, 1980.

[3] D. Marušič and T. Pisanski, The remarkable generalized Petersen graph, *Math. Slovaca*, **50** (2000), 117–121.

[4] T. Pisanski and B. Servatius, *Configurations from a Graphical Viewpoint*, Birkhäuser Advanced Texts, Birkhäuser, New York, 2013.

Hermitian codes for Secure and Private Information Retrieval

Francesco Ghiandoni

University of Perugia (Italy)

(Joint work with M. Giulietti, E. Mezzano, M. Timpanella)

Private information retrieval (PIR) addresses the question of how to retrieve data items from a database without disclosing information about the identity of the data items retrieved. The rate of a PIR scheme is measured as the ratio of the gained information over the downloaded information. Secure PIR complements this problem by further requiring the contents of the data to be kept secure. In particular, X-secure and T-private information retrieval (XST-PIR) is a form of PIR where data security is guaranteed against collusion among up to X servers and the user's privacy is ensured against collusion among up to T servers. Cross-subspace alignment (CSA) Reed-Solomon codes have been recently proposed by Jia et al. [1] as a means to construct XST-PIR schemes. In [2] and [3] Makkonen et al. reinterpret and generalize such CSA codes as algebraic geometric (AG) codes from curves of genus $0, 1$, respectively, and from higher-genus hyperelliptic curves.
In this talk we show a XST-PIR scheme coming from hermitian codes, i.e., AG codes over the Hermitian curve. Such scheme offers interesting tradeoffs between the field size, file size, number of colluding servers, and the total number of servers. When the field size is fixed, this translates in some cases to higher retrieval rates than those of [2, 3]. In addition, the new scheme exists also for some parameters where the original ones do not.

References

[1] Z. Jia, H. Sun, and S. A. Jafar. Cross subspace alignment and the asymptotic capacity of X-secure T-private information retrieval, *IEEE Transactions on Information Theory*, vol. 65, no. 9, pp. 5783–5798, 2019.

[2] O. Makkonen, D. A. Karpuk, and C. Hollanti. Algebraic geometry codes for cross-subspace alignment in private information retrieval. *2024 IEEE International Symposium on Information Theory*, pp. 2874-2879, 2024.

[3] O. Makkonen, D. A. Karpuk, and C. Hollanti. Secret Sharing for Secure and Private Information Retrieval: A Construction Using Algebraic Geometry Codes. arXiv preprint arXiv:2408.00542, 2024.

Connection between t-packings and QMDS codes

Alessandro Giannoni

University Federico II of Naples

(D. Bartoli, G. Marino, Y. Zhou)

We studied additive codes, defined as $\mathbb{F}_q$-linear subspaces $C \subseteq \mathbb{F}_{q^h}^n$ of length n and dimension r over $\mathbb{F}_q$. Such a code is said to be of type $[n, r/h, d]_q^h$, where d denotes the minimum Hamming distance and the normalized dimension r/h may be fractional. A central object of interest is the class of quasi-MDS (QMDS) codes, those additive codes achieving the generalized Singleton bound:

$$d = n - \left\lceil \frac{r}{h} \right\rceil + 1.$$

In this work, we construct explicit families of additive QMDS codes whose lengths exceed those of the best-known $\mathbb{F}_{q^h}$-linear MDS codes, such as Reed–Solomon codes. By leveraging $\mathbb{F}_q$-linearity and geometric tools like partial spreads and dimensional dual arcs, we show that additive structures allow longer codes without sacrificing optimality in distance. We also examine dual codes and give conditions under which the QMDS property is preserved under duality.

Generalizing two families of scattered quadrinomials in $\mathbb{F}_{q^{2t}}[X]$

Giovanni Giuseppe Grimaldi

University of Perugia (Italy)

The $\mathbb{F}_{q^{2t}}$-linearized quadrinomial

$$\psi_{m,h,s} = m(x^{q^s} - h^{1-q^{s(t+1)}}x^{q^{s(t+1)}}) + x^{q^{s(t-1)}} + h^{1-q^{s(2t-1)}}x^{q^{s(2t-1)}} \tag{1}$$

has been the subject of intense study and has been generalized through several stages. This is shown to be scattered under the following hypotheses:

- (a) for $m = 1$ and $h \in \mathbb{F}_{q^{2t}}$ with $\mathrm{N}_{q^{2t}/q^t}(h) = -1$, see [1, 2, 3, 4, 6].
- (c) for $h \in \mathbb{F}_q$ and $m \in \mathbb{F}_{q^t}$ such that it is neither a $(q+1)$-th nor $(q-1)$-th power of an element beloging to $\ker \mathrm{Tr}_{q^{2t}/q^t}$, see [5].

