ALCOMA 15

Algebraic Combinatorics and Applications

MARCH 15-20, 2015
KLOSTER BANZ, GERMANY

UNIVERSITÄT
BAYREUTH

Welcome from the organizing committee

It is a pleasure to welcome everyone to the Fourth International ALCOMA Conference on Algebraic Combinatorics and Applications in the beautiful Kloster Banz.

The primary focus of ALCOMA lies in the connections between combinatorial designs, geometry and codes. A special focus of this conference is on q-analogues of designs and their recent application in random network coding.

ALCOMA 15 is dedicated to the memory of Axel Kohnert, our longtime colleague and friend. Axel has passed away on 11 Dec. 2013 in the aftermath of a tragic accident in Oct. 2013 at the age of 51. This loss is still unconceivably for us. Axel was one of the organizers of ALCOMA99, the first conference of this series, and was the main organizer of ALCOMA 5 and 10. His work established the international success of this conference series.

We are proud that the most reknown experts in this area agreed to come. Also the list of speakers of invited and contributed talks is very distinguished and we are looking forward having a great conference with exciting discussions.

We thank the COST Action IC1104 “Random Network Coding and Designs over GF(q)” and the Oberfrankenstiftung for their generous funding of the conference.

The impressive former monastery *Kloster Banz* is located in the Bavarian region *Upper Franconia*, which is famous for its beer and the good and solid Franconian food.

Once again, welcome to Kloster Banz. Please let us know if there is anything we can help you with to ensure you having a great time during your stay at Kloster Banz.

Adalbert Kerber
Michael Kiermaier
Reinhard Laue
Mario-Osvin Pavčević
Alfred Wassermann

Social Program

- Sunday 19:00 – 23:00: Welcome buffet (Bierstübla)
- Monday 19:00: Reception (Kaisersaal)
- Tuesday 18:00: Guided tour through Kloster Banz (Foyer)
- Wednesday 14:00 – 22:00: Excursion to Bamberg
- Thursday 10:00: Conference photo
- Thursday 19:00: Conference dinner

Web page: http://alcoma15.uni-bayreuth.de
Version March 16, 2015 – 13:00

Conference Program

Monday, March 16th

9:00	**Opening** (Kutschenhalle)	
9:30	Plenary lecture **(Kutschenhalle)** Chair: *M. Greferath* Jonathan Jedwab: *Constructions of complex equiangular lines*	
10:30	**Coffee**	
	Room S3 Chair: *E. Byrne*	**Room S4** Chair: *D. Vukobratović*
11:00	Klara Stokes *Spread codes and the Klein correspondence*	Dimitris E. Simos *Combinatorial designs and the analysis of their application to channel estimation*
11:25	Ilaria Cardinali *Polar Grassmann codes part I*	Sara D. Cardell *Performance of SPC product codes under the erasure channel*
11:50	Luca Giuzzi *Polar Grassmann codes part II*	Gábor P. Nagy *On the rates of codes for high noise binary symmetric channels*
12:15	**Lunch (Alberada)**	
14:00	Plenary lecture **(Kutschenhalle)** Chair: *T. Helleseth* Thomas Honold: *Remarks on constant-dimension subspace codes*	
	Room S3 Chair: *C. Bachoc*	**Room S4** Chair: *T. van Trung*
15:00	Wolfgang Willems *Algebraic structures of MRD codes*	Masakazu Jimbo *Cyclic codes with large minimum distances and related combinatorial designs*
15:25	John Sheekey *A new family of maximum rank distance codes*	Ying Miao *Strongly separable codes*
15:50	**Coffee**	
16:20	Kai-Uwe Schmidt *Symmetric rank distance codes*	Faina Solov'eva *Linear coordinates for perfect codes and STS*
16:45	Ferruh Özbudak, Kamil Otal *Non-Gabidulin MRD codes*	Sanja Rukavina *Self-dual codes from extended orbit matrices of symmetric designs*
17:10	Anna-Lena Trautmann *Characterizations of MRD and Gabidulin codes*	Tomoko Adachi *Secret sharing scheme utilizing combinatorial design*
19:00	**Reception (Kaisersaal)**	
19:45	**Dinner**	

Tuesday, March 17th

9:00	Plenary lecture **(Kutschenhalle)** Gabriele Nebe: *Automorphisms of extremal codes*	Chair: *A. Kerber*
10:00	**Coffee**	
	Room S3 Chair: *D. Panario*	**Room S4** Chair: *J. Doyen*
10:30	Assia Rousseva *New results on Griesmer codes and arcs*	Doris Dumičić Danilović *Construction of block designs admitting a solvable automorphism group*
10:55	Jens Zumbrägel *On bounds for batch codes*	Oktay Olmez *Partial geometric designs with prescribed automorphisms*
11:20	Rouzbeh Touserkani *Generation and propagation in graphs*	Tanja Vučičić *Hadamard difference sets and corresponding regular partial difference sets in groups of order 144*
11:45	Anastasia Vasil'eva *Distance regular colorings of Cayley graphs of Z^n*	Marco Buratti *Hamiltonian cycle systems and their automorphism groups*
12:10	**Lunch (Alberada)**	
14:00	Plenary lecture **(Kutschenhalle)** Tor Helleseth: *Coding and stream ciphers*	Chair: *P. Farkas*
	Room S3 Chair: *G. Nebe*	**Room S4** Chair: *R. Laue*
15:00	Tatsuya Maruta *On the geometric construction of optimal linear codes*	Tran van Trung *Construction of simple 3-designs using resolution*
15:25	Darwin Villar *On extremal type III codes*	Marcus Greferath *On mosaics of combinatorial designs*
15:50	**Coffee**	
16:20	Janne Kokkala *Classification of unrestricted 8-ary MDS codes*	Vedran Krčadinac *Tiling groups with difference sets*
16:45	Bernardo Rodrigues *On a 14-dimensional self-orthogonal code invariant under the simple group $G_2(3)$*	Denis Krotov *On the q-ary Steiner and other-type trades*
17:10	Leo Creedon *Towards a group ring construction of codes using dihedral groups*	Dean Crnković *On some Menon designs and related structures*
18:00	**Guided tour through Kloster Banz** (Foyer)	
19:30	**Dinner**	

Wednesday, March 18th

9:00	Plenary lecture **(Kutschenhalle)** Alexander Pott: *Vectorial bent functions*	Chair: *J. Climent*
10:00	**Coffee**	
10:30	Plenary lecture **(Kutschenhalle)** Daniel Panario: *Open problems for polynomials over finite fields and applications*	Chair: *J. Jedwab*
11:30	Plenary lecture **(Kutschenhalle)** Dejan Vukobratović: *Codes on random geometric graphs*	Chair: *J. Jedwab*
12:30	**Lunch (Alberada)**	
14:00	**Excursion**	

Thursday, March 19th

9:00	Plenary lecture **(Kutschenhalle)** Chair: *M. Braun* Eimear Byrne: *On the index coding and caching problem*	
10:00	**Coffee**	**Conference photo**
	Room S3 Chair: *T. Etzion*	**Room S4** Chair: *A. Pott*
10:30	Heide Gluesing-Luerssen *Constructions of subspace codes*	Leo Storme *Cameron-Liebler k-classes in $PG(2k+1,q)$*
10:55	Patric Östergård *New lower bounds for constant dimension subspace codes*	Markus Grassl *Maximal partial symplectic spreads over small fields*
11:20	Sascha Kurz *ILP techniques for binary subspace codes*	Daniele Bartoli *Complete $(k,3)$-arcs from quartic curves*
11:45	Daniel Heinlein *Towards a classification of special partial spreads and subspace codes*	Katharina Kusejko *Simultaneous diagonalization of conics in $PG(2,q)$*
12:10	**Lunch (Alberada)**	
14:00	Plenary lecture **(Kutschenhalle)** Chair: *T. Honold* Jan De Beule: *Tight sets in finite geometry*	
	Room S3 Chair: *K. Metsch*	**Room S4** Chair: *S. Blackburn*
15:00	Francesco Pavese *Subspace Codes in $PG(2n-1,q)$*	Vasyl Ustimenko *On combinatorics of projective geometry and multivariate cryptography*
15:25	Güneş Karabulut Kurt *Network coding in wireless systems: impact of wireless links*	Joachim Rosenthal *McEliece type cryptosystem based on Gabidulin codes*
15:50	**Coffee**	
16:20	Ragnar Freij *Local repairability through almost-uniform matroids*	Ivan Landjev *On the existence of spreads in projective Hjelmslev spaces*
16:45	Thomas Westerbäck *Matroid theory and locally repairable codes*	Laurence Um *Quaternary convolutional codes and linear systems*
17:10	Oliver Gnilke *Designs on Matroids*	Harald Gropp *Configurations — 10 years later*
17:35		David Thomson *Generalized Sudoku arrays and other combinatorial objects with strong regularity*
19:00	**Conference dinner**	

Friday, March 20th

9:00	Plenary lecture **(Kutschenhalle)** Michael Braun: *A survey on designs over finite fields*			Chair: *J. Rosenthal*
10:00	**Coffee**			
	Room S3	Chair: *M. Elia*	**Room S4**	Chair: *J. De Beule*
10:30	Anamari Nakić *On q-analogs of 3-(v,k,λ_3) designs*		Lucia Moura *Variable strength covering arrays*	
10:55	Michael Kiermaier *Recursive construction of subspace designs*		André G. Castoldi *Ordered orthogonal array construction using LFSR sequences*	
11:20	Netanel Raviv *q-analogue of binary cyclic sequences*		Andrea Švob *Transitive combinatorial structures invariant under some subgroups of $S(6,2)$*	
11:45	Relinde Jurrius *The dual q-matroid and the q-analogue of a complement*		Kristijan Tabak *Norm invariance method and application*	
12:10	**Lunch (Alberada)**			
14:00	**MC Meeting**			

Abstracts

Constructions of complex equiangular lines

Jonathan Jedwab

Simon Fraser University, Burnaby BC, Canada

How many equiangular lines can be placed in complex space of dimension d? This is a highly challenging question, lying at the intersection of algebraic combinatorics and quantum information theory.

A simple linear algebraic argument shows the answer to be at most d^2. Zauner conjectured in 1999 that sets of d^2 equiangular lines indeed exist for every d, and specified a potential construction method for such sets. His method has been successfully applied for twenty dimensions d, the largest being 48, but the sets of lines it produces become enormously complicated as d increases and the associated computations rapidly become infeasible. It remains unclear whether Zauner's conjecture is true, and if so whether his construction method can be successfully applied for infinitely many values of d.

I shall describe a radically different approach to the construction of large sets of complex equiangular lines, involving the modification of known combinatorial designs. This new approach produces examples with transparent combinatorial structure, including a simple set of $d^2/4$ equiangular lines for infinitely many dimensions d.

This is joint work with Amy Wiebe.

Spread codes and the Klein correspondence

Klara Stokes

University of Skövde

A subspace code is a set of subspaces of some vector space over F_q. If all the subspaces are of the same dimension k, then the code is called a constant-dimension subspace code and the code is contained in the Grassmannian $G_{\mathbb{F}_q}(n,k)$. A t-spread is a collection of subspaces of $PG(n,\mathbb{F}_q)$ that partitions the points. This ensures that all elements of the spread is on a certain distance from each other, when regarded as elements of $G_{\mathbb{F}_q}(n+1,t+1)$. Therefore t-spreads make attractive subspace codes. In this talk I will describe a new decoder for spread codes which is based on intersections in the Grassmannian.

Polar Grassmann Codes Part I

Ilaria Cardinali

University of Siena (IT)

Let $V := V(m,q)$ be an m-dimensional vector space defined over a finite field F_q and for $k = 1,\dots,m-1$ denote by $\mathscr{G}_{m,k}$ the k-Grassmannian of V naturally embedded in the k-th exterior power $\bigwedge^k V$ of V.

In this talk we will describe a family $\mathscr{P}_{n,k}$ of projective codes arising from the subvarieties of $\mathscr{G}_{2n+1,k}$ defined by the linear subspaces being totally singular with respect to a given non-degenerate quadratic form of V.

We will discuss the parameters of $\mathscr{P}_{n,2}$ focusing on line polar Grassmann codes, namely $\mathscr{P}_{n,2}$. Suitable Encoding/Decoding techniques for $\mathscr{P}_{n,2}$ will be reported in the second part of the talk (Polar Grassmann Codes II).

[1] I. Cardinali and L. Giuzzi, *Codes and caps from orthogonal Grassmannians*, Finite Fields Appl. **24** (2013), 148-169.

[2] I. Cardinali, L. Giuzzi and A. Pasini, *Line Polar Grassmann Codes of Orthogonal Type*, submitted, arxiv:1407.6149

Polar Grassmann Codes Part II

Luca Giuzzi

Università di Brescia (IT)

Let $\mathscr{P}_{n,2}$ be a line orthogonal Grassmann code. In this talk we will introduce an efficient enumerative coding and decoding strategy for $\mathscr{P}_{n,2}$. More precisely, we will define an enumerative coding scheme on the lines of a non-degenerate parabolic quadric and then we will apply such enumeration technique to implement the codes $\mathscr{P}_{n,2}$. We shall also discuss encoding and error correction for such codes.

