5th Pythagorean Conference

An advanced research workshop in Finite Geometry, Cryptology, Algebraic Combinatorics, Coding Theory, Combinatorial Designs

Marco Buratti, Ilias S. Kotsireas, Spyros S. Magliveras, Alfred Wassermann (eds.)

JUNE 1-6, 2025
KALAMATA, GREECE
HOTEL HORIZON BLU

Welcome from the organizing committee

June 1st, 2025

It is a pleasure to welcome everyone to the Fifth Pythagorean Conference in Kalamata, Greece, an advanced research workshop in

- Finite Geometry
- Cryptology
- Algebraic Combinatorics
- Coding Theory
- Combinatorial Designs

Explore Cutting-Edge Combinatorics!

Arrigo Bonisoli, Università di Modena e Reggio Emilia, Italy
Marco Buratti, Sapienza Università di Roma, Italy
Cafer Çalişkan, Antalya Bilim University, Turkey
Otokar Grosek, Slovak Technical University, Bratislava, Slovakia
Gábor Korchmáros, Università della Basilicata, Italy
Ilias S. Kotsireas, Wilfrid Laurier University, Waterloo, ON, Canada
Spyros S. Magliveras, Florida Atlantic University, Boca Raton, FL, USA
Alfred Wassermann, Universität Bayreuth, Germany

Social Program

- Sunday: Arrival day
- Wednesday 2:20 pm: Conference excursion
- Wednesday 8:30 pm: Conference dinner

Web page: https://cargo.wlu.ca/5thPythagorean/web.html
Version May 27, 2025 – 13:00

Invited speakers

Ferdinand Ihringer has obtained his PhD in 2015 from Giessen University. Currently, he is a tenure-track assistant professor at the Southern University of Science and Technology in Shenzhen. In the past, he held two postdoctoral fellowships of the Research Foundation - Flanders (FWO) and one postdoctoral fellowship of the Pacific Institute for the Mathematical Sciences (PIMS). He was an invited speaker at various conferences, workshops, colloquia and seminars. Most notably, in 2023, he was one of eight plenary speakers at CanaDAM, a biennial conference with more than 320 participants in that year.

Donald L. Kreher is an emeritus professor of Mathematical Sciences from Michigan Technological University, where he was a professor for 29 years. He coauthored with Douglas R. Stinson fifteen research papers and the internationally acclaimed textbook: "Combinatorial Algorithms: Generation Enumeration and Search". He has numerous other publications in computational and algebraic methods for determining the structure and existence of combinatorial configurations. In 1995, Professor Kreher was awarded the Marshall Hall Medal from the Institute of Combinatorics and its Applications. He is currently the production manager and an editor-in-chief for the Bulletin of the Institute of Combinatorics and its Applications (BICA).

Klavdija Kutnar obtained her PhD from University of Primorska in 2008. She was elected the fourth rector of the University of Primorska in 2019 and is now running her second mandate. Her main research area is algebraic graph theory. She has been actively involved in various editorial boards of esteemed mathematical journals. She has been a member of the editorial board of the journal Ars Mathematica Contemporanea since 2016 and assumed the position of editor-in-chief in 2018. She is also a member of the editorial boards for the Bulletin of the Institute of Combinatorics and its Applications and Algebraic Combinatorics, and managing editor of the journal ADAM – The Art of Discrete and Applied Mathematics. She played a key role as the Deputy Chair of the Organizing Committee for the 8th European Congress of Mathematics in 2021. She is currently serving as a scientific committee member of Balkan Mathematics Conference (EMS – Regional Conference Series) and as a chair of EMS Meetings Committee.

Sam Mattheus obtained his PhD from Vrije Universiteit Brussel in 2022. Afterwards he moved to University of California San Diego for one year supported by a Fulbright and BAEF fellowship. Since 2023 he is a postdoc at Vrije Universiteit Brussel. His research ranges from finite geometry and association schemes to extremal graph theory and Ramsey theory. In 2023, he was awarded the Kirkman Medal of the Institute of Combinatorics and its Applications.

Alessandro Montinaro began his academic career as an Assistant Professor at the University of Salento in 2005, where he is now an Associate Professor. His main field of interest is Discrete Mathematics with particular attention to Design Theory. His major contributions concern the construction of combinatorial designs with a rich group of symmetries. He is author or coauthor of more than forty scientific papers published in the main international journals on Combinatorics. In particular, he has collaborations with S. H. Alavi, S. Zhou and C. E. Praeger. He served as a referee (multiple times) for 16 journals. Also, he served as a reviewer for Research Funding Organizations. He attended several conferences/workshops. He is an Associate Editor of *Innovations in Incidence Geometry* and *Note di Matematica*.

Maura Paterson obtained her PhD from Royal Holloway, University of London in 2005, under the supervision of Simon Blackburn and Peter Wild. She subsequently undertook postdoctoral research there in collaboration with Sean Murphy, and then with Keith Martin. In 2009 she joined Birkbeck, University of London, where she is now a Professor of Mathematics in the School of Computing and Mathematical Sciences. Her main area of research interest is applications of combinatorics to problems arising from cryptography and information security.

Dimitris E. Simos holds a PhD in Discrete Mathematics and Combinatorics from National Technical University of Athens and a habilitation degree in Applied Computer Science from Graz University of Technology. He is Key Researcher for the Applied Discrete Mathematics for Information Security research area with SBA Research located in Vienna and leads its Mathematics for Testing, Reliability and Information Security (MATRIS) research group. He is also the Head of Strategic Research at SBA Research responsible for shaping and implementing the strategic R&D agenda of the research center. He is further an Associate Professor (non-tenured track) with Graz University of Technology and holds a Guest Researcher appointment with the US National Institute of Standards and Technology (NIST), Applied Computational Mathematics Division (ACMD). During his career Dimitris has (co)-authored over 150 papers in Discrete Mathematics and their applications to Computational and Computer Science and has been awarded the rank of Fellow of the Institute of Combinatorics and its Applications (FTICA) and the Applications of Computer Algebra Early Researcher Award (ACA-ERA 2024). Last, he is the Founding Editor and current Lead Section Editor of the Springer Nature Computer Science (SNCS) journal section on combinatorial methods and models in system testing (COMSYT) and has served as the Austrian Delegate to the United Nations Commission on Science and Technology for Development (UN CSTD). His research interests include Combinatorial Designs and their applications to Software Testing, Algorithms, Quantum Computing, Cryptography and all aspects of Information Security, as well as, Design of Experiments and their interplay with Computer Algebra, Symbolic Computation, Mathematical Modelling, Optimization and Disaster Management.

Tommaso Traetta is an Associate professor at the University of Brescia (Italy) since 2021.
In 2010, he obtained his PhD in Mathematics and Computer Science under the supervision of Marco Buratti and was later awarded, by the Institute of Combinatorics and its Applications (ICA), the 2013 Kirkman Medal that recognizes excellent research in the early stage of a researcher career. From 2015 to 2017, he has been a Marie-Curie Fellow, and more recently he has been invited as a visiting Professor at Toronto Metropolitan University (Canada) and Jiaotong University (China).
During his career, he has been plenary speaker, or invited speaker in special sessions, at 13 international conferences; he has presented contributed talks at more than 25 further conferences and gave several seminars. He has also been a member of the organizing committee for special sessions and co-organizer of the international conference Discretaly.
His research interests include: Combinatorial design theory, (infinite) Graph decompositions, Difference Families, Regular Steiner triple systems, Automorphisms of combinatorial structures, Graph factorizations, packings and coverings, Graph labelings, and applications to DNA self-assembly, Heffter arrays and Graph embeddings, Combinatorial matrices.
He has published 34 papers in international refereed journals and is a Co-Managing Editor of Ars Combinatoria. He is a member of the ICA Prize Canvassing Committee.

Charlene Weiss obtained her PhD in Mathematics from Paderborn University, Germany, in 2023. In 2024/2025 she was working as a substitute professor for Geometry at Otto von Guericke University Magdeburg, Germany. Since April 2025, she has a postdoctoral position at the University of Amsterdam, funded by the DAAD (German Academic Exchange Service). Her research focuses on algebraic combinatorics, particularly association schemes, and their applications to coding theory, design theory, and finite geometry.

Yue Zhou is a professor at the National University of Defense Technology, China. He mainly studies finite geometry, algebraic combinatorics and their applications in coding and cryptography. He has published nearly 50 papers in journals such as Adv. Math., J. Cryptology, JCTA, Combinatorica, etc. In 2016, he won the Kirkman Medal of the Institute of Combinatorics and its Applications. He serves as a member of the editorial boards of Designs, Codes and Cryptography and Journal of Combinatorial Designs.

Conference Program

Monday, June 2nd

8:30	**Opening**
8:45	**Plenary lecture** Yue Zhue: *On the Existence of Dense Packing of Lee Spheres*
	Contributed talks
9:30	Ferruh Özbudak *On the Second Generalized Covering Radius of Binary Primitive Triple-Error-Correcting BCH Codes*
9:50	Mark Pankov *Geometry of equidistant codes*
9:50	Gioia Schulte *Evaluation codes arising from symmetric polynomials*
10:30	**Coffee**
	Contributed talks
11:00	Jonathan Jedwab *Quaternary Legendre pairs of even length*
11:20	Patric Östergård *Classifying Generalized Howell Designs*
11:40	Anton Betten *A Flag Transitive Large Set of Desargues Configurations*
12:00	Mariusz Meszka *Two-factorizations of some regular graphs*
12:20	Lucia Moura *New families of covering arrays of strength 3 and 4 using LFSR sequences*
12:40	Edoardo Persichetti *On Practical Post-Quantum Signatures from the Code Equivalence Problem*
13:00	**Lunch**
15:15	**Plenary lecture** Klavdija Kutnar: *Hamilton compression*
16:00	**Coffee**
	Contributed talks
16:30	John Baptist Gauci *Algebraic structures of MRD codes*
16:50	Robert Jajcay *Cyclic codes with large minimum distances and related combinatorial designs*
17:10	Tatiana Jajcayova *A new family of maximum rank distance codes*
17:30	Nancy E. Clarke *Pursuit-evasion on graphs arising from combinatorial designs*
17:50	Renata Del-Vecchio *Integral Hypergraphs*
18:10	Francesco Romeo *Sequentially Cohen-Macaulay binomial edge ideals of graphs*

Tuesday, June 3rd

8:45	**Plenary lecture** Sam Mattheus: *Combinatorics of finite spherical buildings*
	Contributed talks
9:30	Philipp Heering *Erdős-Ko-Rado problems and Uniqueness*
9:50	Ivan Landjev *Quadratic sets and $(t \bmod q)$-arcs in PG(r, q)*
10:10	Assia Rousseva *A Reducibility Theorem for Minihypers*
10:30	**Coffee**
	Contributed talks
11:00	Emanuel Juliano *Fixed Point Free Automorphisms in Graphs Classes*
11:20	Anargyros Katsampekis *Splittings of toric ideals of graphs*
11:40	Jelena Sedlar *An alternative approach to the Five Line Conjecture*
12:00	Robin Simoens *Design switching on graphs*
12:20	Vladislav Taranchuk *On the Chromatic Number of Grassmann Graphs*
12:40	Piotr Wojciechowski *Transitivity in weighted directed graphs*
13:00	**Lunch**
15:15	**Plenary lecture** Donald Kreher: *Near-factorization of finite groups*
16:00	**Coffee**
	Contributed talks
16:30	Mark R. Sepanski *Robinson–Schensted shapes arising from cycle decompositions*
16:50	Shaul Zemel *Stable Higher Specht Polynomials and Representations of Finite and Infinite Symmetric Groups*
17:10	Assaf Goldberger *Automorphism actions with nilpotent non-commutative coefficient group, constructed via cohomology*
17:30	Arianna Dionigi *On Galois subcovers of the Hermitian curve*
17:50	Barbara Gatti *Maximal Curves Over Finite Fields*
18:10	Tony Shaska *Rational points of weighted hypersurfaces over finite fields and an application to isogeny-based cryptography*

Wednesday, June 4th

8:45	**Plenary lecture** Charlene Weiß: *Codes and Designs in Polar Spaces*
	Contributed talks
9:30	Benedek Kovàcs *Constructing affine* $[3,1]$*-avoiding sets from graphs and linear codes*
9:50	Michael Hurley *New Geometric Large Sets*
10:10	Peter Horak *Some Conjectures and Results on Tilings*
10:30	**Coffee**
10:55	**Plenary lecture** Tommaso Traetta: *Highly symmetric Steiner and Kirkman triple systems*
	Contributed talks
11:40	Raúl Falcón *Study of symmetries of Latin squares by local permutation polynomials*
11:20	González Regadera *Coloring Latin squares by paratopisms*
11:40	Jaime Gutierrez *Local permutation polynomials and Latin hypercubes*
11:20	Ludwig Kampel *Locating single Failure Inducing* t*-way Interactions with* 0^t*-Locating Arrays*
13:00	**Lunch**
14:20	**Excursion**
20:30	**Conference dinner**

Thursday, June 5th

8:45	**Plenary lecture** Ferdinand Ihringer: *On Boolean Degree 1 Functions, Anti-Designs, and Cameron-Liebler Sets in Finite Vector Spaces*
	Contributed talks
9:30	Bart De Bruyn *Combinatorial characterizations of ovoidal cones*
9:50	Adam Tyc *Maximal cliques in the collinearity graphs of geometries of simplex codes*
10:10	Zijian Zhou *Neighborhoods of Vertices in the Isogeny Graph of Principally Polarized Superspecial Abelian Surfaces*
10:30	**Coffee**
	Contributed talks
11:00	Chris Mitchell *New constructions for orientable sequences*
11:20	Onur Ağırseven *On the Buratti-Horak-Rosa Conjecture for Small Supports*
11:40	Lukas Klawuhn *Designs of perfect matchings*
12:00	Vedrana Mikulić Crnković *Quasi-strongly regular digraphs and new strongly regular digraph with parameters* $(165, 60, 36, 23, 21)$
12:20	Juliana Palmen *Further results on decomposition of low degree circulant graphs into cycles*
12:40	Prangya Parida *Cover-free Families on Graphs*
13:00	**Lunch**
15:15	**Plenary lecture** Alessandro Montinaro: *2-Designs admitting a flag-transitive automorphism group*
16:00	**Coffee**
	Contributed talks
16:30	Usman Mushrraf *One weight sum-rank metric codes*
16:50	Krzysztof Petelczyc *Geometry of binary simplex codes and symmetric block designs*
17:10	Mariusz Żynel *Automorphisms of geometries related to binary equidistant codes*
17:30	Zita Abreu *Optimal Multidimensional Convolutional Codes*
17:50	Carlos Vela Cabello *The neighbor graph of binary Linear Complementary Dual Codes*
18:10	Ivona Traunkar *Self-orthogonal and LCD codes related to some combinatorial structures*

Friday, June 6th

8:45	**Plenary lecture** Maura Paterson: *Strong External Difference Families, Graph Labeling and Near Factorizations of Finite Groups*
	Contributed talks
9:30	Valentino Smaldore *A family of strongly regular graphs from hyperbolic quadrics*
9:50	Jurgen Mezinaj *A Neurosymbolic Approach to Galois Group of Septics*
10:10	Patricija Šapokaitė *Coadjoint Matroids and Dependencies on Hypergraphs*
10:30	**Coffee**
11:00	**Plenary lecture** Dimitris E. Simos: *Applications of Combinatorial Designs to Software Engineering, Cyber Security and Disaster Science*

Abstracts

On the Existence of Dense Packing of Lee Spheres

Yue Zhou
National University of Defense Technology
yue.zhou.ovgu@gmail.com

Based on the packing density of cross-polytopes in $\mathbb{R}^n$, more than 50 years ago Golomb and Welch proved that the packing density of Lee spheres in $\mathbb{Z}^n$ must be strictly smaller than one provided that the dimension $n > 2$ and the radius r of the Lee sphere is large enough compared with n. In the same paper [1], they conjectured that there is no perfect packing of Lee spheres of radius r in $\mathbb{Z}^n$ for $n \geq 3$ and $r \geq 2$. This conjecture still remains open. All the partial results based on geometric ideas are obtained for fixed dimension n and radius r which is comparatively large enough. In this talk, we concentrate on this conjecture with fixed radius r and different dimension n.
First, we prove the existence of asymptotically optimal coverings of the facets of the Lee sphere $S(n, r)$ centered at the origin by its translates as $n \to \infty$, which shows the difficulty of the proof of the Golomb-Welch conjecture by local analysis. Then we look at the constructions of packings of Lee spheres with density $\delta_n \to \frac{2^r}{(2r+1)r!}$ as $n \to \infty$. When $r = 2$, we further improve the packing density to $\delta_n \to \frac{2}{3}$ as $n \to \infty$.
In the second part we focus on the lattice tiling cases of the Golomb-Welch conjecture. We present a method to improve the symmetric polynomial criteria originally introduced by Kim [2] and generalized by Qureshi [3], Zhang and Ge [5]. By the new criteria, we can prove the lattice tiling case of the Golomb-Welch conjecture for $r = 3$ and every $3 \leq n \leq 1000$ except for $n = 122, 634$.

References

[1] S. W. Golomb and L. R. Welch. Perfect codes in the Lee metric and the packing of polyominoes. *SIAM Journal on Applied Mathematics*, 18(2):302–317, 1970.

[2] D. Kim. Nonexistence of perfect 2-error-correcting Lee codes in certain dimensions. *European Journal of Combinatorics*, 63:1 – 5, 2017.

[3] C. Qureshi. On the non-existence of linear perfect Lee codes: The Zhang-Ge condition and a new polynomial criterion. *European Journal of Combinatorics*, 83:103022, 2020.

[4] A. Xiao and Y. Zhou. On the packing density of Lee spheres. *Designs, Codes and Cryptography*, Apr. 2024. published online.