In this talk, we will provide some sufficient conditions for the polynomial in (1) to be scattered. These will include and generalize those above obtained in previous works. Moreover, we highlight the relation with linear sets of the projective line and rank distance codes.

References

[1] D. Bartoli, C. Zanella, F. Zullo, *A new family of maximum scattered linear sets in* $\mathrm{PG}(1, q^6)$, Ars Mathematica Contemporanea **19**, 125–145 (2020).

[2] G. Longobardi, G. Marino, R. Trombetti, Y. Zhou, *A large family of maximum scattered linear sets of* $\mathrm{PG}(1, q^n)$ *and their associated MRD codes*, Combinatorica **43**, 681–716 (2023).

[3] G. Longobardi, C. Zanella, *Linear sets and MRD-codes arising from a class of scattered linearized polynomials*, J. Algebraic Combin. **53**, 639–661 (2021).

[4] A. Neri, P. Santonastaso, F. Zullo, *Extending two families of maximum rank distance codes*, Finite Fields Appl. **81** (2022).

[5] V. Smaldore, C. Zanella, F. Zullo, *New scattered quadrinomials*, Linear Algebra and its Applications **702**, 143–160 (2024).

[6] C. Zanella, F. Zullo, *Vertex properties of maximum scattered linear sets of* $\mathrm{PG}(1, q^n)$, Discrete Math. **343**(5) (2020).

The random generation of Latin rectangles based on the assignment problem

Fariha Iftikhar

Budapest University of Technology and Economics (Hungary)

(Joint work with G.P. Nagy)

Let A be a $k \times n$ Latin rectangle, viewed as an ordered tuple of pairwise orthogonal permutations. We study a randomized construction of such rectangles based on the classical assignment problem. Given a random cost matrix $w \in [0,1]^{n \times n}$, the Hungarian algorithm produces successive minimum-cost permutations $\alpha_1, \ldots, \alpha_k$, which form the rows of A. Each rectangle A thus corresponds to a convex polytope $P_\Gamma(A)$ in the cost space, and the probability of generating A equals $\mathrm{Vol}(P_\Gamma(A))$.

We establish structural properties of these polytopes. In particular, their volume is invariant under simultaneous column and symbol permutations (CS-equivalence), and we show that disjoint unions of bipartite graphs correspond to prism products of polytopes, implying multiplicativity of volumes. Exact volume computations for small parameters $(k,n) \in \{(4,4),(3,5),(3,6)\}$ confirm that the process is efficient but non-uniform, giving a negative answer to a problem posed in 2009 and listed in the online compilation of open problems in loop theory and quasigroup theory [2]. For instance, among the CS-classes of Latin squares of order four, the probabilities differ by a factor of more than three.

References

[1] F. Iftikhar, G. P. Nagy, *The random generation of Latin rectangles based on the assignment problem*, Discrete Appl. Math. 378 (2026), 329–336.

[2] Wikipedia contributors, *List of problems in loop theory and quasigroup theory — Wikipedia, The Free Encyclopedia*, `https://en.wikipedia.org/w/index.php?title=List_of_problems_in_loop_theory_and_quasigroup_theory&oldid=1277495759`, [Online; accessed 6-May-2025].

Balanced biregular cages

György Kiss

ELTE, Budapest (Hungary) & University of Primorska, Koper (Slovenia)

(Joint work with Gabriela Araujo-Pardo and Tamás Szőnyi)

The cage problem is a classical problem in extremal graph theory. A (k, g)-graph is a k-regular graph with girth g. A (k, g)-*cage* is a (k, g)-graph of minimum order.

In this talk we consider some generalizations of the cage problem. Instead of regular graphs, we consider biregular graphs of given girth.

An $(m, n; g)$-*bipartite biregular graph* is a bipartite graph of even girth g having degree set equal to $\{m, n\}$ and satisfying the additional property that the vertices in the same bipartition set have the same degree. We prove new lower and upper bounds for the problem of bipartite biregular cages. For girth 6, we give the exact parameters of the $(m, n; 6)$-bipartite biregular cages when $n \equiv -1 \pmod{m}$ using the existence of a Steiner system $S(2, k = m, v = 1 + n(m-1) + m)$. For girth $g = 2r$ and $r = \{4, 6, 8\}$, we use results on t-good structures given by ovoids, spreads, and sub-polygons in generalized polygons to obtain $(m, n; 2r)$-bipartite biregular graphs, some of them are $(m, n; 2r)$-bipartite biregular cages.

