Finite Geometries
Fifth Irsee Conference

10 - 16 September 2017
Irsee, Germany

Organisers: Ilaria Cardinali - Michel Lavrauw - Klaus Metsch - Alexander Pott

1 Information

The Fifth Irsee Conference on Finite Geometries extends a series of previous meetings which took place at the Isle of Thorns (2000), in Oberwolfach (2001), and in Irsee (2003, 2006, 2011 and 2014).

Conference topics

Combinatorial structures in Galois geometries; Finite Incidence Geometry; Algebraic curves and varieties over finite fields; Geometric and algebraic coding theory; Finite groups and geometries; Algebraic design theory.

Main speakers

John Bamberg (Univeristy of Western Australia, Australia)
Dieter Jungnickel (Augsburg University, Germany)
Karen Meagher (University of Regina, Canada)
Olga Polverino (Università degli Studi della Campania "Luigi Vanvitelli", Italy)
Joachim Rosenthal (University of Zurich, Switzerland)
Kai-Uwe Schmidt (Paderborn University, Germany)
Leo Storme (Ghent University, Belgium)

Organising committee

Ilaria Cardinali (University of Siena, Italy)
Michel Lavrauw (Sabancı University, Turkey / University of Padua, Italy)
Klaus Metsch (Justus-Liebig-Universität Gießen, Germany)
Alexander Pott (Otto von Guericke University, Germany)

Venue

The Irsee Monastery Swabian Conference and Educational Centre.

Schwäbisches Tagungs- und Bildungszentrum
Kloster Irsee, Klosterring 4, D-87660 Irsee, Germany
Tel.: +49 (0)8341 906-00, Fax: +49 (0)8341 74278,
hotel@kloster-irsee.de

This conference was supported by

DFG Deutsche Forschungsgemeinschaft

Otto von Guericke Universität Magdeburg

2 Schedule

	Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**
09:00-09:50	Polverino	Jungnickel	Rosenthal	Bamberg	Schmidt
10:00-10:50			Maegher		
10:00-10:20	Marino	Buratti		Ihringer	Jurrius
10:25-10:45	Csajbók	Davis		Lansdown	Gow
10:50	BREAK	BREAK	BREAK	BREAK	BREAK
11:20-12:10			Storme		
11:20-11:40	Zullo	Tonchev		Pavese	Rousseva
11:45-12:05	Havlicek	Wang		Piñero	Feng
12:10-12:30	Van de Voorde	Năstase		Xiang	Vandendriessche
12:35-12:55	Trombetti	Alderson		Gavrilyuk	Takáts
13:00	LUNCH	LUNCH	LUNCH	LUNCH	LUNCH
14:35-14:55	Rodgers	Traetta		Napolitano	Taniguchi
15:00-15:20	Longobardi	Sin		Szőnyi	Do Duc
15:25-15:45	Abdukhalikov	Merola		Bishnoi	Enge
15:50-16:10	D'haeseleer	Nakić		Mattheus	Özbudak
16:15	BREAK	BREAK		BREAK	BREAK
16:45-17:05	Giuzzi	De Bruyn		De Beule	Korchmáros
17:10-17:30	Ghorpade	De Boeck		Landjev	Bartoli
17:35-17:55	Popiel	Mühlherr		Winterhof	Ball
18:00-18:20				Betten	
18:00	RECEPTION				
18:30		DINNER			
19:00	DINNER		DINNER	DINNER	CONFERENCE DINNER
20:00		CEREMONY			

Contents

3 Invited abstracts

Delsarte designs from finite polar spaces

John Bamberg

The University of Western Australia

When *extremal configuration* comes to mind, one may think of a cage (in graph theory), a Steiner system (in design theory), a perfect code (in coding theory), or an ovoid of a finite polar space (in finite geometry). In many cases, there is an algebraic way to express the extremal phenomenon which introduces, for example, eigenvalue bounds that can provide insight into the existence of such configurations. Delsarte [1, §3.4] defined a combinatorial object known as a $\mathcal{T}$-*design*, as a particularly regular subset with respect to a given association scheme. This allowed extremal configurations from seemingly disparate areas of combinatorics to be studied with unified techniques. In this talk, the speaker will give an overview of configurations in finite polar spaces that arise naturally as Delsarte designs such as ovoids, hemisystems, spreads, tight sets, and m-systems.

References

[1] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. No. 10 (1973).

Extension Sets, Affine Designs, and Hamada's Conjecture

Dieter Jungnickel

University of Augsburg

(Joint work with Yue Zhou and Vladimir D. Tonchev)

Hamada's conjecture states that the p-rank of any design with the parameters of a geometric design $PG_k(d,q)$ or $AG_k(d,q)$, where q is a power of a prime p, is greater than or equal to the p-rank of the corresponding geometric design; except for a few special cases established about 40 years ago, this is still widely open. However, the additional conjecture that equality holds if and only if the design in question is actually isomorphic to the corresponding geometric design is, in general, not correct.

After a brief review of the current status of this conjecture, we study the special case of affine designs with the parameters of a classical design $\mathcal{D} = AG_2(3,q)$. For this, we introduce the notion of an *extension set* for an affine plane of order q to study affine designs $\mathcal{D}'$ with the same parameters which are very close to the geometric design in the following sense: there are blocks B' and B of $\mathcal{D}'$ and $\mathcal{D}$, respectively, such that the residual structures $\mathcal{D}'_{B'}$ and $\mathcal{D}_B$ induced on the points not in B' and B, respectively, agree. Moreover, the structure $\mathcal{D}'(B')$ induced on B' is the q-fold multiple of an affine plane $\mathcal{A}'$ which is determined by an extension set for the affine plane $B \cong AG(2,q)$.

In particular, this new approach gives a purely geometric, computer-free construction for the two known sporadic counterexamples to Hamada's conjecture for the case $q = 4$ (and a theoretical proof of their properties), which were discovered in 2005 by Harada, Lam and Tonchev as the result of a computer search. On the other hand, we also prove that extension sets cannot possibly give any further counterexamples to Hamada's conjecture for the case of affine designs with the parameters of some $AG_2(3,q)$; thus the two counterexamples for $q = 4$ might be truly sporadic. This seems to be the first result which establishes the validity of Hamada's conjecture for some infinite class of affine designs of a special type.

References

[1] Dieter Jungnickel, Yue Zhou & Vladimir D. Tonchev: Extension Sets, Affine Designs, and Hamada's Conjecture. *Designs, Codes and Cryptography.* DOI 10.1007/s10623-017-0344-6.

Approaches to the Erdős-Ko-Rado Theorem

Karen Meagher

University of Regina

(Joint work with Bahman Ahmadi, Peter Borg, Chris Godsil, Alison Purdy and Pablo Spiga)

The Erdős-Ko-Rado (EKR) theorem is a famous result that is one of the cornerstones of extremal set theory. This theorem answers the question "What is the largest family of intersecting sets, of a fixed size, from a base set?" This question may be asked for any type of object for which there is some notion of intersection. For example, there have been recent results that prove that a natural version of the EKR theorem holds for permutations, vector spaces, designs, partial geometries, integer sequences, domino tilings, partitions and matchings.

There are many vastly different proofs of these results, some are simply a straight-forward counting argument, others use graph theory and some require nuanced properties of related matrix algebra. In this talk I will show some of the different proof methods for EKR theorems, with a focus on the more algebraic methods.

Some recent developments in the theory of linear MRD-codes

Olga Polverino

Università degli Studi della Campania "Luigi Vanvitelli"

The vector space $\mathbb{F}_q^{m\times n}$ of $m \times n$ matrices over $\mathbb{F}_q$ can be equipped with the rank metric distance defined by $d(A, B) = rk\,(A - B)$ for $A, B \in \mathbb{F}_q^{m\times n}$, where $rk\,(A - B)$ is the rank of the matrix $A - B$.

A subset $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ endowed with the metric d is called a *Rank Distance code* (RD-code) (see [4] and [5]). The minimum distance of $\mathcal{C}$ is

$$d(\mathcal{C}) = \min_{A,B\in\mathcal{C},\ A\neq B}\{d(A, B)\}.$$

When $\mathcal{C}$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{m\times n}$, we say that $\mathcal{C}$ is an $\mathbb{F}_q$-linear code, and the dimension $\dim_q(\mathcal{C})$ is defined to be the dimension of $\mathcal{C}$ as a subspace over $\mathbb{F}_q$. By [4], the Singleton bound for an $m \times n$ rank metric $\mathbb{F}_q$-linear code $\mathcal{C}$ of dimension k and with minimum rank distance d is

$$k \leq \max\{m, n\}(\min\{m, n\} - d + 1).$$

If this bound is achieved, then $\mathcal{C}$ is a linear *Maximum Rank Distance* code (MRD-code).

In [9] Sheekey pointed out an interesting link between geometric structures over finite fields and linear MRD-codes. Since then various authors have further investigated this link (cfr. [2], [6], [7]) and costructed new families of linear MRD-codes (cfr. [1], [2], [3], [8], [9], [10], [11]).

This talk surveys some of these recent results. In particular, the connection between linear sets and linear MRD-codes will be explored and we shall also discuss some open problems and new research perspectives.

References

[1] B. Csajbók, G. Marino, O. Polverino, C. Zanella: A new family of MRD-codes. Submitted manuscript.

[2] B. Csajbók, G. Marino, O. Polverino and F. Zullo: Maximum scattered linear sets and MRD-codes. *J. Algebraic. Combin.* (2017), 1–15, DOI: 10.1007/s10801-017-0762-6.

[3] B. Csajbók, G. Marino and F. Zullo: New maximum scattered linear sets of the projective lines, manuscript.

[4] P. Delsarte: Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory Ser. A* **25** (1978), 226–241.

[5] E. Gabidulin: Theory of codes with maximum rank distance, *Probl. Inf. Transm.* **21**(3) (1985), 3–16.

[6] G. Lunardon: MRD-codes and linear sets, *J. Combin. Theory Ser. A* **149** (2017), 1–20.

[7] G. Lunardon, R. Trombetti and Y. Zhou: On kernels and nuclei of rank metric codes, *J. Algebraic Combin.*, to appear. DOI 10.1007/s10801-017-0755-5.

[8] G. Lunardon, R. Trombetti and Y. Zhou: Generalized Twisted Gabidulin Codes, http://arxiv.org/abs/1507.07855 http://arxiv.org/abs/1507.07855.

[9] Otal, K., zbudak, F.: Explicit Construction of Some Non-Gabidulin Linear Maximum Rank Distance Codes, *Advances in Mathematics of Communications* **10** (3) (2016).

[10] J. Sheekey: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* **10**(3) (2016), 475–488.

[11] S. Puchinger, J. Rosenkilde n Nielsen, and J. Sheekey: Generalized Twisted Gabidulin Codes, https://arxiv.org/abs/1703.0809.

An Overview on Post-Quantum Cryptography with an Emphasis on Code based Systems

Joachim Rosenthal

University or Zürich

With the realization that a quantum computer would make many practically used public key cryptographic systems obsolete (compare with the reports [1, 2]) it became an important research topic to design public key systems which are expected to be secure even if a powerful quantum computer would exist.

In the talk we will explain about the major possible candidates for post-quantum cryptography and we will then concentrate on so called code based systems which were first proposed in 1978 by Robert McEliece who demonstrated how the hardness of decoding a general linear code up to half the minimum distance can be used as the basis for a public key crypto system.

References

[1] Use of Public Standards for the Secure sharing of Information Among National Security Systems. Technical report, Committee on National Security Systems, July 2015. CNSS Advisory Memorandum.

[2] Report on Post-Quantum Cryptography. Technical report, National Institute of Standards and Technology, February 2016. NISTIR 8105.

[3] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipane. Enhanced public key security for the McEliece cryptosystem. *J. Cryptology*, 29:1–27, 2016. arXiv: 1108.2462, 2011.

[4] J. Bolkema, H. Gluesing-Luerssen, C. A. Kelley, K. Lauter, B. Malmskog, and J. Rosenthal Variations of the McEliece Cryptosystem. *arXiv preprint arXiv:1612.05085*, 2016.