[5] T. Zhang and G. Ge. Perfect and quasi-perfect codes under the l_p metric. *IEEE Trans. Inform. Theory*, 63(7):4325–4331, 2017.

On the Second Generalized Covering Radius of Binary Primitive Triple-Error-Correcting BCH Codes

Ferruh Özbudak & İlknur Öztürk
Sabancı University, Türkiye
ferruh.ozbudak@sabanciuniv.edu &
ilknur.ozturk@sabanciuniv.edu

The covering radius is a basic geometric parameter of a code. The study of the covering radius of error-correcting codes plays an important role in coding theory, with applications in communication systems as error detection, data compression, testing, and in other areas. The problem of finding the covering radius of a given code is very hard in general. There are only a few classes of codes with special parameters in which the covering radii are known.

The covering radius of binary primitive BCH codes was determined in [3]. In [5], the problem of the determination of the covering radius for an arbitrary Melas code was completed. Recently, in [6] and [7], the covering radius of generalized Zetterberg type codes have been obtained for all finite fields of odd characteristic.

The generalized covering radius extends this concept, offering an enriched perspective by detailing code properties. For some application and connections to other areas we refer, for example, [1] and [2].

The second generalized covering radius of binary primitive double-error-correcting BCH codes has been determined in [8]. Using methods from coding theory, combinatorics and the arithmetic of algebraic varieties over finite fields, we previously determined the third generalized covering radius of binary primitive double-error-correcting BCH codes [4]. In this work we obtain results on the second generalized covering radius of binary primitive triple-error-correcting BCH codes using similar methods.

References

[1] D. Elimelech, M. Firer, and M. Schwartz, The generalized covering radii of linear codes, IEEE Transactions on Information Theory, 2021, vol. 67, pp. 8070-8085.

[2] D. Elimelech, H. Wei, and M. Schwartz, On the generalized covering radii of Reed-Muller codes, IEEE Transactions on Information Theory, 2022, vol. 68, pp. 4378-4391.

[3] S. D. Cohen, The length of primitive BCH codes with minimal covering radius, Designs, Codes and Cryptography, vol. 10, pp. 5–16, 1997.

[4] F. Özbudak, and İ. Öztürk, The third generalized covering radius for binary primitive double-error-correcting BCH codes, submitted, 2025.

[5] M. Shi, T. Helleseth, F. Özbudak, and P. Solé, Covering radius of Melas codes, IEEE Transactions on Information Theory, 2022, vol. 68, pp. 4354-4364.

[6] M. Shi, T. Helleseth, F. Ozbudak, Covering radius of generalized Zetterberg type codes over finite fields of odd characteristic, IEEE Transactions on Information Theory, 2023, vol. 69, pp. 7025-7048.

[7] M. Shi, S. Li, T. Helleseth, and F. Özbudak, Determining the covering radius of all generalized Zetterberg codes in odd characteristic, IEEE Transactions on Information Theory, 2025, doi: 10.1109/TIT.2025.3544025.

[8] L. Yohananov and M. Schwartz, The second generalized covering radius of binary primitive double-error-correcting BCH codes, arXiv preprint, arXiv:2409.10420, 2024.

Geometry of equidistant codes

Mark Pankov
Faculty of Mathematics and Computer Science,
University of Warmia and Mazury,
Słoneczna 54, 10-710 Olsztyn, Poland
pankov@matman.uwm.edu.pl

We present a brief survey of recent results and problems concerning the point-line geometries of equidistant codes. The main place is occupied by automorphisms and maximal cliques in the collinearity graphs. We describe relations to symmetric block designs and normal rational curves.

Evaluation codes arising from symmetric polynomials

Gioia Schulte
University of Salento, Italy
gioia.schulte@unisalento.it
Joint work with Barbara Gatti, Gábor Korchmáros, Gábor P. Nagy, Vincenzo Pallozzi Lavorante

Datta and Johnsen [1] introduced a new family of evalutation codes in a vector space of dimension ≥ 2 over a finite field $\mathbb{F}_q$ 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 of the Datta-Johnsen codes is found in the recent paper [2] where the approach is a combination of Galois theoretical methods with Weil-type bounds for hypersurfaces.
In this talk we deal with another generalization by taking m-dimensional linear systems of symmetric polynomials. We thoroughly work out the case of $m = 3$. Computation for small values of $q = 7, 9$ shows that carefully chosen such generalized Datta-Johnsen codes $\left[\frac{1}{2}q(q-1), 3, d\right]$ have minimum distance d equal to the optimal value minus 1.

Keywords: evaluation code, symmetric polynomials, finite field

References

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

[2] G. Micheli, V. Pallozzi Lavorante, P. Waitkevich. "Codes from a_m-invariant polynomials", *Des. Codes and Cryptogr.*, 2024, https://doi.org/10.1007/s10623-024-01550-3.

Quaternary Legendre pairs of even length

Jonathan Jedwab, Thomas Pender
Simon Fraser University
jed@sfu.ca

One of the most famous open problems in discrete mathematics is Paley's 1933 conjecture that there is a Hadamard matrix of order $n > 2$ if and only if n is a multiple of 4. It has long been known that this conjecture would follow from the existence of a pair of binary Legendre sequences for every odd length. It has recently been shown that this conjecture would also follow from the existence of a pair of quaternary Legendre sequences for every even length.
We use finite fields to give the first general constructions of quaternary Legendre sequences of even length. Firstly, we modify a classical construction due to Szekeres to show that there is a quaternary Legendre sequence of even length $(q-1)/2$ for every prime power q congruent to 1 modulo 4. Secondly, we use the Gray map to show that there is a quaternary Legendre pair of length $2p$ for every odd prime p for which $2p-1$ is a prime power.

Classifying Generalized Howell Designs

Patric R. J. Östergård
Department of Information and Communications Engineering
Aalto University School of Electrical Engineering
P.O. Box 15600, 00076 Aalto, Finland
patric.ostergard@aalto.fi

A t-GHD$_k(s, v; \lambda)$ generalized Howell design is an $s \times s$ array, each cell of which is either empty or contains a k-subset of elements of some set X of size v such that (i) each element of X appears exactly once in each row and in each column and (ii) no t-subset of elements from X appears in more than λ cells. Computer-aided classification of such designs is here considered in the framework of permutation codes with specific properties. Computations show among other things that there is a unique 2-GHD$_3(7, 18; 1)$; that there are 340 2-GHD$_3(7, 21; 1)$ (correcting an earlier result); and that the known 2-GHD$_5(8, 40; 1)$ is unique. Double counting is used to validate the results.

	pyt	hag	ore	vni	cfk	bdj
bhp		cei	aky	dfr	jno	gtv
cov	dhi		gnp	jkt	abr	efy
dny	krv	fjp		bcg	eht	aio
aft	ben	dko	hjv		giy	cpr
ijr	fgo	bvy	cdt	aep		hkn
egk	acj	nrt	bfi	hoy	dpv	

A Flag Transitive Large Set of Desargues Configurations

Anton Betten
Kuwait University
anton.betten@ku.edu.kw

We discuss partitions of the set of 3-subsets of the set $1, \ldots, 10$ into 12 pairwise disjoint Desargues configurations. This is an instance of a structure in the theory of combinatorial designs called a large set. The 3-subsets are called lines. The Desargues configuration is the incidence structure of 10 points and 10 lines arising in the theorem of Desargues. Using computer, the complete number of possibilities of such large sets is determined. Exactly one example has the additional property that the automorphism group acts flag transitively on the object. This means that any incident point / line pair can be mapped to any other. The automorphism group of the object is isomorphic to the automorphism group of the symmetric group of 6 things, of order 1440. Here we recall that the symmetric group of degree 6 is the only symmetric group admitting a non-trivial outer automorphism. The talk will discuss the classification of all large sets with these parameters and an analysis of the specific flag transitive object.

Two-factorizations of some regular graphs

Mariusz Meszka
AGH University of Kraków, Poland
meszka@agh.edu.pl

A *k-factorization* of G is a collection $\{F_1, F_2, \ldots, F_t\}$ of edge-disjoint k-factors such each edge of G belongs to exactly one F_i. We say that G has an *F-factorization* if each F_i, $i = 1, 2, \ldots, t$, is isomorphic to F.

One of the best-known open problems concerning two-factorizations is the famous Oberwolfach problem, posed by G. Ringel in 1967, which asks whether, for any two-factor F, the complete graph K_n (when n is odd) or $K_n \setminus I$ (when n is even and I is a one-factor removed from K_n) admits an F-factorization. Several years later A. Rosa suggested the following extension of the Oberwolfach problem, the so-called Hamilton-Waterloo problem, which asks for the existence of a two-factorization of K_n or $K_n \setminus I$ (depending on the parity of n) in which r of its two-factors are isomorphic to a given two-factor R, and the remaining q two-factors are isomorphic to a given two-factor Q, for any admissible r and q.

Results related to both these problems will be presented. Moreover, algorithmic methods for constructing two-factorizations will be discussed.

New families of covering arrays of strength 3 and 4 using LFSR sequences

Lucia Moura
University of Ottawa, Canada
lmoura@uottawa.ca
Joint work with Kianoosh Shokri and Brett Stevens

A *covering array* of strength t, denoted by $\mathrm{CA}(N; t, k, v)$, is an $N \times k$ array C over an alphabet with v symbols with the property that for any subarray consisting of t columns of C, every t-tuple of the alphabet appears at least once as a row of the subarray. An additional parameter λ is used when we require that every t-tuple of the alphabet appears at least λ times as a row of the subarray. An *orthogonal array* is a special case of a covering array, where each t-tuple appears exactly λ times, so in this case $N = \lambda v^t$. Given t, k, v, we aim to determine $\mathrm{CAN}(t, k, v)$ which is the minimum N for which a $\mathrm{CA}(N; t, k, v)$ exists. This is a hard problem in general, so we seek good upper bounds for CAN obtained from constructions.

Raaphorst, Moura and Stevens [3] gave a construction for a $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$, for every prime power q, using linear feedback shift register (LFSR) sequences over finite fields. In a recent paper with Kianoosh Shokri [4], we explore using this "good" ingredient to build covering arrays of strength 3 with a larger number of columns via recursive constructions and elimination of redundant rows. Several of these covering arrays improve the best upper bounds currently found in Colbourn's covering array tables [1]. In this talk, I describe these results and discuss our ongoing work to generalize the main result in each of the papers [3, 4] for the case of strength 4. There are interesting connections to finite geometry, as we seek to generalize [3] using a geometrical perspective discussed in [2]. This is joint work with Kianoosh Shokri and Brett Stevens.

References

[1] C. J. Colbourn, Covering Array Tables, https://www.public.asu.edu/~ccolbou/src/tabby/catable.html, accessed April 2024.

[2] C. J. Colbourn, C. Ingalls, J. Jedwab, M. Saaltink, K. W. Smith, and B. Stevens, Sets of mutually orthogonal projective and affine planes, *Combinatorial Theory* **1** (2024), #8.

[3] S. Raaphorst, L. Moura and B. Stevens, A construction for strength-3 covering arrays from linear feedback shift register sequences, *Designs, Codes and Cryptography* **76** (2014), 949–968.

[4] K. Shokri and L. Moura, New families of strength-3 covering arrays linear feedback shift register sequences, *Journal of Combinatorial Designs* **33** (2025), 156–171.

On Practical Post-Quantum Signatures from the Code Equivalence Problem

Edoardo Persichetti
Department of Mathematics and Statistics, Florida Atlantic University
epersichetti@fau.edu

The design of secure post-quantum digital signatures is a particularly important and current topic, especially considering the presence of initiatives such as NIST's call for proposals. While lattice-based designs offer intriguing solutions (some of which were recently standardised) NIST itself expressed the desire for alternatives, based on different security assumptions. Code-based signatures are historically challenging to design, due to the intrinsic nature of the Hamming metric, and the syndrome decoding problem; however, a recent approach exploiting the notion of code equivalence offers an interesting alternative. In this talk, we briefly summarise the state of the art, introduce the LESS signature scheme, and then present recent developments which greatly contribute to making it one of the most promising code-based signature schemes in literature.

Hamilton compression

Klavdija Kutnar
University of Primorska, Slovenia
klavdija.kutnar@upr.si

Given a graph X with a Hamilton cycle C, the *compression factor* $\kappa(X,C)$ *of* C is the order of the largest cyclic subgroup of $\mathrm{Aut}(C) \cap \mathrm{Aut}(X)$, and the *Hamilton compression* $\kappa(X)$ *of* X is the maximum of $\kappa(X,C)$ where C runs over all Hamilton cycles in X.
Motivated by Gregor, Merino and Mütze generalization of the well-known open problem regarding the existence of vertex-transitive graphs without Hamilton paths/cycles we have recently started to investigate existence of Hamilton cycles, admitting large rotational symmetry, in certain families of vertex-transitive graphs.
The work discussed in this talk is a joint work with Dragan Marušič and Andriaherimanana Sarobidy Razafimahatratra.

References:

P. Gregor, A. Merino and T. Mütze, The Hamilton compression of highly symmetric graphs, *Annals of Combin.* **28** (2024), 379–437.
L. Lovász, *Combinatorial Problems and Exercises*, Budapest, Akademiai Kiadó & Amsterdam-New York-Oxford, North-Holland Publishing Company, 1979.
K. Kutnar, D. Marušič, A. S. Razafimahatratra, Infinite families of vertex-transitive graphs with prescribed Hamilton compression, *Annals of Combin.* **28** (2024), 1243–1255.
K. Kutnar, D. Marušič, A. S. Razafimahatratra, Hamiltonicity of certain vertex-transitive graphs revisited, *Discrete Math.* **348** (2025), article no. 114350.

On the algebraic connectivity of a subfamily of generalized Petersen graphs

John Baptist Gauci
Department of Mathematics, Faculty of Science, University of Malta
john-baptist.gauci@um.edu.mt
Joint work with James Zammit

In 1973, Fiedler showed that the second smallest eigenvalue λ_2 of the Laplacian matrix $L(G)$ of a simple graph G is zero if and only if G is disconnected. Due to this relationship, λ_2 is called the algebraic connectivity of G, and is usually denoted by $\alpha(G)$. It serves as a key indicator of whether a graph is connected or not.
Since its introduction by Fiedler, algebraic connectivity has been widely studied, particularly in relation to vertex and edge connectivity. Researchers have also explored its connections with various graph invariants, such as the independence number and matching number, and have characterized graphs that attain some set bounds. A number of bounds for $\alpha(G)$ have been established leading to deep insights into the spectral properties of graphs. Additionally, researchers have extensively studied graphs that maximize or minimize $\alpha(G)$ within specific families.
In this talk, we examine the algebraic connectivity of a subfamily of generalized Petersen graphs, discussing bounds that make use of certain structural properties.

Classification and Extremal Properties of Graphs Sharing Properties of Vertex-Transitive Graphs

Robert Jajcay
Comenius University, Bratislava, Slovakia
Robert.Jajcay@fmph.uniba.sk

While many problems in Graph Theory do not require the considered graphs to be vertex- or edge-transitive, ultimately, some of the best constructions yield graphs that just 'happen' to be vertex- or edge-transitive. We choose to address this observation in the context of the Cage and Degree/Diameter Problems, two of the fundamental problems in Extremal Graph Theory, and focus on classes of extremal graphs that are not necessarily vertex-transitive but share the cycle structure properties of vertex-transitive (or often specifically Cayley) graphs.
After a brief survey of the role of vertex-transitive graphs in these areas, we introduce three interconnected concepts sharing the properties of vertex- or edge-transitive graphs: edge-girth regular, girth-regular and vertex-girth-regular graphs. All of these concept can be best understood via the concept of the *girth-cycle signature* defined for each vertex u to be the multi-set containing the numbers of girth-cycles passing through the edges adjacent to u. Using this concept, a k-regular graph of girth g, a (k,g)-graph, is called *edge-girth-regular*, $egr(k,g,\lambda)$-graph, if the girth-cycle signature of each vertex is the same and the number of girth-cycles through each edge is equal to a constant λ. A (k,g)-graph is called *girth-regular* if the girth-cycle signature of each vertex is the same (without requiring all the members of the signature to be the same), and is called *vertex-girth-regular*, $vgr(k,g,\Lambda)$, if the *sum* of the numbers in the girth-cycle signature of each vertex is the same and equal to Λ. Clearly, each edge-girth-regular graph is girth-regular and each girth-regular graph is vertex-girth-regular (with none of the classes equal). In addition, vertex-transitive graphs are necessarily girth- and vertex-girth-regular and edge-transitive graphs are edge-girth-regular (with all the classes distinct again).
In view of the connections of the above defined classes of graphs to the Cage and Degree/Diameter Problems, we shall present some classifications for small parameter sets k, g, λ, and Λ, and investigate the extremal properties of graphs in these classes. The results presented are based on collaboration with the presenter's co-authors listed below.

References

[1] Š. Glevitzká, R. Jajcay, M. Lekse and P. Potočnik, Cubic girth-regular graphs of girth 6 and their signatures, in preparation.

[2] R. Jajcay, J. Jooken, and I. Porupsánszki, On vertex-girth-regular graphs: (Non-)existence, bounds and enumeration, submitted for publication.

[3] A. Zavrtanik Drglin, S. Filipovski, R. Jajcay and T. Raiman, Extremal edge-girth-regular graphs, Graphs and Combinatorics 37 (6) 2139-2154 (2021).

[4] R. Jajcay, Gy. Kiss and Š. Miklavič, Edge-girth-regular graphs, Europ. J. of Comb. 72, (2018), 70-82.