[1] I. Cardinali and L. Giuzzi, *Enumerative Coding for Line Polar Grassmannians*, Submitted.

Combinatorial Designs and the Analysis of their Application to Channel Estimation

Philipp Grabenweger‡, Christoph Pacher‡ and Dimitris E. Simos†[1,2]

† SBA Research, Vienna, Austria
‡ AIT Austrian Institute of Technology, Digital Safety & Security Department, Vienna, Austria

We consider a binary symmetric channel with crossover probability p, i.e. a BSCP(p). So far we have analyzed maximum likelihood (ML) estimation of p based on the syndrome of a low-density parity-check code (LDPC) with constant check node degree. We could obtain analytical expressions for the ML estimator, for its bias and its mean squared error (MSE). However, we have derived these results under the assumption that the check equations are statistically independent, a condition that is strictly speaking not fulfilled.

These regularity conditions needed by LDPC codes for channel estimation, can also be met by other discrete structures like combinatorial designs. Promising candidates arise from incomplete block designs (IBDs) and important subclasses of them like regular graph designs (RGDs). Here we mainly report on studies of the latter structures which enjoy certain overlapping and intersection properties. In particular, we analyze different families of them and optimize their parameters in terms of bit error estimators. Our findings indicate that RGDs can also be used for the analysis of bit error estimation by using the concurrence matrices of the respective designs. In particular, we extend the previous results by a more complete analysis taking correlations of different orders between the syndrome bits into account and now obtain a perfect agreement between the analytical results and numerical simulations.

[1] Corresponding author.

[2] This work was carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme. This Programme is supported by the Marie Curie Co-funding of Regional, National and International Programmes (COFUND) of the European Commission.

Performance of SPC product codes under the erasure channel

Sara D. Cardell[1], Joan-Josep Climent[1] and Alberto López Martín[2]

[1]**Departament D'Estadística e Investigació Operativa**
Universitat d'Alacant
[2]**Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro**

The single parity-check (SPC) code is one of the most popular MDS error detection codes, since it is very easy to implement [1]. One bit is appended to an information sequence of length $n-1$, such that the resultant codeword has an even number of ones. Two or more SPC codes can be used jointly to obtain an SPC product code. This product code has 4 as minimum distance, then it can recover all erasure patterns with one, two, and three erasures. However, up to $2n-1$ erasures can be corrected in some special cases. Furthermore, a codeword of length n^2 can be represented by an erasure pattern of size $n \times n$, where the unique information considered is the position of the erasures. In [1], authors proposed an approach of the post-decoding erasure rate of the SPC product code. This process was based on observing the structure of the erasure patterns, classifying them into correctable or uncorrectable. In this work, we represent each erasure pattern by a binary matrix where there is a 1 in the position of the erasures. Then, the problem of counting patterns can be seen as a problem of counting binary matrices. In [2], the author used Kotska numbers to count binary matrix with a fixed row and column sum. Here, we use the same idea to provide an expression that helps to count the number of strict uncorrectable erasure patterns.

References

[1] Kousa, M. A.: A novel approach for evaluating the performance of SPC product codes under erasure decoding. IEEE Transactions on Communications **50**(1), 7–11 (2002).

[2] Brualdi, R. A.: Algorithms for constructing (0,1)-matrices with prescribed row and column sum vectors. Discrete Mathematics **306**(23), 3054–3062 (2006).

On the rates of codes for high noise binary symmetric channels

Gábor P. Nagy

University of Szeged (Hungary)

In my talk, I will present some experimental results on the following "challenge": You have to send a random message $\mathbf{m}$ of $k = 3000$ bits through a binary symmetric channel with bit error probability $p = 0.1$. Find (and implement in SAGE) encoding and decoding functions $E : \mathbb{F}_2^k \to \mathbb{F}_2^n$, $D : \mathbb{F}_2^n \to \mathbb{F}_2^k$ which reduce the bit error probability of the channel to $p^* = 0.001$. The winner is the code (E,D) with the highest rate k/n. (Joint research with M. Maróti.)

Remarks on Constant-Dimension Subspace Codes

Thomas Honold

Department of Information Science and Electronics Engineering
Zhejiang University, Hangzhou, China

Network Coding has revived the problem of determining the maximum number of k-dimensional subspaces of $\mathbb{F}_q^n$ mutually intersecting in a subspace of dimension at most $t \in \{0, 1, \ldots, k-2\}$. The case $t = 0$, known to geometers as maximal partial spreads, has been most explored, with complete results in the cases $k = 2$, any q, and $k = 3$, $q = 2$. In my talk I will discuss the case $t = 1$, $k = 3$ (the maximum number of planes in $\mathrm{PG}(n-1, q)$ intersecting mutually in at most a point) from various perspectives.

Algebraic structures of MRD codes

Wolfgang Willems

Otto-von-Guericke Universität
Magdeburg

We relate MRD codes in the matrix algebra $(\mathbb{F}_q)_{n,n}$ of minimum distance n with algebraic structures in finite geometry like quasifields, semifields, division algebras. In particular, finite semifields lead to linear MRD codes over a prime field which are essentially different from Gabidulin codes. The talk reports on joint work with J. de la Cruz, M. Kiermaier and A. Wassermann.

Maximum rank distance codes and finite semifields

John Sheekey

Universiteit Gent

A *rank metric code* is a code consisting of $n \times n$ matrices with the distance function $d(X,Y) := \operatorname{rank}(X - Y)$. Rank metric codes have close ties to *subspace codes*, which have important applications in network coding.

Maximum rank distance (MRD) codes are rank metric codes $\mathscr{C}$ meeting the Singleton-like bound $|\mathscr{C}| = q^{n(n-d+1)}$, where d is the minimum distance. Linear MRD-codes for each parameter were constructed by Delsarte, and later by Gabidulin. The first non-trivial example of a non-linear MRD-code was recently given by Cossidente, Marino and Pavese for the case $n = 3$, $d = 2$.

In the case $n = d$, linear MRD-codes correspond to *finite (pre)semifields*, that is, nonassociative division algebras. Semifields have received much attention in recent years, though their applications to coding theory have not been exploited to date. We will give an overview on the theory of semifields, and their links to codes.

In this talk we will introduce a new family of linear MRD-codes for each parameter, which are in general inequivalent to any previously known code.

Symmetric rank-distance codes

Kai-Uwe Schmidt

Otto-von-Guericke University, Magdeburg, Germany

Consider a set Y of symmetric matrices over $\mathbb{F}_q$ with the property that, for all distinct $A, B \in Y$, the rank of $A - B$ is at least a given integer d. Let's call such a set a *d-code*. For fixed d, one is usually interested in d-codes containing as many elements as possible. For odd q, I present a sharp bound for the size of a d-code Y that is closed under addition and provide constructions of such sets for which equality holds. Moreover, in case of equality, it is possible to obtain the number of hyperbolic and elliptic matrices of a given rank in Y. These results can be directly translated to classical coding theory. For example, they give the weight enumerators of certain cyclic codes, for which numerous special cases have been previously obtained using long ad hoc calculations. The principal new insights come from a better understanding of the association scheme of symmetric bilinear forms.

A Construction of Some Non-Gabidulin MRD codes

Kamil Otal, Ferruh Özbudak and Eda Tekin

Middle East Technical University

Considering isometries of the rank metric, the equivalence of any two rank metric codes is given in [4]. Up to this equivalence, non-Gabidulin MRD codes are investigated in [2] and the authors obtained some nice results especially for the full rank case.

In this study we investigate rank metric codes using multivariable linearized polynomials. We give a method producing various (linear) rank metric codes including Gabidulin and non-Gabidulin both for the full rank and not full rank case. In this way we give an answer to a question in [2]. Also, some computational results are given.

References

[1] J. Berson, *Linearized polynomial maps over finite fields*, Journal of Algebra, v. 399, pp. 389-406, 2014.

[2] J. Cruz, M. Kiermaier, A. Wassermann and W. Willems, *Algebraic structures of MRD codes*, preprint.

[3] E. M. Gabidulin, *The theory with maximal rank metric distance*, Probl. Inform. Transm., 21, pp. 1-12, 1985.

[4] K. Morrison, *Equivalence of rank-metric and matrix codes and automorphism groups of Gabidulin codes*, ArXiv:1304.0501v1, 2013.

Characterizations of MRD and Gabidulin codes

Anna-Lena Trautmann

University of Zurich
Balsbergweg 7
8302 Kloten
Schweiz

Maximum rank distance (MRD) codes are a class of optimal matrix codes useful for network coding, among others. Until recently, the only known construction for these codes was the one of Delsarte (1973) and, independently, Gabidulin (1985). The respective codes are commonly called “Gabidulin codes”. If we use the isomorphism of the vector space over a finite field GF(q) of dimension n and the extension field GF(q^n) of the same field of degree n, we can represent such a matrix code as a block code over the extension field. A q^n-linear matrix code can thus be represented by a generator matrix with entries from the extension field GF(q^n). In this talk we will show some decision criteria, if a given generator matrix gives rise to an MRD code, and furthermore, if such a code is a Gabidulin code. Moreover, these criteria can be used to find non-Gabidulin MRD codes for small parameter sets.

Cyclic codes with large minimum distances and related combinatorial designs

Masakazu Jimbo* **and Satoshi Noguchi**

Nagoya University, Nagoya, JAPAN

For an odd prime power q and positive integers $1 \leq s < q-1$ and $m > 1$, we give a construction of $[q^m - 1, (q-s)^m, d]_q$ cyclic codes with minimum distance $d \geq s\frac{q^m-1}{q-1}$ by utilizing the well-known technique of BCH codes. Moreover, a relation between their extended codes and colored 2-designs are stated.

Strongly Separable Codes

Ying Miao

Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba, Ibaraki 305-8573, Japan

Binary t-frameproof codes (t-FPCs) are used in multimedia fingerprinting schemes where the identification of authorized users taking part in the averaging collusion attack is required. In this paper, a binary strongly $\bar{t}$-separable code ($\bar{t}$-SSC) is introduced to improve such a scheme based on a binary t-FPC. A binary $\bar{t}$-SSC has the same traceability as a binary t-FPC but has more codewords than a binary t-FPC. A composition construction for binary $\bar{t}$-SSCs from q-ary $\bar{t}$-SSCs is described, which stimulates the research on q-ary $\bar{t}$-SSCs with short length. Several infinite series of optimal q-ary $\bar{2}$-SSCs of length 2 are derived from the fact that a q-ary $\bar{2}$-SSC of length 2 is equivalent to a q-ary $\bar{2}$-separable code of length 2. Combinatorial properties of q-ary $\bar{2}$-SSCs of length 3 are investigated, and a construction for q-ary $\bar{2}$-SSCs of length 3 is provided. These $\bar{2}$-SSCs of length 3 have more than 12.5% codewords than 2-FPCs of length 3 could have.

This is a joint work with J. Jiang and M. Cheng.

Linear coordinates for perfect codes and STS

I. Yu. Mogilnykh, F. I. Solov'eva

Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk, Russia; Emails: {ivmog,sol}@math.nsc.ru

We suggest two new characteristics for perfect codes and Steiner triple systems (briefly STS) which allowed us to investigate the symmetry group of certain Mollard codes [1] and solve the problem of the existence of transitive nonpropeliner perfect codes [2]. A *perfect binary code* of length n is a collection of binary vectors of length n such that any binary vector is at distance at most 1 from some codeword. A STS is a collection of blocks (subsets) of size 3 of the n-element point set $P(S)$, such that any pair of distinct elements is exactly in one block. The set of codewords of weight 3 in a perfect code C, that contains the all-zero word is a STS, which we denote $\mathrm{STS}(C)$. With a STS S we associate a *Steiner quasigroup* $(P(S),\cdot)$ to be the point set $P(S)$ of S with a binary operation $\cdot$ such that $i\cdot j=k$, if (i,j,k) is a triple of S and $i\cdot i=i$.

For a STS S on points $\{1,\dots,n\}$ and $i\in\{1,\dots,n\}$, define $\nu_i(S)$ to be the number of different *Pasch configurations*, incident to i, i. e. the collection of triples $\{(i,j,k),(i,j_1,k_1),(i_1 j,j_1),(i_1,k,k_1)\}$. The *kernel* $Ker(C)$ of a code C is the subspace $\{x\in C: x+C=C\}$. For a perfect code C of length n containing the all-zero word for a coordinate position i we consider $\mu_i(C)$ to be the number of code triples, containing i from $Ker(C)$ of the code C: $\mu_i(C)=|\{x\in \mathrm{STS}(C)\cap \mathrm{Ker}(C): i\in supp(x)\}|$. We say that a coordinate i is μ-*linear* for a code C of length n if $\mu_i(C)$ takes the maximal possible value, i. e. $(n-1)/2$. Obviously, two coordinate positions i,j of S or C are in different orbits by symmetry groups of S or C respectively if $\nu_i(S)\neq\nu_j(S)$ or $\mu_i(C)\neq\mu_j(C)$ respectively. We say that a point $i\in\{1,\dots,n\}$ is ν-*linear* for a STS S of order n if $\nu_i(S)$ takes the maximal possible value, i. e. $(n-1)(n-3)/4$. By $Lin_\nu(S)$ and $Lin_\mu(C)$ denote the sets of ν-linear coordinates of S and μ-linear coordinates of C respectively. $Lin_\nu(S)$ and $Lin_\mu(C)$ are characteristics of a proximity of a STS S and a perfect code C to projective STS and the Hamming code respectively.