[5] A. Couvreur, A. Otmani, J.-P. Tillich, and V. Gauthier-Umaña. A polynomial-time attack on the BBCRS scheme. In *Public-key cryptography—PKC 2015*, volume 9020 of *Lecture Notes in Comput. Sci.*, pages 175–193. Springer, Heidelberg, 2015.

[6] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan. A polynomial time attack against algebraic geometry code based public key cryptosystems. In *2014 IEEE International Symposium on Information Theory*, pages 1446–1450, 2014.

[7] R. McEliece. A public-key cryptosystem based on algebraic coding theory. In *DSN Progress Report*, volume 42, pages 114–116, 1978.

[8] V. Weger. A code-based cryptosystem using GRS codes. Master Thesis at the University of Zürich (Switzerland), 2016.

Codes in classical association schemes

Kai-Uwe Schmidt

Paderborn University

Association schemes arise naturally on certain sets of bilinear, Hermitian, and quadratic forms over finite fields. A code in such an association scheme is, roughly speaking, a subset such that different elements in the subset are far apart in the rank metric on the underlying space. Such objects have close connections to structures in finite geometry, such as quasifields, semifields and (partial) spreads in projective and polar spaces, and to structures in coding theory, namely classical codes and subspace codes. In this talk, I will survey old and recent results on these association schemes and codes therein and discuss several open problems.

Cameron-Liebler sets in different settings

Leo Storme

Ghent University

Within combinatorics, Erdős-Ko-Rado type problems form a large research field. They have been defined in many domains [2, 5].

Cameron-Liebler sets are one of the other types of substructures in finite projective spaces. One of the nice aspects of Cameron-Liebler sets is that they can be defined in many equivalent ways, thus showing their intrinsic geometric relevance.

After a large number of results regarding Cameron-Liebler sets of lines in 3-dimensional projective spaces, Cameron-Liebler sets of k-spaces in the $(2k+1)$-dimensional spaces $\mathrm{PG}(2k+1,q)$ were defined [6]. Here, links to Erdös-Ko-Rado results were used to obtain results on these Cameron-Liebler sets of k-spaces in $\mathrm{PG}(2k+1,q)$.

These links motivated to initiate research aimed at defining Cameron-Liebler sets in different settings. When defining Cameron-Liebler sets in a new setting, the first aim is to find a substructure which can be defined in similar equivalent ways as in the projective space setting. The second aim is to find examples and characterization results on these Cameron-Liebler sets in those new settings.

This talk will report on this research aimed at defining Cameron-Liebler sets in different settings. For instance, research on Cameron-Liebler sets in finite sets [3], finite projective spaces [4, 6], and finite classical polar spaces [1] will be discussed, and also the many links with the research on Erdős-Ko-Rado type problems will be discussed.

References

[1] M. De Boeck, M. Rodgers, L. Storme, and A. Švob, Cameron-Liebler sets of generators in finite classical polar spaces. (In preparation).

[2] M. De Boeck and L. Storme, Theorems of Erdős-Ko-Rado type in geometrical settings. *Science China Math.* **56** (2013), 1333-1348.

[3] M. De Boeck, L. Storme, and A. Švob, The Cameron-Liebler problem for sets. *Discrete Math.* **339** (2016), 470-474.

[4] A.L. Gavrilyuk and K. Metsch, A modular equality for Cameron-Liebler line classes. *J. Combin. Theory, Ser. A* **127** (2014), 224-242.

[5] Chris Godsil and Karen Meagher, *Erdős-Ko-Rado Theorems: Algebraic Approaches.* Cambridge University Press 2015.

[6] M. Rodgers, L. Storme, and A. Vansweevelt, Cameron-Liebler k-classes in $\mathrm{PG}(2k+1,q)$. *Combinatorica*, to appear.

4 Contributed abstracts

Hyperovals and bent functions

Kanat Abdukhalikov

UAE University

We consider Niho bent functions (they are equivalent to bent functions which are linear on the elements of a Desarguesian spread). We show that Niho bent functions are in one-to-one correspondence with line ovals in an affine plane [1]. Furthermore, Niho bent functions are in one-to-one correspondence with ovals (in a projective plane) with nucleus at a fixed point. These connections and bent functions from [2] allow us to present new simple descriptions of Subiaco and Adelaide hyperovals and their automorphism groups.

References

[1] K. Abdukhalikov, Bent functions and line ovals, Finite Fields and Their Applications, 47 (2017), 94–124.

[2] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit, Construction of bent functions via Niho power functions, J. Combin. Theory Ser. A 113(5) (2006), 779–798.

Higher Dimensional Optical Orthogonal Codes

Tim Alderson

University of New Brunswick Saint John

New constructions of higher dimensional optical orthogonal codes will be presented. In particular, infinte families of codes with ideal off-peak autocorrelation 0, and cross correlation 1 will be provided. Bounds will be established to show that the codes produced are optimal. All codes are constructed using Singer subgroups of $\mathrm{PG}(k, q)$, or an affine analogue in $\mathrm{AG}(k, q)$.

Planar arcs

Simeon Ball

Universitat Politècnica Catalunya

(Joint work with Michel Lavrauw)

Let $\mathrm{PG}_2(\mathbb{F}_q)$ denote the projective plane over $\mathbb{F}_q$. An *arc* (or planar arc) of $\mathrm{PG}_2(\mathbb{F}_q)$ is a set of points in which any 3 points span the whole plane. An arc is *complete* if it cannot be extended to a larger arc.

In 1967 Beniamino Segre proved that the set of tangents to a planar arc of size $q+2-t$, when viewed as a set of points in the dual plane, is contained in an algebraic curve of small degree d. Specifically, if q is even then $d=t$ and if q is odd then $d=2t$.

The main result to be presented here is the following theorem from [1].

Theorem 1 *Let S be a planar arc of size $q+2-t$ not contained in a conic. If q is odd then S is contained in the intersection of two curves, sharing no common component, each of degree at most $t+p^{\lfloor \log_p t \rfloor}$.*

This leads directly to the following theorem.

Theorem 2 *If q is odd then an arc of size at least $q-\sqrt{q}+3+\max\{\sqrt{q}/p, \frac{1}{2}\}$ is contained in a conic.*

There are examples of complete arcs of size $q+1-\sqrt{q}$ in $\mathrm{PG}_2(\mathbb{F}_q)$ when q is square, first discovered by Kestenband [2] in 1981.

It has long been conjectured that if $q \neq 9$ is an odd square then any larger arc is contained in a conic.

References

[1] Simeon Ball and Michel Lavrauw, Planar arcs, preprint (2017). `https://arxiv.org/abs/1705.10940`.

[2] B. C. Kestenband, Unital intersections in finite projective planes, *Geom. Dedicata*, **11** (1981) 107–117.

$\mathbb{F}_{p^2}$-maximal curves with many automorphisms are Galois-covered by the Hermitian curve

Daniele Bartoli

University of Perugia

(Joint work with Maria Montanucci and Fernando Torres)

The Hermitian curve $\mathcal{H}_q \ : \ y^q + y = x^{q+1}$, for a prime power q, is the best known example of $\mathbb{F}_{q^2}$-maximal curve, i.e curve whose number $N(\mathcal{H}_q)$ of $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound $N(\mathcal{H}_q) = q^2 + 1 + 2g(\mathcal{H}_q)q$. Each curve $\mathcal{Y}$ which is covered by an $\mathbb{F}_{q^2}$-maximal curve is also $\mathbb{F}_{q^2}$-maximal.

It is an open problem to decide whether any $\mathbb{F}_{p^2}$-maximal curve is $\mathbb{F}_{p^2}$-covered by the Hermitian curve $\mathcal{H}_p$ or not. We give an affirmative answer for $\mathbb{F}_{p^2}$-maximal curves $\mathcal{X}$ having a large automorphism group, showing that if

$$|Aut(\mathcal{X})| > 84(g(\mathcal{X}) - 1)$$

then $\mathcal{X}$ is Galois covered by $\mathcal{H}_p$.

Also, we show that this result does not extend to curves whose full automorphism group satisfies $|Aut(\mathcal{X})| \leq 84(g(\mathcal{X}) - 1)$, as we construct an $\mathbb{F}_{71^2}$-maximal curve $\mathcal{F}$ of genus 7, having a Hurwitz automorphism group of order 504 which is not Galois covered by $\mathcal{H}_{71}$. The curve $\mathcal{H}$ is the positive characteristic analog of the so called Fricke-MacBeath curve in zero characteristic, and it is the first known example of $\mathbb{F}_{p^2}$-maximal curve which is not Galois-covered by the Hermitian curve $\mathcal{H}_p$.

Classifying Cubic Surfaces over Small Finite Fields

Anton Betten

Colorado State University

(Joint work with James W.P. Hirschfeld and Fatma Karaoglu)

This talk will outline some recent results regarding the classification of cubic surfaces with 27 lines over small finite fields by computer [1]. We will discuss several approaches. One approach is associated with the classical theory of Schlaefli [6],[5] regarding a double six of lines in projective three-space. Another approach is associated with the blow-up of six general points in a plane [4].

Both approaches rely on being able to classify smaller objects such as the mentioned double sixes or the sets of points in general position. To this end, a poset classification algorithm is used. This algorithm has already been used for different classification problems in finite geometry (cf. [2],[3]).

If time permits, we want to look at a family of cubic surfaces with 27 lines which are invariant under a group Sym_4.

References

[1] A. Betten, J.W.P. Hirschfeld and F. Karaoglu. Classification of Cubic Surfaces with Twenty-Seven Lines over the Finite Field of Order Thirteen. Submitted.

[2] Anton Betten. Rainbow cliques and the classification of small BLT-sets. In *ISSAC 2013—Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, pages 53–60. ACM, New York, 2013.

[3] A. Betten, The packings of PG(3, 3), *Des. Codes and Cryptogr.* **79** (2016), 583–595.

[4] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry.* Wiley Classics Library. John Wiley & Sons, Inc., New York, 1994. Reprint of the 1978 original.

[5] J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford University Press, Oxford, 1985, x+316 pp.

[6] L. Schläfli, An attempt to determine the twenty-seven lines upon a surface of the third order and to divide such surfaces into species in reference to the reality of the lines upon the surface, *Quart. J. Math.* **2** (1858), 55–110.

Minimal multiple blocking sets

Anurag Bishnoi

Ghent University

(Joint work with Sam Mattheus and Jeroen Schillewaert)

A well known result of Bruen and Thas says that any minimal blocking set in a finite projective plane of order n has at most $n\sqrt{n}+1$ points. I will be talking about the following generalization of this result to minimal *multiple* blocking sets, that we have obtained recently.

Theorem 3 *Let S be a minimal t-fold blocking set in a finite projective plane of order n. Then*

$$|S| \leq \frac{1}{2}n\sqrt{4tn-(3t+1)(t-1)}+\frac{1}{2}(t-1)n+t.$$

The proof involves using the so-called expander mixing lemma from spectral graph theory on the incidence graph of the projective plane, and it directly implies that if equality occurs in this bound then every line intersects the blocking set in t points or $\frac{1}{2}(\sqrt{4tn-(3t+1)(t-1)}+t-1)+1$ points. We will see how this proof method can be easily adapted to different scenarios, giving us old and new results in finite geometry.

We have also shown that if n is a prime power, then equality occurs in our bound only in the following three cases:

(1) $t=1$, n is a square and the blocking set S is a unital;

(2) $t=n-\sqrt{n}$, n is a square, and S is the complement of a Baer subplane;

(3) $t=n$ and S is the set of all points except one.

The best construction that we have of a large minimal t-fold blocking set is in $\mathrm{PG}(2,q)$ for q square, and it has size $q\sqrt{q}+1+(t-1)(q-\sqrt{q}+1)$ for $2<t\leq\sqrt{q}+1$ (for $t=2$ there is a better construction of size $q\sqrt{q}+q$ due to Francesco Pavese). We will discuss this construction and pose some open problems regarding large minimal multiple blocking sets.

In/out the jungle of differences

Marco Buratti

University of Perugia

Difference methods are often very useful, sometimes even crucial, in the construction of various kinds of combinatorial designs. Anyway to make research in this, as in many other fields of mathematics, is sometimes like to move in a jungle. In this talk I would like to show how it happens that some authors/explorers are afraid to enter the "jungle of differences" and reach their target by means of a long "circumnavigation" or how some places of this jungle are on the contrary visited by many authors over the years but, very unfortunately, they never meet each other.