Partial automorphisms of combinatorial structures

Tatiana B. Jajcayova
Comenius University, Bratislava, Slovakia
jajcayova@fmph.uniba.sk

Even though researchers often tend to focus on combinatorial structures possessing many symmetries, the majority of combinatorial structures (for instance graphs) are in fact asymmetric, i.e., having no non-trivial symmetries at all. In our talk, we attempt to reconcile these two seemingly opposing views, and we will argue that asymmetric and highly symmetric structures are not that far apart as it may seem. For example, removing just a single vertex from a vertex transitive graph may result in a graph with a trivial automorphism group; while removing a vertex from a graph belonging to the family of minimal asymmetric graphs (introduced by Nešetřil) always leads to a graph with a non-trivial automorphism group. Such situations call for the use of the concept of a partial automorphism which is an isomorphism between two induced substructures.

The set of all partial automorphisms of a given combinatorial structure together with composition of partial maps and taking partial inverses forms inverse monoid which is an analouge of the concept of an automorphism group. We believe, that inverse monoids of partial automorphisms captures better the local properties of the considered combinatorial structures. The problem of determining the full automorphism group of a combinatorial structure is one of the well-known hard problems. The focus of our project is on an extension of the automorphism group problem to that of inverse monoid problem. The goal is to apply the algebraic methods of partial permutation semigroup theory to the class of combinatorial structures that admit none or only very few total automorphisms and resist the use of methods from permutation group theory. In our presentation, we describe the algebraic structure of such inverse monoids by the means of the standard tools of inverse semigroup theory and give a characterization of inverse monoids which arise as inverse monoids of partial graph automorphisms. The results involving partial automorphisms and use of inverse monoids may offer new insights into some long open problems from Graph Theory, as we will illustrate with examples.

Pursuit-evasion on graphs arising from combinatorial designs

Nancy E. Clarke
Acadia University
nancy.clarke@acadiau.ca
Joint work with A. Burgess, R. Cameron, P. Danziger, S. Finbow, C. Jones, and D. Pike

Cops and Robber is a well-studied pursuit-evasion game played on graphs. In this talk, we discuss a variation of the game with an alternate capture condition. Instead of a win for the cop side resulting from at least one of the cops occupying the same vertex as the robber as in the original game, the cops in this surrounding version win by occupying each of the robber's neighbouring vertices. Our parameter of interest is the minimum number of cops that suffice to win on a graph G. We present a variety of results for this parameter, including exact values for several classes of graphs as well as more general bounds. In particular, we present results for graphs arising from combinatorial designs.

Integral Hypergraphs

Renata Del-Vecchio and Lucas Portugal Lima
Universidade Federal Fluminense
Niteroi, RJ, Brazil
rrdelvecchio@id.uff.br

Although the study of hypergraphs and their structural properties can be considered a fruitful area, with many published articles, the Spectral Theory for hypergraphs is still at an early stage. Spectral Theory for hypergraphs has two distinct approaches, via tensors and via matrices. The option in this work is the matrix approach, which has been increasingly recognized in recent years.

In this paper we introduce the concept of integral hypergraphs - hypergraphs whose all adjacency eigenvalues are integers, in analogy to integral graphs, noting that the search for integral graphs is one of the important problems in Spectral graph Theory. We study integrality for uniform hypercycles obtaining a characterization of integral uniform hypercycles in two specific cases: $3-$uniform and $4-$uniform hypercycles. As in the case of graphs, there are few integral hypercycles. From these cases, a more general result is left as a conjecture.

We also present infinite families of integral hypergraphs, especially hypergraphs built by two operations, the s-extension of a graph and the k-power of a graph.

Sequentially Cohen-Macaulay binomial edge ideals of graphs

Francesco Romeo
Department of Electrical and Information Engineering "Maurizio Scarano",
University of Cassino and Southern Lazio, 03043 Cassino, Italy
francesco.romeo@unicas.it

Let G be a simple graph with the vertex set $[n]$ and the edge set $E(G)$, let K be a field and $R = K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ be a polynomial ring in $2n$ indeterminates. The *binomial edge ideal* of G is the ideal J_G of R generated by all binomials $f_{ij} = x_i y_j - x_j y_i$, such that $i < j$ and $\{i, j\} \in E(G)$. The notion of binomial edge ideals was introduced by Herzog et al. in [6], and independently by Ohtani in [10]. Many algebraic properties and invariants of such ideals were described *via* the combinatorics of the underlying graph: as an example special subsets of vertices of the graph whose removal disconnect the graph play a crucial role in the computation of several invariants, e.g. Krull dimension (see [7] for a nice survey on this topic). One of the main problems in the study of binomial edge ideals is to classify the Cohen-Macaulay ones, and significant progress in this direction has been recently made in [1],[2],[3],[9]. A nice and deeply studied generalization of the Cohen-Macaulay property is the sequentially Cohen-Macaulay one, due to Stanley (see [12]). For what concerns binomial edge ideals, sequentially Cohen-Macaulay property has been studied for some particular classes of graphs [13, 11, 4]. In this talk, we present some classes of graphs whose binomial edge ideal is sequentially Cohen-Macaulay and we give some combinatorial necessary conditions for the sequentially Cohen-Macaulay property, by using interpretations of a characterization given in [5]. The presented results are extracted from [8] and another work in progress.

References

[1] D. Bolognini, A. Macchia, G. Rinaldo, F. Strazzanti, A combinatorial characterization of S_2 binomial edge ideals. *Eur. J. Comb* **126**, 104–123 (2025).

[2] D. Bolognini, A. Macchia, G. Rinaldo, F. Strazzanti, Cohen-Macaulay binomial edge ideals of small graphs. *J. Algebra* **638**, 189–213 (2024) https://doi.org/10.1016/j.jalgebra.2023.09.029

[3] D. Bolognini, A. Macchia, F. Strazzanti, Cohen-Macaulay binomial edge ideals and accessible graphs. *J. Algebraic Comb.* **55**, 1139–1170 (2022) https://doi.org/10.1007/s10801-021-01088-w

[4] V. Ene, G. Rinaldo, N. Terai, Sequentially Cohen-Macaulay binomial edge ideals of closed graphs. *Res. Math. Sci.* **9**, 39 (2022) https://doi.org/10.1007/s40687-022-00334-2

[5] A. Goodarzi, Dimension filtration, sequential Cohen–Macaulayness and a new polynomial invariant of graded algebras. *J. Algebra* **456**, 250–265 (2016) https://doi.org/10.1016/j.jalgebra.2016.01.045

[6] J. Herzog, T. Hibi, F. Hreinsdóttir, T. Kahle, J. Rauh, Binomial edge ideals and conditional independence statements. *Adv. Appl. Math.* **45**, 317–333 (2010) http://doi.org/10.1016/j.aam.2010.01.003

[7] J. Herzog, T. Hibi, H. Ohsugi, *Binomial Ideals*. Graduate Texts in Mathematics **279**, Springer Cham (2018) https://doi.org/10.1007/978-3-319-95349-6

[8] E. Lax, G. Rinaldo, F. Romeo, Sequentially Cohen-Macaulay binomial edge ideals, *arXiv preprint* https://arxiv.org/abs/2405.08671, 2024.

[9] A. LERDA, C. MASCIA, G. RINALDO, F. ROMEO, (S_2)-condition and Cohen-Macaulay binomial edge ideals. *J. Algebraic Comb.* **57**, 589–615 (2023) https://doi.org/10.1007/s10801-022-01173-8

[10] M. OHTANI, Graphs and ideals generated by Some 2-minors. *Commun. Algebra* **39**(3), 905–917 (2011) https://doi.org/10.1080/00927870903527584

[11] P. SCHENZEL, S. ZAFAR, Algebraic properties of the binomial edge ideal of a complete bipartite graph. *An. Ştiinţ. Univ. "Ovidius" Constanţa Ser. Mat.* **22**(2), 217–237 (2014) https://doi.org/10.2478/auom-2014-0043

[12] R. P. STANLEY *Combinatorics and Commutative Algebra*, 2nd ed. Progress in Mathematics **41** Birkhäuser, Boston, MA (1996) https://doi.org/10.1007/b139094

[13] S. ZAFAR On approximately Cohen-Macaulay Binomial edge ideal, *Bull. Math. Soc. Sci. Math. Roumanie* **55**(103)(4), 429–442 (2012)

Combinatorics of finite spherical buildings

Sam Mattheus
Vrije Universiteit Brussel
sam.mattheus@vub.be

We will give an introduction to finite spherical buildings, which is the geometry of flags in projective and polar spaces. In this setting, known extensions of the classical Erdős-Ko-Rado theorem to projective and polar spaces can be generalized to the setting of flags. While some proofs of the former rely on the underlying commutative association schemes and ideas developed by Delsarte, the corresponding association scheme in the latter case, also known as the Iwahori-Hecke algebra, no longer enjoys this commutativity property. Nevertheless, we will see that it is possible to overcome this difficulty and obtain sharp bounds on Erdős-Ko-Rado sets of flags. Moreover, we are able to obtain classification results for the largest Erdős-Ko-Rado sets of flags in a majority of the cases, which is one of the few such results in which the underlying association scheme is not commutative. We will conclude by sketching some interesting problems in this area.
Based on joint works with Jan De Beule, Philipp Heering, Jesse Lansdown and Klaus Metsch.

Erdős-Ko-Rado problems and Uniqueness

Philipp Heering
JLU Giessen (Germany) — Geometry, Topology and Discrete Mathematics
philipp.heering@math.uni-giessen.de
Joint work with Jan De Beule, Jesse Lansdown, Sam Mattheus and Klaus Metsch

The Erdős-Ko-Rado problem is a cornerstone of extremal combinatorics, given a suitable notion of "intersection", it asks the following questions: What is the maximum size of a set of intersecting objects? What is their structure? We will focus on the latter question. Algebraic methods have been highly effective in addressing the size question. We discuss a new algebraic tool called "Antidesigns" that allows us to determine the structure in certain cases, even if the underlying association scheme is not commutative. Moreover, we discuss the limitations of these tools. Our objects will be chambers in finite spherical buildings and our notion of intersection will be non-oppositeness. We conclude with open problems related to finite spherical buildings and Antidesigns.

Keywords: Erdős-Ko-Rado problem, design orthogonality, finite geometry

References

[1] Jan De Beule, Sam Mattheus, Klaus Metsch. An algebraic approach to Erdös-Ko-Rado sets of flags in spherical buildings., *J. Combin. Theory Ser. A*, **192**:Paper No. 105657, 33, 2022.

[2] Philipp Heering, Jesse Lansdown, Klaus Metsch. Maximum Erdős-Ko-Rado sets of chambers and their antidesigns in vector-spaces of even dimension, *arXiv:2406.00740*, 2024.

[3] Philipp Heering, Klaus Metsch. Maximal cocliques and the chromatic number of the Kneser graph on chambers of PG$(3, q)$, *Journal of Combinatorial Designs*, **32**(7):388–409, 2024.

[4] Philipp Heering. On the largest independent sets in the Kneser graph on chambers of PG$(4, q)$, *Discrete Mathematics*, **348**(5), 2025.

Quadratic sets and $(t \bmod q)$-arcs in $\mathrm{PG}(r, q)$

Ivan Landjev
Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences,
8 Acad. G. Bonchev str., 1113 Sofia, Bulgaria
ivan@math.bas.bg
Joint work with Sascha Kurz and Assia Rousseva

An arc $\mathcal{K}$ in the geometry $\mathrm{PG}(r, q)$ is called a $(t \bmod q)$-arc if $\mathcal{K}(L) \equiv t \pmod q$ for every line L in $\mathrm{PG}(r, q)$. If in addition the maximal multiplicity of a point is t then the arc $\mathcal{K}$ is called a strong $(t \bmod q)$-arc.
The $(t \bmod q)$-arcs arise in connection with the extendability problem for arcs and linear codes, but are objects that are interesting in their own right. Strong $(t \bmod q)$-arcs can be obtained by the so-called lifting construction from $(t \bmod q)$-arcs in geometries of smaller dimension. Arcs obtained by this construction are called lifted arcs. It is known that all strong $(1 \bmod q)$-arcs in $\mathrm{PG}(r, q)$ are just the hyperplanes or the complete space for every r and every prime power q. This fact is equivalent to Hill-Lizak's extension theorem for linear codes. It was proved that all strong $(2 \bmod q)$ arcs in $\mathrm{PG}(r, q)$, $r \geq 3$, q odd are lifted.
For $t \geq 3$ the situation is more complicated. It was even conjectured that all strong $(3 \bmod 5)$-arcs in geometries of dimension $r \geq 3$ are lifted. This conjecture turns out to be wrong. There exist strong non-lifted $(3 \bmod 5)$-arcs in $\mathrm{PG}(3, 5)$ of respective sizes 128, 143, 168. The first one is related to the exceptional 20-cap in $\mathrm{PG}(3, 5)$ discovered by Abatangelo, Korchmáros and Larato. The other two are obtained from the elliptic and hyperbolic quadric in $\mathrm{PG}(3, 5)$, respectively, by a construction which can be generalized to geometries of larger dimension over larger fields of odd characteristic. Arcs obtained by this construction are called quadratic arc. We prove the following theorems.

Theorem 1 *Every strong* $(3 \bmod 5)$ *arc in* $\mathrm{PG}(4, 5)$ *is either a lifted, or a quadratic arc.*

Theorem 2 *Let every strong* $(3 \bmod 5)$*-arc in* $\mathrm{PG}(r-1, 5)$ *be either lifted, or a quadratic* $(3 \bmod 5)$*-arc. Then every strong* $(3 \bmod 5)$*-arc in* $\mathrm{PG}(r, 5)$ *is also either lifted, or quadratic.*

A Reducibility Theorem for Minihypers

Assia Rousseva
Faculty of Mathematics and Informatics,
Sofia University "St. Kl. Ohridski", 5 J. Bourchier blvd, 1164 Sofia
assia@fmi.uni-sofia.bg
Joint work with Ivan Landjev and Konstantin Vorobev

A multiset $\mathcal{F}$ in $\mathrm{PG}(r,q)$ is called an (n,w)-minihyper if its total point multiplicity is $|\mathcal{F}| = n$, $\mathcal{F}(H) \leq w$ for every hyperplane H, and there is a hyperplane H_0 with $\mathcal{F}(H_0) = w$. The existence of an (n,w)-minihyper in $\mathrm{PG}(k-1,q)$ with maximal point multiplicity s is equivalent to that of a linear code with parameters $[sv_k - n, k, sv_{k-1} - w]_q$. Here $v_k = (v^k - 1)/(v-1)$.

In this talk we prove the following reducibility theorem for minihypers:

Theorem 1. Let $\mathcal{F}$ be an (n,w)-minihyper in $\mathrm{PG}(r,p)$, p a prime, with $w \equiv n - p \pmod{p^2}$. Assume that $\mathcal{F}$ has the following properties:

(1) $\mathcal{F}(H) \equiv n - p$ or $n \pmod{p^2}$ for every hyperplane H in $\mathrm{PG}(r,p)$;

(2) for every hyperplane H with $\mathcal{F}(H) \equiv n \pmod{p^2}$ $\mathcal{F}|_H$ is a divisible minihyper with divisor p;

(3) for every hyperplane H with $\mathcal{F}(H) \equiv n - p \pmod{p^2}$ $\mathcal{F}|_H$ is reducible to a divisible minihyper with divisor p.

Then $\mathcal{F} = \mathcal{F}' + \chi_L$ where $\mathcal{F}'$ is a $(n - v_2, w - v_1)$-minihyper, and L is a line.

This theorem can be formulated as an extension theorem for arcs and linear codes.

Fixed Point Free Automorphisms in Graphs Classes

Emanuel Juliano
Federal University of Minas Gerais, Brazil
emanueljulianoms@gmail.com

Let X be a graph, and $\phi : V(X) \to V(X)$ be an automorphism of X. We say that ϕ is a fixed point free (FPF) automorphism if for all $v \in V(X)$ we have $\phi(v) \neq v$. Lubiw [4] introduced the FPFAUT problem, which asks whether there exists a fixed point free (FPF) automorphism for a given graph, and proved that this problem is NP-complete.
Despite the negative result, there exist polynomial-time algorithms for specific graph classes. For instance, it follows from an old result of Jordan [3, 5] that the answer to the FPFAUT problem is trivially true when restricted to the class of vertex-transitive graphs. Moreover, Cameron [2] has shown that with the generators of the automorphism group in hand, it is also possible to compute the FPF automorphisms of a vertex-transitive graph.
In this talk, we present a polynomial-time algorithm for the FPFAUT problem when restricted to graph classes with unique tree representations. The algorithm can be modified to compute FPF involutions, which are related to some special equitable partitions. This generalizes the result of Abiad et al. [1].
Based on a joint work with Aida Abiad, Gabriel Coutinho, Vinicius F. dos Santos and Sjanne Zeijlemaker.

References

[1] A. Abiad, C. Hojny, and S. Zeijlemaker, *Characterizing and computing weight-equitable partitions of graphs*, Linear Algebra Appl., vol. 645, pp. 30–51, 2022.

[2] P. J. Cameron and T. Wu, *The complexity of the weight problem for permutation and matrix groups*, Discrete Math., vol. 310, no. 3, pp. 408–416, 2010.

[3] C. Jordan, *Recherches sur les substitutions*, J. Math. Pures Appl., vol. 17, pp. 351–367, 1872.

[4] A. Lubiw, *Some NP-complete problems similar to graph isomorphism*, SIAM J. Comput., vol. 10, no. 1, pp. 11–21, 1981.

[5] J.-P. Serre, *On a theorem of Jordan*, Math. Medley, vol. 29, pp. 3–18, 2002.