Theorem. *1. Let C be a perfect binary code. Then we have*

$$Lin_\mu(C)\subseteq Lin_\nu(STS(C)).$$

2. A subdesign of a STS *S on the points $Lin_\nu(S)$ is projective.*

3. A subcode of a perfect code C on the coordinates $Lin_\mu(C)$ is a Hamming code.

References

1. I. Yu. Mogilnykh, F. I. Solov'eva, On symmetry group of Mollard code, submitted to *Electronic Journal of Combin.*

2. I. Yu. Mogilnykh, F. I. Solov'eva, Transitive propelinear perfect codes, Discrete Mathematics. 2015. V. 338. P. 174–182.

* The research was financed by the Russian Science Foundation (project No 14-11-00555).

Self-dual codes from extended orbit matrices of symmetric designs

Sanja Rukavina

Department of Mathematics
University of Rijeka, Croatia

We consider codes spanned by the rows of an orbit matrix of a symmetric design with respect to the action of an automorphism group that acts with all orbits of the same length. We define an extended orbit matrix and show that under some condition the rows of the extended orbit matrix span a code that is self-dual with respect to a certain scalar product.

This is a joint work with Dean Crnković.

Secret Sharing Scheme utilizing Combinatorial Design

Tomoko Adachi

Department of Information Sciences, Toho University, 274-8510, Japan
E-mail: adachi@is.sci.toho-u.ac.jp

A secret sharing scheme is a method to distribute shares of a secret value K among a set of participants P such a way that only the qualified subsets of P are able to reconstruct the value of K from their shares. In 1979, Shamir introduced the secret sharing scheme which was based Lagrange's interpolation formula. This scheme is called Shamir's threshold scheme. A secret sharing scheme has been studied by many scientists until today.

Since the security of a system depends on the amount of information that must be kept secret, the size of the shares given to the participants is key point in the design of secret sharing schemes. Hence, the information rate is an important criterion for measure to a secret sharing scheme.

In this talk, we investigate a secret sharing scheme utilizing combinatorial design and information rate.

Automorphisms of extremal codes.

Gabriele Nebe

RWTH Aachen University, Germany, nebe@math.rwth-aachen.de

Extremal codes are self-dual binary codes with largest possible minimum distance. In 1973 Neil Sloane published a short note asking whether there is an extremal code of length 72. Since then many mathematicians search for such a code, developing new theoretical tools to narrow down the structure of its automorphism group, as well as computational methods to enumerate all extremal codes invariant under a given permutation group. The state of the art is that the automorphism group of such a putative extremal code of length 72 is very small: its order is at most 5.

The methods for studying this question involve explicit and constructive applications of well known classical theorems in algebra and group theory, like Burnside's orbit counting theorem and quadratic reciprocity, as well as basic representation theoretic methods and tools from the theory of quadratic forms.

New results on Griesmer Codes and Arcs

Assia Rousseva [1]

Faculty of Mathematics and Informatics,
Sofia University, 5 J. Bourchier blvd, 1164 Sofia, Bulgaria

Ivan Landjev

New Bulgarian University, 21 Montevideo str., 1618 Sofia, Bulgaria

A central problem in coding theory is to optimize one of the three main parameters (length, dimension, minimum distance) of a linear code over a given field for fixed values of the other two. The most popular version of this problem is to determine the minimal length of an $[n,k,d]_q$-code, denoted by $n_q(k,d)$, given k,d and the prime power q. The exact values for $n_q(k,d)$ have been determined for all d in the following cases: $q=2, k \leq 8$, $q=3, k \leq 5$, $q=4, k \leq 4$, $q=5,7,8,9$, $k \leq 3$.

In the case of four-dimensional codes over $\mathbb{F}_5$ there exist only four values of d for which the exact value of $n_q(k,d)$ is unknown: $d = 81, 82, 161, 162$. In this talk, we announce the nonexistence of linear codes with parameters $[104,4,82]_5$ and $[204,4,162]_5$ which implies that $n_5(4,82) = 105$ and $n_5(4,162) = 205$.

Our approach to this problem is geometric. It has been known for a long time that one can associate an arc with every linear code in such way that classes of semilinearly isomorphic linear codes are associated with classes of projectively equivalent arcs. Furthermore, we use a newly developed technique for proving t-extendability of arcs associated with Griesmer codes. For every arc $\mathscr{K}$ we define an arc $\widetilde{\mathscr{K}}$ in the dual space whose structure gives information about the extendability of $\mathscr{K}$. In the case of $(104,22)$- and $(204,42)$-arcs $\widetilde{\mathscr{K}}$ turns out to be a $(3 \mod 5)$-arc in $\mathrm{PG}(3,5)$. Generally, $(t \mod q)$-arcs are defined as multisets of points for which every point is of multiplicity at most t and every subspace of dimension at least 1 has multiplicity $\equiv t \pmod q$. We prove that in the case of $(104,22)$- and $(204,42)$-arcs the arc $\widetilde{\mathscr{K}}$ can only be the sum of three hyperplanes. This implies their triple extendability to the nonexistent $(107,22)$-arc (resp. $(207,42)$-arc).

[1] This research is supported by the Scientific Research Fund of Sofia University.

On bounds for batch codes

Jens Zumbrägel

Institute of Algebra, TU Dresden

In a scenario where a client wants to receive many elements from a large database, it is often desirable to have some load balancing. Batch codes, introduced by Ishai et al, aim at providing this by dividing the database between several servers, so that the client needs only to communicate with a small subset of the servers to obtain sufficient information to reconstruct all desired elements.

Recently, Lipmaa and Skachek initiated the study of linear batch codes, which are, in particular, of potential use in distributed storage systems. The authors show that binary linear batch codes correspond to classical binary linear error-correcting codes with lower-bounded minimum distance.

In the present work we generalise this result, to include nonbinary linear codes and general nonlinear batch codes. Namely, if $\varphi : A^k \to A^n$ is the encoder for an (n,k,m) (primitive) batch code over some alphabet A, then $C = \varphi(A^k) \subseteq A^n$ is an error-correcting code of minimum distance at least m. This result enables one to apply a wider range of upper bounds from coding theory to the batch codes scenario. From a mathematically precise definition of batch codes we also obtain further bounds on the parameters of these codes, by making use of combinatorial counting arguments.

This is joint work with Vitaly Skachek, University of Tartu.

Generation and Propagation in Graphs

Rouzbeh Touserkani

School of Computer Science, IPM, Tehran, Iran.

In graph theory, there are too many parameters and numbers with motivation from theory or application which describe the properties of a given graph. In lack of a hierarchy or a unifying framework, there is no guideline for introducing absent concepts and parameters. In such condition, seeking for unifying frameworks is a demanded area of research in graph theory. This work can be seen as another attempt in this direction.

Consider a situation in which a quantity, say information or some material, can be generated and propagated in a given network. Let g (g') be the rate of generation in each vertex (edge), and p (p') be the rate of propagation in each vertex (edge). Call the 4-tuple $(g,g';p,p')$ a *GP-code*.

For a given graph G and a given *GP*-code consider the following integer programming problem:

$$\begin{array}{ll} \text{Minimize} & \sum_{v\in V(G)} x_v \\ \text{subject to} & \sum_{v\in[u]} \geq (p'd_u+p)x_u+(g'd_u+g) \\ & \sum_{v\in V(G)} x_v > 0 \end{array}$$

Where $[u]$ denotes the closed neighborhood of vertex u and the first constrain is valid for every vertex u. The optimum value of this problem is called $(g,g';p,p')$-parameter. As an evidence for the power of the above model for representing known graph parameters we show that many parameters like Independence number, (total) Domination number, 2-packing number, Deffensive alliance number, and Girth can be modeled as GP-parameters.

Distance regular colorings of Cayley graphs of $\mathbb{Z}^n$

Anastasia Vasil'eva

Sobolev Institute of Mathematics,
Novosibirsk State University, Novosibirsk, RUSSIA
vasilan@math.nsc.ru

A vertex partition $(V_1,\ldots,V_k)$ of a graph G is called a perfect coloring (or equitable partition, or regular partition, or partition design) if for every $i, j \in \{1,\ldots,k\}$ there is an integer a_{ij} such that every vertex from V_i has exactly a_{ij} neighbors from V_j. The matrix $A = (a_{ij})$ is called the parameter matrix of the coloring. A perfect coloring $(V_1,\ldots,V_k)$ is distance regular if its parameter matrix is three-diagonal (i.e. $(V_1,\ldots,V_k)$ is the distance coloring with respect to V_1). In this case the set V_1 is called a distance regular code and nonzero off-diagonal elements of the parameter matrix form the intersection array of the code:

$$[a_{21}, a_{32}, \ldots, a_{k,k-1} \mid a_{12}, a_{23}, \ldots, a_{k-1,k}].$$

We study distance regular colorings of the infinite Cayley graph of $\mathbb{Z}^n$ with m generators, $m \geq n$. It is shown that for an arbitrary distance regular coloring the sequences of below-diagonal elements and above-diagonal elements of the parameter matrix are monotonic, i.e.:

$$1 \leq a_{21} \leq a_{32} \leq \ldots \leq a_{k,k-1} \leq 2m+1,$$

$$2m+1 \geq a_{12} \geq a_{23} \geq \ldots \geq a_{k-1,k} \geq 1.$$

Moreover, for any n and m there are only few series of reducible colorings for the Cayley graph of $\mathbb{Z}^n$ with m generators with the increasing number of colors; every irreducible coloring has at most $2m+1$ colors.

Construction of block designs admitting a solvable automorphism group

Doris Dumičić Danilović

Department of mathematics
University of Rijeka, Croatia

In this talk we will describe a method for the construction of block designs admitting a solvable automorphism group using tactical decomposition. The first step is the construction of mutually nonisomorphic orbit matrices for arbitrary block design and its persumed automorphism group, which is a generalisation of the algorithm for obtaining orbit matrices for some symmetric design and its automorphism group described in [1]. The second step in the construction is often called indexing of orbit matrices, which is construction of block designs from orbit matrices. Indexing often lasts too long, therefore we develop an algorithm for the refinement of orbit matrices, based on the application of the composition series for a solvable automorphism group which acts on a block design. We have applied the mentioned method for the construction of some new block designs admitting a solvable automorphism group.

(joint work with D. Crnković and S. Rukavina)

References

[1] V. Ćepulić, On Symmetric Block Designs (40,13,4) with Automorphisms of Order 5, Discrete Math. 128(1-3), 45-60 (1994)

Partial geometric designs with prescribed automorphisms

Oktay Olmez

Department of Mathematics, Faculty of Science, Ankara University, Tandogan, Ankara, 06100, Turkey

In this talk, we will be interested in construction of certain designs, known as partial geometric designs, with specified automorphisms. A *partial geometric design* with parameters $(v,b,k,r;\alpha,\beta)$ is a 1-design with parameters (v,b,k,r) whose point-block incidence matrix N satisfies:

$$NJ = rJ, \;\; JN = kJ, \;\; \text{and} \;\; NN^tN = (\beta-\alpha)N + \alpha J$$

where J denotes the all-ones matrix. Well-studied examples of partial geometric designs include 2-designs, transversal designs and partial geometries.

The well-known Kramer-Mesner theorem provides a method that can often be used to determine the existence or nonexistence of 2-designs having specified automorphisms. We will generalize the Kramer-Mesner theorem to provide a construction method for partial geometric designs with prescribed automorphisms.

Hadamard difference sets and corresponding regular partial difference sets in groups of order 144

Tanja Vučičić (joint work with Joško Mandić)

Department of Mathematics, Faculty of Science
University of Split, Croatia
vucicic@pmfst.hr

There are 197 groups of order 144. Solving the problem of difference set (DS) existence in these groups has not been completed yet. This talk deals with a new method for their construction applicable to transitive incidence structures, as well as the construction of several related incidence structures.

The considered $(144,66,30)$ difference sets belong to the Hadamard family with parameter triples of the form $(4u^2,2u^2-u,u^2-u)$, $u \in \mathbb{N}$. They can be obtained by the well-known 'product method' for Hadamard difference sets (HDS). The input in this case are $(36,15,6)$ HDSs (exactly 35 inequivalent such DSs exist) and a trivial Hadamard difference set in the group of order 4 consisting of a single point.