Maximum scattered subspaces and maximum rank distance codes

Bence Csajbók

University of Campania "Luigi Vanvitelli", Caserta, Italy
&
MTA–ELTE Geometric and Algebraic Combinatorics Research Group
ELTE Eötvös Loránd University, Budapest, Hungary

(Joint works with Giuseppe Marino, Olga Polverino, Corrado Zanella and Ferdinando Zullo)

Let V be an r-dimensional vector space over $\mathbb{F}_{q^n}$, $n, r > 1$, and let U be an $\mathbb{F}_q$-subspace of V. If the one-dimensional $\mathbb{F}_{q^n}$-spaces of V meet U in $\mathbb{F}_q$-subspaces of dimension at most one, then U is called *scattered* (w.r.t. the Desarguesian spread).

In [1] Blokhuis and Lavrauw proved that the rank of a scattered subspace is at most $rn/2$, they also showed that this bound can always be achieved when r is even. Later, existence results and explicit constructions were given for infinitely many values of r, n, q (rn even) but there were still infinitely many open cases.

In this talk I will present examples of scattered subspaces with rank $rn/2$ for every values of r, n, q (rn even) [2]. Scattered subspaces of this rank will be called maximum scattered.

An $\mathbb{F}_q$-linear maximum rank distance code (or MRD-code) $\mathcal{M}$ with parameters $(m, n, q; d)$ is an $\mathbb{F}_q$-subspace of the vector space of $m \times n$ matrices over $\mathbb{F}_q$ such that the non-zero matrices of $\mathcal{M}$ have rank at least d and the size of $\mathcal{M}$ reaches the theoretical upper bound $q^{\max\{m,n\}(\min\{m,n\}-d+1)}$. In [4] Sheekey showed that maximum scattered $\mathbb{F}_q$-subspaces of a 2-dimensional $\mathbb{F}_{q^n}$-space yield MRD-codes with parameters $(n, n, q; n-1)$.

I will present some recent results regarding MRD-codes arising from maximum scattered subspaces. In particular, a generalization of Sheekey's result [2] and new families of MRD-codes with parameters $(6, 6, q; 5)$ and $(8, 8, q; 7)$ [3].

References

[1] A. Blokhuis and M. Lavrauw, On two-intersection sets with respect to hyperplanes in projective spaces, *J. Combin. Theory Ser. A* **99** (2002), 177–382.

[2] B. Csajbók, G. Marino, O. Polverino and F. Zullo, Maximum scattered linear sets and MRD-codes, to appear in *J. Algebraic Combin.*

[3] B. Csajbók, G. Marino, O. Polverino and C. Zanella, A new family of MRD-codes, submitted manuscript.

[4] J. Sheekey, A new family of linear maximum rank distance codes, *Adv. Math. Commun.* **10** (2016), 177–382.

Difference sets in groups of order 256

James Davis

University of Richmond

(Joint work with John Dillon, Jonathan Jedwab, and Ken Smith)

There are 56,092 nonisomorphic groups of order 256. At the last Irsee conference, we reported that there were four of these groups where the existence of a difference set was still unknown. The search has been completed: we will report on the result of that search, and we will point to future work based on those results.

(Small) blocking sets of non-Desarguesian projective and affine planes

Jan De Beule

Vrije Universiteit Brussel

(Tamás Héger, Tamás Szőnyi and Geertrui Van de Voorde)

In this talk we will discuss a construction of a blocking set of the Hall plane of order q^2, that does not satisfy the 1 mod p property. This answers a question of Gordon Royle, and yields an example of a blocking set of a non-Desarguesian affine plane of order q^2 of size considerably smaller than $2q^2 - 1$.

The construction relies on a particular representation of the Hall plane of order q^2. The use of this representation makes it also possible to connect the obtained blocking sets with value sets of certain polynomials, and this connection will be discussed as well.

New families of KM-arcs

Maarten De Boeck

UGent

(Joint work with Geertrui Van de Voorde)

A *KM-arc of type* t in $\mathrm{PG}(2,q)$ is a set of $q+t$ points in the Desarguesian projective plane $\mathrm{PG}(2,q)$ such that any line contains 0, 2 or t points of this set, with $2 \leq t < q$. These sets are named after Korchmáros and Mazzocca who introduced these point sets in [4] as a generalisation of hyperovals. If a KM-arc of type t in $\mathrm{PG}(2,q)$ exists, then q is even and t is a divisor of q. Further results were obtained in [3, 4]. Among others, it was showed that the t-secants are concurrent.

In [4] Korchmáros and Mazzocca constructed KM-arcs of type 2^i in $\mathrm{PG}(2,2^h)$ for all $i > 0$ such that $h-i$ is a divisor of h. In [3] Gács and Weiner gave a geometrical description of the KM-arcs described in [4] and constructed a family of KM-arcs of type 2^i in $\mathrm{PG}(2,2^h)$ for all i such that there is an m such that $h-i+m$ is a divisor of h and a KM-arc of type 2^m in $\mathrm{PG}(2,2^{h-i+m})$ exists. Vandendriessche constructed in [5] a family of KM-arcs of type $q/4$ in $\mathrm{PG}(2,q)$, which was later extended in [1].

In [1, 4] the translation KM-arcs were studied. In this talk, based on [2], we define and investigate elation KM-arcs, generalising the translation KM-arcs. We introduce families of KM-arcs of type $q/8$ and $q/16$ in $\mathrm{PG}(2,q)$, solving the existence problem for some parameter values, and incorporating some sporadic examples into infinite families.

References

[1] M. De Boeck and G. Van de Voorde. A linear set view on KM-arcs. *J. Algebraic Combin.*, 44(1):131–164, 2016.

[2] M. De Boeck and G. Van de Voorde. Elation KM-arcs. *Preprint*, 2017.

[3] A. Gács and Zs. Weiner. On $(q+t)$-arcs of type $(0,2,t)$. *Des. Codes Cryptogr.*, **29 (1-3)** (2003), 131–139.

[4] G. Korchmáros and F. Mazzocca. On $(q+t)$-arcs of type $(0,2,t)$ in a desarguesian plane of order q. *Math. Proc. Cambridge Philos. Soc.*, **108 (3)** (1990), 445–459.

[5] P. Vandendriessche. Codes of Desarguesian projective planes of even order, projective triads and $(q+t,t)$-arcs of type $(0,2,t)$. *Finite Fields Appl.*, **17 (6)** (2011), 521–531.

On the Mathon bound for regular near hexagons

Bart De Bruyn

Ghent University

A finite graph Γ of diameter $d \geq 2$ is called *distance-regular* if there exist constants a_i, b_i, c_i ($i \in \{0, 1, \ldots, d\}$) such that $|\Gamma_1(x) \cap \Gamma_i(y)| = a_i$, $|\Gamma_1(x) \cap \Gamma_{i+1}(y)| = b_i$ and $|\Gamma_1(x) \cap \Gamma_{i-1}(y)| = c_i$ for any two vertices x and y at distance i from each other. A point-line geometry $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ is called a *regular near hexagon with parameters* (s, t, t_2) if its collinearity graph is a distance-regular graph with diameter 3, intersection array $\{b_0, b_1, b_2; c_1, c_2, c_3\} = \{s(t+1), st, s(t-t_2); t_2+1, t+1\}$ and does not contain any $K_{1,1,2}$'s as induced subgraphs (i.e. no complete graphs on four vertices minus an edge). If $s \neq 1$, then an inequality due to Rudi Mathon states that $t \leq s^3 + t_2(s^2 - s + 1)$. In fact, in the special case that $t = s^3 + t_2(s^2 - s + 1)$, it can be shown that any distance-regular graph of diameter 3 and intersection array $\{b_1, b_1, b_2; c_1, c_2, c_3\} = \{s(t+1), st, s(t-t_2); 1, t_2+1, t+1\}$ cannot contain $K_{1,1,2}$'s as induced subgraphs and hence must be the collinearity graph of a regular near hexagon.

In my talk, I will discuss several proofs of this Mathon inequality. These proofs give additional structural information about the regular near hexagon in case t attains the Mathon bound. This additional structural information can be (and has already been) useful for showing the non-existence of distance-regular graphs with certain parameters. Part of this work is joint with Frédéric Vanhove.

An improvement to the sunflower bound

Jozefien D'haeseleer

Ghent University

Consider the vector space $V(n,q)$ of dimension n over the finite field of order q.

A *t-intersecting constant dimension code* is a set of k-dimensional spaces pairwise intersecting in t-dimensional spaces.

The classical example of a t-intersecting constant dimension code is a *sunflower*. This is a set of k-dimensional spaces pairwise intersecting in a fixed t-dimensional space.

Within the theory on t-intersecting constant dimension codes, it is a known result that large t-intersecting constant dimension codes are equal to sunflowers. More precisely, the following result is known.

Theorem 1 *Let C be a t-intersecting constant dimension code of k-dimensional spaces, where*

$$|C| > \left(\frac{q^k - q^t}{q-1}\right)^2 + \left(\frac{q^k - q^t}{q-1}\right) + 1,$$

then C is a sunflower.

This lower bound is called the *sunflower bound.*

It is generally believed that the lower bound of the preceding theorem is too large. This motivates the research to improve this lower bound.

In this talk, I will present an improvement to the sunflower bound for 1-intersecting 4-dimensional spaces [1].

Via techniques involving Shearer's lemma, it is proven that every 1-intersecting constant dimension code C of 4-dimensional spaces, of size $|C| > q^6$, is equal to a sunflower.

References

[1] J. D'haeseleer, Subspace codes en hun meetkundige achtergrond. Master project Ghent University. Academic year 2016-2017.

Bounds on Cyclotomic Numbers

Tai Duc Do

School of Physical and Mathematical Sciences,

Nanyang Technological University, Singapore.

(Joint work with K. H. Leung and B. Schmidt)

Let $q = p^t = ek + 1$ with p being a prime and $e, k \in \mathbb{Z}^+$ being divisors of $q-1$. Let g is a primitive element of $\mathbb{F}_q$ and let C_0 be the subgroup of $\mathbb{F}_q^*$ of order f. Define

$$C_i = g^i C_0,\ i = 0, 1, ..., e-1.$$

For $0 \leq i, j \leq e-1$, the number of solutions of $1 + x = y, x \in C_i, y \in C_j$, is denoted by (i, j) and this number is called *cyclotomic number* of order e.

In [1], it was proved that $(0, 0) \leq 2$ if p is *sufficiently large* compared to f and generally, $(i, j) \leq \lceil f/2 \rceil$ if $p > 3f/2 - 1$. In our study, we aim to find exact bounds between p and f under which the values of all cyclotomic numbers are at most 3.

The main idea of our study is to transform (under some condition on p and f) equations over $\mathbb{F}_q$ into equations over the field of complex numbers, which often can be solved completely. For example, the equation $1 + x = y$ with $x, y \in C_0$ implies that $1 + \zeta_f^i = \zeta_f^j$ for some $i, j \in \mathbb{Z}$, where ζ_f is a complex root of unity of order f. A typical result of our study is: if $p > (\sqrt{14})^{f/\mathrm{ord}_f(p)}$, then $(i, j) \leq 3$ for all $0 \leq i, j \leq e-1$.

References

[1] K. Betshumiya, M. Hirasaka, T. Komatsu, A. Munemasa: Upper bounds on cyclotomic numbers. *Linear Algebra and its Applications* (2013).

Solving relative norm equations in abelian number fields

Andreas Enge

INRIA Bordeaux–Sud-Ouest, France

(Joint work with Bernhard Schmidt, NTU, Singapore)

Solving the complex norm equation

$$X\overline{X} = n$$

with an integer n for an element X in a cyclotomic field has a number of applications in finite geometry. For instance, the existence of cyclic difference sets depends on the solvability (with coefficients 0 and 1) of such an equation.

We present an algorithm that finds all solutions to the equation over an abelian field, that is, a subfield of a cyclotomic field, under the assumption that a solution exists. The algorithm is inspired by recent progress on breaking lattice-based cryptosystems and has a polynomial complexity.