Another possible generalization is the following. An $(r, s; g)$-*balanced biregular graph* is a graph of girth g having degree set equal to $\{r, s\}$ and satisfying the additional property that the number of vertices of degree r equals to the number of vertices of degree s. We construct relatively small balanced biregular graphs from incidence graphs of finite projective , affine and biaffine planes. We also show that some of the obtained graphs are balanced biregular cages.

References

[1] G. Araujo-Pardo, Gy. Kiss, T. Szőnyi, *A little more about bipartite biregular cages, block designs and generalized polygons*, Bol. Soc. Mat. Mex. 31 (2025), Paper 20.

[2] G. Araujo-Pardo, Gy. Kiss, *On balanced biregular cages*, manuscript.

A lower bound on the minimum weight of some geometric codes

Giovanni Longobardi

University of Naples Federico II

(joint work with B. Csajbók, G. Marino, R. Trombetti)

Let $\mathcal{D}(m,q)$ be the $2-(v,q+1,1)$ design of points and lines of the m-dimensional finite projective space $\mathrm{PG}(m,q)$, where $q=p^h$ and $v=\frac{q^{m+1}-1}{q-1}$. The p-ary code $\mathcal{C}=\mathcal{C}(m,q)$ associated with this design is the $\mathbb{F}_p$-subspace generated by the incidence vectors of the lines. The dual code $\mathcal{C}^\perp(m,q)$ is the $\mathbb{F}_p$-subspace of vectors in $\mathbb{F}_q^v$ that are orthogonal to all vectors of $\mathcal{C}(m,q)$ with respect to the standard inner product. These are particular examples of so-called *geometric codes*.

Determining the minimum weight of $\mathcal{C}^\perp(m,q)$ is a difficult and challenging problem. In [1], Bagchi and Inamdar proved that the minimum weight of $\mathcal{C}^\perp(m,q)$ is bounded from below by

$$2\left(\frac{q^m-1}{q-1}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right).$$

Such problems in coding theory can be naturally translated into questions concerning the size of sets or multi-sets of points in projective or affine spaces, with special intersection properties with respect to the lines of $\mathrm{PG}(m,q)$, as shown for instance in [2].

In this talk, using this geometric approach and exploiting properties of certain kinds of polynomials, we will present a significant improvement of the bound given in 2002 by Bagchi and Inamdar, in the case $h>1$ and $m,p>2$.

References

[1] B. Bagchi, S. P. Inamdar. Projective geometric codes. *J. Combin. Theory Ser. A*, **99**(1) (2002), 128–142.

[2] S. Ball, A. Blokhuis, A. Gács, P. Sziklai, Zs. Weiner. On linear codes whose weights and length have a common divisor. *Adv. Math.*, **211** (2007), 94–104.

How to decompose the affine plane into parabolas

Martin Mačaj

Comenius University, Bratislava (Slovakia)

(Joint work with David Wilsch)

In 2003, J. Šiagiová and M. Meszka found a packing of 5 copies of the Hoffman-Singleton graph into K_{50} in which all the graphs shared a group of automorphisms of order 25 acting semiregularly on vertices.

We show that there are exactly 16 such packings and that they all stem from unique system of 5 mutually disjoint ovals in the projective plane of order 5 with a common tangent.

We will also discuss the existence of q mutually disjoint ovals with a common tangent in the projective plane of order q for other orders.

References

[1] A. J. Hoffman and R. R. Singleton, *On Moore Graphs with Diameters 2 and 3*, IBM Journal of Research and Development, vol. 4, no. 5, 497-504, Nov. 1960, https://doi.org/10.1147/rd.45.0497

[2] J. Šiagiová and M. Meszka, *A covering construction for packing disjoint copies of the Hoffman-Singleton graph into* K_{50}, J. Combin. Designs, 11 (2003), 408-412. https://doi.org/10.1002/jcd.10049

On the (weakly) uniform structure of bipartite graphs which admit a dual adjacency matrix (candidate)

Giusy Monzillo

University of Primorska (Slovenia)

The Q-polynomial property of distance-regular graphs was introduced by Delsarte in his doctoral thesis, and it has been extensively studied since then. It is known that if a distance-regular graph is Q-polynomial, then for each vertex x there exists a so-called *dual adjacency matrix with respect to* x, say $A^* = A^*(x)$. Furthermore, in such a case, the adjacency matrix A of the graph and A^* satisfy

$$A^3A^* - A^*A^3 + (\beta+1)(AA^*A^2 - A^2A^*A) = \gamma(A^2A^* - A^*A^2) + \rho(AA^* - A^*A) \qquad (1)$$

for some scalars β, γ, ρ.