The construction by our method started from the known $(144,66,30)$ DSs, i.e. from regular symmetric designs equivalent to them. New DSs with the same parameters are obtained as subdesigns of the transitive overstructures developed from the known block designs. According to Cameron and Praeger (P.J. Cameron and C.E. Praeger, *Block-transitive t-designs I: point-imprimitive designs* , Discrete Mathematics 118 (1993), 33-43.), the overstructures have to be block designs themselves. Building an adequate overstructure relies on the well chosen overgroup, say G, of the full automorphism group H of an initial design. It turns out that holomorph of H is an appropriate choice for G.

Eventually our method yielded 1364 nonisomorphic $(144,66,30)$ DSs in 131 groups of order 144. They were subjected to a construction procedure, based on the work of S.L. Ma, for regular partial difference sets (PDS) and strongly regular graphs with parameters $(144,66,30,30)$ and $(144,65,28,30)$. The existence of regular PDSs of cardinality 66 was confirmed in 51 groups of order 144. The constructed 1125 inequivalent such PDSs correspond to 43 nonisomorphic strongly regular graphs of valency 66. The existence of regular PDSs of cardinality 65 was confirmed in 53 groups. The constructed 1209 inequivalent such PDSs correspond to 78 nonisomorphic strongly regular graphs of valency 65.

The full automorphism groups of the obtained graphs, as well as those of symmetric designs, were explored using software package MAGMA.

Hamiltonian cycle systems and their automorphism groups

Marco Buratti

Università di Perugia

A Hamiltonian cycle system of odd (even) order v, briefly a $\mathrm{HCS}(v)$, is a decomposition of the complete graph K_v (the complete graph K_v minus a 1-factor) into Hamiltonian cycles. I will survey known results and open problems about the automorphism groups of a $\mathrm{HCS}(v)$.

Coding and Stream Ciphers

Tor Helleseth[1] and Sondre Rønjom[2]

[1]Department of Informatics, University of Bergen, Norway and [2]NSM, Norway

Stream ciphers have many applications in modern communication systems. Important building blocks in many constructions of stream ciphers are the filter generator and the nonlinear combiner generator. These constructions consist of one of more linear feedback shift registers combined with a Boolean function. Based on the content of the involved shift registers the Boolean function provides a keystream.

This talk will survey some attacks on the filter generator and nonlinear combiner generator including the Rønjom-Helleseth attack and some recent generalizations considering the Boolean function as a univariate polynomial. Furthermore a discussion of some connections to coding theory will be provided. The concept of algebraic immunity of Boolean function is discussed and compared with the newer concept of spectral immunity that is determined by coding theoretic properties of a code defined by the Boolean function.

Furthermore, a discussion will be given of how the problem of good selections of the tapping positions in a filter generator may be related to the subspace distance of invariant cyclic subspaces.

On the geometric construction of optimal linear codes

Tatsuya Maruta

Department of Mathematics and Information Sciences
Osaka Prefecture University, Sakai, Osaka 599-8531, Japan
(Joint work with Yuuki Kageyama)

A linear code of length n, dimension k and minimum Hamming weight d over $\mathbb{F}_q$, the field of q elements, is called an $[n,k,d]_q$ code. A fundamental problem in coding theory is to find $n_q(k,d)$, the minimum length n for which an $[n,k,d]_q$ code exists. In this talk, we construct some optimal linear codes over $\mathbb{F}_q$ through projective geometry, using the geometric methods such as projective dual and geometric puncturing.

On extremal type III Codes

Darwin Villar

Lehrstuhl D für Mathematik, RWTH Aachen.

Self-dual ternary Codes have been studied over the last century, being well known for instance two important families, the QR- and Pless Codes. In this paper we summarize some results obtained from studying the automorphism group of extremal type III codes of length 36, 60 and 52, from where some new extremal codes are obtained.

1 Introduction

Besides the interest they grow by themselves, the study of self-dual ternary codes is also important due to their close relation to unimodular lattices. Vera Pless [6] discovered in 1969 a family of self-dual ternary codes $\mathscr{P}(p)$ of length $2(p+1)$ for primes p with $p \equiv -1 \pmod 6$. Together with the extended quadratic residue codes $\mathrm{XQR}(q)$ of length $q+1$ (q prime, $q \equiv \pm 1 \pmod{12}$) they define a series of self-dual ternary codes of high minimum distance (see [4, Chapter 16, §8]). For $p = 5$, the Pless code $\mathscr{P}(5)$ coincides with the Golay code $\mathfrak{g}_{12}$ which is also the extended quadratic residue code $\mathrm{XQR}(11)$ of length 12.

Using invariant theory of finite groups, A. Gleason [2] has shown that the minimum distance of a self-dual ternary code of length $4n$ cannot exceed $3\lfloor \frac{n}{12} \rfloor + 3$. Self-dual codes that achieve equality are called *extremal*. Both constructions, the Pless symmetry codes and the extended quadratic residue codes yield extremal ternary self-dual codes for small values of p. In [9] some of the extremal codes found have been used to construct extremal unimodular lattices.

This short note presents a new extremal $[52,26,15]_3$ Code, non-equivalent to the one already known [7] and that is related to an unimodular lattice of norm 5[8]. As well as the study of the automorphis Group of other ternary codes such as the [36,18,12] and the [60,30,18], where also a new extremal code appears.

References

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language.* J. Symbolic Comput. 24 (1997) 235-265.

[2] Andrew M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities.* Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3, pp. 211–215. Gauthier-Villars, Paris, 1971.

[3] Florence Jessie MacWilliams, *Combinatorial Properties of Elementary Abelian Groups.* Ph.D. dissertation, Harvard University, Cambridge, MA, 1962.

[4] Florence Jessie MacWilliams, Neil J.A. Sloane, *The theory of error-correcting codes.* North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[5] Vera Pless, *Symmetry codes over GF(3) and new five-designs.* J. Combinatorial Theory Ser. A 12 (1972) 119-142.

[6] Vera Pless, *On a new family of symmetry codes and related new five-designs.* Bull. Amer. Math. Soc. 75 (1969) 1339-1342.

[7] Philippe Gaborit, Ayoub Otmani, *Experimental constructions of self-dual codes.* Finite Fields and Their Applications Vol. 9, Issue 3. (2003) 372-394.

[8] Philippe Gaborit, *Construction of new extremal unimodular lattices.* European Journal of Combinatorics Vol. 25, Issue 4. (2004) 549?564.

[9] Masaaki Harada, Masaaki Kitazume, Michio Ozeki, *Ternary Code Construction of Unimodular Lattices and Self-Dual Codes over Z6.* Journal of Algebraic Combinatorics Vol. 16 (2002) 209-223.

Classification of unrestricted 8-ary MDS codes

Janne I. Kokkala

Department of Communications and Networking
Aalto University School of Electrical Engineering
P.O. Box 13000, 00076 Aalto, Finland

A q-ary maximum distance separable (MDS) code C with length n, dimension k and minimum distance $d = n - k + 1$ over an alphabet $\mathscr{A}$ of size q is a set of q^k *codewords* that are elements of $\mathscr{A}^n$, such that the Hamming distance between two distinct codewords in C is at least d. When $\mathscr{A}$ is a finite field $\mathbb{F}_q$ and C is a vector subspace of $\mathbb{F}_q^n$, then C is *linear*, otherwise it is *nonlinear*. When studying codes that can be either linear or nonlinear, they are called *unrestricted*. Two codes are called *equivalent* if one can be obtained from another by a permutation of coordinates followed by permutations of symbols at each coordinate separately. Sets of mutually orthogonal Latin squares of order 8, corresponding to two-dimensional 8-ary MDS codes, and 8-ary MDS codes with $d = 3$ have been classified in earlier studies. These results are used here to complete the classification of all 8-ary MDS codes with $d \geq 3$ using a computer search.

This is joint work with Patric R. J. Östergård.

On a 14-dimensional self-orthogonal code invariant under the simple group $G_2(3)$

Bernardo Rodrigues

School of of Mathematical Sciences
University of KwaZulu-Natal
Durban 4041
South Africa

In this talk we examine a certain 14-dimensional lattice as an irreducible binary self-orthogonal code constructed from a rank-4 representation of the simple Chevalley group $G_2(3)$. We establish some properties of the code and the nature of some classes of codewords. Further we describe the structure of the stabilizer of codewords in the code, and determine transitive designs invariant under $G_2(3)$.

Towards A Group Ring Construction of Codes using Dihedral Groups

Leo Creedon

Institute of Technology Sligo
Ireland

An $[n,k,d]$ code is a code with length n, rank k and minimum distance d. In [1] a new technique for constructing codes from group rings and circulant matrices is given. This was applied in [2] to construct the extended binary Galoy code (the unique $[24,12,8]$ linear block code). Subsequently, in [3] a similar technique was used to construct the self-dual, doubly-even and extremal $[48,24,12]$ binary linear block code. Here these results are generalised (using the semi-simplicity of the underlying group algebra) to use unitary units to construct linear block codes of length $n = 3(2^m)$ for any positive whole number n. Some of these results are based on joint work with Fergal Gallagher and Ian McLoughlin.

References:

[1] Paul Hurley and Ted Hurley. Codes From Zero-Divisors and Units in Group Rings. Int. J. Information and Coding Theory, Vol. 1, No. 1, 2009.
[2] Ian McLoughlin and Ted Hurley. A group ring construction of the extended binary Golay code. IEEE Transactions on Information Theory, 54:4381–4383, September 2008.
[3] Ian McLoughlin. A group ring construction of the [48,24,12] type II linear block code. Designs, Codes and Cryptography April 2012, Volume 63, Issue 1, pp 29-41.

Construction of simple 3-designs using resolution

Tran van Trung

University of Duisburg-Essen
Faculty of Mathematics
Thea-Leymann-Straße 9, 45127 Essen, Germany

We focus on the construction of simple 3-designs using (s,σ)-resolution. The concept of resolution of $t-(v,t,\lambda)$ designs may be viewed as a natural generalization of the concept of parallelism for $t-(v,k,\lambda)$ designs. If a $t-(v,k,\lambda)$ design has a parallellism we necessarily have $k|v$; this condition is no longer true for (s,σ)-resolution in general. In [(1) TvT, Recursive constructions for 3-designs and resolvable 3-designs, J. Statist. Plann. Inference 95, (2001) 341–358, and (2) TvT, Construction of 3-designs using parallelism, J. Geom. 67 (2000) 223–235] it has been shown that 3-designs with parallelism can be used for constructing simple 3-designs. In this talk we show that the methods in the previous papers can be extended to (s,σ)-resolvable 3-designs. The extended methods provide a rich source of new 3-designs.

On Mosaics of Combinatorial Designs

Marcus Greferath

Department of Mathematics and System Analysis,
Aalto University, Helsinki,
Finland
marcus.greferath@aalto.fi

t-designs are collections of subsets of a given set, such that any t-subset of that set is contained in the same number of members of the given collection. This talk will introduce a notion of decomposition that has not been addressed in the literature as of yet: the ambient space of a design will be tiled by the blocks of a family of suitable designs. We will show a few examples and a first general result.

Remark: The talk is based on joint research with Mario Pavcevic from the University of Zagreb in the context COST Action IC1104.

Tiling groups with difference sets

Vedran Krčadinac

Department of Mathematics, Faculty of Science, University of Zagreb
Bijenička 30, HR-10000 Zagreb, Croatia

We report on a joint work with Ante Ćustić and Yue Zhou about tilings of groups with mutually disjoint difference sets. A general construction and a few sporadic examples will be presented. We also have some necessary existence conditions and nonexistence results. Tilings consisting of exactly two difference sets are equivalent to the co-called skew Hadamard or antisymmetric difference sets.

On the q-ary Steiner and other-type trades

Denis S. Krotov, Ivan Yu. Mogilnykh, Vladimir N. Potapov

Sobolev Institute of Mathematics, Novosibirsk 630090, Russia, and Novosibirsk State University, Novosibirsk 630090, Russia

We introduce the concept of a clique bitrade, which generalizes several known types of bitrades, including latin bitrades, Steiner $(k-1,k,v)$ bitrades, extended 1-perfect bitrades. For a distance-regular graph G, we show a one-to-one correspondence between the clique bitrades that meet the weight-distribution lower bound on the cardinality and the bipartite isometric subgraphs that are distance-regular with certain parameters. As an application of the results, we find the minimal cardinality of q-ary Steiner $(k-1,k,v)$ bitrades and show a connection of such bitrades with dual polar subgraphs of the Grassmann graph $J_q(v,k)$. The research was financed by the Russian Science Foundation (grant No 14-11-00555).

On some Menon designs and related structures

Dean Crnković

Department of mathematics
University of Rijeka, Croatia

In this talk we present a construction of two classes of Menon designs and the corresponding cyclic or 1-rotational derived designs. Further, we describe a construction of a class of Siamese twin Menon designs which lead to amicable regular Hadamard matrices. From orbit matrices of some Menon designs we construct classes of self-orthogonal or self-dual codes.