Finite flag-transitive affine planes with a solvable automorphism group

Tao Feng

Zhejiang University

In this talk, we report some recent progress on finite flag-transitive affine planes with a solvable automorphism group. Under a mild number-theoretic condition involving the order and dimension of the plane, the translation complement must contain a linear cyclic subgroup that either is transitive or has two equal-sized orbits on the line at infinity. We develop a new approach to the study of such planes by associating them with planar functions and permutation polynomials in the odd order and even order case respectively. In the odd order case, we characterize the Kantor-Suetake family by using Menichetti's classification of generalized twisted fields and Blokhuis, Lavrauw and Ball's classification of rank two commutative semifields. In the even order case, we develop a technique to study permutation polynomials of DO type by quadratic forms and characterize such planes that have dimensions up to four over their kernels.

On tight sets of hyperbolic quadrics

Alexander Gavrilyuk

University of Science and Technology of China

A set M of points of a finite polar space $\mathcal{P}$ is called tight if the average number of points of M collinear with a given point of M equals the maximum possible value [1, 2]. In the case when $\mathcal{P}$ is a hyperbolic quadric $Q^+(2n+1,q)$, the notion of tight sets generalises that of Cameron-Liebler line classes in $PG(3,q)$, whose images under the Klein correspondence are the tight sets of the Klein quadric $Q^+(5,q)$.

In this talk, we will discuss an extension of the necessary condition for the existence of Cameron-Liebler line classes obtained in [3] to the general case of tight sets of hyperbolic quadrics.

References

[1] Bamberg J., Kelly S., Law M., Penttila T.: Tight sets and m-ovoids of finite polar spaces. J. Comb. Theory Ser. A 114(7), 1293–1314 (2007).

[2] Drudge K.W.: Extremal sets in projective and polar spaces. Thesis (PhD), The University of Western Ontario, Canada, 1998.

[3] Gavrilyuk A.L., Metsch K.: A modular equality for Cameron-Lieber line classes. J. Combin. Theory Ser. A 127, 224–242 (2014).

Maximal hyperplane sections of Schubert varieties over finite fields

Sudhir R. Ghorpade

Indian Institute of Technology Bombay

(Joint work with Prasant Singh)

Let ℓ, m be integers with $1 \leq \ell < m$ and V be an m-dimensional vector space over a field $\mathbb{F}$. Consider the Grassmannian $G_\ell(V)$ of ℓ-dimensional subspaces of V with its Plücker embedding in $\mathbb{P}(\bigwedge^\ell V)$. Let $I(\ell, m) = \{\alpha = (\alpha_1, \ldots, \alpha_\ell) : 1 \leq \alpha_1 < \cdots < \alpha_\ell \leq m\}$ be the poset with the "Bruhat-Chevalley partial order" given by $\beta \leq \alpha \Leftrightarrow \beta_i \leq \alpha_i \ \forall\ i$. Fix any $\alpha \in I(\ell, m)$ and a partial flag $A_1 \subset \cdots \subset A_\ell$ of subspaces of V such that $\dim A_i = \alpha_i$ for $i = 1, \ldots, \ell$, and let

$$\Omega_\alpha(\ell, m) = \{L \in G_\ell(V) : \dim(L \cap A_i) \geq i \text{ for all } i = 1, \ldots, \ell\}$$

be the corresponding Schubert variety in $G_\ell(V)$. These are projective algebraic varieties defined by equations over $\mathbb{Z}$ and the Grassmannian is a special case with $\alpha_i = m - \ell + i$ for $i = 1, \ldots, \ell$. Now suppose $\mathbb{F}$ is the finite field $\mathbb{F}_q$ with q elements. Using the cellular decomposition, it is easy to see that

$$|\Omega_\alpha(\ell, m)(\mathbb{F}_q)| = n_\alpha := \sum_{\substack{\beta \in I(\ell,m) \\ \beta \leq \alpha}} q^{\delta(\beta)} \quad \text{where} \quad \delta(\beta) := \sum_{i=1}^{\ell} (\beta_i - i).$$

While the embedding, $G_\ell(V) \hookrightarrow \mathbb{P}(\bigwedge^\ell V)$ is nondegenerate (i.e., $G_\ell(V)$ is not contained in any hyperplane of $\mathbb{P}(\bigwedge^\ell V)$), the induced embedding of $\Omega_\alpha(\ell, m)$ in $\mathbb{P}(\bigwedge^\ell V)$ is, in general, not nondegenerate. However, it is not difficult to see (using the Hodge postulation formula) that $\Omega_\alpha(\ell, m)$ embeds nondegenerately in $\mathbb{P}^{k_\alpha - 1}$, where

$$k_\alpha = \det_{1 \leq i,j \leq \ell} \left(\binom{\alpha_j - j + 1}{i - j + 1} \right).$$

We are interested in the maximum number, say e_α, of $\mathbb{F}_q$-rational points that can lie on a section of $\Omega_\alpha(\ell, m)$ by a hyperplane in $\mathbb{P}^{k_\alpha - 1}$. It was conjectured in 1998 that this maximum number is given by $n_\alpha - q^{\delta(\alpha)}$. In the special case of Grassmannians (i.e. when $\alpha_i = m - \ell + i,\ \forall\ i$), this is a classical result of Nogin [4] .The conjecture after being established in several special cases by Chen [1] Guerra-Vincenti [3], Ghorpade-Tsfasman [2], was proved in the affirmative by Xiang [5] in 2008. We shall give an alternative proof of the validity of this conjecture. It can be argued that our proof is somewhat simpler and cleaner. Moreover, it paves the way for determining the number of hyperplanes in $\mathbb{P}^{k_\alpha - 1}$ for which the corresponding hyperplane sections of $\Omega_\alpha(\ell, m)$ have the maximum number of $\mathbb{F}_q$-rational points. In this talk, we will provide relevant background and outline these results and their applications to coding theory.

References

[1] H. Chen, On the minimum distance of Schubert codes, *IEEE Trans. Inform. Theory* **46** (2000), 1535–1538.

[2] S. R. Ghorpade and M. A. Tsfasman, Schubert varieties, linear codes and enumerative combinatorics, *Finite Fields Appl.* **11** (2005), 684–699.

[3] L. Guerra and R. Vincenti, On the linear codes arising from Schubert varieties, *Des. Codes Cryptogr.* **33** (2004), 173–180.

[4] D. Yu. Nogin, Codes associated to Grassmannians, *Arithmetic, Geometry and Coding Theory* (Luminy, 1993), R. Pellikaan, M. Perret, S. G. Vlăduţ, Eds., Walter de Gruyter, Berlin, 1996, pp. 145–154.

[5] X. Xiang, On the minimum distance conjecture for Schubert codes, *IEEE Trans. Inform. Theory* **54** (2008), 486–488.

Transparent embeddings of point-line geometries

Luca Giuzzi

University of Brescia

(Joint work with Ilaria Cardinali and Antonio Pasini)

A (full) projective embedding of a point-line Geometry $\Gamma = (\mathcal{P}, \mathcal{L})$ into the projective space $\Sigma = \mathrm{PG}(V)$ is an injective map $\varepsilon : \mathcal{P} \to \Sigma$ satisfying the following two properties:

(E1) the image of ε spans Σ;

(E2) every line of Γ is mapped by ε onto a line of Σ.

Let $|\varepsilon|$ be the image of ε. We introduce and discuss the notion of *transparent embedding*; see [1]: a projective embedding ε of Γ is *transparent* when, in addition to (E1)–(E2), the following also holds:

(T1) the preimage of any projective line $\ell \subseteq |\varepsilon|$ is an element of $\mathcal{L}$ (i.e. a line of Γ).

We extensively investigate the transparency of Plücker embeddings of projective and polar Grassmannians as well as spin embeddings of half-spin geometries and dual polar spaces of orthogonal type. As a consequence, we derive Chow-like [2] theorems on the automorphism group $\mathrm{Aut}(|\varepsilon|) \subseteq \mathrm{P\Gamma L}(V)$ of the image in terms of the group of automorphisms $\mathrm{Aut}(\Gamma)$ of the geometry Γ. Applications of these results to the study of the monomial automorphism group of projective codes arising from embeddings are also discussed.

References

[1] I. Cardinali, L. Giuzzi and A. Pasini On transparent embeddings of point-line geometries, J. Combin. Theory, Series A, *to appear* (arXiv:1611.07877)

[2] W.L. Chow. On the geometry of algebraic homogeneous spaces. *Ann. of Math. (2)*, 50:32–67, 1949.

Constant rank subspaces of bilinear forms over finite fields

Rod Gow

University College Dublin, Ireland

Let V be a vector space of dimension n over the finite field $\mathbb{F}_q$ and let $\mathcal{M}$ be a subspace of bilinear forms defined on $V \times V$. We say that $\mathcal{M}$ is a constant rank m subspace if each non-zero element of $\mathcal{M}$ has rank m, where $1 \leq m \leq n$.

We have shown elsewhere that the dimension of a constant rank m subspace of bilinear forms is at most n provided that $q \geq m + 1$. (Some restriction on the size of q relative to m seems to be necessary.)

The purpose of this talk is to describe properties of constant rank subspaces of bilinear forms whose dimensions are maximal (note that the maximal dimension may be less than n for certain types of forms). Our findings are possibly of greatest interest when the forms are either alternating or symmetric, and they relate to common radicals, spreads and common totally isotropic subspaces.

Versions of our findings are available on arXiv.

Linear sets in the projective line over the endomorphism ring of a finite field

Hans Havlicek

Vienna University of Technology

(Joint work with Corrado Zanella)

We exhibit $\mathbb{F}_q$-linear sets of rank $t \geq 2$ in the projective line $\mathrm{PG}(1, q^t)$, where q is a power of a prime. By means of the field reduction map $\mathcal{F}$ the point set of $\mathrm{PG}(1, q^t)$ turns into a Desarguesian spread $\mathcal{D}$ that is contained in the Grassmannian $\mathcal{G}_{2t,t,q}$ comprising all $(t-1)$-dimensional subspaces of the projective space $\mathrm{PG}(2t-1, q)$. We present a counterpart of this correspondence. It is based upon the endomorphism ring $E = \mathrm{End}_q(\mathbb{F}_{q^t})$ of the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^t}$ and the projective line $\mathrm{PG}(1, E)$ over the ring E. Each $a \in \mathbb{F}_{q^t}$ defines the mapping $\rho_a \in E$ taking $x \in \mathbb{F}_{q^t}$ to xa. This yields a monomorphism $\mathbb{F}_{q^t} \to E$ of rings and an embedding

$$\iota\colon \mathrm{PG}(1, q^t) \to \mathrm{PG}(1, E)$$

Furthermore, there is a bijection

$$\Psi : \mathrm{PG}(1, E) \to \mathcal{G}_{2t,t,q}.$$

taking distant points (in the sense of ring geometry) of $\mathrm{PG}(1, E)$ to complementary subspaces from $\mathcal{G}_{2t,t,q}$ and vice versa; in particular, we have $\mathrm{PG}(1, q^t)^{\iota\Psi} = \mathcal{D}$.

Each point T of $\mathrm{PG}(1, E)$ determines two subsets of $\mathrm{PG}(1, E)$. The first one, L_T, comprises all points of the subline $\mathrm{PG}(1, q^t)^\iota$ that are non-distant to T. The second one, L'_T, is the orbit of T under the group of all projectivities of $\mathrm{PG}(1, E)$ that fix the subline $\mathrm{PG}(1, q^t)^\iota$ pointwise. The sets L_T, with T varying in $\mathrm{PG}(1, E)$, are precisely the images under ι of the $\mathbb{F}_q$-linear sets of rank t in $\mathrm{PG}(1, q^t)$.

Our main result is the following characterisation:

Theorem 1 *A scattered linear set of* $\mathrm{PG}(1, q^t)$ *arising from* $T \in \mathrm{PG}(1, E)$ *is of pseudoregulus type if, and only if, there exists a projectivity* φ *of* $\mathrm{PG}(1, E)$ *such that* $L_T^\varphi = L'_T$.