In [2], Terwilliger introduced a generalization of the Q-polynomial property: a graph is said to be *Q-polynomial with respect to a vertex x* if it has a *dual adjacency matrix with respect to x*.

The aim of finding examples of graphs with the above *new* property justifies our following definition. Let Γ denote a finite, simple, connected graph with vertex set X. Fix $x \in X$ and let $\varepsilon \geqslant 3$ be the eccentricity of x. For mutually distinct scalars $\{\theta_i^*\}_{i=0}^{\varepsilon}$, define a diagonal matrix $A^* = A^*(\theta_0^*, \theta_1^*, \ldots, \theta_\varepsilon^*) \in \mathrm{Mat}_X(\mathbb{R})$ as follows:

$$(A^*)_{yy} = \theta^*_{\partial(x,y)},$$

where $y \in X$ and ∂ is the shortest path-length distance function of Γ. We say that A^* is a *dual adjacency matrix candidate of Γ with respect to x* if the adjacency matrix $A \in \mathrm{Mat}_X(\mathbb{R})$ of Γ and A^* satisfy (1) for some scalars $\beta, \gamma, \rho \in \mathbb{R}$.

In this talk, we investigate the relation between two *objects* that a bipartite graph can possess: a dual adjacency matrix candidate and a uniform structure (in the sense of Terwilliger [1]). To do that, we first define a *weakly uniform structure* by slightly relaxing the conditions of a uniform structure. The main result is the following:

Theorem ([3])**.** *A bipartite graph Γ admits a dual adjacency matrix candidate with respect to x if and only if Γ admits a weakly uniform structure with respect to x; in particular, for $\beta = 2$, the latter weakly uniform structure is an actual uniform structure.*

References

[1] P. Terwilliger. The incidence algebra of a uniform poset. *Coding theory and design theory*, Part I, IMA Vol. Math. Appl., **20**, 193-212 (1990).

[2] P. Terwilliger. A Q-Polynomial Structure Associated with the Projective Geometry $L_N(q)$. *Graphs and Combinatorics*, **39**(4): 63, (2023).

[3] B. Fernández, R. Maleki, Š. Miklavič, and G. Monzillo. *On the uniform structure of bipartite graphs admitting a dual adjacency matrix candidate*, preprint.

On linear codes with random multiplier vectors and the maximum trace dimension property

Gábor Péter Nagy

University of Szeged (Hungary)

(Joint work with M. Erdélyi, P. Hegedüs és S.Z. Kiss)

Let C be an $[n,k,d]_{q^m}$ linear code and let $h = n+1-k-d$ denote its Singleton defect. The trace code $\mathrm{Tr}(C)$ is a linear code of the same length n over the subfield $\mathbb{F}_q$, namely, the image of the componentwise trace map $\mathbb{F}_{q^m} \to \mathbb{F}_q$. It is clear that the dimension of the trace code over $\mathbb{F}_q$ is at most mk. If equality holds, then we say that C has maximum trace dimension. Computing the exact dimension of trace codes and their duals plays an important role in some code-based public key cryptographic schemes.

We give a lower bound for the probability of maximum trace dimension in the probability model of random multipliers in terms of the Singleton defect. Namely, we prove that

$$P_C \geqslant 1 - \frac{1-q^{-m(h+k)}}{(q-1)q^{n-m(h+k)}},$$

where P_C denotes the proportion of multiplier vectors $\mathbf{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_{q^m}^*)^n$ such that the linear code $C_{\mathbf{a}} = \{(a_1x_1, \ldots, a_nx_n) | \mathbf{x} \in C\}$ has maximum trace dimension. In particular, if $n \geqslant m(k+h)$, or equivalently $d \geqslant n(1-1/m)+1$, then $P_C > 0$. It follows that $P_C \geqslant 1/2$, whenever $q \neq 2$ or $n \neq m(h+k)$. This shows that the Monte Carlo method of generating a random code $C_{\mathbf{a}}$ of maximum trace dimension is very effective. For $q = 2$ and $n = m(h+k)$, new ideas are needed.

On combinatorial structure of imprimitive graphs, part I

Safet Penjić

University of Primorska (Slovenia)

Let $(X, \mathcal{R})$ denote a symmetric d-class association scheme on v vertices with primitive (ordinary) idempotents $E_0, E_1, \ldots, E_d$. An association scheme is said to be *imprimitive* if some graph in the scheme is disconnected. It is well known that the following statements are equivalent:

(i) $(X, \mathcal{R})$ is imprimitive;

(ii) For some subset $\mathcal{J} = \{j_0 = 0, j_1, \ldots, j_s\} \subseteq \{0, 1, \ldots, d\}$ and some ordering of the vertices,

$$\sum_{h=0}^{s} E_{j_h} = \frac{1}{r}\left(I_w \otimes J_r\right),$$

for some integers w, r with $v = wr$ and $1 < w, r < v$.