Vectorial bent functions

Alexander Pott

Faculty of Mathematics, Otto-von-Guericke-University Magdeburg, 39106 Magdeburg

Bent functions have been studied for many years: They are Boolean functions of highest possible nonlinearity defined on a finite dimensional vector space over a finite field. The most classical examples can be constructed from quadratic forms. There is, up to equivalence, only one such quadratic bent function. Vectorial bent functions are **vector spaces** of bent functions. In the quadratic case, these are vector spaces of symmetric matrices of full rank. In my talk, I will recall some of the known constructions. In particular, I will address the problem about the equivalence of vectorial bent functions (which is less trivial than in the Boolean case) as well as the problem about extandibility (is it possible to embed a vector space of bent functions into a larger one?).

Open Problems for Polynomials over Finite Fields and Applications

Daniel Panario

School of Mathematics and Statistics
Carleton University

We survey open problems for univariate polynomials over a finite field.

- We first comment in some detail on the existence and number of several classes of polynomials. The open problems here are of a more theoretical nature.

- Then, we center in classes of low-weight (irreducible) polynomials. The conjectures here are more practically oriented.

- Finally, we give brief descriptions of a selection of open problems from several areas including factorization of polynomials, special polynomials (APN functions, permutation), and relations between integer numbers and polynomials.

Codes on Random Geometric Graphs

Dejan Vukobratovic

Department of Power, Electronics and
Communications Engineering,
University of Novi Sad,
Novi Sad, Serbia
Email: dejanv@uns.ac.rs, Web: http://ktios.net/vukobratovic

Recent revival in random access wireless communications establishes strong connections between sparse-graph codes such as Low-Density Parity Check (LDPC) codes and random access ALOHA-type schemes. Using these connections, random access ALOHA-type schemes have recently being designed that approach the throughput limits of random access systems. Motivated by exploiting these connections in dense deployments of small base stations that serve massive user populations (a scenario referred to as Machine-to-Machine or M2M communications), we arrive at sparse-graph code design problems constrained by underlying random geometric graphs. In this talk, we discuss the design of codes on random geometric graphs that aim at maximizing the total throughput such a massive-scale user population could deliver into the distributed radio access infrastructure.

On the Index Coding and Caching Problem

Eimear Byrne

School of Mathematical Sciences
University College Dublin

The index coding problem has recently attracted a great deal of attention, in part due to its suitability for applications in wireless communications and in for broadcasting media files such as video. In this scenario, the sender has a large file, all or part of which is requested by a number of clients. It is assumed that each client already has part of the file, called its side information, and that this is known to the sender, as well as the requests of each client. The server then makes a number of broadcasts, which is received by all users. Each client combines its own information with the transmission to retrieve the data it wants. The index coding problem chiefly concerns minimizing the number of broadcasts, which occurs if the sender encodes information prior to its transmission.

In this talk we will give an overview of the Index Coding Problem, and extend it to include the case of coded side information. We will give bounds on the minimal number of transmissions N and discuss error-correction. This more general viewpoint has applications to relay networks. In addition, it allows us to demonstrate a link between index coding, caching problems and covering radius for rank-metric codes. The Caching Problem has many similarities with index coding. As in the ICP there is a central server who wishes to broadcast data to a number of clients in two phases, called the *placement phase* and the *delivery phase*. In the placement phase, the sender distributes files for storage in users' caches and it is assumed that this occurs at low traffic times. In the delivery phase, data is encoded and transmitted to all users according to the different demands of each user. This phase operates at peak-traffic times, so the object is again to minimize the number of transmissions N. The CP differs from the ICP in that in the delivery phase the sender chooses what data will be stored at each receiver and is unaware of the user demands a priori to the placement phase, while in the ICP the data stored at each receiver is randomly determined. We will demonstrate how coding theory for the rank metric plays a role towards solving the caching problem, especially for caching with coded side information. This is joint work with Marco Calderini (Univ. Trento).

Constructions of Subspace Codes

Heide Gluesing-Luerssen and Carolyn Troha
University of Kentucky

This note is devoted to constructions of subspace codes. Recall that a *subspace code* of length n is a collection of subspaces in $\mathbb{F}^n$. The code is called a *constant dimension code* if all subspaces have the same dimension. The *subspace distance* between two subspaces is defined as $\mathrm{d_S}(\mathscr{V},\mathscr{W}) := \dim\mathscr{V} + \dim\mathscr{W} - 2\dim(\mathscr{V}\cap\mathscr{W})$. Note that for a constant-dimension code of dimension k the subspace distance is always even and upper bounded by $2k$. If this bound is attained, the code is called a *partial spread*. A *rank-metric code* is a subset of some matrix space $\mathbb{F}^{k\times m}$ endowed with the rank metric $\mathrm{d_R}(A,B) = \mathrm{rk}(A-B)$. The minimum distance of a subspace code or rank-metric code is defined in the usual way.

We present a construction that results in constant dimension codes of large length by linking constant dimension codes of smaller length without decreasing the distance. For $i = 1,2$ and $l \in [N_i] := \{1,\dots,N_i\}$ let $U_{i,l} \in \mathbb{F}^{k\times n_i}$ be of rank k and define the codes $\mathscr{C}_i = \{\mathrm{im}(U_{i,l}) \mid l \in [N_i]\}$, where $\mathrm{im}(M)$ denotes the rowspace of the matrix M. Let $\mathscr{C}_R$ be a linear rank-metric code in $\mathbb{F}^{k\times n_2}$ with cardinality N_R. Define $\mathscr{C} := \tilde{\mathscr{C}}_1 \cup \tilde{\mathscr{C}}_2 \cup \tilde{\mathscr{C}}_3$, where

$$\tilde{\mathscr{C}}_1 = \{\mathrm{im}(U_{1,l}\,|\,0_{k\times n_2}) \mid l \in [N_1]\}, \qquad \tilde{\mathscr{C}}_2 = \{\mathrm{im}(0_{k\times n_1}\,|\,U_{2,l}) \mid l \in [N_2]\},$$
$$\tilde{\mathscr{C}}_3 = \{\mathrm{im}(U_{1,l}\,|\,M) \mid l \in [N_1], M \in \mathscr{C}_R\backslash\{0\}\},$$

Then $\mathscr{C}$ is a constant dimension code of length $n := n_1 + n_2$, dimension k, cardinality $N := N_2 + N_1 N_R$, and subspace distance $\mathrm{d_S}(\mathscr{C}) = \min\{\mathrm{d_S}(\mathscr{C}_1),\, \mathrm{d_S}(\mathscr{C}_2),\, 2\mathrm{d_R}(\mathscr{C}_R)\}$.

A particular instance of linkage leads to a simple way of constructing partial spreads that have the same cardinality as the best known partial spreads. As a special case one recovers the constructions of large partial spreads by Etzion/Vardy [4] and Gorla/Ravagnani [5].

Similarly, one can easily construct very large codes with distance $2(k-1)$. The resulting codes do not quite reach the cardinality of the codes found by Braun/Reichelt [1], but the latter have been found by extended computer search, whereas the linkage codes are readily available once $\mathscr{C}_1$ and $\mathscr{C}_2$ have been found. In general, the linkage codes are larger than the codes obtained with the aid of the (modified) multilevel construction [2, 3].

In special cases, decoding the linkage code can easily be reduced to decoding the constituent codes.

References

[1] M. Braun and J. Reichelt. q-analogs of packing designs. *J. Comb. Designs*, 22:306–321, 2014.

[2] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Trans. Inform. Theory*, IT-55:2909–2919, 2009.

[3] T. Etzion and N. Silberstein. Codes and designs related to lifted MRD codes. *IEEE Trans. Inform. Theory*, IT-59:1004–1017, 2013.

[4] T. Etzion and A. Vardy. Error-correcting codes in projective space. *IEEE Trans. Inform. Theory*, IT-57:1165–1173, 2011.

[5] E. Gorla and A. Ravagnani. Partial spreads in random network coding. *Finite Fields Appl.*, 26:104–115, 2014.

New Lower Bounds for Constant Dimension Subspace Codes

Patric R. J. Östergård

Department of Communications and Networking
Aalto University School of Electrical Engineering
P.O. Box 13000, 00076 Aalto, Finland

Let $\mathscr{A}_q(n,d,k)$ denote the maximum cardinality of a set $\mathscr{C}$ of k-dimensional subspaces of an n-dimensional vector space over the finite field of order q, $\mathbb{F}_q$, such that any two different subspaces $U,W \in \mathscr{C}$ have a distance $d(U,W) := \dim(U+W) - \dim(U \cap W)$ of at least d. Lower bounds on $\mathscr{A}_q(n,d,k)$ can be obtained by explicitly constructing corresponding sets $\mathscr{C}$. When searching for such sets with a prescribed group of automorphisms, the search problem leads to instances of the maximum weight clique problem. The main focus is here on subgroups with small index in the normalizer of the Singer cyclic group of $\mathrm{GL}(n,q)$. With a stochastic maximum weight clique algorithm and a systematic consideration of groups of the above mentioned type, new lower bounds on $\mathscr{A}_2(8,4,4)$ and $\mathscr{A}_2(n,4,3)$ for $8 \le n \le 11$ are obtained.

This is joint work with Michael Braun and Alfred Wassermann.

ILP techniques for binary subspace codes

Sascha Kurz

University of Bayreuth, Germany

Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4 have been exhaustively classified up to isomorphism recently. We apply integer linear programming techniques to study the mixed dimensional case.

Towards a classification of special partial spreads and subspace codes

Daniel Heinlein

University of Bayreuth

Kötter and Kschischang introduced a new approach of network coding by converting data in subspaces of a common vector space $\mathbb{F}_q^n$. It is possible to define a metric ($d(U,V) := \dim(U+V) - \dim(U \cap V)$) on the set of all subspaces of $\mathbb{F}_q^n$. The topic is therefore accessible for ideas of coding theory. In the case of constant dimension codes, all such subspaces have the same dimension k.

In my talk, I present the main problem to find maximum codes in the constant dimension setting, i.e., maximum subsets of k-dimensional subspaces of the $\mathbb{F}_q^n$ such that the minimum distance of the code is greater than a constant. Equivalently one can claim that the pairwise intersection is not too big: $\dim(U \cap V) \leq s-1$.

The problem can be transformed to a graph theoretic problem namely maximum clique or maximum independent set. This perspective can then be transformed to a binary linear problem which makes dealing with symmetry rather easy by applying special constraints.

There is also a connection to geometry: The case with $k = 2$ and $s = 1$ is known as partial spread.

Cameron-Liebler k-classes in PG$(2k+1,q)$

Leo Storme

Ghent University
Department of Mathematics
Krijgslaan 281
9000 Ghent
Belgium

(joint work with Morgan Rodgers and Andries Vansweevelt)

Cameron-Liebler line sets $\mathscr{L}$ in PG$(3,q)$ are sets of lines sharing a constant number x of lines with every spread of PG$(3,q)$.

Recently, a lot of progress was made on Cameron-Liebler line sets by Gavrilyuk and Metsch [3] who eliminated a large number of possible values for the parameter x, and, independently, two groups [1, 2] constructed a new infinite class of Cameron-Liebler line sets.

In [4], the concept of Cameron-Liebler line sets in PG$(3,q)$ was extended to Cameron-Liebler k-classes in PG$(2k+1,q)$. These sets of k-spaces in PG$(2k+1,q)$ can again be defined as sets of k-spaces having a constant number x of k-spaces in common with every k-spread of PG$(2k+1,q)$, but many equivalent definitions also hold.

We characterized the Cameron-Liebler k-classes in PG$(2k+1,q)$ with parameters $x=1$ and $x=2$, and eliminated the existence of Cameron-Liebler k-classes in PG$(2k+1,q)$ with parameter x small, $x \geq 3$. To prove the non-existence of these Cameron-Liebler k-classes in PG$(2k+1,q)$ with parameter x small, $x \geq 3$, results on the Erdős-Ko-Rado problem on k-spaces in PG$(2k+1,q)$ were used.

In this talk, we present the many equivalent definitions of Cameron-Liebler k-classes in PG$(2k+1,q)$, discuss the characterization results for $x=1$ and $x=2$, and the non-existence proofs for Cameron-Liebler k-classes in PG$(2k+1,q)$ with parameter x small, $x \geq 3$.

References

[1] J. De Beule, J. Demeyer, K. Metsch, and M. Rodgers, A new family of tight sets in $\mathscr{Q}^+(5,q)$. *Des. Codes Cryptogr.*, to appear.

[2] T. Feng, K. Momihara, and Q. Xiang, Cameron-Liebler line classes with parameter $x = \frac{q^2-1}{2}$. (arXiv:1406.6526).

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

[4] M. Rodgers, L. Storme, and A. Vansweevelt, Cameron-Liebler k-classes in PG$(2k+1,q)$. (In preparation).