References

[1] H. Havlicek and C. Zanella: Linear sets in the projective line over the endomorphism ring of a finite field, *J. Algebr. Comb.*, to appear.
DOI 10.1007/s10801-017-0753-7

Strongly Regular Graphs Related To Polar Spaces

Ferdinand Ihringer

Consider the n-dimensional vector space over a finite field of order q: $\mathbb{F}_q^n$. Let s be a non-degenerate reflexive sesquilinear form on $\mathbb{F}_q^n$. We define a graph Γ as follows. The points are the 1-dimensional subspaces that vanish on s. Two points x and y are adjacent if $s(x, y) = 0$. It is well-known that Γ is a strongly regular graph. Recently, triggered by a result by Abiad and Haemers, several new strongly regular graphs with the same parameters were constructed for $q = 2$ and sufficiently large n (e.g. $n \geq 6$ for Abiad et al.). Here all the results use Godsil-McKay switching sets. We will present a generalization of one of these constructions that works for all q. Particularly, this implies that a strongly regular graph $srg(v, k, \lambda, \mu)$ with the same parameters as the collinearity graph of a finite classical polar space of rank at least 3 is not determined by its parameters v, k, λ and μ.

A q-analogue of perfect matroid designs

Relinde Jurrius

University of Neuchtel, Switzerland

Perfect matroid designs (PMD) are matroids where flats of equal rank have equal cardinality. An important class of PMDs are Steiner systems. In the 1970's – 1980's, matroid theory and PMDs helped achieving results about the existence of Steiner systems and designs [1].

Nowadays, the q-analogues of designs and Steiner systems attract much attention. The existence and construction of non-trivial q-Steiner systems seems (at the moment) to be not so easy. Since recently the q-analogue of a matroid was (re-)defined [2], it is natural to ask if the q-analogue of PMD's might help in studying the q-analogues of Steiner systems. In this talk we will discuss this possibility, supported by preliminary results.

References

[1] M. Deza, Perfect Matroid Designs, in *Matroid Applications* ed. N. White, pp.54–72, Encyc. Math. Appl. **40**, Cambridge University Press, 1992.

[2] R. Jurrius and R. Pellikaan, *Defining the q-analogue of a matroid*, `arXiv:1610.09250`, submitted.

Hemisystems of the Hermitian Surface

Gábor Korchmáros

University of Basilicata

(Joint work with G.P. Nagy and P. Speziali)

We present a new approach to hemisystems of the Hermitian surface of $PG(3, q^2)$ that depends on maximal curves, that is, algebraic curves defined over $\mathbb{F}_{q^2}$ whose number of points defined over $\mathbb{F}_{q^2}$ attains the Hasse-Weil upper bound. Our discussion addresses the following issues.

- Construction of the Cossidente-Penttila hemisystem from a rational maximal curve.
- Construction of new hemisystems for certain values $q \equiv 1 \pmod 4$ which are invariant under a subgroup of $PGU(4, q)$ isomorphic to $PSL(2, q) \rtimes C_{(q+1)/2}$ where $C_{(q+1)/2}$ is a cyclic group of order $(q + 1)2$.

On Some Open Problems in Finite Ring Geometries

Ivan Landjev [1]

New Bulgarian University

Let R be a finite chain ring of length 2 with $R/\operatorname{Rad} R \cong \mathbb{F}_q$. Denote by $\Pi = \mathrm{PHG}(n, R)$ be the n-dimensional projective Hjelmslev geometry over R, and by $\mathrm{AHG}(n, R)$ the affine Hjelmslev geometry obtained from $\mathrm{PHG}(n, R)$ by deleting a neighbour class of hyperplanes. Below we present a list of open problems whose solution might be of interest.

1. *The maximal arc problem.* It is known that the maximal number of points in $\mathrm{PHG}(2, R)$ no three of which are collinear is $q^2 + q + 1$, for q even, and q^2, for q odd. In case of equality, each neighbour class of points has at most one point. Arcs meeting the above bounds are known to exist if $\operatorname{char} R = 4$, or $\operatorname{char} R = p$, p odd. If $\operatorname{char} R = 2$ there are no arcs of size $q^2 + q + 1$. Thus the question on the size of a maximal arc in $\mathrm{PHG}(2, R)$ is open for chain rings with $\operatorname{char} R = 2$, or $\operatorname{char} R = p^2$, p odd.

2. *Blocking sets.* Find the size of the smallest non-trivial (not containing a line) blocking set in $\mathrm{PG}(2, R)$. There are several candidates obtained as Rédei-type blocking sets.

3. *Affine blocking sets.* The minimal size of a blocking set in $\mathrm{AHG}(2, q)$ is suspected to be $q(2q - 1)$ in analogy with the $(2q - 1)$-bound in $AG(2, q)$. Prove or disprove.

4. *Necessary and sufficient condition for the existence of non-free spreads.* As in the classical case, we define a spread $\mathcal{S}$ to be a partition of the pointset of Π into subspaces of fixed shape κ. It is clear that the number of points in a subspace of shape κ divides the number of points in Π. If the elements of $\mathcal{S}$ are Hjelmslev subspaces, i.e. *free* submodules of R^n, this necessary condition is also sufficient. If the subspaces in $\mathcal{S}$ are not Hjelmslev subspaces this numerical condition is not sufficient anymore. Find a sufficient condition for the existence of spreads by subspaces of shape κ in $\mathrm{PHG}(n, q)$.

5. *Spreads with minimal non-free intersection.* The proof of the existence of spreads of Hjelmslev subspaces repeats the classical one for spreads in $\mathrm{PG}(n, q)$. However the submodules in a spread obtained from this proof have a rather large intersection as submodules. It is natural to ask whether there exist spreads for which the subspaces have a minimal intersection (as submodules). In particular, for $\mathrm{PHG}(3, R)$ we ask whether there exists a spread of lines no two of which are neighbours. Such spreads are known to exist for the chain rings with 4 and 9 elements (computer construction).

6. *The p-rank incidence matrix of the projective Hjelmslev plane.* Find a formula for the p-rank of the incidence matrix of the projective Hjelmslev plane $\mathrm{PHG}(2, R)$.

[1]This research is supported by the Scientific Research Fund of Sofia University under Contract 80-10-55/19.04.2017.

m-ovoids of regular near polygons

Jesse Lansdown

Lehrstuhl B für Mathematik
RWTH Aachen University

(Joint work with John Bamberg and Melissa Lee)

A regular near polygon, or $2d$-gon, is an incidence geometry with a distance regular collinearity graph of diameter d and the property that for any point P and line ℓ there is a unique nearest point Q to P on ℓ. An m-ovoid is a set of points such that every line is incident with exactly m points of the set, and is called a hemisystem in the case where m is equal to half the points on a line. De Bruyn and Vanhove [1] proved that a regular near $2d$-gon satisfies

$$\frac{(s^i-1)(t_{i-1}+1-s^{i-2})}{s^{i-2}-1} \leq t_i+1 \leq \frac{(s^i+1)(t_{i-1}+1+s^{i-2})}{s^{i-2}+1}$$

for $s,t \geq 2$ and $i \in \{3,\dots,d\}$. Moreover, they showed that any regular $2d$-gon ($d \geq 3$, $s \geq 2$) attaining the lower bound for $i=3$ is isomorphic to a dual polar space $DQ(2d,q)$, $DW(2d-1,q)$ or $DH(2d-1,q^2)$. We have recently found that if a regular $2d$-gon satisfies

$$t_i+1 = \frac{(s^i+(-1)^i)(t_{i-1}+1+(-1)^i s^{i-2})}{s^{i-2}+(-1)^i}$$

then any non-trivial m-ovoid is a hemisystem. An immediate consequence is that nontrivial m-ovoids of $DQ(2d,q)$, $DW(2d-1,q)$ and $DH(2d-1,q^2)$ are hemisystems, for $d \geq 3$. Thus we also generalise work of Segre[3], Cameron, Goethals and Seidel[2], and Vanhove[4].

References

[1] B. De Bruyn and F. Vanhove. Inequalities for regular near polygons, with applications to m-ovoids. *European J. Combin.*, 34(2):522–538, 2013.

[2] P. J. Cameron, J.-M. Goethals, and J. J. Seidel. Strongly regular graphs having strongly regular subconstituents. *J. Algebra*, 55(2):257–280, 1978.

[3] B. Segre. Forme e geometrie hermitiane, con particolare riguardo al caso finito. *Ann. Mat. Pura Appl. (4)*, 70:1–201, 1965.

[4] F. Vanhove. A Higman inequality for regular near polygons. *J. Algebraic Combin.*, 34(3):357–373, 2011.

Pre-sympletic semifields

Giovanni Longobardi

University of Naples 'Federico II'

(Joint work with G. Lunardon)

Using the known sympletic semifields of order q^3, q a prime power, and exploiting a projection argument in $PG(2, q^3)$, we will construct a family of semifields called *pre-sympletic semifields* which have rank three on their left nucleus.
In even characteristic we will exhibit a new semifield with center $\mathbb{F}_2$, which belongs to the relevant family.

Classes and equivalence of linear sets in $\mathrm{PG}(1, q^n)$

Giuseppe Marino

Università degli Studi della Campania "Luigi Vanvitelli"

(Joint work with Bence Csajbók and Olga Polverino)

Linear sets are natural generalizations of subgeometries. One of the most natural questions about linear sets is their equivalence. Two linear sets L_U and L_V of $\mathrm{PG}(r-1, q^n)$ are said to be $\mathrm{P\Gamma L}$-*equivalent* (or simply *equivalent*) if there is an element φ in $\mathrm{P\Gamma L}(r, q^n)$ such that $L_U^\varphi = L_V$. In the applications it is crucial to have methods to decide whether two linear sets are equivalent or not. In this talk we investigate the equivalence problem of $\mathbb{F}_q$-linear sets of rank n of $\mathrm{PG}(1, q^n)$, also in terms of the associated variety, projecting configurations, $\mathbb{F}_q$-linear blocking sets of Rédei type and MRD-codes.

From [1], an $\mathbb{F}_q$-linear set L_U of rank n in $\mathrm{PG}(W, \mathbb{F}_{q^n}) = \mathrm{PG}(1, q^n)$ is said to be *simple* if for any n-dimensional $\mathbb{F}_q$-subspace V of W, L_V is equivalent to L_U only if U and V lie on the same orbit of $\Gamma\mathrm{L}(2, q^n)$. Examples of non-simple $\mathbb{F}_q$-linear sets in $\mathrm{PG}(1, q^n)$ are those of pseudoregulus type (cf. [3], [2]). We will show that $U = \{(x, \mathrm{Tr}_{q^n/q}(x)) \colon x \in \mathbb{F}_{q^n}\}$ defines a simple $\mathbb{F}_q$-linear set for each n. We also provide examples of non-simple linear sets not of pseudoregulus type for $n > 4$ and finally we prove that all $\mathbb{F}_q$-linear sets of rank 4 are simple in $\mathrm{PG}(1, q^4)$.

References

[1] B. Csajbók, G. Marino and O. Polverino: Classes and equivalence of linear sets in $\mathrm{PG}(1, q^n)$. Submitted manuscript, https://arxiv.org/abs/1607.06962 .

[2] B. Csajbók and C. Zanella: On linear sets of pseudoregulus type in $\mathrm{PG}(1, q^t)$, *Finite Fields Appl.* **41** (2016), 34–54.

[3] G. Lunardon, G. Marino, O. Polverino and R. Trombetti: Maximum scattered linear sets of pseudoregulus type and the Segre Variety $\mathcal{S}_{n,n}$, *J. Algebraic Combin.* **39** (2014), 807–831.

A step towards the weak cylinder conjecture

Sam Mattheus

Vrije Universiteit Brussel

(Joint work with J. De Beule, J. Demeyer, P. Sziklai)

The weak cylinder conjecture [1] asserts that a set S of p^2 points in $\mathrm{AG}(3,p)$ not determining at least p directions must be a cylinder (the points on p parallel lines). Many researchers have tried to attack this problem, and its stronger variant, without success. We strengthen the assumption just slightly by requiring at least $p+1$ non-determined directions, and then reduce the problem to a question concerning a function $w(X,Y) : \mathrm{AG}(2,p) \to \mathbb{F}_p$ satisfying 4 properties. We will discuss this reduction and its relation to the original problem. In particular, showing the non-existence of such a function $w(X,Y)$ implies our weaker version of the cylinder conjecture. In this way we have shown, assisted by computer, that the weaker cylinder conjecture is true for all primes at most 13. For larger p, the question remains open.