Splittings of toric ideals of graphs

Anargyros Katsampekis and Apostolos Thoma
Department of Mathematics, University of Ioannina,
Ioannina 45110, Greece
katsampekis@uoi.gr, athoma@uoi.gr

Let G be a finite, connected and undirected graph having no loops and no multiple edges on the vertex set $V(G) = \{v_1, \ldots, v_n\}$, and let $E(G) = \{e_1, \ldots, e_m\}$ be the set of edges of G. Let $K[e_1, \ldots, e_m]$ be a polynomial ring over a field K, where we treat the e_i's as indeterminates. Similarly, we consider the polynomial ring $K[v_1, \ldots, v_n]$. The toric ideal of G, denoted by I_G, is the kernel of the K-algebra homomorphism $\phi_G : K[e_1, \ldots, e_m] \longrightarrow K[v_1, \ldots, v_n]$ defined by $\phi_G(e_i) = v_{j_i}v_{k_i}$, where $e_i = \{v_{j_i}, v_{k_i}\}$ for all $1 \leq i \leq m$. This talk aims to answer [1, Question 5.1], namely to classify all graphs G such that I_G is a subgraph splittable toric ideal. We say that I_G is subgraph splittable if there exist subgraphs G_1 and G_2 of G such that $I_G = I_{G_1} + I_{G_2}$, where both I_{G_1} and I_{G_2} are not equal to I_G. We give a complete answer to the above problem. Our approach is based on the graphs $G\backslash e$ and G^e_S, where e is an edge of G and S is a minimal system of binomial generators of I_G. We show that I_G is subgraph splittable if and only if there is an edge e of G and a minimal generating set of binomials S of I_G such that $I_G = I_{G^e_S} + I_{G\backslash e}$ is a subgraph splitting. As an application of our results, we prove that the toric ideal of a complete bipartite graph is not subgraph splittable and the toric ideal of the wheel graph is subgraph splittable if and only if either $n = 4$ or n is odd. We also study the case that G coincides with the complete graph K_n on n vertices. We show that I_{K_n} is subgraph splittable if and only if $n \geq 4$.

References

[1] G. Favacchio, J. Hofscheier, G. Keiper, A. Van Tuyl, Splittings of toric ideals, J. Algebra **574** (2021), 409–433.

An alternative approach to the Five Line Conjecture

Jelena Sedlar
University of Split, Faculty of Civil Engineering, Architecture and Geodesy, Croatia
jsedlar@gradst.hr
Joint work with Riste Škrekovski

A Fano coloring is an edge-coloring of a cubic graph by points of the Fano plane such that the colors of any three edges meeting at a vertex form a line. A natural problem is to determine the minimum value of k such that every bridgeless graph admits a k-line Fano coloring. It is conjectured that every bridgeless cubic graph admits a 4-line Fano coloring. This is the strongest possible conjecture, since it is known that 3 lines are not sufficient to color each bridgeless cubic graph. A 5-line conjecture is a relaxation of the 4-line conjecture, which states that every bridgeless cubic graph admits a 5-line Fano coloring. It is known that a 5-line Fano coloring is equivalent to a proper edge colorings in which colors are non-zero elements of the group $\mathbb{Z}_4 \times \mathbb{Z}_2$ and the sum of the three colors meeting at each vertex is zero. We give a characterization of proper $\mathbb{Z}_4 \times \mathbb{Z}_2$ colorings in terms of a matching in a 2-factor of a bridgeless cubic graph G. If a matching of a 2-factor of G does not satisfy the characterization, we further provide two sufficient conditions under which a matching can be modified to satisfy the characterization. This yields the construction of 5-line Fano coloring for many snarks.

Design switching on graphs

Robin Simoens
Ghent University & Universitat Politècnica de Catalunya
robin.simoens@ugent.be

A switching method is a graph operation used to obtain cospectral graphs (graphs with the same adjacency spectrum). It needs the graph to have a switching set holding some conditions. Abiad and Haemers [2] found a switching method that uses a switching set of size seven. In this talk, I present a new combinatorial description of this switching method, based on the Fano plane, as described in [1].
Moreover, the operation can in fact be generalized to a switching method based on any symmetric combinatorial design. This also generalizes other previously known switching methods such as the one in [3, Section 7.1], when applied to the point-hyperplane design of a projective space.
This talk is based on joint work with Aida Abiad and Nils van de Berg [1] and ongoing joint work with Ferdinand Ihringer.

References

[1] A. Abiad, N. van de Berg and R. Simoens, Switching methods of level 2 for the construction of cospectral graphs, *preprint* (arXiv:2401.06618), 2024.

[2] A. Abiad and W.H. Haemers, Cospectral graphs and regular orthogonal matrices of level 2, *Electron. J. Comb.* #P13, 2012.

[3] A.E. Brouwer, F. Ihringer and W.M. Kantor, Strongly Regular Graphs Satisfying the 4-Vertex Condition, *Combinatorica* **43**, 257–276, 2023.

On the Chromatic Number of Grassmann Graphs

Vladislav Taranchuk
Ghent University, Belgium
vlad.taranchuk@ugent.be
Joint work with Jozefien D'haeseleer and Himanshu Gupta

While much work has been done on the chromatic number of Johnson graphs and Kneser graphs, much less is known about the chromatic number of Grassmann graphs. In this talk we will give a brief survey of results regarding the chromatic number of several Johnson graphs, Kneser graphs, and Grassmann graphs. Furthermore, we will present new upper bounds on the chromatic number of Grassmann graphs. This talk is based on joint work with Jozefien D'haeseleer and Himanshu Gupta.

Transitivity in weighted directed graphs

Piotr J. Wojciechowski
Department of Mathematical Sciences
The University of Texas at El Paso, USA
piotrw@utep.edu

A *transitive system* is a tuple $(X, \mathcal{R}, G, f)$ where X is a nonempty set, $\mathcal{R}$ is a reflexive and transitive relation on X, $(G, +, 0)$ is an abelian group and $f : \mathcal{R} \to G$ is a *transitive mapping* satisfying

(i) for every $x \in X$, $f(x, x) = 0$ and

(ii) if $(x, y), (y, z) \in \mathcal{R}$ then $f(x, y) + f(y, z) = f(x, z)$.

Transitive systems provide a wide research area with applications. A state of the art of this research will be presented in the talk.
In graph-theoretic language, transitive systems are directed, weighted and transitive graphs with the weights obeying the triangle equality. A natural question often arises: Is it possible to fill in the missing connections in the system and preserve its transitivity? If the answer is positive, we say that the system *can be completed*. In all cases observed in [1],[2],[3] if a graph admits a transitive system that cannot be completed in one abelian group, then the same is true for every nontrivial abelian group. So, for example, no matter what nontrivial group we consider, no system imposed on the graph in Fig. 1 can be completed. There is something intrinsic to some graphs that predetermines the existence of such a "universally bad" situation. These graphs are called *defective*.

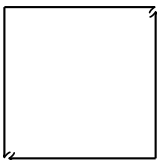

Figure 1: The simplest defective graph.

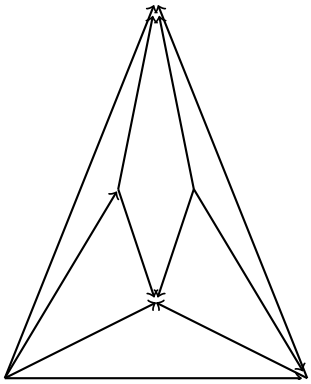

Figure 2: A soluble graph.

On the other hand, there are graphs featuring the opposite: they "know" that no matter what group of weights is considered, any transitive system can be completed. An example of such a graph is shown in Fig. 2. Those "good" graphs are called *soluble*. Our paper [2] is devoted to various techniques of obtaining soluble graphs. A graph which is either soluble or defective is called *conclusive*.

There are several identified classes of conclusive graphs. In terms of size, at this moment we can tell that every graph of up to 10 vertices is conclusive. A practical application of this knowledge is that within these classes we can use the group $\mathbb{Z}_2$ to determine if every imposed transitive system can be completed or not, which obviously optimizes the process.
Although at present we do not know if every graph is conclusive, the most recent result asserts that all *planar* graphs are!

References

[1] G. Cigler, M. Jerman, and P. J. Wojciechowski, "Transitive systems and conclusive partial orders", *Discret. Appl. Math* 314 (2022), 129-141.

[2] G. Cigler and P. J. Wojciechowski, "Algebraic properties of soluble posets", *Discret. Appl. Math* 348 (2024), 211-220.

[3] G. Cigler, V. Kreinovich, J.Urenda, P. J. Wojciechowski "A feasible algorithm for solubility of transitive graphs", *Mathematical Proceedings of the Royal Irish Academy* 122A (2022), 27-32.

Near-factorization of finite groups

Donald L. Kreher
Michigan Technological University
kreher@mtu.edu

Let $(G, \cdot)$ be a finite multiplicative group with identity e. For $A, B \subseteq G$, define

$$AB = \{gh : g \in A, h \in B\}$$

and note that AB is a multi-set.
We say that (A, B) is a near-factorization of G with index λ if $|A| \times |B| = \lambda(|G| - 1)$ and each element of $G \setminus \{e\}$ occurs λ times in the product AB. We abbreviate this by writing $AB = \lambda(G \setminus \{1\})$. If (A, B) is a near-factorization with index λ, then we say that B is a λ-mate of A. A λ-mate with $\lambda = 1$ is simply called a mate.
Some new structural properties of near-factorizations in certain classes of groups are established. In particular if there is a near-factorization (A, B), then there is an explicit formula for B in terms of A. This leads to an efficient method for computing the λ-mate B of a subset $A \subseteq G$, if it exists. All noncyclic abelian groups of order less than 200 were examined in a search for a possible nontrivial near-factorization with index 1 and all of these possibilities were ruled out, either by theoretical criteria or by exhaustive computer searches. (In contrast, index 1 near-factorizations in cyclic or dihedral groups are known to exist by previous results.)
Collaborators: Bill Martin, Maura Paterson, and Doug Stinson.

Robinson–Schensted shapes arising from cycle decompositions

Martha Du Preez, William Q. Erickson, Jonathan Feigert, Markus Hunziker, Jonathan Meddaugh, Mitchell Minyard, Kyle Rosengartner, Mark R. Sepanski
Baylor University, USA
Mark_Sepanski@baylor.edu

At the heart of classical algebraic combinatorics is the representation theory of the symmetric group S_n. In turn, much of this theory can be expressed in terms of integer partitions. In this paper, we describe the subtle relationship between two partitions closely associated with each element $\sigma \in S_n$: the *cycle type* of σ, on one hand, and the *shape* of σ, via the Robinson–Schensted correspondence, on the other hand. Although separately each of these partitions is fundamental to the general theory, the two had not yet been studied *together* until a very recent paper treating the special case where σ is a cyclic (or almost cyclic) permutation. (The most closely related works study cycle types and descents, or shapes and inversions.) A natural question is the following: which shapes arise from the elements of a given cycle type?

It is well known that the conjugacy classes of S_n (and also its irreducible complex representations) can be naturally labeled by the integer partitions α of n (written as $\alpha \vdash n$). In particular, the conjugacy class of $\sigma \in S_n$ is labeled by the partition $\alpha = (\alpha_1, \ldots, \alpha_r)$ giving the *cycle type* of σ, which is easily read off from the expression of σ in disjoint cycle notation: $\sigma = (\alpha_1\text{-cycle})(\alpha_2\text{-cycle}) \cdots (\alpha_r\text{-cycle})$. (As usual, we write partitions so that $\alpha_1 \geq \cdots \geq \alpha_r \geq 1$.) We will write C_α to denote the conjugacy class of S_n consisting of elements with cycle type α.

Another key concept in the representation theory of S_n (and in algebraic combinatorics in general) is the Robinson–Schensted (RS) correspondence. The RS correspondence is a bijection $S_n \xrightarrow{\text{RS}} \coprod_{\lambda \vdash n} \mathrm{SYT}(\lambda) \times \mathrm{SYT}(\lambda)$, where $\mathrm{SYT}(\lambda)$ denotes the set of standard Young tableaux with shape λ, meaning that the partition λ gives the row lengths of the tableaux. If the RS correspondence takes σ to a pair $(P, Q) \in \mathrm{SYT}(\lambda) \times \mathrm{SYT}(\lambda)$, then we say that λ is the *RS shape* of σ, which we denote by writing $\mathrm{sh}(\sigma) = \lambda$. The main problem in this paper is to describe the elements of $\mathcal{S}_\alpha := \{\mathrm{sh}(\sigma) : \sigma \in C_\alpha\}$.

As a preliminary result, for all $\alpha = (\alpha_1, \ldots, \alpha_r) \vdash n$, we prove that the partitions in $\mathcal{S}_\alpha$ have Young diagrams fitting inside a certain bounding box: $\mathcal{S}_\alpha \subseteq \mathcal{B}_\alpha$, where $\mathcal{B}_\alpha$ consists of all partitions of n with at most $\big(n - r + \#\{i : \alpha_i = 2\} + \delta_{1,\alpha_r}\big)$ many rows and $\big(n - r + \#\{i : \alpha_i = 1\}\big)$ many columns.

For certain cycle types α, the containment $\mathcal{S}_\alpha \subseteq \mathcal{B}_\alpha$ is, in fact, an equality. We can thus reframe our main problem as follows: classify the cycle types α such that $\mathcal{S}_\alpha = \mathcal{B}_\alpha$, and for the remaining cycle types α, determine the complement $\mathcal{B}_\alpha \setminus \mathcal{S}_\alpha$. The main result of this paper solves this problem in the case $r = 2$, that is, when $\alpha = (\alpha_1, \alpha_2)$. Namely, if n is odd, then $\mathcal{S}_\alpha = \mathcal{B}_\alpha$. If n is even, then $\mathcal{S}_\alpha = \mathcal{B}_\alpha$ unless α is one of five types. The exceptional α are $(n-1, 1)$, $\big(\frac{n}{2}, \frac{n}{2}\big)$ with $4 \mid n$, $\big(\frac{n}{2}, \frac{n}{2}\big)$ with $4 \nmid n$, $(4, 2)$, and $(5, 3)$. In these case, respectively, $\mathcal{B}_\alpha \setminus \mathcal{S}_\alpha$ is $\{\big(\frac{n}{2}, \frac{n}{2}\big)\}$, $\{(n-2, 1, 1),\ (3, 1, \ldots, 1)\}$, $\{(n-2, 1, 1)\}$, $\{(2, 2, 2)\}$, and $\{(2, 2, 2, 2)\}$.

Stable Higher Specht Polynomials and Representations of Finite and Infinite Symmetric Groups

Shaul Zemel
Hebrew University of Jerusalem, Israel
shaul.zemel@mail.huji.ac.il

We show how to normalize the higher Specht polynomials of Ariki, Terasoma, and Yamada in a compatible way in order to define a stable version of these polynomials, as eventually symmetric functions. We also decompose the non-transitive actions of Haglund, Rhoades, and Shimozono into orbits, and show how the associated basis of higher Specht polynomials of Gillespie and Rhoades respects that decomposition. We also generalize these higher Specht polynomials in a way that produces several decompositions of the space of homogeneous polynomials of degree d in n variables into irreducible representations of S_n, each natural for its own reasoning. Finally, we use them to determine the maximal completely reducible sub-representation of the infinite symmetric group on polynomials and on eventually symmetric functions, as well as a conjectural filtration on these full representations, with maximal completely reducible quotients.

Automorphism actions with nilpotent non-commutative coefficient group, constructed via cohomology

Assaf Goldberger
Tel-Aviv University, Israel
assafg@tauex.tau.ac.il

Automorphism groups of weighing and Hadamard matrices, and other types of combinatorial actions, have been studied extensively. Objects like group-developed matrices, cocyclic matrices and group frames can be defined via selecting a suitbale group of automorphism symmetries. It is customary to discuss automorphism actions is term of projective monomial representations and centralizer algebras. In this talk we sketch another interpretation of automorphisms in terms of group cohomology. These definitions extend naturally to matrices with non-commutative coefficients, and we show how to construct all matrices over any nilpotent coefficient group, given the underlying permutation action.

On Galois subcovers of the Hermitian curve

Arianna Dionigi
University of Perugia - Department of Mathematics and Computer Science
ariannadionigi.98@libero.it
Joint work with Barbara Gatti

A problem of current interest, also motivated by applications to Coding theory, is to find explicit equations for *maximal* curves, that are projective, geometrically irreducible, non-singular curves defined over a finite field $\mathbb{F}_{q^2}$ whose number of $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound $q^2 + 2\mathfrak{g}q + 1$ where $\mathfrak{g}$ is the genus of the curve.
For curves which are Galois covered of the Hermitian curve, this has been done so far ad hoc, in particular in the cases where the Galois group has prime order and also when has order the square of the characteristic.
In this talk we will discuss explicit equations of all Galois covers of the Hermitian curve with Galois group of order dp where p is the characteristic of $\mathbb{F}_{q^2}$ and d is a prime other than p. We also compute the generators of the Weierstrass semigroup at a special $\mathbb{F}_{q^2}$-rational point of some of the curves.

Keywords: Maximal curves, Function fields, Galois cover, Weierstrass semigroup

Maximal Curves Over Finite Fields

Barbara Gatti
University of Salento & University of Basilicata
barbara.gatti@unisalento.it

A (projective, geometrically irreducible, non-singular) curve $\mathcal{X}$ defined over a finite field $\mathbb{F}_{q^2}$ is *maximal* if the number N_{q^2} of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound, that is $N_{q^2} = q^2+2\mathfrak{g}q+1$ where $\mathfrak{g}$ is the genus of $\mathcal{X}$. An important question, also motivated by applications to algebraic-geometry codes, is to find explicit equations for maximal curves. By a theorem of Serre, every curve which is covered over $\mathbf{F}_{q^2}$ by a $\mathbf{F}_{q^2}$-maximal curve is also $\mathbf{F}_{q^2}$-maximal. Serre's theorem has given an impulse to the study of explicit equations for maximal curves covered by the Hermitian curve. For curves of high genera which are Galois covered of the Hermitian curve, this has been done so far in the cases where the Galois group has prime order, or has order the square of the characteristic, or has order the product of the characteristic and another prime. In this talk we exhibit these explicit equations and make some remarks. For the case of genus $\mathfrak{g} = \frac{1}{8}(q-1)^2$ where $q \equiv 1 \pmod 4$ we show some new properties of the automorphism group, Weierstrass semigroup and Frobenius embedding.