Let Γ denote a connected k-regular graph on v vertices with adjacency algebra $\mathcal{A}$. In this talk, we present a combinatorial structure of Γ under the assumption that $I_w \otimes J_r \in \mathcal{A}$ for some integers w, r with $v = wr$ and $1 < w, r < v$. Some of the techniques that we use, as well as the necessary background material, can be found in [1, 2, 3].

This is work in progress and is joint work with Edwin van Dam and Giusy Monzillo.

References

[1] M. A. Fiol and S. Penjić, On symmetric association schemes and associated quotient-polynomial graphs, *Algebr. Comb.* **4** (2021), 947–969, doi:10.5802/alco, `https://doi.org/10.5802/alco`.

[2] G. Monzillo and S. Penjić, On commutative association schemes and associated (directed) graphs, *Electron. J. Combin.* **32** (2025), Paper No. 1.54, 38, doi:10.37236/12973, `https://doi.org/10.37236/12973`.

[3] G. Monzillo and S. Penjić, On the combinatorial structure and algebraic characterizations of distance-regular digraphs, *Discrete Math.* **348** (2025), Paper No. 114512, 26, DOI:10.1016/j.disc.2025.114512, `https://doi.org/10.1016/j.disc.2025.114512`.

Polycirculant LCF codes for cubic graphs

Tomaž Pisanski

University of Primorska and IMFM (Slovenia)

(Joint work in progress with Leah Berman and Gábor Gévay)

Every cubic Hamiltonian graph of order n can be represented by a sequence of length n with non-zero integer entries, known as the LCF code[3], which denotes the oriented spans along the Hamilton cycle. When the LCF code consists of a subsequence of length k, repeating m times it is termed a *polycirculant[4] LCF code of base k and exponent m*. We recall the following theorem:

Theorem 1. *The existence of a polycirculant LCF code with exponent $m, m > 1$ in a cubic graph is equivalent to the existence of a semi-regular automorphism of order m such that the quotient voltage graph has a Hamilton cycle with a net voltage relatively prime to m.*

We apply this result to an algorithm that generates all polycirculant LCF codes for a given graph. Characterizing cubic graphs that admit polycirculant LCF codes remains a challenging problem, even for highly symmetric graphs. For example, according to the online census of arc-transitive graphs[2], the graph F56B from the Foster census[1] is the smallest cubic arc-transitive Hamiltonian graph that does not possess a polycirculant LCF code. We present some observations based on the run of this algorithm on small generalized Petersen graphs.

References

[1] I. Z. Bouwer, editor. *The Foster census. R. M. Foster's census of connected symmetric trivalent graphs. Co-editors: W. W. Chernoff, B. Monson, Z. Star. With a foreword by H. S. M. Coxeter and a biographical preface by S. Schuster.* Winnipeg (Canada): Charles Babbage Research Centre, 1988.

[2] M. Conder, P. Potočnik, Edge-transitive cubic graphs: analysis, cataloguing and enumeration, *J. Algebra*, 685 (2026), 703-737.

[3] R. Frucht. A canonical representation of trivalent Hamiltonian graphs. *J. Graph Theory*, 1:45–60, 1977.

[4] T. Pisanski. A classification of cubic bicirculants. *Discrete Math.*, 307(3-5):567–578, 2007.

Difference sets for higher-dimensional symmetric designs

Lucija Relić

University of Zagreb (Croatia)

(Joint work with A. Bahmaniam, V. Krčadinac, M.O. Pavčević, S. Suda)

An n-dimensional symmetric (v, k, λ) design of propriety d is a $v \times \cdots \times v$ array over $\{0, 1\}$ such that every $(d-1)$-dimensional subarray contains exactly k ones, and scalar products of all pairs of parallel $(d-1)$-subarrays are λ. Cubes of symmetric designs and projection cubes, recently studied in [1], [2], and [3], arise as special cases with propriety 2 and with $\lambda = 0$, respectively. In this talk we restrict to 3-dimensional symmetric designs of propriety 3, studied in [4], and their associated difference sets. We define (v, k, λ) difference sets of propriety 3 as subsets $D \subseteq G^2$ satisfying three difference conditions involving left and right differences. We present the relationships between different types of cubes and their corresponding difference set properties.