References

[1] S. Ball, *On the graph of a function in many variables over a finite field*, Des. Codes Cryptogr. **47** (2008), 1-3, p159-164

On Kaleidoscope Designs

Francesca Merola

Roma Tre University

(Joint work with Marco Buratti)

In this talk I would like to discuss a somewhat natural notion that can be considered when studying designs; in order to do this, let us start with an example. Let $\mathcal{F}$ be a set of Fano planes, namely 2-$(7,3,1)$-designs, such that the seven lines of each plane are colored with seven different colors $c_0, c_1, \ldots, c_6$, and that the points of the planes of $\mathcal{F}$ belong to a given v-set $\mathcal{P}$. We say that $\mathcal{F}$ is a *Fano-Kaleidoscope* of order v if for any two distinct points x, y of $\mathcal{P}$ and any color $c_i \in \{c_0, c_1, \ldots, c_6\}$ there is exactly one Fano plane of $\mathcal{F}$ whose c_i-colored line contains x and y.

This example can be thought of as the smallest instance of the following general idea: consider a set $\mathcal{D}$ of 2-$(n,h,1)$ designs whose vertices belong to a given v-set $\mathcal{P}$; in each design let the b blocks be colored with b different colors $c_0, c_1, \ldots, c_{b-1}$. We say that $\mathcal{D}$ is a *Kaleidoscope Design* of order v and type $(n,h,1)$ if, once more, for any two distinct points x, y of $\mathcal{P}$ and any color c_i there is exactly one design of $\mathcal{D}$ in which the block having color c_i contains x and y.

This concept can be studied in the framework of colored designs and edge-colored graph decompositions, see for instance the work by Colbourn and Stinson (1998), Caro, Roditty and Schönheim (1995, 1997, 2002), Adams, Bryant and Jordon (2006), and the important asymptotic existence result by Lamken and Wilson (2000). It seems nevertheless interesting to consider concrete examples and constructions of such "two-tiered" designs; these seem quite hard to obtain in general. For the Fano Kaleidoscopes described above, we will show existence results using difference methods and known constructions for Pairwise Balanced Designs. We will also sketch what could be done in the general case, presenting some first examples and constructions in the case in which the type is the 2-$(9,3,1)$ design, where the situation seems already way more difficult.

EKR-sets in finite buildings

Bernhard Mühlherr

JLU Gießen

(Joint work with F. Ihringer and K. Metsch.)

Over the last decades, EKR-sets have been studied in various finite combintarial objects. In particular, there have been several contributions to the EKR-problem in finite projective spaces and finite polar spaces. We formulate the EKR-problem for finite buildings in a fairly general framework. It turns out that the earlier contributions on finite projective spaces and polar spaces provide the solution of some special cases. Thus, our general setup provides a lot of new EKR-problems for these spaces and it seems that some of them are more interesting than others. However, our main motivation for putting these earlier results in a building theoretic perspective is to investigate EKR-sets in finite buildings of exceptional type. The questions that arise in this context are closely related to the so called center conjecture for spherical buildings and it is our hope that the recent proof of this conjecture provides some inspiration for making progress on the EKR-problem.

I intend to give a survey talk: I will explain the building theoretic version of the EKR-problem and its connections to the center conjecture.

Graph decompositions in projective geometries

Anamari Nakić

University of Zagreb

(Joint work with Marco Buratti and Alfred Wassermann)

This work has been inspired by the connection between graph decompositions, classic Steiner 2-designs and Steiner 2-designs over a finite field. It is well known that any Steiner 2-design $\mathrm{S}(2,k,v)$ can be viewed as a decomposition of the complete graph of order v into cliques of order k. In addition, any $\mathrm{S}(2,k,v)$ over $\mathbb{F}_q$ can be viewed as a $\mathrm{S}(2,\frac{q^k-1}{q-1},\frac{q^v-1}{q-1})$ whose points are those of the projective geometry $\mathrm{PG}(v-1,q)$ and whose blocks are $(k-1)$-dimensional subspaces of $\mathrm{PG}(v-1,q)$. It is then natural to propose the following new notion of *a graph decomposition in a projective geometry.*

Let G be a graph whose vertices are the points of a projective space $\mathrm{PG}(n,q)$ and let Γ be a subgraph of G. A (G,Γ)-design over $\mathbb{F}_q$ is a decomposition of G into copies of Γ with the property that the vertex-set of each of these copies is a subspace of $\mathrm{PG}(n,q)$. It is clear, from this definition, that any Steiner 2-design over $\mathbb{F}_q$ can be interpreted as a special graph decomposition in a projective geometry.

We will present results and examples that we obtained on this topic.

An inequality for the line–size sum in a finite linear space

Vito Napolitano

Università degli Studi della Campania "Luigi Vanvitelli"

In this talk, we present an inequality which provides a lower bound for the sum of the line sizes in terms of points and minimum point degree and which is also related with clique partitions of the complete graph K_n.

The Structure of the Minimum Size Supertail of a Subspace Partition

Esmeralda Năstase

Xavier University

(Joint work with Papa Sissokho)

Let $V = V(n, q)$ denote the vector space of dimension n over the finite field with q elements. A *subspace partition* $\mathcal{P}$ of V is a collection of nontrivial subspaces of V such that each nonzero vector of V is in exactly one subspace of $\mathcal{P}$. For any integer d, the *d-supertail* of $\mathcal{P}$ is the set of subspaces in $\mathcal{P}$ of dimension less than d, and it is denoted by ST. Let $\sigma_q(n, t)$ denote the minimum number of subspaces in any subspace partition of V in which the largest subspace has dimension t. We prove that if $|ST| = \sigma_q(d, t)$, then the union of all the subspaces in ST constitutes a subspace under certain conditions.

Constructing Sequences from Algebraic Curves

Ferruh Özbudak

Middle East Technical University, Ankara, Turkey

We use properties of algebraic curves over finite fields in order to construct some sequences over finite fields. These sequences have potential for applications in communication, cryptography and related areas. We also give some explicit examples.

Relative m–ovoids of elliptic quadrics

Francesco Pavese

Polytechnic University of Bari

(Joint work with A. Cossidente)

Let $\mathcal{Q}^-(2n+1,q)$ be an elliptic quadric of $\mathrm{PG}(2n+1,q)$. A *relative m–ovoid* of $\mathcal{Q}^-(2n+1,q)$ (with respect to a parablic section $\mathcal{Q} := \mathcal{Q}(2n,q) \subset \mathcal{Q}^-(2n+1,q)$) is a subset $\mathcal{R}$ of points of $\mathcal{Q}^-(2n+1,q) \setminus \mathcal{Q}$ such that every generator of $\mathcal{Q}^-(2n+1,q)$ not contained in $\mathcal{Q}$ meets $\mathcal{R}$ precisely in m points. A relative m–ovoid having the same size as its complement (in $\mathcal{Q}^-(2n+1,q) \setminus \mathcal{Q}$) is called a *relative hemisystem*. In this talk I will show that a nontrivial relative m–ovoid of $\mathcal{Q}^-(2n+1,q)$ is necessarily a relative hemisystem, forcing q to be even. Also, I will exhibit an infinite family of relative hemisystems of $\mathcal{Q}^-(4n+1,q)$, $n \geq 2$, admitting $\mathrm{PSp}(2n,q^2)$ as an automorphism group.

A note on the weight distribution of Schubert code $C_\alpha(2, m)$

Fernando L. Piñero

University of Puerto Rico at Ponce

(Joint work with Prashant Singh)

We consider the linear code $C_\alpha(2, m)$ associated to a Schubert variety in $G_{2,m}$. Using resuls from [1] we show that every codeword correspond to a special skew symmetric matrix. The authors in [2] determined several properties of the codes $C_\alpha(2, m)$, including the weight spectrum. In this work we determine the weight distribution of $C_\alpha(2, m)$. Further, we show that the weight of any codeword in $C_\alpha(2, m)$ is divisible by some power of q.

References

[1] D. Yu. Nogin, Codes associated to Grassmannians, *Arithmetic, Geometry and Coding Theory* (Luminy, 1993), R. Pellikaan, M. Perret, S. G. Vlăduţ, Eds., Walter de Gruyter, Berlin, 1996, pp. 145–154.

[2] L. Guerra and R. Vincenti, On the linear codes arising from Schubert varieties, *Des. Codes Cryptogr.* **33** (2004), 173–180.

The symmetric representation of lines in $\mathrm{PG}(\mathbb{F}_q^3 \otimes \mathbb{F}_q^3)$

Tomasz Popiel

Queen Mary University of London

(Joint work with Michel Lavrauw)

Consider the vector space $V = F^3 \otimes F^3$ of 3×3 matrices over a finite field F, and let $G \leq \mathrm{PGL}(V)$ be the setwise stabiliser of the corresponding Segre variety. The G-orbits of lines in $\mathrm{PG}(V)$ were determined by Lavrauw and Sheekey [1] as part of their classification of tensors in $F^2 \otimes V$. I will discuss the related problem of classifying those line orbits that may be represented by *symmetric* matrices, or equivalently, of classifying the line orbits in the span of the Veronese variety $\mathcal{V}_3(F)$ under the natural action of $K = \mathrm{PGL}(3, F)$. Interestingly, several of the G-orbits that have symmetric representatives split under the action of K, and in many cases this splitting depends on the characteristic of F. Connections are also drawn with old work of Jordan, Dickson and Campbell.

References

[1] Michel Lavrauw and John Sheekey, "Canonical forms of $2 \times 3 \times 3$ tensors over the real field, algebraically closed fields, and finite fields", *Linear Algebra and its Applications* **476** (2015) 133–147.

Finite commutative semifields with small rank

Morgan Rodgers

California State University, Fresno

(Joint work with Michel Lavrauw)

Finite semifields are well studied objects in combinatorics and finite geometry and have many connections to other interesting geometric structures. Of particular interest are commutative semifields with odd order, for which few constructions are known. The property of being commutative implies that these semifields have applications to perfect nonlinear functions.

We will first consider commutative semifields which have rank two over their middle nucleus. These objects are equivalent to semifield flocks of a quadratic cone in projective 3-space, and are therefore also equivalent to translation ovoids of $Q(4, q)$. Using a computer to search for appropriate linear sets, we complete the classification of the rank two commutative semifields which are 8-dimensional over their center. This classification relies on a result from [1] which bounds the size of the center as a function of the dimension. We will also consider rank two commutative semifields which are 10-dimensional over their center, and commutative semifields having rank 3 over their middle nucleus.

References

[1] Simeon Ball, Aart Blokhuis, and Michel Lavrauw. On the classification of semifield flocks. *Advances in Mathematics*, **180** (2003), 104–111.

On the Asymptotic Tightness of the Griesmer Bound

Assia Rousseva [1]

Sofia University "St. Kl. Ohridski"

(Joint work with Ivan Landjev)

The Griesmer bound is a lower bound on the length n of a linear code as a function of q, k, and d: $n \geq g_q(k,d) := \sum_{i=0}^{k-1} \lceil d/q^i \rceil$. It is known that for fixed q and k Griesmer codes do exist for all d that are sufficiently large. On the other hand, for fixed q and d and $k \to \infty$, $n_q(k,d) - g_q(k,d) \to \infty$. The following question can be viewed as a version of the main problem of coding theory:

Problem A. Given the integer k and the prime power q, what is the exact value of

$$t_q(k) := \max_d (n_q(k,d) - g_q(k,d)).$$

It is well-known that $t_q(2) = 0$. A question equivalent to Problem A in the case of $k = 3$ was asked by S. Ball in the following way: for a fixed $n - d$, is there always a 3-dimensional code meeting the Griesmer bound (maybe a constant or $\log q$ away)? Geometrically, Problem A can be stated as follows:

Problem B. Find the smallest value of t for which there exists a $(g_q(k,d) + t, g_q(k,d) + t - d)$-arc in $\mathrm{PG}(k-1,q)$ for all d. In terms of minihypers it can also be formulated in the following way:

Problem C. If $d = sq^{k-1} - \lambda_{k-2}q^{k-2} - \ldots - \lambda_1 q - \lambda_0$ find the smallest value of t for which there exists a minihyper with parameters

$$(\lambda_{k-2}v_{k-1} + \ldots + \lambda_1 v_2 + \lambda_0 v_1 - t, \lambda_{k-2}v_{k-2} - \ldots - \lambda_1 v_1 - t)$$

in $\mathrm{PG}(k-1,q)$ with maximal point multiplicity s. ($v_k = (q^k - 1)/(q-1)$)

The existing tables for $n_q(k,d)$ for small q and k provide some exact values for $t_q(k)$. We have for instance: $t_q(2) = 0$ for all q; $t_q(3) = 1$ for all $q \leq 19$; $t_q(3) \leq 2$ for $q = 23, 25, 27, 29$; $t_3(4) = 1$; $t_4(4) = 1$; $t_5(4) = 2$ ($t = 2$ for $d = 25$ only); $t_5(5) \leq 5$. In this talk, we present several general upper bounds on $t_q(k)$, as well as bounds for $t_q(3)$ for large q.