References

[1] A. Cossidente, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, On plane maximal curves, *Compositio Math.* **121** (2000), 163–181.

[2] B. Gatti, G. Korchmáros, Galois subcovers of the Hermitian curve in characteristic p with respect to subgroups of order p^2, *Finite Fields and Their Applications*, **98**, (2024).

[3] A. Dionigi, B. Gatti, Galois subcovers of the Hermitian curve in characteristic p with respect to subgroups of order dp with $d \neq p$ prime, A. Dionigi, B. Gatti, https://arxiv.org/pdf/2405.20005 (to appear in Des. Codes Cryptogr.).

Rational points of weighted hypersurfaces over finite fields and an application to isogeny-based cryptography

Tony Shaska
Department of Mathematics and Statistics
Oakland University, Rochester, MI, 48309
shaska@oakland.edu

This talk investigates the number of rational points on weighted hypersurfaces over finite fields, focusing on the loci of genus 2 curves with (n, n)-split Jacobians. We build on previous work studying these varieties and explore upper bounds, modular congruences, and Serre-type inequalities in weighted projective space. Using explicit equations for these hypersurfaces, we analyze their structure and derive bounds that improve upon classical results.

The study of rational points on algebraic varieties over finite fields is a central theme in arithmetic geometry, with significant implications for cryptography. In [1], we explored the number of rational points on weighted projective varieties and Vojta's conjecture for such varieties and considered the weighted hypersurface in $\mathbb{P}_{\mathbf{w}}$, for $\mathbf{w} = (2, 4, 6, 10)$, namely the locus of genus 2 curves with extra automorphisms, and argued that it is more efficient to search for rational points in the weighted hypersurface rather than embed it into a projective variety and determine rational points there. For example, in [2], it was shown that this particular weighted hypersurface has no rational points of weighted height ≤ 2, a result that would have been much harder to prove if it were considered as a projective hypersurface.

The example above is of particular interest in isogeny-based cryptography since every point in it corresponds to a genus 2 curve with a $(2, 2)$-split Jacobian. In general, the locus of genus 2 curves with (n, n)-split Jacobians for odd n, denoted by $\mathcal{L}_n$, is a weighted hypersurface in the weighted projective space $\mathbb{P}_{\mathbf{w}}$ and has been the focus of very active research in recent years due to its applications in isogeny-based cryptography.

In this talk, we investigate the number of points of $\mathcal{L}_n$ over finite fields. We use specific equations of $\mathcal{L}_n$ and the methods in [1] to determine whether we can obtain bounds that improve upon the classical ones for such hypersurfaces. Given the growing interest in genus 2 isogeny-based cryptosystems, a precise analysis of rational points on these hypersurfaces over F_q provides valuable insights into the security and efficiency of these cryptographic constructions.

References

[1] Salami, Sajad, and Shaska, Tony *Vojta's conjecture on weighted projective varieties* Eur. J. Math. **11**, 1, Paper No. 12 (2025).

[2] Shaska, Elira, and Shaska, Tony *Machine learning for moduli space of genus two curves and an application to isogeny based cryptography* https://arxiv.org/abs/2403.17250 (2024)

Codes and Designs in Polar Spaces

Charlene Weiß
Faculty of Science, University of Amsterdam, Netherlands
chweiss@math.upb.de, c.weiss@uva.nl

A finite classical polar space of rank n is formed by the totally isotropic subspaces of a finite vector space equipped with a nondegenerate form, where n is the maximal dimension of such subspaces. In this talk, we will explore codes and designs in polar spaces and provide an overview of the current state of research in this area. Specifically, we will demonstrate how the theory of association schemes and linear programming can be used to establish bounds on the size of codes and prove nonexistence results for certain types of designs. Additionally, we will discuss how these linear programming bounds give Erdős-Ko-Rado type results. Finally, using a probabilistic method introduced by Kuperberg, Lovett, and Peled, we will establish the existence of t-(n, k, λ) designs in polar spaces of rank n with $k < n$.

Constructing affine $[3,1]$-avoiding sets from graphs and linear codes

Benedek Kovács
Eötvös Loránd University, Budapest, Hungary
benoke981@gmail.com
Joint work with Zoltán Lóránt Nagy

Our main motivating question is the following: in $\mathbb{F}_2^n$, the n-dimensional affine space over $\mathbb{F}_2$, if we are given a set S of size m, then is it necessarily true that there is an affine subspace $F_k \subseteq \mathbb{F}_2^n$ of dimension k (called a *k-flat*) intersecting S in exactly t points? If this holds for a quadruple (n,m,k,t), then we say that $[n,m] \to [k,t]$. In our previous work, we made the conjecture [3] that for every fixed pair (k,t), almost all values m satisfy $[n,m] \to [k,t]$ as $n \to \infty$. Using a combination of techniques such as Szemerédi's Cube Lemma [5, 1] and bounds on sizes of hypercube cuts [2], we proved that the conjecture is true for $t \in \{0, 2^{k-1}, 2^k\}$ and achieved some results in the cases $t = 2^\ell, 3 \cdot 2^\ell$ too (for $1 \le \ell \le k-2$).
In this talk we focus on constructing explicit $[3,1]$-*avoiding* sets in $\mathbb{F}_2^n$. An example is provided by unions of *quarter-spaces*, i.e. $(n-2)$-flats. This construction turns out to be very fruitful, as for any simple graph G on n vertices, we can get a $[3,1]$-avoiding set of size $2^n - I(G)$, where $I(G)$ is the number of independent vertex sets in G (also called the *Fibonacci number* of G, see [4]). This raises the question:
Question. Given an integer $n \ge 1$, let $f(n)$ denote the number of different values that $I(G)$ can take for an n-vertex graph G. Give bounds for $f(n)$ that are as tight as possible.
In this talk, we outline a proof that there exists a positive constant $C > 0$ with

$$2^{n-2^{C(\log n)^{1/2}}} \le f(n) \le 2^{n-0.2075\log_2 n}$$

for all n large enough, and accordingly show a lower bound for the number of values m with $[n,m] \not\to [3,1]$.
We construct another nice family of $[3,1]$-avoiding sets using binary linear codes as well, where we obtain explicit examples of exponentially many different sizes, with the sizes expressible using the weight enumerator polynomial of the code used.

References

[1] Bonin, J. E., Qin, H. (2000). Size functions of subgeometry-closed classes of representable combinatorial geometries. Discrete Mathematics, 224(1-3), 37-60.
[2] Hart, S. (1975). A note on the edges of the n-cube. Discrete Mathematics, Volume 14, Issue 2, 1976, 157-163.
[3] Kovács, B., & Nagy, Z. L. (2025). Avoiding intersections of given size in finite affine spaces $\mathrm{AG}(n,2)$. Journal of Combinatorial Theory, Series A, 209, 105959.
[4] Prodinger, H., & Tichy, R. F. (1982). Fibonacci numbers of graphs. The Fibonacci Quarterly, 20(1), 16-21.
[5] Setyawan, Y. (1998). Combinatorial Number Theory: Results of Hilbert, Schur, Folkman, and Hindman. Simon Fraser University.

New Geometric Large Sets

Michael Robert Hurley
State University of New York Oswego
michael.hurley@oswego.edu

Let V be an n-dimensional vector space over the field of q elements. By a *geometric* t-$[q^n, k, \lambda]$ design we mean a collection $\mathcal{D}$ of k-dimensional subspaces of V, called blocks, such that every t-dimensional subspace T of V appears in exactly λ blocks in $\mathcal{D}$. A *large set*, $LS\,[N]\,[t, k, q^n]$, of geometric designs is a collection of N disjoint t-$[q^n, k, \lambda]$ designs that partitions $\begin{bmatrix} V \\ k \end{bmatrix}$, the collection of k-dimensional subspaces of V. In this work we construct non-isomorphic large sets using methods based on incidence structures known as the Kramer-Mesner matrices. These structures are induced by particular group actions on the collection of subspaces of the vector space V. Subsequently, we discuss and use computational techniques for solving certain linear problems of the form $AX = B$, where A is a large integral matrix and X is a $\{0, 1\}$ solution. These techniques involve (i) lattice basis-reduction, including variants of the LLL algorithm, and (ii) linear programming. Inspiration came from the 2013 work of Braun, Kohnert, Östergard, and Wassermann, [1], who produced the first nontrivial large set of geometric designs with $t \geq 2$. Bal Khadka and Michael Epstein provided the know-how for using the LLL and linear programming algorithms that we implemented to construct the large sets.

2000 Mathematics Subject Classification: 05B25, 05B40, 05E18.
Key words. Geometric t-designs, large sets of geometric t-designs, t-designs over $GF(q)$, parallelisms, lattice basis reduction, LLL algorithm.

References

[1] M. Braun, A. Kohnert, P. Östergard, A. Wassermann, *Large Sets of t-Designs over Finite Fields*, JCTA 124 (2014), pp. 195-202.

Some Conjectures and Results on Tilings

Peter Horak
University of Washington, USA
horak@uw.edu

Tilings and tessellations belong to the oldest structures not only in geometry but in all mathematics. They have attracted the attention of best mathematicians. Even one of Hilbert's problems is on the topic. Tiling problems do not always have a geometric background, sometimes there is even an unexpected relation of tiling to other parts of mathematics. For example, the roots of the Minkowski conjecture on tiling the n-space by unit cubes can be traced to geometry of numbers and to positive definite quadratic forms; Hao Wang's work on tilings has been inspired by decision problems; there is a well-known relation of Penrose tilings to crystallography, etc.
As a short historical introduction, we present the conjecture of Minkowski. Its last open case was solved only 3 years ago.
Our interest in tilings stems from coding theory, especially from the area of error-correcting codes in Lee metric. Therefore, in this talk we will focus on tiling the n-space by unit cubes or by a cluster (the union) of unit cubes; a special attention will be paid to the famous and long-standing Golomb-Welch conjecture.

Highly symmetric Steiner and Kirkman triple systems

Tommaso Traetta
University of Brescia, Italy
tommaso.traetta@unibs.it

Steiner (STS) and Kirkman (KTS) triple systems have been extensively studied over the past 150 years, in light of their connections with geometry, group theory, finite fields and their applications to coding theory and cryptography. Nonetheless, some recent new applications [6] further highlight the strong benefits of working with systems having automorphisms [5] with a prescribed action.

In this talk, after surveying some of the most recent advances on Steiner and Kirkman triple systems, we focus our attention on the f-pyramidal ones, that is, those having an automorphism group fixing f points and acting sharply transitively on the remaining ones. Regular and 1-rotational STSs are examples of f-pyramidal systems with $f = 0$ or 1, respectively. We will present the latest progress concerning the existence of f-pyramidal STSs and KTSs [1, 2, 3, 4] and some new types of difference families and difference matrices which play a central role in our constructions.

References

[1] S. Bonvicini, M. Buratti, M. Garonzi, G. Rinaldi, T. Traetta, The first families of highly symmetric Kirkman Triple Systems whose orders fill a congruence class, Des. Codes Cryptogr. 89 (2021), 2725–2757.

[2] S. Bonvicini, M. Buratti, G. Rinaldi, T. Traetta, Some progress on the existence of 1-rotational Steiner triple systems, Des. Codes Cryptogr. 62 (2012), 63–78.

[3] M. Buratti, G. Rinaldi, T. Traetta, 3−pyramidal Steiner triple systems, Ars Math. Contemp. 13 (2017), 95–106.

[4] Y. Chang, T. Traetta, J. Zhou, On f-pyramidal Steiner triple systems over abelian groups, preprint.

[5] J. Doyen, W.M. Kantor, Automorphism groups of Steiner triple systems, Algebraic Combin. 5 (2022), 593–608.

[6] D. Lusi, C.J. Colbourn, The spectrum of resolvable Bose triple systems, Discrete Math. 346 (2023), 113396.

Study of symmetries of Latin squares by local permutation polynomials

Raúl M. Falcón
Universidad de Sevilla
rafalgan@us.es
Joint work with Jaime Gutiérrez and Jorge Jiménez-Urroz

A local permutation polynomial (LPP) in the polynomial ring $\mathbb{F}_q[x, y]$, with q a prime power, is a polynomial $\sum_{i,j=0}^{q-1} c_{i,j} x^i y^j \in \mathbb{F}_q[x, y]$ such that both polynomials $f(x, a)$ and $f(a, x)$ in $\mathbb{F}_q[x]$ act as permutations on $\mathbb{F}_q$ for every $a \in \mathbb{F}_q$ (see [3]). It is equivalent to a Latin square L_f of order q that is defined so that $L_f[i, j] = f(i, j)$ for all $i, j \in \mathbb{F}_q$. In cryptography, Latin squares and LPPs are used to generate pseudorandom sequences with high period growth [2, 4].
The above mentioned equivalence among Latin squares and LPPs gives rise to a natural translation of notions and results on both theories [1]. This talk delves into this topic by focusing on the natural translation to LPPs of the concepts of isotopism, conjugation and paratopism of Latin squares. More specifically, we show how this translation makes much easier the study of symmetries of Latin squares, which play a relevant role in their enumeration and classification. Thus, for instance, we say that two LPPs f and g in $\mathbb{F}_q[x, y]$ are isotopic if there exist three permutation polynomials $\pi_1, \pi_2, \pi_3 \in \mathbb{F}_q[x]$ such that

$$f(\pi_1(x), \pi_2(y)) = \pi_3(g(x, y)). \tag{0.1}$$

They are principal isotopic if $\pi_3(x) = x$, the trivial permutation in $\mathbb{F}_q[x]$. Then, every LPP over $\mathbb{F}_2[x, y]$ and $\mathbb{F}_3[x, y]$ is principal isotopic to $x + y$.

References

[1] J. Gutiérrez and J. Jiménez Urroz. Local permutation polynomials and the action of e-Klenian groups. *Finite Fields Appl.* **91**: paper 102261, 2023.

[2] N. A. Moldovyan, A. V. Shcherbacov and V. A. Shcherbacov. Some applications of quasigroups in cryptology. *Comput. Sci. J. Moldova* **24**: 55–67, 2016.

[3] G.L. Mullen. Local permutation polynomials over $\mathbb{Z}_p$. *Fibonacci Q.* **18**: 104–108, 1980.

[4] G.L. Mullen. Permutation polynomials and nonsingular feedback shift registers over finite fields. *IEEE Trans. Inform. Theory* **35**: 900–902, 1989.

Coloring Latin squares by paratopisms

Manuel González-Regadera
Universidad de Sevilla
manuelgonzalezregadera@gmail.com
Joint work with Raúl M. Falcón and María Dolores Frau

Let S_n be the symmetric group on the set $[n] := \{1, \ldots, n\}$. Two Latin squares L_1 and L_2 with entries in $[n]$ are paratopic if there exist a permutation $\pi \in S_3$ and a triple $f := (f_1, f_2, f_3) \in S_n \times S_n \times S_n$ such that $L_2\left[f_{\pi(1)}(e_{\pi(1)}),\ f_{\pi(2)}(e_{\pi(2)})\right] = f_{\pi(3)}(e_{\pi(3)})$ whenever $L_1[e_1, e_2] = e_3$. The pair $(\pi; f)$ is then a paratopism from L_1 to L_2. It is an isotopism if π is the trivial permutation; and an isomorphism if besides, $f_1 = f_2 = f_3$. Further, the pair $(\pi; f)$ is an autoparatopism if $L_1 = L_2$. (This is an autotopism if π is trivial.) It is known [3] that every autoparatopism is conjugate to either an isotopism or a paratopism of the form $((12);\ (\mathrm{Id}_n, f_2, f_3))$ or $((123);\ (\mathrm{Id}_n, \mathrm{Id}_n, f_3))$.
The set of autoparatopisms of a Latin square is a group acting on its cells, which can be colored according to the corresponding orbits. In this talk we show how this coloring only depends on both the isomorphism class of the Latin square, and the conjugate class of the autoparatopism under consideration. Then, we show how the study of feasible colorings makes much easier the problem of computing critical sets of Latin squares having a given paratopism of the form $((123);\ (\mathrm{Id}_n, \mathrm{Id}_n, f_3))$ in their autoparatopism group. This problem generalizes that one concerning critical sets of Latin squares having a given isotopism in their autotopism group, which has completely been solved for Latin squares of order up to five [2], and also for order up to six when the mentioned autotopism is trivial [1]. In cryptography, these problems play a relevant role to define new secret sharing schemes.

References

[1] P. Adams, R. Bean and A. Khodkar. A census of critical sets in the Latin squares of order at most six. *Ars Comb.* **68**: 203–223, 2003.

[2] R. M. Falcón, L. Johnson and S. Perkins. A census of critical sets based on non-trivial autotopisms of Latin squares of order up to five. *AIMS Math.* **6**: 261–295, 2021.

[3] Mendis, M. J. L., Wanless, I. Autoparatopisms of quasigroups and Latin squares. *J. Comb. Des.* **25**, 51–74, 2017.

Local permutation polynomials and Latin hypercubes

Jaime Gutierrez
Universidad de Cantabria
jaime.gutierrez@unican.es
Joint work with Raúl M. Falcón and Jorge Jiménez-Urroz

There is a bijective map between n-dimensional Latin hypercubes of order a prime power q and local permutation polynomials in n variables with coefficients in the finite field $\mathbb{F}_q$ of degree smaller than q in each variable. In this talk, I will study how the algebraic variety described by the set of coefficients of these polynomials allows the establishment of new approaches to the problems of counting, enumerating and classifying Latin hypercubes. I will also analyse the set of orthogonal Latin hypercubes and its relation to an orthogonal system of polynomials.