Maximal Partial Symplectic Spreads over Small Fields

Markus Grassl

Institut für Optik, Information und Photonik
Universität Erlangen-Nürnberg
Max-Planck-Institut für die Physik des Lichts, Erlangen
Markus.Grassl@mpl.mpg.de

A symplectic spread is a collection of totally isotropic subspaces of $\mathbb{F}_q^{2n}$, equipped with a symplectic inner product, which mutually intersect trivially. It is well known that the maximal size of a symplectic spread is q^n+1, and that the maximum can always be achieved. A maximal partial symplectic symplectic spread is a collection of totally isotropic subspaces with trivial pairwise intersection that is not a proper subset of a larger partial symplectic spread.

Maximal partial spreads have been studied in particular in the context of generalized quadrangles, corresponding to the case $n=2$, see, e. g., [1]. Results on the size of maximal partial spreads have been obtained for $n=2$ with the field size q increasing [3, 4]. Maximal partial spreads have applications in quantum information theory. They correspond to so-called weakly unextendible mutually unbiased bases (MUBs) [2]. In this context, we are interested in the size of maximal partial spreads over small fields, but with increasing dimension n.

In the talk we will illustrate the connection between maximal partial symplectic spreads and weakly unextendible MUBs. Further, we will discuss techniques for finding partial spreads over small finds and proving their maximality. Theoretical and computational results are summarized in Table 1. In particular, we have:

Theorem 1 *For q even, there exists a maximal partial symplectic spread of size q^n+1 in $\mathbb{F}_q^{4n}$.*

We conjecture that these maximal partial spreads are of minimal size.

Table 1: Size of maximal partial symplectic spreads in vector spaces $\mathbb{F}_q^{2n}$

$d=q^n$	q	n	size	remark
4	2	2	$3,5$	complete
8	2	3	$5,9$	complete
16	2	4	$5,8,9,11,13,17$	complete
16	4	2	$5,9,11,13,17$	complete
32	2	5	$9,\ldots,15,17,33$	
64	2	6	$9,13,\ldots,47,49,51,57,65$	
64	4	3	$17,\ldots,43,49,65$	
64	8	2	$9,17,21,\ldots,47,49,51,57,65$	see [1]
128	2	7	$21,\ldots,31,33,35,37,39,45,49,53,57,61,65,129$	
256	2	8	$17,28,\ldots,205,209,211,213,214,215,225,227,241,257$	
256	4	4	$17,33,35,\ldots,205,209,211,213,214,215,225,227,241,257$	
256	16	2	$17,33,46,\ldots,205,209,211,213,214,215,225,227,241,257$	more than in [1]
9	3	2	$5,8,10$	complete
27	3	3	$10,\ldots,20,28$	complete
81	3	4	$18,\ldots,68,70,73,74,82$	
81	9	2	$22,\ldots,68,70,73,74,82$	see [1]
243	3	5	$32,\ldots,120,123,154,163,244$	search ongoing
25	5	2	$13,\ldots,20,22,24,26$	complete, see [1]
125	5	3	$27,\ldots,90,101,126$	
49	7	2	$14,17,\ldots,42,44,48,50$	see [1]
121	11	2	$28,\ldots,106,109,110,112,120,122$	more than in [1]
169	13	2	$40,\ldots,140,145,146,148,158,170$	more than in [1]
289	17	2	$67,\ldots,238,241,\ldots,248,257,258,260,274,290$	more than in [1]
361	19	2	$82,\ldots,302,307,\ldots,314,325,326,328,344,362$	more than in [1]

References

[1] M. Cimráková, S. De Winter, V. Fack, and L. Storme, *On the smallest maximal partial*

ovoids and spreads of the generalized quadrangles $W(q)$ and $Q(4,q)$, European Journal of Combinatorics, 28 (2007), pp. 1934–1942.

[2] P. MANDAYAM, S. BANDYOPADHYAY, M. GRASSL, AND W. K. WOOTTERS, *Unextendible Mutually Unbiased Bases from Pauli Classes*, Quantum Information & Computation, 14 (2014), pp. 823-844.

[3] V. PEPE, C. RÖSSING, AND L. STORME, *A spectrum result on maximal partial ovoids of the generalized quadrangle $Q(4,q)$, q odd*, Contemporary Mathematics, 518 (2010), pp. 349–362.

[4] C. RÖSSING AND L. STORME, *A spectrum result on maximal partial ovoids of the generalized quadrangle $Q(4,q)$, q even*, European Journal of Combinatorics, 31 (2010), pp. 349—361.

Complete $(k,3)$-arcs from quartic curves

Daniele Bartoli

Department of Mathematics, Ghent University,
Building S22, Krijgslaan 281, B 9000 Gent, Belgium
(joint work with Massimo Giulietti and Giovanni Zini)

A (k,r)-arc in $\mathrm{PG}(2,q)$, the projective Galois plane over the finite field with q elements $\mathbb{F}_q$, is a set of k points no $(r+1)$ of which are collinear and such that there exist r collinear points. A natural problem in this context is the construction of infinite families of *complete* (k,r)-arcs, that is, arcs that are maximal with respect to set theoretical inclusion. From the standpoint of Coding Theory, complete (k,r)-arcs correspond to linear $[k,3,k-r]_q$-codes which cannot be extended to a code with a larger minimum distance. If $r=3$ the associated code is a Near MDS code, that is, a code C such that the Singleton defects of C and its dual $C^{\perp}$ is equal to 1. While in the case $r=2$ the theory is well developed and quite rich of constructions, for most $r>2$, the only known infinite families either are consist of the set of $\mathbb{F}_q$-rational points of some irreducible curve of degree r, or arise from the theory of 2-character sets in $\mathrm{PG}(2,q)$. In particular, no general description of a complete $(k,3)$-arc other than the set of $\mathbb{F}_q$-rational points of an irreducible cubic seems to be known.

In this talk I will present an algebraic construction of complete $(k,3)$-arcs in $\mathrm{PG}(2,q)$, with $q=p^h$, $p>2$, $p\equiv 2 \bmod 3$, of size roughly

$$2\sqrt{\frac{p}{\sigma}q},$$

where $\sigma=p^{h'}$, h' odd divisor of h, satisfies $3600\sigma^6\leq q$.

It is worth noticing that the order of magnitude of these $(k,3)$-arcs is significantly smaller than that of the previously known families, since complete $(k,3)$-arcs arising from cubic curves have at least $q+1-2\sqrt{q}$ points. Almost all the points of the $(k,3)$-arcs constructed belong to the set of $\mathbb{F}_q$-rational points of the quartic curve $\mathscr{Q}$ with equation $Y=X^4$. To prove that the all the points inside the quartic are covered we use some results on maximal independent subsets of abelian groups. In order to show that the 3-secants of the $(k,3)$-arc cover a point P off the quartic curve $\mathscr{Q}$, we construct an algebraic curve $\mathscr{H}_P$ defined over $\mathbb{F}_q$ describing the collinearity of three points of the arc and P, prove that $\mathscr{H}_P$ has an absolutely irreducible component defined over $\mathbb{F}_q$, apply the Hasse-Weil bound to guarantee the existence of a suitable $\mathbb{F}_q$-rational point in $\mathscr{H}_P$, and finally deduce that P is collinear with three points in the arc. The main difficulty here is that $\mathscr{H}_P$ is not a plane curve, but a curve embedded in the 3-dimensional space. This is why the theory and the language of Function Fields have been used in order to show that $\mathscr{H}_P$ possesses an absolutely irreducible component defined over $\mathbb{F}_q$.

Simultaneous diagonalization of conics in $PG(2, q)$

Katharina Kusejko

ETH Zürich

Consider two symmetric 3×3 matrices A and B with entries in $GF(q)$, for $q = p^n$, p an odd prime. The zero sets of $v^T Av$ and $v^T Bv$ can be viewed as (possibly degenerate) conics in the finite projective coordinate plane of order q, denoted by $PG(2, q)$. Using combinatorial properties of pencils of conics in $PG(2, q)$, we are able to tell when it is possible to find a regular matrix S with entries in $GF(q)$, such that $S^T AS$ and $S^T BS$ are both diagonal matrices. This is equivalent to the existence of a collineation, which maps two given conics into two conics in diagonal form. For two proper conics, we will in particular compare the situation in $PG(2, q)$ to the real projective plane and compare the geometrical properties of being diagonalizable with our combinatorial results.

Tight sets in finite geometry

Jan De Beule

Ghent University

Let Γ be a strongly regular graph with parameters (n,k,λ,μ). Let A be its adjacency matrix. if $0 < k < n-1$, then it is well known that:

- the matrix A has three eigenvalues k, e^+ and e^-;
- the eigenvalue k has multiplicity 1 and its eigenspace is generated by the all-one vector $\mathbf{j}$;
- let V^+, V^- respectively, be the eigenspace corresponding to the eigenvalue e^+, e^- respectively, then $\mathbb{C}^n = \langle \mathbf{j} \rangle \perp V^+ \perp V^-$.

A vector $\chi \in \mathbb{C}^n$ is called a *weighted tight set* if $\chi \in \langle \mathbf{j} \rangle \perp V^+$, in other words, χ is orthogonal to V^-.

Strongly regular graphs occur frequently in finite geometry. Consider e.g. a finite classical polar space $\mathscr{P}$, and call Γ the graph with the points of $\mathscr{P}$ as vertices and two different vertices being adjacent if and only if the corresponding points are collinear. The graph Γ will be strongly regular and its parameters are well known. Let χ be a weighted tight set of Γ, then geometrically, χ associates a complex weight to each point of $\mathscr{P}$. When χ is a $0,1$ vector, the corresponding point set *behaves combinatorially as a disjoint union of generators*, and this property is often used as definition of a *tight set of a finite classical polar space*, probably for the first time by S.E. Payne in 1987.

A well studied example of tight sets of a particular polar space are the so-called Cameron-Liebler line classes. A *Cameron-Liebler line class with parameter x* is a set $\mathscr{L}$ of lines of $\mathrm{PG}(3,q)$ that has exactly x lines in common with any spread of $\mathrm{PG}(3,q)$. Using the Klein correspondence, it is clear that such an object is a tight set of the polar space $\mathrm{Q}^+(5,q)$. Cameron-Liebler line classes were introduced by Cameron and Liebler in 1982, and they conjectured (roughly spoken), that no non-trivial Cameron-Liebler exists, a conjecture that was disproven by the construction of an infinite family of Cameron-Liebler line classes with parameter $x = \frac{q^2+1}{2}$ by Bruen and Drudge in 1999.

In the talk, the history of tight sets in finite geometry will be surveyed. Their relation with strongly regular graphs will be play an important role. Then we focus and survey on Cameron-Liebler line classes, and non-exsistence results, and we present the construction of an infinite family with parameter $\frac{q^2-1}{2}$ for $q \equiv 5,9 \pmod{12}$, which is joint work with J. Demeyer, K. Metsch, and M. Rodgers.

In the second part, we focus on ongoing research (jointly with J. Bamberg and F. Ihringer) on tight sets of finite classical polar spaces and their interaction with *ovoids*. An ovoid of a polar space is a $0,1$-vector $\chi \in \langle \mathbf{j} \rangle \perp V^-$. The combinatorial interaction between ovoids and tight sets is well understood, and the objective of this ongoing research is to obtain a unified approach to show non-existence of ovoids in several particular cases were this is known (or expected to be true) in a unified way.

References

[1] John Bamberg, Alice Devillers, and Jeroen Schillewaert. Weighted intriguing sets of finite generalised quadrangles. *J. Algebraic Combin.*, 36(1):149–173, 2012.

[2] John Bamberg, Shane Kelly, Maska Law, and Tim Penttila. Tight sets and m-ovoids of finite polar spaces. *J. Combin. Theory Ser. A*, 114(7):1293–1314, 2007.

[3] A.A. Bruen and K. Drudge. The construction of Cameron–Liebler line classes in $\mathrm{PG}(3,q)$. *Finite Fields and Their Applications*, 5(1):35–45, 1999.

[4] P.J. Cameron and R.A. Liebler. Tactical decompositions and orbits of projective groups. *Linear Algebra and its Applications*, 46:91–102, 1982.

[5] Jan De Beule, Jeroen Demeyer, Klaus Metsch, and Morgan Rodgers. A new family of tight sets in $\mathrm{Q}^+(5,q)$. *Designs, Codes and Cryptography*, pages 1–24, 2014, doi: 10.1007/s10623-014-0023-9.

[6] Ph. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973.

[7] Ph. Delsarte. Pairs of vectors in the space of an association scheme. *Philips Res. Rep.*, 32(5-6):373–411, 1977.

[8] Jörg Eisfeld. On the common nature of spreads and pencils in PG(d,q). *Discrete Mathematics*, 189(1-3):95–104, 1998.

[9] J. A. Thas. Ovoidal translation planes. *Arch. Math. (Basel)*, 23:110–112, 1972.

[10] J. Tits. Ovoïdes et groupes de Suzuki. *Arch. Math.*, 13:187–198, 1962.