[1]This research is supported by the Scientific Research Fund of Sofia University under Contract 80-10-55/19.04.2017.

Embedding of Classical Polar Unitals in PG$(2, q^2)$

Alessandro Siciliano

University of Basilicata

(Joint work with Gábor Korchmáros and Tamás Szőnyi)

A unital, that is, a block-design $2-(q^3+1, q+1, 1)$ is embedded in a projective plane Π of order q^2 if its points and blocks are points and lines of Π. A unital embedded in PG$(2, q^2)$ is Hermitian if its points and blocks are the absolute points and lines of a unitary polarity of PG$(2, q^2)$. A classical polar unital is a unital isomorphic, as a block-design, to a Hermitian unital. We prove that there exists only one embedding of the classical polar unital in PG$(2, q^2)$, namely the Hermitian unital.

Smith normal forms associated with graphs

Peter Sin

University or Florida

Let A be an adjacency matrix of a connected graph. The abelian group with A as relation matrix is called the Smith group of the graph. If instead of A we take the Laplacian matrix L of the graph then the finite part of the corresponding abelian group is called the critical group of the graph. The cyclic decomposition of the Smith group and critical group are given by the Smith normal forms of A and L respectively. This talk will be a survey of recent results on the comput ation of Smith and critical groups of some well known families of graphs, with particular emophasis on strongly regular graphs and representation-theoretic techniques.

Blocking sets with respect to special substructures of projective planes

Tamás Szőnyi

ELTE Eötvös Loránd University, Budapest, Hungary

(Joint work with Aart Blokhuis and Leo Storme)

A substructure S of a projective plane is a set of points P and a set of lines L with the property that that every line $\ell \in L$ contains at least 2 points of P. A blocking set in S is a subset B of P with the property that every line in L contains at least one point of B. The aim is to prove (non-trivial) lower bounds on the size of blocking sets. This setting is too general to get interesting results, so we shall consider special substructures, as suggested by Franco Mazzocca. For example, the affine plane is such a substructure and for that case we have the famous results of Jamison, Brouwer-Schrijver, when the plane is desarguesian. This shows that one can get interesting results and the small blocking sets are not always related to small blocking sets of the entire projective plane. Another interesting substructure (again in the desarguesian plane) is to consider exterior (or secant) lines with respect to a given conic. In these cases there are results by Aguglia-Korchmáros, Giulietti-Montanucci, Blokhuis-Korchmáros-Mazzocca.

In the present talk we consider the following substructure: let us consider a desarguesian plane of order q^2 and let P be the union of the points of t disjoint Baer subplanes. It is well known that every line intersects P in either t or $q+t$ points. Let L be the set of lines meeting P in exactly $q+t$ points. One construction for a blocking set in this substructure is to take one subline in each Baer subplane, another one is to take one of the Baer subplanes. For small t, the first construction has size $t(q+1)$ and we show that they are the smallest blocking sets of this substructure if t is less than $\sqrt{q}/2$. For large t (=very close to q^2-q+1) , the other trivial construction is optimal.

On the metric dimension of affine planes, biaffine planes and generalized quadrangles

Marcella Takáts

MTA-ELTE Geometric and Algebraic Combinatorics Research Group

(Joint work with Daniele Bartoli, Tamás Héger and György Kiss)

In this talk we study the metric dimension of the incidence graph of particular partial linear spaces.

For a connected graph $G = (V, E)$ and $x, y \in V$, $d(x, y)$ denotes the distance of x and y (that is, the length of the shortest path joining x and y). A vertex $v \in V$ is *resolved* by $S = \{v_1, \ldots, v_n\} \subset V$ if the ordered list $(d(v, v_1), d(v, v_2), \ldots, d(v, v_n))$ is unique. S is a *resolving set* for G if it resolves all the elements of V. The *metric dimension* $\mu(G)$ of G is the size of a smallest resolving set for it. A *metric basis* of G is a resolving set for G of size $\mu(G)$. Resolving set of a point-line geometry refers to the resolving set of its incidence graph.

Resolving sets of graphs have been studied since the mid '70s, and a lot of study has been carried out in distance-regular graphs ([1, 2, 3]). The current study has been motivated by the work of Bailey. In [4] Héger and Takáts determined the metric dimension of projective planes of order $q \geq 23$ and listed all metric bases for projective planes of order $q \geq 23$.

In the talk we prove that the metric dimension of an *affine plane* of order $q \geq 13$ is $3q - 4$ and describe all resolving sets of that size if $q \geq 23$. The metric dimension of a *biaffine plane*(also called a flag-type elliptic semiplane) of order $q \geq 4$ is shown to fall between $2q - 2$ and $3q - 6$, while for Desarguesian biaffine planes the lower bound is improved to $8q/3 - 7$ under $q \geq 7$, and to $3q - 9\sqrt{q}$ under certain stronger restrictions on q. We determine the metric dimension of *generalized quadrangles* of order $(s, 1)$, s arbitrary. We derive that the metric dimension of generalized quadrangles of order (q, q), $q \geq 2$, is at least $\max\{6q - 27, 4q - 7\}$, while for the classical generalized quadrangles $W(q)$ and $Q(4, q)$ it is at most $8q$.

References

[1] R. F. Bailey, The metric dimension of small distance-regular and strongly regular graphs. *Australas. J. Combin.* **62**:1 (2015), 18–34.

[2] R. F. Bailey, On the metric dimension of imprimitive distance-regular graphs. *Ann. Comb.* **20**:4 (2016), 641–659.

[3] R. F. Bailey, P. J. Cameron, Base size, metric dimension and other invariants of groups and graphs. *Bull. Lond. Math. Soc.* **43** (2011), 209–242.

[4] T. Héger, M. Takáts, Resolving sets and semi-resolving sets in finite projective planes, *Electron. J. Combin.* **19**:4 (2012), #P30.

[5] D. Bartoli, T. Héger, Gy. Kiss, M. Takáts, On the metric dimension of affine planes, biaffine planes and generalized quadrangles, submitted.

A variation of the dual hyperoval $\mathcal{S}_c$ using a presemifield.

Hiroaki Taniguchi

National Institute of Technology, Kagawa College

The concept of higher dimensional dual hyperovals (DHOs) are introduced in [1]. For $GF(2)$-vector spaces V and W, bilinear DHO $\mathcal{S}$ in $V \oplus W$ is defined as $\mathcal{S} = \{X(t) \mid t \in V\}$ where $X(t) = \{(x, B(x,t)) \mid x \in V\} \subset V \oplus W$ using a $GF(2)$-bilinear mapping $B : V \oplus V \to W$ which satisfies some conditions. Let $V_1 := V(l, GF(2^r))$, the vector space over $GF(2^r)$ of rank l. In [2], we construct a DHO called $\mathcal{S}_c$, or $\mathcal{S}_c(l, GF(2^r))$, for $rl \geq 4$ and $c \in GF(2^r)$ with $Tr(c) = 1$, using a $GF(2)$-bilinear mapping $B : V \oplus V \to W$ with $V = V_1 \oplus GF(2)$ and $W = \overline{V_1 \otimes_{GF(2^r)} V_1}$, the symmetric tensor space over $GF(2^r)$. Let $S = (GF(2^r), +, \star)$ be a presemifield which is non-isotopic to commutative presemifields. In this talk, using the multiplication of the presemifield S, we modify W to $W^{'}$, and define a bilinear mapping $B^{'} : V \to W^{'}$ from B. Then we have a bilinear DHO $\mathcal{S}$ from the bilinear mapping $B^{'}$. We prove that $\mathcal{S}$ is not isomorphic to $\mathcal{S}_c$. We also investigate on isomorphism problems of such DHOs.

References

[1] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, Contribution to Algebra and Geometry, **40** (1999), 503–532.

[2] H. Taniguchi, New dimensional dual hyperovals, which are not quotients of the classical dual hyperovals, Discrete Mathematics, **337** (2014), 65–75.

Resolvable designs and maximal arcs in projective planes

Vladimir D. Tonchev

Michigan Technological University

Let $D = \{X, \mathcal{B}\}$ be a Steiner 2-$(v, k, 1)$ design with point set X, collection of blocks $\mathcal{B}$, and let v be a multiple of k, $v = nk$. A *parallel class* is a set of $v/k = n$ pairwise disjoint blocks, and a *resolution* is a partition R of $\mathcal{B}$ into $r = (v-1)/(k-1)$ disjoint parallel classes. A design is *resolvable* if it admits a resolution.

Two resolutions R_1, R_2,

$$R_1 = P_1^{(1)} \cup P_2^{(1)} \cup \cdots P_r^{(1)}, \ R_2 = P_1^{(2)} \cup P_2^{(2)} \cup \cdots P_r^{(2)}$$

are *compatible* if they share one parallel class, $P_i^{(1)} = P_j^{(2)}$,
and $|P_{i'}^{(1)} \cap P_{j'}^{(2)}| \leq 1$ for $i' \neq i$ and $j' \neq j$.

In this talk, we discuss an upper bound on the maximum number of mutually compatible resolutions of a resolvable 2-$(nk, k, 1)$ design D. The bound is attainable if and only if D is embeddable as a maximal $(kq - q + k, k)$-arc in a projective plane of order $q = (v-k)/(k-1)$.

The maximal sets of mutually compatible resolutions of 2-$(52, 4, 1)$ designs associated with maximal $(52, 4)$-arcs in the known projective planes of order 16 have been computed recently. The results of these computations show that some 2-$(52, 4, 1)$ designs are embeddable as maximal arcs in two different planes.

References

[1] V. D. Tonchev, On resolvable Steiner 2-designs and maximal arcs in projective planes, *Designs, Codes, and Cryptography*, to appear, https://link.springer.com/article/10.1007/s10623-016-0243-2, arXiv:1606.00697.

On f-pyramidal Steiner triple systems

Tommaso Traetta

University of Perugia

(Joint work with Marco Buratti and Gloria Rinaldi)

A design is called f-pyramidal when it has an automorphism group fixing f points and acting sharply transitively on the others. We consider the problem of determining the set of values of v for which there exists an f-pyramidal Steiner triple system of order v. Although this problem has been deeply investigated when $f = 1$ [1, 3, 4], it remains open for a special class of values of v. For the next admissible value of f, which is $f = 3$, we provide a complete solution [2]. However, for greater values of f this problem remains widely open.

In this talk, we will present the most recent results on this subject.

References

[1] 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.

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

[3] M. Mishima. *The spectrum of* 1*-rotational Steiner triple systems over a dicyclic group*. Discrete Math. **308** (2008), 2617–2619.

[4] K. T. Phelps, A. Rosa. *Steiner triple systems over arbitrary groups*. Discrete Math. **33** (1981), 57–66.

Nuclei and automorphism groups of generalized twisted Gabidulin codes

Rocco Trombetti

University of Naples Federico II

(Joint work with Yue Zhou)

Generalized twisted Gabidulin codes were introduced by John Sheekey in [1]. The automorphism group of any generalized twisted Gabidulin code as a subset of $m \times n$ matrices over $\mathbb{F}_q$, when $m = n$, has been completely determined in [2].