The work discussed in this talk is a joint work with Raúl M. Falcón and Jorge Jiménez-Urroz.

References

[1] Falcón, R., Gutierrez, J., Urroz, J. An algebraic approach to Latin hypercubes by LPPs over finite fields. *Preprint(2023), Universidad de Sevilla*

[2] Gutierrez, J., Urroz, J. Local permutation polynomials and the action of e-Klenian groups, *Finite Fields Appl.* **91** (2023), paper 102261.

[3] McKay, B.D., Wanless, I.M. A census of small Latin hypercubes, *SIAM J. Discrete Math.* **22** (2008), 719–736.

[4] Laywine, C., Mullen, G. Discrete Mathematics Using Latin Squares, *John Wiley and Sons*, Inc., New York, 1998.

[5] H. Niederreiter, Permutation polynomials in several variables over finite fields, Proc. Jpn. Acad. 46 (1970) 1001-1005.

Locating single Failure Inducing t-way Interactions with 0^t-Locating Arrays

Ludwig Kampel, Irene Hiess, Marlene Koelbing, Michael Wagner, and Dimitris Simos
MATRIS Research Group, SBA Research, Floragasse 7, 1040 Vienna, Austria
AAAM Research, Assoc. for Advancing Applications of Mathematics,
Schliemanngasse 9, 1210 Vienna, Austria
lkampel@sba-research.org

Abstract

Covering arrays are combinatorial designs that find application in (combinational) Combinatorial Testing, where a tester is faced with the problem of detecting all failures of a so-called *System Under Test* whose input is represented by (row) vectors, where it is assumed that the failures of the SUT are due to certain sub-combinations of its input vectors. The tester can only select the test vectors and observe the result (failure or non-failure) of each test.

Locating arrays are combinatorial designs that find application in Combinatorial Testing - Fault Localization, where the tester has to select the test vectors in such a way that it is also possible to identify *which* sub-combination of the input vectors trigger a failure of the SUT.

We propose 0^t*-locating arrays* which can be applied for *adaptive* Combinatorial Testing - Fault Localization, where a tester is allowed to perform two (or more) rounds of testing. We motivate the study of these objects through their application in (Software) Testing. After defining the notion of 0^t-Locating Arrays, we establish links to existing combinatorial designs, but also show that the notion of 0^t-Locating Arrays can be distinguished from these by formulating basic properties.

Keywords: Combinatorial Testing - Fault Localization, Locating Arrays, Superimposed Codes, Cover-Free Families

Introduction In (combinational) Combinatorial Testing (CT) we are faced with the problem of testing a so-called *System Under Test* (SUT) whose input is represented by (row) vectors. An introduction to CT can be found in [1]; see also [2]. The underlying assumption of CT is that misbehavior of the SUT, i.e. its *failure* is due to certain sub-combinations of its input vectors. The *goal of CT* is to detect such misbehavior by means of a set of input vectors, called *test suite* and their respective testing results, which come from the execution of the input vectors on the SUT and their annotation according to whether the SUT results in failure or not. Combinatorial Design Theory offers a solution to this problem, see for example [2], based on the notion of *Covering Arrays* [3], [4], and generalizations thereof. A covering array of strength t over a v-ary alphabet is an $N \times k$ array, denoted as $\mathsf{CA}(N; t, k, v)$, with the property that in any $N \times t$ sub-array each v-ary t-tuple appears *at least once as a row*. Covering arrays can therefore be understood as a generalization of orthogonal arrays [5]. A selection of t columns of an array, together with a v-ary t-tuple is also called a *t-way interaction*, and is formally denoted as a set of pairs $\{(u_1, p_1), \ldots, (u_t, p_t)\}$, where $u_i \in \{0, \ldots, v-1\}$ represent the v-ary values and the pairwise disjoint p_i represent the t different columns. We say that a covering array $\mathsf{CA}(N; t, k, v)$ *covers* all t-way interactions given appropriate number of columns k and alphabet size v.

The goal of *Combinatorial Testing-Fault Localization* (CT-FLA) is to identify *which* sub-combinations (more precisely, which t-way interaction) of the input vectors trigger a misbehavior of the SUT. Again, this goal shall be achieved by means of a set of input vectors together with their annotation resulting from test execution. This means that the set of input vectors must obey the necessary combinatorial properties that allow to identify which t-way interactions trigger the failures of the SUT.

We can distinguish CT-FLA into *non-adaptive* methods, i.e., only a single set of test vectors can be applied to the SUT; and *adaptive* methods, where multiple rounds of testing can be done, i.e., test vectors can be selected based on the testing results of previous rounds.

Several combinatorial designs have been proposed to address the problem faced in non-adaptive CT-FLA. Among them are *locating arrays* and *detecting arrays* [6] or *error locating arrays* [7] as well as generalized notions, such as detecting arrays with constraints [8]. For example, (d,t)-*locating arrays* (d, t)-$\mathsf{LA}(N; t, k, v)$ are introduced in [6], as covering arrays that have the additional property that any

set of d different t-way interactions yields a unique set of rows where its elements are covered; refer to [6] for the precise definition.

Methods for adaptive CT-FLA are based on alternating rounds of test selection and test execution and use, for example, statistical ranking [9], [10], or follow a *one factor at a time* approach [11].

0^t-Locating Arrays We propose 0^t-locating arrays, which can be applied for *adaptive* CT-FLA, when a tester has to inspect an input vector that induces a failure of the SUT and wants to identify a *single* failure-inducing t-way interaction that is covered by the vector.

Definition 1 *A 0^t-locating array is a binary $N \times k$ array with the property that there are no two t-way interactions, whose values are all 0, that are covered by exactly the same rows of the array. More formally, let A denote an $N \times k$ array and τ, τ' denote t-way interactions $\tau = \{(0, p_1), \ldots, (0, p_t)\}$, $\tau' = \{(0, p'_1), \ldots, (0, p'_t)\}$, with $0 \leq p_1 < p_2 < \cdots < p_t \leq k$ and $0 \leq p'_1 < p'_2 < \cdots < p'_t \leq k$. Further, let $\rho_A(\tau)$ denote the set of rows of A that cover the t-way interaction τ. Then A is a 0^t-locating array (denoted as 0^t-LA(N;t,k)) if and only if,*

$$\forall\tau\forall\tau' \rho_A(\tau) = \rho_A(\tau') \Rightarrow \tau = \tau'.$$

Proposition 3 *We can show the following:*

1. *A $\mathsf{CA}(N; (t+1), k, 2)$ is a 0^t-LA(N;t,k).*
2. *A $(1, t+1)$-superimposed code family is a 0^t-LA(N;t,k).*
3. *Not every 0^t-LA(N;t,k) is a $(1, t+1)$-superimposed code.*

Related Work and Related Notions The proposed notion of 0^t-locating arrays is clearly related to other notions of combinatorial design theory that find application in combinatorial testing, such as the already mentioned covering arrays [3], as well as locating and detecting arrays [6] and further, for example, to *covering arrays on graphs* [12] and *partial covering arrays* [13]. However, as Proposition 3 indicates 0^t-LAs might be even more closely related to combinatorial designs appearing in combinatorial group testing [14], such as the already mentioned (w, r)-superimposed codes for $w = 1$ [15], respectively, to cover-free families [16], [17]. This does not come at a surprise, considering that the application of adaptive CT-FLA that motivates the study of 0^t-locating arrays, resembles a combinatorial group testing problem where defective items (failure-inducing t-way interactions) require to be identified and distinguished from non-defective ones.

References

[1] Kuhn, D.R., Kacker, R.N., Lei, Y.: Introduction to Combinatorial Testing, 1st edn. Chapman & Hall/CRC Innovations in Software Engineering and Software Development Series. Taylor & Francis, Boca Raton, FL, USA (2013)

[2] Hartman, A.: Software and hardware testing using combinatorial covering suites. In: Graph Theory, Combinatorics and Algorithms: Interdisciplinary Applications, pp. 237–266. Springer, Boston, MA (2005). https://doi.org/10.1007/0-387-25036-0_10

[3] Colbourn, C.J.: Combinatorial aspects of covering arrays. Le Mathematiche **LIX**(I-II), 125–172 (2004)

[4] Hartman, A., Raskin, L.: Problems and algorithms for covering arrays. Discrete Mathematics **284**(1), 149–156 (2004)

[5] Hedayat, A.S., Sloane, N.J.A., Stufken, J.: Orthogonal Arrays: Theory and Applications, 1st edn. Springer, New York (1999)

[6] Colbourn, C.J., McClary, D.W.: Locating and detecting arrays for interaction faults. Journal of Combinatorial Optimization **15**(1), 17–48 (2008)

[7] Martínez, C., Moura, L., Panario, D., Stevens, B.: Locating errors using elas, covering arrays, and adaptive testing algorithms. SIAM Journal on Discrete Mathematics **23**(4), 1776–1799 (2009)

[8] Jin, H., Shi, C., Tsuchiya, T.: Constrained detecting arrays: Mathematical structures for fault identification in combinatorial interaction testing. Information and Software Technology **153**, 107045 (2023) https://doi.org/10.1016/j.infsof.2022.107045

[9] Ghandehari, L.S., Lei, Y., Kung, D., Kacker, R., Kuhn, R.: Fault localization based on failure-inducing combinations. In: 2013 IEEE 24th International Symposium on Software Reliability Engineering (ISSRE), pp. 168–177 (2013). https://doi.org/10.1109/ISSRE.2013.6698916

[10] Sh. Ghandehari, L., Lei, Y., Kacker, R., Kuhn, R., Xie, T., Kung, D.: A combinatorial testing-based approach to fault localization. IEEE Transactions on Software Engineering **46**(6), 616–645 (2020) https://doi.org/10.1109/TSE.2018.2865935

[11] Niu, X., Nie, C., Leung, H., Lei, Y., Wang, X., Xu, J., Wang, Y.: An interleaving approach to combinatorial testing and failure-inducing interaction identification. IEEE Transactions on Software Engineering **46**(6), 584–615 (2020) https://doi.org/10.1109/TSE.2018.2865772

[12] Meagher, K., Stevens, B.: Covering arrays on graphs. Journal of Combinatorial Theory, Series B **95**(1), 134–151 (2005)

[13] Sarkar, K., Colbourn, C.J., De Bonis, A., Vaccaro, U.: Partial covering arrays: Algorithms and asymptotics. Theory of Computing Systems **62**(6), 1470–1489 (2018) https://doi.org/10.1007/s00224-017-9782-9

[14] Du, D.-Z., Hwang, F.K.-m.: Combinatorial Group Testing and Its Applications vol. 12. World Scientific, Singapore (1999)

[15] Kim, H.K., Lebedev, V.: On optimal superimposed codes. Journal of Combinatorial Designs **12**(2), 79–91 (2004) https://doi.org/10.1002/jcd.10056

[16] Füredi, Z.: On r-cover-free families. J. Comb. Theory Ser. A **73**(1), 172–173 (1996) https://doi.org/10.1006/jcta.1996.0012

[17] Stinson, D.R., Wei, R.: Generalized cover-free families. Discrete Mathematics **279**(1), 463–477 (2004) https://doi.org/10.1016/S0012-365X(03)00287-5

On Boolean Degree 1 Functions, Anti-Designs, and Cameron-Liebler Sets in Finite Vector Spaces

Ferdinand Ihringer
Southern University of Science and Technology, China
Ferdinand.Ihringer@gmail.com

It is easy to see that if f is a real, n-variate affine function which is Boolean on the n-dimensional hypercube (that is, $f(x) \in \{0,1\}$ for $x \in \{0,1\}^n$), then $f(x) = 0$, $f(x) = 1$, $f(x) = x_i$ or $f(x) = 1 - x_i$. The same classification holds if we restrict $\{0,1\}^n$ to elements with Hamming weight k if $n - k, k \geq 2$. Here the concept corresponds to an anti-design.
Let $V(n,q)$ denote the n-dimensional vector space over the field with q elements. Since work by Cameron and Liebler in 1982, it has been asked if a similar classification holds for k-spaces in $V(n,q)$. It is known due to the work by Drudge (1998) and subsequent work that for $(n,k) = (4,2)$ such a classification is impossible. In our talk we will discuss the history of the problem. Furthermore, we will show that for fixed $q, k \geq 2$ and n sufficiently large, a Boolean degree 1 function on the k-spaces of $V(n,q)$ corresponds to one of the following:

1. The empty set.
2. All k-spaces through a fixed 1-space P.
3. All k-spaces in a fixed hyperplane H.
4. The union of the previous two examples when P is not in H.
5. The complement of any of the previous cases.

The solves the classification problem of Cameron-Liebler classes asymptotically.

Combinatorial characterizations of ovoidal cones

Bart De Bruyn
Ghent University, Belgium
Bart.DeBruyn@UGent.be
Joint work with Geertrui Van de Voorde

For a solid Π in the projective space $\mathrm{PG}(4,q)$, an ovoid O in $\Pi \cong \mathrm{PG}(3,q)$ and a point $x \in \Pi$, the set of points obtained by joining x with the points of O is called an *ovoidal cone*. We will characterise ovoidal cones by their intersection numbers. Specifically, we show that a set of points of $\mathrm{PG}(4,q)$ which blocks all planes and intersects solids in $q+1$, q^2+1 or q^2+q+1 points is a plane or an ovoidal cone, and determine all examples that arise when the blocking condition is omitted.

References

[1] B. De Bruyn and G. Van de Voorde. Characterising ovoidal cones by their hyperplane intersection numbers. *J. Combin. Des.* 33 (2025), 5–26.

Maximal cliques in the collinearity graphs of geometries of simplex codes

Adam Tyc
University of Warmia and Mazury in Olsztyn, Poland
adam.tyc@matman.uwm.edu.pl
Joint work with Mark Pankov

We consider the point-line geometry whose maximal singular subspaces correspond to q-ary simplex codes of dimension k. It follows from Fisher's inequality that maximal cliques in the collinearity graph of this geometry contain at most $n = (q^k - 1)/(q - 1)$ elements and maximal singular subspaces are n-cliques of this graph. If $q = 2$, then $n = 2^k - 1$ and there is a one-to-one correspondence between $(2^k - 1)$-cliques of the collinearity graph and symmetric $(2^k - 1, 2^{k-1}, 2^{k-2})$-designs. For the case when $q \geq 5$ there is a class of n-cliques distinct from maximal singular subspaces. In the case when $k = 2$, some of these cliques are normal rational curves.

Neighborhoods of Vertices in the Isogeny Graph of Principally Polarized Superspecial Abelian Surfaces

Zijian Zhou
National University of Defence Technology, China
zhouzijian.edu@gmail.com

Supersingular isogeny-based cryptography has emerged as a promising candidate for post-quantum cryptographic systems. The security of these systems relies on the difficulty of finding paths in isogeny graphs between supersingular elliptic curves, even for quantum computers. Recent advances have extended these cryptographic constructions to higher-dimensional abelian varieties, such as superspecial abelian surfaces, which offer new opportunities for cryptographic applications.
In [2], Xu et al. proved the graph's structure for supersingular elliptic curves. In this talk, we generalize the study of isogeny graphs from elliptic curves to abelian surfaces, focusing on the structure of the (ℓ, ℓ)-isogeny graph of principally polarized superspecial abelian surfaces (PPSSAS). Particularly, we study the local structure of vertices $[E \times E']$ in this graph, where at least one of the elliptic curves E or E' is defined over the finite field $\mathbb{F}_p$.
We provide a detailed analysis of the geometric properties of these vertices within the isogeny graph. Specifically, we present a complete classification of the loops and neighborhoods of vertices $[E \times E']$ in the (ℓ, ℓ)-isogeny graph, extending previous work on elliptic curves to higher-dimensional abelian varieties. We also give explicit constructions of isogenies and their kernels, which reveal the underlying algebraic and geometric structures of the graph.

References

[1] Zheng Xu, Yi Ouyang, and Zijian Zhou. Neighborhood of vertices in the isogeny graph of principally polarized superspecial abelian surfaces. *Finite Fields and Their Applications*, 103:102579, 2025.

[2] S. Li, Y. Ouyang, Z. Xu, Neighborhood of the supersingular elliptic curve isogeny graph at $j = 0$ and 1728, *Finite Fields and Their Applications*, 61 (2020), 101600.

[3] Y. Ouyang, Z. Xu, Loops of isogeny graphs of supersingular elliptic curves at $j = 0$, *Finite Fields and Their Applications*, 58 (2019), 174-176.

[4] D. Mumford, Abelian Varieties. *Tata Institute of Fundamental Research Studies in Mathematics*, vol. 5 (2008). Tata Institute of Fundamental Research, Bombay.

New constructions for orientable sequences

Chris J. Mitchell and Peter R. Wild
Royal Holloway, University of London
me@chrismitchell.net

Orientable sequences of order n are infinite periodic sequences with symbols drawn from a finite alphabet of size k with the property that any particular subsequence of length n occurs at most once in a period *in either direction*. They were introduced in the early 1990s [2, 3] in the context of possible applications in position sensing. Gabrić and Sawada [4] provide an interesting discussion of further possible applications as well as their relationship to strings relevant to DNA computing. Bounds on the period for such sequences [1] and a range of methods of construction have been devised although, apart from very small cases, a significant gap remains between the largest known period for such a sequence and the best known upper bound.

We give a new general method of construction for orientable sequences using graph-theoretic techniques, involving subgraphs of the de Bruijn graph with special properties. We then describe two different approaches for generating such subgraphs. This enables us to construct orientable sequences with periods meeting the upper bound when $n = 2$ and $n = 3$ (k odd), as well as sequences with period very close to the bound for $n = 3$ and k even. For $4 \leq n \leq 8$, in some cases the sequences produced have periods larger than for any previously known sequences.