References

[1] V. Krčadinac, M.O. Pavčević, K. Tabak *Cubes of symmetric designs*, Ars Math. Contemp. 25 (2025), no. 1, Paper No. 10, 16 pp.

[2] V. Krčadinac, L. Relić, *Projection cubes of symmetric designs*, to appear in Math. Comput. Sci. (2025). `https://arxiv.org/abs/2411.06936`

[3] V. Krčadinac, M.O. Pavčević, *On higher-dimensional symmetric designs*, to appear in Exp. Math. (2025). `https://arxiv.org/abs/2412.09067`

[4] A. Bahmanian, V. Krčadinac, L. Relić, S. Suda, *Three-dimensional symmetric designs of propriety 3*, preprint, 2025.

On the construction of extremal Type II codes over $\mathbb{Z}_{2^k}$

Sanja Rukavina

University of Rijeka (Croatia)

(Joint work with S. Ban Martinović)

Extremal Type II $\mathbb{Z}_{2^k}$-codes are a class of self-dual $\mathbb{Z}_{2^k}$-codes with Euclidean weights divisible by $2^{(k+1)}$ and the largest possible minimum Euclidean weight for a given length.

The topic of this talk is the construction of extremal Type II $\mathbb{Z}_{2^k}$-codes using the doubling method. With this method we have constructed new extremal $\mathbb{Z}_{2^k}$-codes for $k \in \{2, 3, 4\}$.

References

[1] S. Ban, D. Crnković, M. Mravić and S. Rukavina, *New extremal Type II $\mathbb{Z}_4$-codes of length 32 obtained from Hadamard matrices*, Discrete Math. Algorithms Appl., **11**, 1950057 (18 pp.) (2019)

[2] S. Ban and S. Rukavina, *Construction of extremal Type II $\mathbb{Z}_8$-codes via doubling method*, arXiv: 2405.00584, (2024)

[3] S. Ban and S. Rukavina, *On some new extremal Type II $\mathbb{Z}_4$-codes of length 40*, Math. Commun., **25(2)**, 253–268 (2020)

[4] S. Ban Martinović and S. Rukavina, *New extremal Type II $\mathbb{Z}_4$-codes of length 64*, Appl. Algebra Eng. Commun. Comput., https://doi.org/10.1007/s00200-024-00674-2 (2024)

Evaluation codes from linear systems of conics

Gioia Schulte

University of Salento, University of Basilicata (Italy)

A new family of evalutation codes in a vector space of dimension $\geqslant 2$ over a finite field $\mathbb{F}_q$ was given in [1] where linear combinations of elementary symmetric polynomials are evaluated on the set of all distinguished points, that is points with pairwise distinct coordinates. A generalization arises from m-dimensional linear systems of symmetric polynomials; see [2]. In this talk we present some new results and open problems in this direction. Computation for small values of $q = 7, 9$ shows that carefully chosen 3-dimensional linear systems produce $\left[\frac{1}{2}q(q-1), 3, d\right]$-codes that have minimum distance d equal to the optimal value minus 1.

References

[1] M. Datta, T. Johnsen. *Codes from symmetric polynomials*, Des. Codes and Cryptogr., **91**, 747–761, 2023.

[2] B. Gatti, G. Korchmáros, G. P. Nagy, V. Pallozzi Lavorante, G. Schulte, *Evaluation codes arising from symmetric polynomials*, Des. Codes and Cryptogr., **93**, 3361–3373, 2025.

On edge-transitive dihedrants

Luka Šinkovec

University of Primorska (Slovenia)

(Joint work with I. Kovács)

Let Γ be a Cayley graph over a dihedral group D_{2n} (a dihedrant for short) and G be the group of automorphisms of Γ acting transitively on the edges of Γ. The problem of classifying such graphs was proposed by Song et al. [5]. It is currently solved only under additional assumptions on Γ or G, see [1, 2, 3, 4]. In this talk, we introduce two new infinite families of edge-transitive dihedrants and show that the graph Γ is either described in the earlier papers, belongs to one of the two new families, or the group G satisfies certain conditions. Using these conditions, we also classify Γ in the case when G is a solvable group. This generalizes a result of Pan et al. [4] dealing with the case where $D_{2n} \leqslant G$ and D_{2n} is normal in G.

References

[1] S. F. Du, A. Malnič, and D. Marušič, Classification of 2-arc-transitive dihedrants, J. Combin. Theory Ser. B 98 (2008), 1349–13472.