This talk is based on results contained in [3], in which we deal with the same problem for $m < n$. Precisely, for such codes we determine, under certain conditions on their parameters, the middle nucleus and the right nucleus, which are important invariants with respect to the equivalence for rank metric codes. Furthermore, we also use them to derive necessary conditions on the automorphisms of any generalized twisted Gabidulin code.

References

[1] J. Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10(3):475–488, 2016.

[2] G. Lunardon, R. Trombetti, and Y. Zhou. Generalized twisted Gabidulin codes. *arXiv:1507.07855 [cs, math]*, July 2015. arXiv: 1507.07855.

[3] R. Trombetti, Y. Zhou. Nuclei and automorphism groups of generalized twisted Gabidulin codes, 2016. arXiv:1611.04447.

Classification of Hyperovals in PG(2, 64)

Peter Vandendriessche

Ghent University

Definition. A hyperoval in PG(2, q) is a set of $q + 2$ points, no three collinear.

It is easily shown that hyperovals only exist for q even. Hyperovals have been classified in PG(2, q), $q \leq 32$ [1], but the techniques used there are not sufficient to handle PG(2, 64).

In this talk I will describe a new exhaustive search technique that has lead to a full classification of the hyperovals in PG(2, 64), proving the conjecture that no hyperoval with trivial automorphism group exists in this plane.

References

[1] T. Penttila and G.F. Royle, Classification of hyperovals in PG(2, 32), *Journal of Geometry* **50** (1994), 151–158.

The number of points of weight 2 in a linear set on a projective line

Geertrui Van de Voorde

University of Canterbury, Christchurch

(Joint work with John Sheekey)

It is well know that a linear set $\mathcal{L}$ of rank $k+1$ contained in a line $L = \mathrm{PG}(1, q^t)$ can be constructed as the projection onto L of a k-dimensional subgeometry $\Omega = \mathrm{PG}(k, q)$ from a certain $(k-2)$-dimensional subspace Π of $\mathrm{PG}(k, q^t)$, skew from Ω and L (see [2]). In this setting, the weight of a point P of $\mathcal{L}$ equals $\dim(\langle \Pi, P\rangle \cap \Omega) + 1$.

It was shown in [1] that the existence of an i-club in $\mathrm{PG}(1, 2^t)$ is equivalent to a translation KM-arc of type 2^i of rank t (i-clubs are linear sets that have one point of weight i and all others of weight 1). Motivated by a computer result about the non-existence of 2-clubs of rank t for certain values of t and q, our aim is to investigate the possibilities for the number of weight 2 points in a linear set.

In this talk, we will report on work in progress. We will show how to represent points of $\mathrm{PG}(k, q^n)$ as $\mathbb{F}_q$-linear maps and how to link our problem to the problem of the number of rank 2 maps that are contained in a certain subspace.

References

[1] M. De Boeck and G. Van de Voorde. A linear set view on KM-arcs. *J. Algebraic Combin.* **44(1)** (2016), 131–164.

[2] G. Lunardon and O. Polverino. Translation ovoids of orthogonal polar spaces. *Forum Math.* **16** (2004), 663–669.

Partial Difference Sets in Abelian Groups

Zeying Wang

Michigan Technological University

Recently we proved a theorem for strongly regular graphs that provides numerical restrictions on the number of fixed vertices and the number of vertices mapped to adjacent vertices under an automorphism. We then used this result to develop some new techniques to study regular partial difference sets in Abelian groups. Our main results so far are the proof of non-existence of PDS in Abelian groups with small parameters [1, 3], a complete classification of PDS in Abelian groups of order $4p^2$ [2], and a proof that no non-trivial PDS exist in Abelian groups of order $8p^3$ [4].

In this talk I plan to give an overview of these results with a focus on our most recent work on the PDS in Abelian groups of order $8p^3$, where p is a prime number ≥ 3.

References

[1] S. De Winter, E. Kamischke and **Z. Wang**, Automorphisms of strongly regular graphs with applications to partial difference sets, *Designs, Codes and Cryptography*, **79**, 471–485 (2016)

[2] S. De Winter and **Z. Wang**, Classification of partial difference sets in Abelian groups of order $4p^2$, *Designs, Codes and Cryptography*, (2016). doi:10.1007/s10623-016-0280-x

[3] S. De Winter and **Z. Wang**, Non-existence of two types of partial difference sets, *Discrete Mathematics*, accepted in 2017.

[4] S. De Winter, **Z. Wang**, *Non-existence of non-trivial regular partial difference sets in Abelian groups of order* $8p^3$, preprint.

Packing Sets

Arne Winterhof

Austrian Academy of Sciences (RICAM, Linz)

(Joint work with Ily Shkredov and Oliver Roche-Newton)

For a given subset $A \subseteq G$ of a finite abelian group $(G, \circ)$, we study the problem of finding a large packing set B for A, that is, a set $B \subseteq G$ such that $|A \circ B| = |A||B|$. Rusza's covering lemma and the trivial bound imply the existence of such a B of size $|G|/|A|^2 \le |G|/|A \circ A^{-1}| \le |B| \le |G|/|A|$. We show that these bounds are in general optimal. More precisely, denote by $\nu(A)$ the maximal size of an A-packing set, then essentially any $\nu(A)$ in the interval $[|G|/|A|^2, |G|/|A|]$ can appear for some $|A|$.

The case that G is the multiplicative group of the finite field $\mathbb{F}_p$ of prime order p and $A = \{1, 2, \ldots, \lambda\}$ for some positive integer λ is particularly interesting in view of the construction of limited-magnitude error correcting codes. Here we construct a packing set B of size $|B| \gg p(\lambda \log p)^{-1}$ for any $\lambda \le 0.9p^{1/2}$. This result is optimal up to the logarithmic factor.

Applications of Linear Algebraic Methods in Combinatorics and Finite Geometry

Qing Xiang

University of Delaware

(Joint work with Ferdinand Ihringer and Peter Sin)

Most combinatorial objects can be described by incidence, adjacency, or some other $(0,1)$-matrices. So one basic approach in combinatorics is to investigate combinatorial objects by using linear algebraic parameters (ranks over various fields, spectrum, Smith normal forms, etc.) of their corresponding matrices. In this talk, we will look at some successful examples of this approach; some examples are old, and some [1] are new. In particular, we will talk about the recent bounds [2] on the size of partial spreads of $H(2d-1,q^2)$ and on the size of partial ovoids of the Ree-Tits octagon.

References

[1] Jordan Ellenberg, Dion Gijswijt, On large subsets of $\mathbf{F}_q^n$ with no three-term arithemetic progressions, Annals Math. **185** (2017), 339–343.

[2] Ferdinand Ihringer, Peter Sin, Qing Xiang, New bounds for partial spreads of $H(2d-1,q^2)$ and partial ovoids of the Ree-Tits octagon, to appear in J. Combin. Theory (A), `arXiv:1604.06172`

New maximum scattered linear sets of the projective line

Ferdinando Zullo

Università degli Studi della Campania "Luigi Vanvitelli"

(Joint work with Bence Csajbók and Giuseppe Marino)

A point set L_U of $\mathrm{PG}(1,q^n)=\mathrm{PG}(W,\mathbb{F}_{q^n})$ is said to be an $\mathbb{F}_q$-**linear set of rank** k if it is defined by the non-zero vectors of a k-dimensional $\mathbb{F}_q$-subspace U of W

$$L_U=\{\langle \mathbf{u}\rangle_{\mathbb{F}_{q^n}} : \mathbf{u}\in U\setminus\{\mathbf{0}\}\}.$$

Also, L_U is said to be **maximum scattered** if $k=n$ and $|L_U|=\dfrac{q^n-1}{q-1}$. In this case U is a **maximum scattered** $\mathbb{F}_q$-subspace of W.

It may happen that two $\mathbb{F}_q$-linear sets L_U and L_V of $\mathrm{PG}(1,q^n)$ are $\mathrm{P\Gamma L}(2,q^n)$-equivalent (or simply equivalent) even if the $\mathbb{F}_q$-subspaces U and V are not in the same orbit of $\Gamma\mathrm{L}(2,q^n)$. The Γ**L-class** of an $\mathbb{F}_q$-linear set L_U of $\mathrm{PG}(1,q^n)=\mathrm{PG}(W,\mathbb{F}_{q^n})$ of rank n with maximum field of linearity $\mathbb{F}_q$ is the number of ΓL-inequivalent $\mathbb{F}_q$-subspaces of W defining L_U (see [2]).

The ΓL-class of a linear set is a projective invariant and plays a crucial role in the study of linear sets up to equivalences.

In [1] and [5] are presented the first examples of maximum scattered $\mathbb{F}_q$-linear sets of the projective line $\mathrm{PG}(1,q^n)=\mathrm{PG}(W,\mathbb{F}_{q^n})$, which result to be non-equivalent. More recently in [3] and in [6], new examples of maximum scattered $\mathbb{F}_q$-subspaces of W have been constructed, but the equivalence problem of the corresponding maximum scattered linear sets is left open.

In [4], by means of the study of the ΓL-class, we show that the $\mathbb{F}_q$-linear sets presented in [3] and in [6], for $n=6$ and $n=8$, are new. Also, we present another example of maximum scattered $\mathbb{F}_q$-linear set in $\mathrm{PG}(1,q^6)$, giving new MRD-codes.

References

[1] A. Blokhuis and M. Lavrauw: Scattered spaces with respect to a spread in $PG(n,q)$, *Geom. Dedicata* **81** No.1–3 (2000), 231–243.

[2] B. Csajbók, G. Marino and O. Polverino: Classes and equivalence of linear sets in $\mathrm{PG}(1,q^n)$, https://arxiv.org/abs/1607.06962.

[3] B. Csajbók, G. Marino, O. Polverino and Zanella: A new family of MRD-codes, submitted.

[4] B. Csajbók, G. Marino and F. Zullo: New maximum scattered linear sets of the projective line, manuscript.

[5] G. Lunardon and O. Polverino: Blocking Sets and Derivable Partial Spreads, *J. Algebraic Combin.* **14** (2001), 49–56.

[6] J. Sheekey: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* **10**(3) (2016), 475–488.

5 Participants

Abdukhalikov, Kanat
Al-Ogaidi, Awss
Alderson, Tim
Ball, Simeon
Bamberg, John
Bartoli, Daniele
Betten, Anton
Bishnoi, Anurag
Brown, Julia
Buratti, Marco
Coulter, Robert
Csajbók, Bence
Davis, Jim
De Boeck, Maarten
De Bruyn, Bart
Do Duc Tai
Doyen, Jean
Durante, Nicola
Enge, Andreas
Feng, Tao
Gavrilyuk, Alexander
Ghorpade, Sudhir
Giuzzi, Luca
Gow, Roderick
Hans Havlicek
Ihringer, Ferdinand
Jan De Beule
Jungnickel, Dieter
Jurrius, Relinde
Karaoğlu, Fatma
Korchmáros, Gábor
Landjev, Ivan
Lansdown, Jesse
Lavrauw, Michel
Longobardi, Giovanni
Lunardon, Guglielmo
Maegher, Karen
Marino, Guiseppe
Mattheus, Sam
Mazzocca, Franco
Meidl, Wilfried
Merola, Francesca
Metsch, Klaus
Montanucci, Maria
Mühlherr, Bernhard
Nakić, Anamari
Napolitano, Vito
Nastăse, Esmeralda
Özbudak, Ferruh
Pavese, Francesco
Piñero, Fernando
Polverino, Olga
Popiel, Tomasz
Pott, Alexander
Rodgers, Morgan
Rosenthal, Joachim
Rousseva, Assia
Schmidt, Kai-Uwe
Sin, Peter
Storme, Leo
Sziklai, Peter
Szőnyi, Tamás
Takáts, Marcella
Taniguchi , Hiroaki
Tommaso Traetta
Tonchev, Vladimir
Trombetti, Rocco
Van de Voorde, Geertui
Vandendriessche, Peter
Wassermann, Alfred
Werner, Daniel
Winterhof, Arne
Xiang, Qing
Zeyng Wang
Zullo, Fernando