References

[1] A. Alhakim, C. J. Mitchell, J. Szmidt, and P. R. Wild, *Orientable sequences over non-binary alphabets*, Cryptography and Communications **16** (2024), 1309–1326.

[2] J. Burns and C. J. Mitchell, *Coding schemes for two-dimensional position sensing*, Cryptography and Coding III (M. J. Ganley, ed.), Oxford University Press, 1993, pp. 31–66.

[3] Z.-D. Dai, K. M. Martin, M. J. B. Robshaw, and P. R. Wild, *Orientable sequences*, Cryptography and Coding III (M. J. Ganley, ed.), Oxford University Press, Oxford, 1993, pp. 97–115.

[4] D. Gabrić and J. Sawada, *Constructing k-ary orientable sequences with asymptotically optimal length*, Designs, Codes and Cryptography **93** (2025), to appear.

On the Buratti-Horak-Rosa Conjecture for Small Supports

Onur Ağırseven
UNAFFILIATED (USA/TURKEY)
onura.marlboro.edu@gmail.com
Joint work with M. A. Ollis, Emerson College, USA

Label the vertices of the complete graph K_v with the integers $\{0, 1, \ldots, v-1\}$ and define the *length* ℓ of the edge between distinct vertices labeled x and y by $\ell(x, y) = \min(|y - x|, v - |y - x|)$. A *realization* of a multiset L of size $v - 1$ is a Hamiltonian path through K_v whose edge labels are L. The *Buratti-Horak-Rosa (BHR) Conjecture* is that there is a realization for a multiset L with support contained in $\{1, 2, \ldots, \lfloor \frac{v-1}{2} \rfloor\}$ if and only if for any divisor d of v the number of multiples of d in L is at most $v - d$. We use "grid-based graphs", which are useful for constructing particular types of realizations, called "linear realizations," especially when the multiset in question has at most three distinct elements [1, 2, 3]. Our current focus is mainly on multisets with support of the form $\{1, x, y\}$, for which we had previously constructed standard linear realizations when $y - x \leq 2$, including all cases when the number of 1-edges is at least y [1, 3]. We will present our recent results extending these constructions to many cases with $y - x > 2$. These constructions considerably extend the parameters for which the BHR Conjecture is known to hold.

MSC2020: 05C38, 05C78
Keywords: complete graph, Hamiltonian path, edge-length, realization, grid-based graph.

References

[1] O. Ağırseven and M. A. Ollis, Grid-based graphs, linear realizations and the Buratti-Horak-Rosa Conjecture, *submitted*, arXiv:2402.08736.

[2] O. Ağırseven and M. A. Ollis, A Coprime Buratti-Horak-Rosa Conjecture and Grid-Based Linear Realizations, *submitted*, arXiv:2412.05750.

[3] O. Ağırseven and M. A. Ollis, Construction Techniques for Linear Realizations of Multisets with Small Support, *submitted*, arXiv:2502.00164.

Designs of perfect matchings

Lukas Klawuhn
Paderborn University
klawuhn@math.upb.de
Joint work with John Bamberg

It is well-known that the complete graph K_{2n} on $2n$ vertices can always be decomposed into perfect matchings, called a 1-factorisation. In such a decomposition, every edge of K_{2n} appears in exactly 1 perfect matching. This was generalised by Jungnickel and Vanstone to *hyperfactorisations*. These are sets of perfect matchings such that every pair of disjoint edges of K_{2n} appears in a constant number of perfect matchings. Hyperfactorisations are examples of Cameron's partition systems and were rediscovered by Stinson who called them *hyperresolutions*. We generalise all these ideas to λ-factorisations of K_{2n} and characterise them algebraically as Delsarte designs in an association scheme using the theory of Gelfand pairs. We use this characterisation to derive divisibility conditions and non-existence results. Furthermore, we explore a connection to finite geometry, giving rise to explicit constructions of λ-factorisations.

This is joint work with John Bamberg (University of Western Australia). It is based on ideas developed together with Kai-Uwe Schmidt.

Quasi-strongly regular digraphs and new strongly regular digraph with parameters $(165, 60, 36, 23, 21)$

Vedrana Mikulić Crnković
University of Rijeka - Faculty of mathematics
vmikulic@math.uniri.hr
Joint work Matea Zubović Žutolija

In this talk we present a method for constructing regular digraphs from a transitive permutation group, which is a generalisation of a construction method described in [1]. We use this method to construct directed quasi-strongly regular graphs from transitive permutation groups of degree up to 30. To illustrate how the construction method works, we prove the existence of a directed strongly regular graph with parameters $(165, 60, 36, 23, 21)$ and describe the construction of two non-isomorphic digraphs with the given parameters.

Keywords: 1-design, strongly regular digraph, quasi-strongly regular digraph, transitive permutation group

References

[1] D. Crnković, V. Mikulić Crnković and A. Švob. On some transitive combinatorial structures constructed from the unitary group $U(3, 3)$. *J. Statist. Plann. Inference*, **144**:19-40, 2014.

Further results on decomposition of low degree circulant graphs into cycles

Juliana Palmen
AGH University of Krakow
jpalmen@agh.edu.pl

A *decomposition* of a graph G is a collection of edge-disjoint subgraphs $H_1, H_2, \ldots, H_t$ of G such that each edge of G belongs to exactly one H_i. We call this collection a *k-factorization* when every H_i is a k-regular spanning subgraph of G.
For a positive integer n and a set $S \subseteq \{1, \ldots, \lfloor(\frac{n}{2}\rfloor)\}$ a *circulant* $C(n, S)$ is a graph $G = (V, E)$ such that $V = \mathbb{Z}_n$ and $E = \{\{u, v\} : \delta(u, v) \in S\}$ where $\delta(u, v) = min\{\pm|u - v| \pmod n\}$.
Some results on decomposition of those graphs into cycles were obtained. Inspired by the work of Bryant and Martin [1], who gave a complete solution for the cycle decomposition of $C(n, \{1, 2\})$, we examine the case when $S = \{1, 3\}$. Among others, we present the results on decomposition of $C(n, \{1, 3\})$ into cycles of odd lengths and into cycles of even lengths.
In [2] Bryan showed that, whenever $n \geq 5$, there exists a 2-factorization of $C(n, \{1, 2\})$ in which one factor is a Hamiltonian cycle and the other factor is isomorphic to any given 2-regular graph of order n. We discuss some open problems concerning the 2-factorization of $C(n, \{1, 3\})$.

References

[1] E. D. Bryant, and G. Martin, Some results on decompositions of low degree circulant graphs, Australas. J Comb. 45 (2009): 251-262.

[2] D. Bryant, Hamilton cycle rich two-factorizations of complete graphs, Journal of Combinatorial Designs 12.2 (2004): 147-155.

Cover-free Families on Graphs

Prangya Parida
University of Ottawa, Canada
ppari017@uottawa.ca
Joint work with Lucia Moura

A family of subsets of a t-set is called a *d-cover-free family* if no subset in the family is contained in the union of any d other subsets. We denote by $t(d, n)$ the minimum t for which there exists a d-cover-free family of a t-set with n subsets. Cover-free families (CFFs) have wide applications in combinatorial group testing, where a d-CFF(t, n) can be used to identify d defective items in a group of n items with t tests [2]. It is well known that $t(1, n)$ can be obtained by applying the famous Sperner's theorem [3]. For $d \geq 2$, we rely on bounds for $t(d, n)$. Erdős, Frankl, and Füredi [8] provided bounds for $t(2, n)$ using the probabilistic method, given by $3.106 \log(n) < t(2, n) < 5.512 \log(n)$. Using a derandomization technique, Porat and Rothschild [1] presented a deterministic polynomial-time algorithm to construct d-CFFs that achieves $t = O(d^2 \log(n))$. Some upper bounds on $t(2, n)$, and in some cases exact bounds for small values of n, were provided by Li, van Rees, and Wei [4] in 2006.

In this talk, we use a graph G to extend the definition of a cover-free family, where vertices correspond to elements of a family of subsets of a t-set and the edges of G impose constraints on pairs of corresponding subsets. Specifically, a family of subsets of a t-set is a G-CFF if, for every edge $\{A, B\}$ in G, the union of the subsets corresponding to A and B does not cover any other subset in the family. A family of subsets of a t-set is a G-in-CFF if, for every edge $\{A, B\}$ in G, the subsets corresponding to A and B are not mutually contained in each other. We define a $\overline{G}$-CFF as a family that is both a G-CFF and a G-in-CFF. We denote by $t(G)$, $t_e(G)$, and $t_{in}(G)$ the minimum value of t for which there exists a $\overline{G}$-CFF, a G-CFF, and a G-in-CFF, respectively. The traditional 2-CFF(t, n) is a special case of a $\overline{G}$-CFF when $G = K_n$. This generalization of cover-free families provides a richer combinatorial structure that lies between being a 1-CFF and a 2-CFF. Using a technique involving vertex coloring, Idalino and Moura [5] showed that for a graph with chromatic number $\chi(G)$ and n vertices, $t(G) \leq \chi(G) \log(n)$.

We will discuss some classical results on cover-free families, along with general constructions of $\overline{G}$-CFFs and specific constructions for certain families of graphs. We prove that for a graph G with n vertices, $t(1, n) \leq t(G) \leq t(2, n)$, and show that for an infinite family of star graphs S_n with n vertices, $t(S_n) = t(1, n)$. Using a result from [6], we show that $t_{in}(G) = t(1, \chi(G))$. Interestingly, we construct CFFs on paths (P_n) and cycles (C_n) with n vertices using a mixed-radix Gray code [7]. This yields an upper bound for $t(P_n)$ and $t(C_n)$ that is smaller than the lower bound of $t(2, n)$ mentioned above and improves the upper bound obtained by vertex coloring, which is $2 \log(n)$. This is joint work with Lucia Moura.

References

[1] E. Porat and A. Rothschild, "Explicit nonadaptive combinatorial group testing schemes", *IEEE Transactions on Information Theory*, vol. 57, no. 12, pp. 7982–7989, 2011.

[2] F. K. Hwang and V. T. Sós, "Non-adaptive hypergeometric group testing", *Studia Scientiarum Mathematicarum Hungarica*, vol. 22, no. 1-4, pp. 257–263, 1987.

[3] E. Sperner, "Ein Satz über Untermengen einer endlichen Menge", *Mathematische Zeitschrift*, vol. 27, no. 1, pp. 544–548, 1928.

[4] P. C. Li, G. H. J. Van Rees, and R. Wei, "Constructions of 2-cover-free families and related separating hash families", *Journal of Combinatorial Designs*, vol. 14, no. 6, pp. 423–440, 2006.

[5] T. B. Idalino and L. Moura, "Group testing and Cover-free families on Hypergraphs", *In preparation*, 2024.

[6] R. P. Dilworth, "A decomposition theorem for partially ordered sets", *Classic Papers in Combinatorics*, pp. 139–144, 1987.

[7] D. E. Knuth, *The Art of Computer Programming, Volume 4A: Combinatorial Algorithms, Part 1*, Pearson Education India, 2011.

[8] P. Erdös, P. Frankl, and Z. Füredi, "Families of finite sets in which no set is covered by the union of two others", *Journal of Combinatorial Theory, Series A*, vol. 33, no. 2, pp. 158–166, 1982.

2-Designs admitting a flag-transitive automorphism group

Alessandro Montinaro
University of Salento (Italy)
Department of Mathematics and Physics "E. De Giorgi"
alessandro.montinaro@unisalento.it

A 2-(v, k, λ) *design* $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ consists of a set $\mathcal{P}$ of v *points* and a set $\mathcal{B}$ of *blocks* such that each block is a k-subset of $\mathcal{P}$ and each pair of distinct points is contained in exactly λ blocks. A *flag* of $\mathcal{D}$ is an incident point-block pair, and a group G of automorphisms of $\mathcal{D}$ is *flag-transitive* if it acts transitively on the set of flags. Such a group G is transitive on both $\mathcal{P}$ and $\mathcal{B}$. Also, G is said to be *point-imprimitive* if it leaves invariant a partition of the point set $\mathcal{P}$ in classes of size c with $1 < c < v$, and *point-primitive* otherwise.
If $\lambda = 1$, then G acts point-primitively on $\mathcal{D}$ by a celebrated result of Higman and McLaughlin [5], and a classification of such 2-designs was achieved by Buekenhout et al. in [4] except when v is a power of a prime and $G \leq A\Gamma L_1(v)$.
If $\lambda > 1$, there are many known families of flag-transitive point-imprimitive 2-designs. Recently, as an effort of several authors [1, 2, 3, 6, 7, 8, 9], a classification of flag-transitive 2-designs with $\lambda = 2$ has been achieved except when v is a power of a prime and $G \leq A\Gamma L_1(v)$.
In my talk, I will give an overview on flag-transitive 2-designs, both in the primitive and imprimitive case, present some constructions, and provide some recent classification results.
The talk is based on joint works with S. H. Alavi, M. Bayat, A. Daneshkhakh, H. Liang, C. E. Praeger, Y. Zhao, Z. Zhang and S. Zhou.

Keywords: Flag-transitive designs, 2-designs, permutation groups.

References

[1] H. Alavi, M. Bayat, A. Daneshkhah, M. Tadbirinia, Classical groups as flag-transitive automorphism groups of 2-designs with $\lambda = 2$, *J. Combin. Theory Ser. A* **206**: 105892, (2024).

[2] S. H. Alavi, almost simple groups as flag-transitive automorphism groups of 2-designs with $\lambda = 2$, *https://doi.org/10.48550/arXiv.2307.05195*.

[3] A. Devillers, H. Liang, C. E. Praeger, B. Xia, On flag-transitive 2-$(v, k, 2)$ design, *J. Combin. Theory Ser. A* **177**: 105309, (2021).

[4] F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck, J. Saxl, Linear spaces with flag-transitive automorphism groups, *Geom. Dedicata* **36**: 89–94, (1990).

[5] D. G. Higman and J. E. McLaughlin, Geometric ABA-Groups, *Illinois J. Math.* **5**: 382–397, (1961).

[6] H. Liang, A. Montinaro, A Classification of the flag-transitive 2-$(v, k, 2)$ designs, *J. Combin. Theory Ser. A* **211**: 105983, (2025).

[7] H. Liang, S. Zhou, Flag-transitive point-primitive automorphism groups of non-symmetric 2-$(v, k, 2)$ designs, *J. Combin. Des.* **24**: 421–435, (2016).

[8] H. Liang, S. Zhou, Flag-transitive point-primitive non-symmetric 2-$(v, k, 2)$ designs with alternating socle, *Bull. Belg. Math. Soc. Simon Stevin* **23**: 559–571, (2016).

[9] A. Montinaro, Y. Zhao, Z. Zhang, S. Zhou, Design with a simple automorphism group, *Finite Fields Appl.* **99**: 102488, (2004).

One weight sum-rank metric codes

Usman Mushrraf
Università degli Studi della Campania "Luigi Vanvitelli"
usman.mushrraf@unicampania.it
Joint work with Ferdinando Zullo

Sum-rank metric codes have gained attention for their applications in network coding and other areas. These codes are also interesting as mathematical objects, they act as a bridge between the Hamming and rank metrics, which can be seen as special cases of the sum-rank metric. In this talk, we will explore linear sum-rank metric codes and examine important properties, such as one weight codes in various dimensions. We will use geometric tools to analyze and characterize classes of one-weight sum-rank metric codes.

Keywords: Sum-rank metric code; Linear set; One-weight code

Geometry of binary simplex codes and symmetric block designs

Krzysztof Petelczyc
University of Białystok (Poland) — Faculty of Mathematics
kryzpet@math.uwb.edu.pl
Joint work with Mark Pankov and Mariusz Żynel

Points of the projective space $\mathrm{PG}(n-1,2)$ can be naturally identified with non-empty subsets of an n-element set. Consider the subgeometry $\mathcal{P}_m(n)$ formed by all $2m$-element subsets. If $n = 2^k - 1$ and $m = 2^{k-2}$ for some integer $k \geq 3$, then maximal singular subspaces of this geometry correspond to binary simplex codes of dimension k.
For $k \geq 4$ the collinearity graph of $\mathcal{P}_m(n)$ contains maximal cliques that are not maximal singular subspaces. Moreover, if such a clique consists of n elements, then it determines a symmetric $(n, 2m, m)$-design isomorphic to the design of points and hyperplane complements of $\mathrm{PG}(k-1,2)$. We focus on so-called *centered* maximal cliques, that are unions of $2^{k-1} - 1$ lines passing through a common point. They can be constructed using bijections between two maximal $(2m-1)$-element cliques of $\mathcal{P}_{m/2}(2m-1)$. The main results concern the case $k = m = 4$. Then $\mathcal{P}_{m/2}(2m-1) = \mathcal{P}_2(7)$ is a rank 3 polar space and every maximal clique of the associated collinearity graph is a Fano plane. The classification of bijective maps of Fano planes gives rise to the classification of centered maximal 15-element cliques in the collinearity graph of $\mathcal{P}_4(15)$. This, together with a construction of a non-centered maximal 15-element clique, provides geometric interpretation of the five well-known symmetric $(15, 8, 4)$-designs.

Keywords: binary simplex code; Fano plane; symmetric block design.