[2] J.-J. Huang, Y.-Q. Feng, J.-X. Zhou, F.-G. Yin, The classification of two-distance transitive dihedrants, J. Algebra 667 (2025), 508–529.

[3] I. Kovács, Arc-transitive dihedrants of odd prime power order, Graphs Combin. 29 (2013), 569–583.

[4] J. Pan, X. Yu, H. Zhang, Z. Huang, Finite edge-transitive dihedrant graphs, Discrete Math. 312 (2012), 1006–1012.

[5] S. J. Song, C. H. Li, and H. Zhang, Finite permutation groups with a regular dihedral subgroup, and edge-transitive dihedrants, J. Algebra 399 (2014), 948–959.

Strongly regular graphs with 2-transitive two-graphs

Valentino Smaldore

Università degli Studi di Padova (Italy)

A two-graph is a pair (V, T), where T is a set of unordered triples of a vertex set V, such that every (unordered) quadruple from V contains an even number of triples from T. The two-graph is called *regular* if each pair of vertices is in a constant number of triples.

Given a graph $\Gamma = (V, E)$, the set of triples T of the vertex set V, whose induced subgraph has an odd number of edges, forms a two-graph on the set V. The two-graph $\Omega(\Gamma) = (V, T)$ is the *associated two-graph* of Γ.

We study the following problem. Let $\Gamma = (V, E)$ be a nontrivial strongly regular graph with associated two-graph $\mathcal{T} = (V, T)$. Write $H = \mathrm{Aut}(\Gamma)$ and $G = \mathrm{Aut}(\mathcal{T})$. Assume that G acts 2-transitively on on V, H is transitive and maximal subgroup of G not containing the unique largest perfect subgroup. We characterize G, H and Γ. This construction would lead to a new construction for strongly regular graphs.

References

[1] A.E. Brouwer, H. Van Maldeghem, *Strongly regular graphs*, Volume 182 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 2022.

[2] P.J. Cameron, *Finite permutation groups and finite simple groups*, Bulletin of the London Mathematical Society, 13(1):1-22, 1981.

[3] D.E. Taylor, *Some topics in the theory of finite groups*, Ph.D. thesis, University of Oxford, 1971.

[4] D.E. Taylor, *Regular 2-graphs*, Proceedings of the London Mathematical Society, (3), 35(2):257-274, 1977.

[5] D.E. Taylor, *Two-graphs and doubly transitive groups*, Journal of Combinatorial Theory, Series A, 61(1):113-122, 1992.

Blocking s-spaces by t-spaces in $\mathbb{F}_q^n$

Dávid R Szabó

HUN-REN Alfréd Rényi Institute of Mathematics (Hungary)

Let $0 \leqslant t \leqslant s \leqslant t \leqslant n$ be integers. In the n-dimensional vector space $\mathbb{F}_q^n$ over the q element field, an (s,t)-*blocking set* is a set t-spaces such that each s-space is incident with at least one chosen t-space. Denote by $f_{s,t}(n,q)$ the cardinality of the smallest such a blocking set. It is a trivial folklore result that $f_{s,t}(n,q) = q^N + O(q^{N-1})$ as $q \to \infty$ for $N \coloneqq (n-s)t$, but determining $f_{s,t}(n,q)$ more precisely is a notoriously difficult problem, as it is equivalent to determining the size of certain q-Turán designs and q-covering designs. For example, the exact value of even $f_{3,2}(n,q)$ is known only for $n \leqslant 5$.

We present an improvement on the upper bounds of Eisfeld and Metsch [3, Theorem 1.2.], [2, Theorem 1.2] for $(s,t) = (3,2)$ via a refined scheme for a recursive construction, which in fact enables improvement in the general case as well.

Theorem 1 ([1, Theorem 1.9])**.** *Let $(s,t) = (3,2)$ and $n \geqslant 6$. Then as $q \to \infty$, we have*

$$f_{3,2}(n,q) \leqslant \mathbf{1}q^N + \mathbf{0}q^{N-1} + \mathbf{2}q^{N-2} + 2q^{N-3} + 3q^{N-4} + 3q^{N-5} + 3q^{N-6} + 3q^{N-7} + O(q^{N-8}),$$
$$f_{3,2}(n,q) \geqslant \mathbf{1}q^N + \mathbf{0}q^{N-1} + \mathbf{2}q^{N-2} + q^{N-3} + 2q^{N-4}.$$

Theorem 2 (General recursive construction, [1, Corollary 3.7])**.** *Let X be an n-dimensional vector space, $K \leqslant X$ be a k-space with $k \leqslant n-s$. For each integer $0 \leqslant i \leqslant \min\{k,s\}$, pick an arbitrary integer $t_i \in [0,i] \cap [t-(s-i),t] \neq \varnothing$.*