Subspace codes in $\mathrm{PG}(2n-1,q)$

Francesco Pavese
(joint work with A. Cossidente)

Dipartimento di Matematica, Informatica ed Economia
Università della Basilicata
Contrada Macchia Romana, I-85100 Potenza, Italy
francesco.pavese@unibas.it

Let V be an r–dimensional vector space over $\mathrm{GF}(q)$, q any prime power. The set $S(V)$ of all subspaces of V, or subspaces of the projective space $\mathrm{PG}(V)$, forms a metric space with respect to the *subspace distance* defined by $d_s(U,U') = \dim(U+U') - \dim(U \cap U')$. In the context of subspace coding theory, the main problem asks for the determination of the larger lengths of codes in the space $(S(V),d_s)$ (*subspace codes*) with given minimum distance and of course the classification of the corresponding optimal codes. Codes in the projective space and codes in the Grassmannian over a finite field referred to as subspace codes and constant–dimension codes, respectively, have been proposed for error control in random linear network coding, see [9]. An $(r,M,d;k)_q$ constant–dimension subspace code is a set $\mathscr{C}$ of k–subspaces of V, where $|\mathscr{C}| = M$ and minimum subspace distance $d_s(\mathscr{C}) = \min\{d_s(U,U') \mid U,U' \in \mathscr{C}, U \neq U'\} = d$.

From a combinatorial point of view an $(r,M,2\delta;k)_q$ constant–dimension subspace code, $\delta > 1$, is a collection $\mathscr{C}$ of $(k-1)$–dimensional projective subspaces of $\mathrm{PG}(r-1,q)$ such that every $(k-\delta)$–dimensional projective subspace of $\mathrm{PG}(r-1,q)$ is contained in at most a member of $\mathscr{C}$ and $|\mathscr{C}| = M$.

For general results on bounds and constructions of subspaces codes, see [8]. More recent constructions and results can be found in [1], [2], [3], [4], [5], [6], [7], [10]. In this talk I will describe a construction of $(2n,M,4;n)_q$ constant–dimension subspace codes, obtained by using a purely geometric approach. In particular a geometric description of an $(8,M,4;4)_q$ constant–dimension subspace code, with $M = q^{12} + q^2(q^2+1)^2(q^2+q+1)+1$, will be provided.

References

[1] A. Cossidente, F. Pavese, On subspace codes, *Des. Codes Cryptogr.*, DOI 10.1007/s10623-014-0018-6.

[2] T. Etzion, N. Silberstein, Codes and Designs Related to Lifted MRD Codes, *IEEE Trans. Inform. Theory* 59 (2013), no. 2, 1004-1017.

[3] T. Etzion, N. Silberstein, Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams, *IEEE Trans. Inform. Theory* 55 (2009), no. 7, 2909-2919.

[4] T. Etzion, A. Vardy, Error-correcting codes in projective space, *IEEE Trans. Inform. Theory* 57 (2011), no. 2, 1165-1173.

[5] M. Gadouleau, Z. Yan, Constant-rank codes and their connection to constant-dimension codes, *IEEE Trans. Inform. Theory* 56 (2010), no. 7, 3207-3216.

[6] E. Gorla, A. Ravagnani, Subspace codes from Ferrers diagrams, preprint (arXiiv:1405.2736).

[7] T. Honold, M. Kiermaier, S. Kurz, Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4, *Contemporary Mathematics* 632 (2015), 157-176.

[8] A. Khaleghi, D. Silva, F. R. Kschischang, Subspace codes, *Cryptography and coding*, 1-21, Lecture Notes in Comput. Sci., Springer, Berlin, 2009.

[9] R. Koetter, F. R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inform. Theory*, 54 (8), 3579-3591, Aug. 2008.

[10] A.-L. Trautmann, J. Rosenthal, New improvements on the echelon-Ferrers construction, in proc. of *Int. Symp. on Math. Theory of Networks and Systems*, 405-408, July 2010.

Network Coding in Wireless Systems: Impact of Wireless Links

Güneş Karabulut Kurt

Department of Communications and Electronics Engineering, Istanbul Technical University, 34469, Istanbul, Turkey, e-mail: gkurt@itu.edu.tr.

Network coding is a powerful tool that can be used to address the design challenges in both wired and wireless networks. The majority of the literature on network coding networks assume error free transmissions, mostly considering wired networks. Although wired networks still constitute a large portion of the current communication networks, there is a transition to wireless networks, especially as the last mile technology.

In wireless networks, the number of end-users along with their corresponding data rate requirements constantly increase, while the network resources such as spectrum and power remain limited. This provides a solid motivation for the application of network coding techniques. However, application of network coding in wireless environments is however fundamentally different than the wired counterparts due to three main characteristics of the wireless links:

1. **Channel impairments:** In wireless networks, fading channels can significantly affect the link quality, making the network more prone to transmission errors. This makes the error free transmission channel assumption invalid and definitely introduces the requirement to consider possible forwarding errors through network coding nodes.

2. **Direct source-destination links:** Although the wireless channel may look disadvantageous as first sight, it also provides spatial diversity through the independent fading channels between distinct node pairs. Cooperative networking techniques can help us exploit this spatial diversity and hence combat the performance degrading effects of the wireless fading channels. Making use of the broadcast nature of the wireless channel, as source node transmits, the overhearing network coding nodes can repeat the received signals, and furthermore the destination can combine all received copies of the information signal to significantly improve the error performance of the system.

3. **Practical limitations** Another commonly used simplifying assumption when considering wireless transmission links is to avoid any practical limitations such as erroneous channel knowledge or synchronization errors. The availability of the ideal channel state information (CSI) is a very frequently considered assumption. However, measured by using a limited number of pilot channels, CSI may not always be ideal. Such practical limitations may further increase the error rates at the intermediate network coding nodes and also at the destination nodes, and hence definitely should be taken into account to assess the error performance of a wireless network coded network.

The main goal of this talk is to formulate and highlight the main constraints and design changes introduced by the wireless links. Their impacts on the error performance of network coding will be quantified. Simulations results will be provided to support the main conclusions.

An geometric approach to locally repairable codes

Ragnar Freij

Aalto University, Finland

In this talk, we study linear locally repairable codes (LRC) from a geometric viewpoint. Generalizing to almost affine codes, the LRC has a very nice matroid representation, where all local and global parameters of the code occur as invariants of the matroid. We show how the known Singleton-type bounds for LRC are really valid for all matroids, and how to determine for which values of the local and global parameters, there are matroids meeting this bound. Finally, we survey some results about the representability of matroids, providing conditions for when the matroids have a representation as linear codes. This is joint work with Thomas Westerbäck, Toni Ernvall and Camilla Hollanti.

Matroid Theory and Locally Repairable Codes

Thomas Westerbäck

Aalto University, Finland

In this talk we will present how locally repairable codes (LRCs) that are almost affine are connected to matroids, and how these topics can be used to give new results in both areas. The parameters (n,k,d,r,δ) of LRCs are generalized to matroids. A bound on the parameters (n,k,d,r,δ) is given for matroids. We prove that the bound is not tight for certain classes of parameters, which implies non-existence results for certain classes of optimal almost affine LRCs. A certain class of matroids, which is a subclass of the gammoids, is constructed. By this construction we prove the existence of optimal linear LRCs for many classes of parameters. The talk is based on a joint work with Toni Ernvall, Ragnar Freij and Camilla Hollanti.

Designs on Matroids

Oliver W. Gnilke

Aalto University,
Department of Mathematics and Systems Analysis

Designs are often divided into two categories, either defined as a collection of subsets, or subspaces of a q-ary vectorspace. Both of these definitions can be unified by using matroids, completely avoiding the need for a field with one element. It then becomes immediately clear why they share so many properties. A design on a matroid is a collection of flats (closed sets). For a general theory of designs on matroids an equicardinality condition on flats of same rank should be asserted. Such matroids are called perfect matroid designs and have been introduced by H.P. Young in 1970. Only a handful examples are known and a complete classification has not been achieved yet.

On Combinatorics of Projective Geometry and Multivariate Cryptography

Vasyl Ustimenko

University of Maria Curie-Sklodowska, vasyl@hektor.umcs.lublin.pl

Linear codes over finite field F_q form a finite projective geometry of dimension $n-1$, which is very important object of Pure Mathematics and Classical Coding Theory. Since late 80th to nowadays some other applications of Finite Projective Geometry to Information Security have appeared (see [1] and [2], devoted to Network Coding). In particular, it was used in Cryptography (see [3], where projective geometry was used for audentification protocols, or [4], where it was used for the symmetric encryption and key exchange protocols. Finite geometries nowadays are widely used as tools for secret sharing.

Public key algorithm of Multivariate Cryptography based on finite projective geometry is introduced here. The variety of $GF_{n-1}(q)$ of maximal flags for the projective geometry over F_q, i. e. the totality of $n-1$ embedded subspaces of ${F_q}^n$, will be used for the generation of polynomial multivariate transformation of ${F_q}^{n(n-1)/2}$. Let $A = A_n(q)$ be the adjacency relation : " two flags are adjacent if their intersection has cardinality 1". The graph of A is $n(q+1)$ - regular. Additionally, we consider the partition of $FG_{n-1}(q)$ into $n!$ Schubert cells. There is the unique largest Schubert cell, which contains $q^{n(n-1)/2}$ flags. The relation $A_n(q)$ and the partition on Schubert cells will allow to define Tits automaton, which is a directed graph of the relation $A_n(q)$, such that arrows are labeled by elements of kind (j, a_j), $a_j \in F_q \cup \{\infty\}$, $1 \leq j \leq n$, where j indicates dimension of common subspaces for flags joined by an arrow and parameter a_j indicates this subspace. The initial and accepting states of Tits automaton have to be elements of the largest Schubert cells.

Finally, we define symbolic Tits automaton with the symbolic initial state $(t_1, t_2, \ldots, t_{n(n-1)/2})$, where t_i are variables and parameters $a_j \neq \infty$ are polynomials in $n-1$ variables. The computation of symbolic Tits automaton induces polynomial transformation E_n of ${F_q}^{n(n-1))/2}$. The map E_n corresponds to "symbolic walk" $S_{n,m}$ of length m in $A_n(q)$. The infinite families of highly nonlinear bijective computable transformations E_n have been introduced.

The public map F is obtained as $T_1 E_n T_2$ where T_1 and T_2 are special affine transformation of ${F_q}^{n(n-1)/2}$. The knowledge on T_1 and T_2 and the decomposition of E_n into transition functions of the symbolic Tits automaton corresponding to walk $S_{n,m}$ allow key holder (Alice) to decrypt.

REFERENCES

1.Anton Betten, Michael Braun, Adalbert Kerber, Axel Kohnert, Alfred Wasserman *Error Correcting Linear Codes Isometry and Applications*, Springer, 2006

2. Andreas Stephan Elsenhans, Axel Kohnert, Alfed Wassermann, *Constructions of codes for Network Coding*, arXiv:1005, 2839[cs].

3. A. Beutelspacher, *Enciphered Geometry, Some Applications of Geometry to Cryptography*, Annals of Discrete Mathematics, v. 37, 1988, 59-68.

4.V. Ustimenko, *Schubert cells in Lie geometries and key exchange via symbolic computations*, Proceedings of the International Conference "Applications of Computer Algebra", Vlora, Albanian Math. J., 2010, Vol 4, n. 4, 135-145.

McEliece type Cryptosystems based on Gabidulin Codes

Kyle Marshall and Joachim Rosenthal

Institute of Mathematics
University of Zürich
8057 Zürich, Switzerland

Assymmetric ciphers based on hard decoding problems belong to the most prominent public key ciphers in the post-quantum crypto area. This is based on the hope that their security might still exist even if a quantum computer is ever built. Since the original paper of Robert McEliece many variants have been proposed and crypto-analysed.

In this talk we will study public key ciphers where the public key represents a disguised Gabidulin code. Using geometric ideas we will introduce a new attack which is capable of breaking several variants proposed in the literature.

On the Existence of Spreads in Projective Hjelmslev Spaces

Ivan Landjev[1]

New Bulgarian University, 21 Montevideo str., 1618 Sofia, Bulgaria

Let R be a finite chain ring with $|R| = q^m$, and $R/\operatorname{Rad} R \cong \mathbb{F}_q$. Denote by $\Pi = \mathrm{PHG}({}_R R^n)$ the (left) $(n-1)$-dimensional projective Hjelmslev geometry over R. As in the classical case, we define a κ-spread of Π to be a partition of its pointset into subspaces of shape $\kappa = (\kappa_1, \ldots, \kappa_n)$. An obvious necessary condition for the existence of a κ-spread $\mathscr{S}$ in Π is that the number of points in a subspace of shape κ divides the number of points in Π. If the elements of $\mathscr{S}$ are Hjelmslev subspaces, i.e. *free* submodules of ${}_R R^n$, this necessary condition is also sufficient. If the subspaces in $\mathscr{S}$ are not Hjelmslev subspaces this numerical condition is not sufficient anymore. For instance, for chain rings with $m = 2$, there is no spread of shape $\kappa = (2,2,1,0)$ in $\mathrm{PHG}({}_R R^4)$. An important (and maybe difficult) question is to find all shapes κ, for which Π has a κ-spread. In this talk, we survey the known facts and present some new results concerning this problem.