Automorphisms of geometries related to binary equidistant codes

Mariusz Żynel
University of Białystok (Poland) — Faculty of Mathematics
mariusz@math.uwb.edu.pl
Joint work with Mark Pankov, Krzysztof Petelczyc

There are two notions of code equivalence. Two codes C_1, C_2 in a vector space V over a finite field are equivalent if either, there is a Hamming weight preserving semilinear isomorphism sending C_1 to C_2, or there is a monomial transformation of V sending C_1 to C_2. The MacWilliams extension theorem says that these two notions of equivalence are the same.
We consider the projective space $\mathcal{P}(V)$ over a vector space $V = \mathbb{F}_2^n$. Lines in $\mathcal{P}(V)$ are of size 3, so $\mathcal{P}(V)$ is a Steiner triple system. The standard basis of V is $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$. For every non-zero vector v of V we have $v = e_I = \sum_{i \in I} e_i$, where I is a non-empty subset of $[n] = \{1, 2, \ldots, n\}$. The i-th coordinate of e_I is either 1, if $i \in I$, or 0 otherwise. We write P_I for the point of $\mathcal{P}(V)$ corresponding to e_I. Its Hamming weight is $|I|$.
Now, let us fix a positive integer m with $3m \leq n$ and take those points of $\mathcal{P}(V)$ whose Hamming weight is $2m$. This set of points $\mathcal{P}_m$ can be considered a *point-line geometry* whose lines are those of the projective space $\mathcal{P}(V)$ contained in $\mathcal{P}_m$. The *Hamming distance* between any two distinct collinear points in $\mathcal{P}_m$ is $2m$. This class of geometries includes: the Pasch configuration ($n = 3m + 1 = 4$), the Cremona-Richmond configuration known also as the generalized quadrangle of type $2, 2$ ($n = 3m = 6$) and a polar space ($n = 4m - 1 = 7$).
We prove that in some non-trivial cases, there are automorphisms of the geometry $\mathcal{P}_m$ induced by a non-monomial semilinear automorphism of V.

Keywords: equidistant code, simplex code, Pasch configuration, Cremona-Richmond configuration, partial Steiner triple system

Optimal Multidimensional Convolutional Codes

Zita Abreu, Raquel Pinto, and Rita Simões
CIDMA – Center for Research and Development in Mathematics and Applications,
Department of Mathematics, University of Aveiro
zita.abreu@ua.pt

A one-dimensional (1D) convolutional code can be described as an $\mathbb{F}[z]$-submodule of $\mathbb{F}[z]^n$, where $\mathbb{F}[z]$ denotes the polynomial ring in a single indeterminate over the field $\mathbb{F}$. One significant advantage of convolutional codes is their enhanced error correction capabilities compared to block codes, especially in scenarios where data is transmitted in a continuous stream. The structure of convolutional codes allows the detection and correction of errors that may occur across multiple transmitted symbols, rather than being limited to fixed blocks. Notable contributions to the theory of convolutional codes were made by Forney, see [4, 5, 6]. The search for convolutional codes with optimal encoding and decoding properties remains an active area of research. An excellent introduction to convolutional codes can be found in the books [1, 2, 3].

Multidimensional (mD) convolutional codes extend the concept of convolutional codes to polynomial rings with multiple variables. Consider the polynomial ring $R = \mathbb{F}[z_1, \ldots, z_m]$ in m indeterminates over $\mathbb{F}$. An m-dimensional convolutional code of length n is defined as an R-submodule of R^n.

mD codes offer significant advantages in the transmission of multidimensional data. For instance, 2D convolutional codes are suited for applications such as transmitting images and videos as 2D data. The importance of 3D convolutional codes is also growing as 3D data transmission becomes more common. With the advancement of higher dimensional codes, we are confident that these applications will find more uses in the future.

While 1D convolutional codes have been extensively studied, 2D convolutional codes have received comparatively less attention. Fornasini and Valcher introduced 2D convolutional codes in [8, 9], and the authors in [10] established an upper bound for the free distance of 2D convolutional codes, along with optimal constructions. Additional studies on 2D convolutional code constructions can be found in [11, 12, 13]. In [20] the authors introduced the concept of column distance for delay-free 2D convolutional codes under certain restrictions. Later, in [21] the authors presented upper bounds on these distances and provide characterizations in terms of the properties of the sliding parity-check matrices of the code. These results led to the definition of the Maximum Separation Set Distance Profile for 2D convolutional codes.

Higher-dimensional convolutional codes have garnered even less research. mD convolutional codes were first introduced in [7, 14] and further examined in [15, 16, 17, 18, 19]. Key distinctions exist between 1D and 2D convolutional codes, as well as between 2D and mD codes, with $m \geq 3$, with these differences being thoroughly explored by Weiner in [7].

In this talk, we introduce the notion of free and column distances for mD convolutional codes. We derive a new upper bound for the free distance of and we introduce a novel construction for a 3D convolutional code with rate $\frac{1}{n}$ and degree $\delta \leq 2$. Additionally, we derive new upper bounds on the column distances, leading to the novel concept of the Maximum Separation Set Distance Profile for mD convolutional codes.

References

[1] R. Johannesson and K.S. Zigangirov, *Fundamentals of Convolutional Coding, Digital and Mobile Communication*. Wiley-IEEE Press, New Jersey, 1999.

[2] J. Lieb, R. Pinto, and J. Rosenthal, "Convolutional Codes", in *Concise Encyclopedia of Coding Theory*, C. Huffman, J. Kim, and P. Sole (eds.), CRC Press, 2021.

[3] S. Lin and D. Costello, *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, Englewood Cliffs, 1983.

[4] G. D. Forney, "Convolutional Codes I: Algebraic Structures", *IEEE Transactions on Information Theory*, vol. IT-16, no. 5, pp. 720–738, 1970.

[5] G. D. Forney, "Structural Analysis of Convolutional Codes via Dual Codes", *IEEE Transactions on Information Theory*, vol. IT-19, no. 5, pp. 512–518, 1973.

[6] G. D. Forney, "Convolutional Codes II: Maximum Likelihood Decoding", *Information and Control*, vol. 25, pp. 222–266, 1974.

[7] P. Weiner, *Multidimensional Convolutional Codes*. PhD thesis, University of Notre Dame, USA, 1998.

[8] M.E. Valcher and E. Fornasini, "On 2D Finite Support Convolutional Codes: An Algebraic Approach", *Multidimensional Systems and Signal Processing*, vol. 5, pp. 231–243, 1994.

[9] E. Fornasini and M.E. Valcher, "Algebraic Aspects of Two-Dimensional Convolutional Codes", *IEEE Transactions on Information Theory*, vol. 40, pp. 1068–1082, 1994.

[10] J.J. Climent, D. Napp, C. Perea, and R. Pinto, "Maximum Distance Separable 2D Convolutional Codes", *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 669–680, 2016.

[11] P. Almeida, D. Napp, and R. Pinto, "MDS 2D Convolutional Codes with Optimal 1D Horizontal Projections", *Designs, Codes and Cryptography*, vol. 86, pp. 285–302, 2018.

[12] P. Almeida, D. Napp, and R. Pinto, "From 1D Convolutional Codes to 2D Convolutional Codes of Rate $1/n$", in *Coding Theory and Applications*, R. Pinto, P. Rocha Malonek, and P. Vettori (eds.), Springer, CIM Series in Mathematical Sciences, vol. 3, 2015.

[13] J.J. Climent, D. Napp, C. Perea, and R. Pinto, "A Construction of MDS 2D Convolutional Codes of Rate $1/n$ Based on Superregular Matrices", *Linear Algebra and its Applications*, vol. 437, no. 3, pp. 766–780, 2012.

[14] H. Gluesing-Luerssen, J. Rosenthal, and P. Weiner, "Duality Between Multidimensional Convolutional Codes and Systems", in *Advances in Mathematical Systems Theory*, pp. 135–150, 2000.

[15] C. Charoenlarpnopparut, "Applications of Gröbner Bases to the Structural Description and Realization of Multidimensional Convolutional Codes", *ScienceAsia*, vol. 35, pp. 95–105, 2009.

[16] C. Charoenlarpnopparut and S. Tantaratana, "Algebraic Approach to Reduce the Number of Delay Elements in the Realization of Multidimensional Convolutional Codes", in *Proceedings of the 47th IEEE International Midwest Symposium Circuits and Systems (MWSCAS 2004)*, pp. 529–532, 2004.

[17] B. Kitchens, "Multidimensional Convolutional Codes", *SIAM Journal on Discrete Mathematics*, vol. 15, pp. 367–381, 2002.

[18] E. Zerz, "On Multidimensional Convolutional Codes and Controllability Properties of Multidimensional Systems over Finite Rings", *Asian Journal of Control*, vol. 12, no. 2, pp. 119–126, 2010.

[19] V. Lomadze, "Non-Catastrophicity in Multidimensional Convolutional Coding", *Discrete Mathematics*, vol. 343, 2020.

[20] D. Napp Avelli, C. Perea, and R. Pinto, "Column distances for 2D-convolutional codes", in *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS)*, pp. 377–102, 2010.

[21] J.I. Iglesias, D. Napp, C. Perea, R. Pinto, and R. Simões, "Separation set distance for 2D Convolutional Codes", in *Proceedings of the 23rd International Symposium on Mathematical Theory of Networks and Systems (MTNS)*, 2018.

The neighbor graph of binary Linear Complementary Dual Codes

Javier de la Cruz, Anna-Lena Horlemann, Marc Newman, Carlos Vela Cabello, Wolfgang Willems
St Gallen University, Switzerland
carlos.velacabello@unisg.ch

Linear complementary dual (LCD) codes were first proposed by Massey in [3]. An LCD code C is defined to be a linear code whose dual code $C^{\perp}$ satisfies that $C \cap C^{\perp} = \{\mathbf{0}\}$. In this same reference, the author proved LCD codes to be an optimal linear coding solution for the two-user binary adder channel. Furthermore, they are also presented as countermeasures to passive and active side channel analyses on embedded cryptosystems, see [1] for a detailed description.
In a similar vein to the study of neighbor graphs of binary self-dual codes in [2], we investigate the neighbor graphs of LCD codes. In this graph, two codes (vertices) are connected by an edge if and only if they share a subcode of co-dimension 1. We show this is a connected, regular graph as well as show how some subtypes of LCD codes induce regular subgraphs. With this, we unveil structural connections between LCD codes which could provide new methods for classifying or searching for LCD codes.

References

[1] C. CARLET AND S. GUILLEY, Complementary dual codes for counter-measures to side-channel attacks, Proceedings of the 4th ICMCTA Meeting, Palmela, Portugal, 2014.

[2] S.T. DOUGHERTY, The neighbor graph of binary self-dual codes, *Des. Codes and Cryptogr.* 90 (2022),409-425.

[3] J.L. MASSEY, Linear codes with complementary duals, *Discret. Math* 106(107) (1992), 337–342.

Self-orthogonal and LCD codes related to some combinatorial structures

Ivona Traunkar
University of Rijeka - Faculty of Mathematics
inovak@math.uniri.hr
Joint work with Vedrana Mikulić Crnković

In this talk we will present methods for constructing self-orthogonal and LCD codes using incidence matrices of some combinatorial structures.

A linear code C is called self-orthogonal if C is contained in its dual and LCD code if the intersection of C with its dual is trivial. Matrix G generates self-orthogonal code if $G \cdot G^T = 0$ and G generates an LCD code if and only if $\det(G \cdot G^T) \neq 0$ (see [1]).
We analyse extensions of the incidence matrix, orbit matrix and submatrices of orbit matrix of a weakly p-self-orthogonal 1-design[1] in order to construct self-orthogonal codes (see [2]), and we extend the methods of construction described in order to construct LCD codes (see [3]).
Additionally, we present methods of obtaining self-orthogonal and LCD codes using incidence matrices and orbit matrices of some combinatorial structures, such as graphs and digraphs.

Keywords: self-orthogonal code, LCD code, weakly p-self-orthogonal design

References

[1] J. L. Massey. Linear codes with complementary duals. *Discrete Math.* **106/107**: 337-342, 1992.

[2] V. Mikulić Crnković and I. Traunkar. Self-orthogonal codes constructed from weakly self-orthogonal designs invariant under an action of M_{11}, *Applicable algebra in engineering communication and computing*, **34(1)**: 139-156, 2023.

[3] V. Mikulić Crnković, I. Traunkar, B. G. Rodrigues. LCD codes constructed from weakly p-self-orthogonal 1-designs. *Advances in Mathematics of Communications*. doi: 10.3934/amc.2024040

[1] A 1-design is weakly p-self-orthogonal if all the block intersection numbers gives the same residue modulo p.

Strong External Difference Families, Graph Labeling and Near Factorizations of Finite Groups

Maura Paterson
Birkbeck, University of London
m.paterson@bbk.ac.uk

Strong external difference families (SEDFs) were defined in 2016 as a way of characterising optimal examples of certain structures arising from an application in cryptography. Specifically, an SEDF is a collection of disjoint subsets $A_1, \ldots, A_m$ of a finite group G with the property that for each i from 1 up to m, the nonzero elements of G occur exactly once as a difference of the form $a_i - a_j$ with $a_i \in A_i$ and $a_j \in A_j$ for some $j \neq i$. In this talk we consider connections with longer-studied combinatorial objects, including graph labelings and near factorizations of finite groups, and we explore recent progress and open questions in the quest to classify SEDFs.

A family of strongly regular graphs from hyperbolic quadrics

Valentino Smaldore
Università degli studi di Padova
valentino.smaldore@unipd.it
Joint work with Antonio Cossidente, Jan De Beule, Giuseppe Marino and Francesco Pavese

Let $Q^+(2n+1,q)$ be a hyperbolic quadric of $PG(2n+1,q)$. Fix a generator n-space S of the quadric. Then $\mathcal{G}_n$ denote the graph whose vertices are the points of $Q^+(2n+1,q) \setminus S$ and where two vertices P and Q are adjacent if the line PQ is secant to $Q^+(2n+1,q)$ or non-trivially intersects S. Then, $\mathcal{G}_n$ is a strongly regular graph with parameters $v = \frac{(q^n+1)(q^{n+1}-1)}{q-1} - \frac{q^{n+1}-1}{q-1} = \frac{q^n(q^{n+1}-1)}{q-1}$, $k = q^{2n}-1$, $\lambda = q^{2n-1}(q-1)-2$ and $\mu = (q^{2n-1}+q^{n-1})(q-1)$. Moreover, if $q=2$, $\mathcal{G}_n$ is cospectral to the tangent graph $NO^+(2n+2,2)$, whose vertex set is $PG(2n+1,2) \setminus Q^+(2n+1,2)$, and two vertices P and Q are adjacent if the line PQ is a tangent.

References

[1] A.E. Brouwer, H. Van Maldeghem, *Strongly Regular Graphs*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2022.

[2] J. W. P. Hirschfeld, J. Thas, *General Galois Geometry*, Springer-Verlag London, 2016.

[3] F. Romaniello, V. Smaldore, *On a graph isomorphic to $NO^+(6,2)$*, Bulletin of the Institute of Combinatorics and its Applications, 2024, 100, pp. 151-161.

A Neurosymbolic Approach to Galois Group of Septics

Jurgen Mezinaj
Department of Mathematics and Statistics
Oakland University
mezinaj@oakland.edu

We introduce a database of irreducible polynomials of degree 7, where each polynomial is encoded in binary form and stored in a Python dictionary. For every polynomial, we compute invariants using transvection formulas and determine the associated Galois groups. Building on this comprehensive dataset, we develop a Neurosymbolic Network that classifies Galois groups. Furthermore, this database will serve as a foundational resource for training models which work for any degree polynomial with a reasonably high degree of accuracy.

Coadjoint Matroids and Dependencies on Hypergraphs

Ragnar Freij-Hollanti and Patricija Šapokaitė
Aalto University, Finland
patricija.sapokaite@aalto.fi

Using the definitions of *matroidal hypergraph cycles* and *matroidal closures* we proposed in [2], we expand our ideas to the concept of the joints of matroids, while also formalising the definition of the coadjoint matroids. By establishing connections between the standard definition of the closure on a matroid, provided in [3] and a matroidal closure, we research the relations between matroids and the *combinatorial derived matroids* (defined in [1]) associated to them.

References

[1] Freij-Hollanti, Ragnar and Jurrius, Relinde and Kuznetsova, Olga. Combinatorial Derived Matroids, *The Electronic Journal of Combinatorics*, **30**:P2.8, 28pp, 2023.

[2] Freij-Hollanti, Ragnar and Šapokaitė, Patricija Matroidal Cycles and Hypergraph Families , *ArXiv*, https://arxiv.org/abs/2410.23932

[3] Oxley, James. *Matroid Theory (Oxford Graduate Texts in Mathematics)*, Oxford University Press, Inc., 2006.

Applications of Combinatorial Designs to Software Engineering, Cyber Security and Disaster Science

Dimitris Simos
SBA Research, Vienna, Austria
dsimos@sba-research.org

C. J. Colbourn, J. H. Dinitz and D.R. Stinson, in their seminal survey on applications of combinatorial designs to communications, cryptography, and networking [*Surveys in Combinatorics*, **1999**. London Mathematical Society Lecture Note Series. Cambridge University Press; pages 37-100], highlighted connections with experimental and applied computer science and that the theory of combinatorial designs grew in part as a consequence of the variety of its potential applications.
More than **25** years later, we pay tribute to their work by illustrating new profound applications of combinatorial designs to the technical and natural sciences. In particular, in this talk, we present various research problems encountered in the important fields of software engineering, cyber security and disaster science and demonstrate that they are prone to combinatorial design interpretations where one can use recursive combinatorial constructions, efficient combinatorial optimization, neural and quantum computing algorithms as well as algebraic or symbolic computation solvers to tackle them.
It comes as no surprise that the rich theory of combinatorial designs and the increasing depth of the connections with various classes of designs not only continues to grow in an astonishing fashion but the many new applications emerged pave the way for a new era of challenging problems in combinatorial design theory.
Based on joint works with Charles Colbourn, Bernhard Garn, Ludwig Kampel, Ilias Kotsireas, Temur Kutsia, Manuel Leithner and Michael Wagner.

List of speakers