If $\mathcal{B}_K(i)$ is an (i,t_i)-blocking set in K, and $\mathcal{B}_Q(i)$ is an $(s-i,t-t_i)$-blocking set in $Q \coloneqq X/K$, then

$$\mathcal{B}_X \coloneqq \bigsqcup_{i=0}^{\min\{k,s\}} \mathcal{B}_K(i) * \mathcal{B}_Q(i)$$

is an (s,t)-blocking in X where $\mathcal{B}_K * \mathcal{B}_Q \coloneqq \{T \leqslant X : K \cap T \in \mathcal{B}_K, \langle K,T\rangle \in \mathcal{B}_Q\}$.

These results are joint work with **Benedek Kovács** and **Zoltán Lóránt Nagy**.

References

[1] Kovács, B., Nagy, Z.L. and Szabó, D.R. *Blocking planes by lines in* PG(n,q), Des. Codes Cryptogr. (2025). https://doi.org/10.1007/s10623-025-01678-w

[2] Metsch, K. (2004). *Blocking subspaces by lines in* PG(n,q), Combinatorica **24** 459-486.

[3] Eisfeld, J., Metsch, K. (1997). *Blocking s-dimensional subspaces by lines in* PG$(2s,q)$, Combinatorica, 17(2), 151-162.

Classifying vertex-transitive graphs of order a product of two distinct primes

Ágnes Szalai

University of Primorska (Slovenia)

(Joint work with Ted Dobson)

In the 1990's two distinct groups of researchers worked on classifying vertex-transitive graphs of order qp, where q and p are distinct primes. This work is mainly concerned with such vertex-transitive graphs whose automorphism group contains a transitive subgroup with a normal block system. Intuitively, this means they primarily consider those graphs with automorphism group an almost simple group.

We give a refined classification when the automorphism group contains a transitive subgroup with a normal block system. It was stated in the 1990's that all such graphs are isomorphic to metacirculant graphs, and we give a classification of metacirculant graphs of order qp into disjoint families. As the isomorphism problem has been solved for metacirculant graphs of order qp, this will lead to an enumeration of vertex-transitive graphs of order qp in future work, a longstanding open problem for which several partial results have been given. Our work also holds for digraphs.

References

[1] Ted Dobson, Aleksander Malnič, and Dragan Marušič, *Symmetry in graphs*, Cambridge Studies in Advanced Mathematics, vol. 198, Cambridge University Press, Cambridge, 2022. MR 4404766

[2] D. Marušič and R. Scapellato, *Classifying vertex-transitive graphs whose order is a product of two primes*, Combinatorica 14 (1994), no. 2, 187–201. MR MR1289072 (96a:05072)

[3] Cheryl E. Praeger and Ming Yao Xu, *Vertex-primitive graphs of order a product of two distinct primes*, J. Combin. Theory Ser. B 59 (1993), no. 2, 245–266. MR MR1244933 (94j:05061)

On automorphism groups and p-rank of algebraic curves in positive characteristic

Marco Timpanella

University of Perugia (Italy)

(Joint work with Massimo Giulietti and Gábor Korchmáros)

In the study of algebraic curves, a fundamental problem is to determine the number of symmetries (or automorphisms) that a given curve can have. This question goes back to the nineteenth century, when significant results were obtained for curves over the complex numbers, particularly through the work of Hurwitz. Much of this theory extends to curves defined over arbitrary fields of characteristic zero, and over the past 125 years the structure and behavior of automorphism groups in this setting have been thoroughly investigated.

In positive characteristic, however, new and remarkable phenomena arise. Automorphism groups may be unexpectedly large compared to the genus of the curve, and the presence of points with stabilizers containing nontrivial p-subgroups (the so-called non-tame case) makes their analysis considerably more involved.

While the relationship between the genus of a curve and its automorphism group is relatively well understood, much less is known about the interaction between automorphism groups and another important birational invariant: the p-rank. In this talk we will delve into this topic and present some recent results in this direction.

References

[1] M. Giulietti, G. Korchmáros, M. Timpanella. On the Dickson-Guralnick-Zieve curve. *Journal of Number Theory* **196**, 114–138 (2019).

[2] H. W. Henn. Funktionenkorper mit großer Automorphismengruppe. *J. Reine Angew. Math.* **302**, 96-115 (1978).

[3] S. Nakajima. p-ranks and automorphism groups of algebraic curves. *Transactions of the American Mathematical Society* **303**, 595-–607 (1987).

Notes