[1] This research is done within the COST Action IC-1004 “Random Network Coding and Designs over GF(q)”.

Quaternary convolutional codes and Linear Systems

Laurence Emilie Um
Pr. Maria Isabel García-Planas

Universitat Politècnica de Catalunya, Spain

As we know from cyclic codes, they can be represented by polynomials, from which we derive the encoding or decoding matrix. From that polynomial representation, we can extend them to convolutional codes. Indeed, as the polynomial representation of convolutional codes allows us to benefit from the linear systems theory, we will be looking at such an extension of convolutional cyclic codes as linear systems to use the linear systems properties, as quaternary codes looking into the $\mathbb{Z}_4$ ring.

Configurations — 10 years later

Harald Gropp
d12@ix.urz.uni-heidelberg.de

Since the conference will take place in Staffelstein, the birth town of Adam Ries (1492) I should start with a few remarks on Rechenmeister in the sixteenth century. However, the main part of my talk is concerned with configurations. These are linear uniform regular hypergraphs. In Thurnau in 2005 my paper was closely related to the second edition of my paper on configurations in the Handbook of Combinatorial Designs. It will be discussed how another revision would look like 10 years later. How will the book of Gruenbaum of 2009 influence the research on configurations? Mainly, how will and how should the story go on after these last years.

500 years ago the Rechenmeister changed the way how mathematics was done in Germany. What happens now, in the first years of the third millennium‘?

Generalized Sudoku arrays and other combinatorial objects with strong regularity

David Thomson

Carleton University

A Sudoku array is a Latin square with additional constraints, also known as a Gerechte design, and hence has stronger regularity than, for example, an orthogonal array. Sudoku arrays can be built by assigning a unique symbol to each coset of the Hamming code on 4 bits. This code has minimum distance 3, which imbues additional regularity conditions on the arrays; these arrays are coined *symmetric Sudokus* in [R. Bailey, P. Cameron and R. Connelly, *Sudoku, gerechte designs, resolutions, affine space, spreads, reguli and Hamming codes*, Amer. Math. Monthly, **155** (2008), 383–404].

In this work, we generalize the Bailey, Cameron, Connelly findings in multiple ways. First, we define d-dimensional Sudoku arrays and show that Reed-Solomon codes admit constructions of our new (highly symmetric) arrays. We also introduce a new *hyperSudoku* array that contains symmetry based on *elementary intervals* used to define low discrepancy point sets. These final arrays have connections to special kinds of combinatorial hypercubes, uniform matroids representable over a finite field and arcs in finite projective space.

Joint work with G. L. Mullen (Penn State), M. Huggan and B. Stevens (Carleton).

A survey on designs over finite fields

Michael Braun

Faculty of Computer Science
University of Applied Sciences
Darmstadt, Germany

This talk provides a survey on the major results on designs over finite fields. The main focus lies on the construction of explicit parameters by computer based approaches and of infinite series. Finally by combination of old and new results we obtain new parameters including new infinite series of 2-designs over finite fields.

On q-analogs of 3-(v,k,λ_3) designs

Anamari Nakić
(Joint work with Maarten De Boeck)

University of Zagreb

A t-(v,k,λ_t) design can be generalized as follows. A t-$(v,k,\lambda_t;q)$ design over a finite field $\mathbb{F}_q$ is a set $\mathscr{B}$ of k-dimensional subspaces of a v-dimensional vector space over $\mathbb{F}_q$, called blocks, with the property that any t-dimensional subspace is contained in exactly λ_t blocks. The emphasis will be on q-analogs of designs for $t = 3$. We address tactical decomposition of q-analogs of designs for $t = 3$. We give insight into the problems we encountered as well as results we obtained.

Recursive construction of subspace designs

Michael Kiermaier

Universität Bayreuth
95440 Bayreuth

Given a v-dimensional vector space V over $\mathbb{F}_q$, a t-$(v,k,\lambda)_q$ *subspace design* D is a set of k-dimensional subspaces of V such that each t-dimensional subspace is contained in exactly λ elements of D. Subspace designs are the q-analog of combinatorial block designs. For $t \geq 2$, the knowledge about concrete constructions and, in particular, infinite families of subspace designs is quite sparse.

A partition of the set of all k-subspaces of V into designs of the same parameters is called a *large set*. Large sets are even harder to construct than single subspace designs. However, for large sets of ordinary block designs, powerful recursive construction methods are known which yield infinite series of large sets and thus, of block designs.

In this talk, recursive constructions for large sets of subspace designs will be presented. As an application, new infinite families of subspace designs are obtained.

This is joint work with Michael Braun, Axel Kohnert and Reinhard Laue.

q-Analogue of Binary Cyclic Sequences

Netanel Raviv and Tuvi Etzion

The Department of Computer Science, Technion, Haifa 3200003, Israel

Subspace codes have recently gained an increasing interest due to their application in random network coding [6]. In particular, several studies [2, 4] have showed that *cyclic subspace codes* are possible candidates for optimal codes with efficient decoding and encoding algorithms. Let $\mathscr{G}_q(n,k)$ be the set of all k-dimensional subspaces of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. For a subspace $V \in \mathscr{G}_q(n,k)$ and $\alpha \in \mathbb{F}^*_{q^n}$ we define the *cyclic shift* of V as $\alpha V \triangleq \{\alpha v \mid v \in V\}$. The set αV is clearly a subspace of the same dimension as V. A subspace code $\mathbb{C} \subseteq \mathscr{G}_q(n,k)$ is called *cyclic* if for every $\alpha \in \mathbb{F}^*_{q^n}$ and every $V \in \mathbb{C}$ we have that $\alpha V \in \mathbb{C}$. The set $\{\alpha V \mid \alpha \in \mathbb{F}^*_{q^n}\}$ is called *the orbit of* V and its size is $\frac{q^n-1}{q^t-1}$ for some t which divides n. If $t=1$ we say that V has a *full length* orbit, and otherwise it has a *degenerate* orbit. In [1] it was shown that a certain set of subspaces in $\mathscr{G}_q(n,k)$ with a degenerate orbit form a cyclic subspace code with a prescribed minimum distance.

A *binary sequence* [5] of length n is an element of $\{0,1\}^n$. For a binary sequence $b = b_0 \cdots b_{n-1}$, a *cyclic shift* of b is a sequence of the form $b_i \cdots b_{n-1} b_0 \text{-} \cdots b_{i-1}$ for some $i \in \{0,\ldots,n-1\}$. The set of all cyclic shifts of b is called the *necklace* of b, and its size must divide n. If the size of the necklace is n we say that b has a *full length* necklace, and otherwise it has a *degenerate* necklace. In [3] it was shown that the number of full length necklaces may be explicitly formulated using the number of degenerate necklaces. The main tool in the proof of this result is the well-known inversion formula by Möbius.

In this talk, we will present the aforementioned subspace code [1], and the enumeration result of full length necklaces of binary sequences [3]. We will show that this subspace code admits degenerate necklaces in a natural way, and a similar formula for the enumeration of subspaces with full length orbit will be derived. We will conclude by a discussion about the connection between the two, and present several open problems for future research.

References

[1] E. Ben-Sasson, T. Etzion, A. Gabizon, and N. Raviv, “Subspace polynomials and cyclic subspace codes,” *arXiv:1404.7739 [cs.IT]*, 2014.

[2] M. Braun, T. Etzion, P. Östergård, A. Vardy, and A. Wasserman, “Existence of q-Analogs of Steiner Systems,” *arXiv:1304.1462*, 2013.

[3] T. Etzion, “An algorithm for generating shift-register cycles,” *Theoretical computer science*, vol. 44, pp. 209-224, 1986.

[4] T. Etzion, and A. Vardy, “Error-Correcting Codes in Projective Space,” *IEEE Trans. on Inform. Theory*, vol. 57, pp. 1165-1173, 2011.

[5] S. W. Golomb, et al. “Shift register sequences,” Laguna Hills, CA: Aegean Park Press, 1982.

[6] R. Koetter and F. R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. on Inform. Theory*, vol. 54, pp. 3579–3591, 2008.

This research was supported in part by the Israeli Science Foundation (ISF), Jerusalem, Israel, under Grant 10/12.
e-mails: etzion@cs.technion.ac.il, netanel.raviv@gmail.com.
The work of Netanel Raviv is part of his Ph.D. thesis performed at the Technion.

The dual q-matroid and the q-analogue of a complement

Relinde Jurrius

University of Neuchâtel, Switzerland

A *matroid* M is a combinatorial object that consists of a pair $(E,\mathscr{B})$ where E is a finite set and $\mathscr{B}$ is a non-empty collection of subsets of E, the *bases* of the matroid, that satisfy the following:

If $B_1,B_2 \in \mathscr{B}$ and $x \in B_1 - B_2$, then there is an element $y \in B_2 - B_1$ such that $B_1 - x \cup \{y\} \in \mathscr{B}$.

Examples of matroids include a set of vectors with their maximal linearly independent sets, and the set of edges of a graph with their maximal cycle-free subsets. We can also associate a matroid to a linear code by looking at the set of columns of a generator matrix.
One of the properties of matroids is that we can define a dual structure. The dual M^* of a matroid M is the pair $(E,\mathscr{B}^*)$ where

$$\mathscr{B}^* = \{E - B : B \in \mathscr{B}\}.$$

The dual matroid is again a matroid: it is not difficult to show that the set $\mathscr{B}^*$ is non-empty and satisfies the axiom above. The relation between matroids, codes and their duals can be used for example to prove the MacWilliams identities.

The q-analogue of a matroid is called a *q-matroid*. Its definition is motivated by network coding: it can be shown that rank metric codes are examples of q-matroids. A q-matroid is a finite space $\mathbb{F}_q^n$ together with a non-empty collection of subspaces, called *bases*, that satisfy an axiom like above. In this talk, we will define the dual of a q-matroid and show that it is again a q-matroid.

The methods we use are part of a more general (and philosophical) question in q-analogues. What do we mean by $E - B$ in terms of subspaces? The orthogonal complement? The quotiënt? The set of all vectors that are in E but not in B? Some subspace of dimension $\dim(E) - \dim(B)$ that has trivial intersection with B? All of these subspaces?
It turns out that the answer to this question strongly depends on the application: most of these suggestions actually appear at places where people study q-analogues. It would be nice to understand better when to choose which q-analogue, and if there is always only one q-analogue that “works”. The speaker invites everyone with an opinion on this to join the discussion.

Variable Strength Covering Arrays

Lucia Moura

University of Ottawa

In this talk, I will discuss Variable Strength Covering Arrays. Covering arrays are generalizations of orthogonal arrays that have been well studied and have applications in software and network testing. A covering array of strength t with n rows and k columns on v symbols is an $n \times k$ array such that in every set of t columns, every possible t-tuple of symbols occur in at least one row. We wish to minimize n for fixed t, k and v. Applications in software and network testing identify the components/parameters of the system with the columns of the array, each component/parameter having v possible configurations/values. The set of rows of the array prescribe a test suite with the smallest possible number of tests, such that every t-way interaction of parameter values is tested in at least one of the tests. In summary, covering arrays are the combinatorial structures that yield the so-called *combinatorial testing* (see ACTS research at NIST). Meagher and Stevens (2005) have introduced the notion of covering arrays on graphs. In this case, a graph is specified with vertices being the columns of the covering array and edges indicating which pairwise interactions must be covered. In terms of the application, the components that interact are connected by an edge, so that the array is not required to give pairwise coverage for components that do not interact. Variable strength covering arrays (VCAs) are a further generalizations of this notion that uses a hypergraph on the colums of the array, with hyperedges of arbitrary size specifying which sets of columns must have coverage. These objects are interesting not only for being nice combinatorial designs but also because they address more complex testing models where different levels of interaction need to be tested among different sets of components. In this talk, I will survey joint work with Raaphorst and Stevens on VCAs and show two upper bounds on their number of rows. The first bound comes from a greedy algorithm that generalizes the density method of Bryce, Cohen and Colbourn (2004, 2007) yielding an upper bound on the number of rows that is logarithmic on the number of columns. The second upper bound uses the probabilistic method and the Lovász Local Lemma.

Ordered Orthogonal Array Construction using LFSR sequences

André Guerino Castoldi

Universidade Estadual de Maringá (Brazil)
Visiting Researcher at the University of Ottawa (Canada)

In this talk, I will present a new construction of ordered orthogonal arrays using Linear Feedback Shift Register (LFSR) sequences constructed using primitive polynomials over finite fields (m-sequences). Raaphorst, Moura and Stevens (2014) introduced a new technique to construct covering arrays of strength 3 based on LFSR sequences. Inspired in some of their results and using a new property on runs of an LFSR sequence, a new construction of ordered orthogonal arrays of general strength is obtained. This is ongoing joint work with Moura, Panario and Stevens.

Transitive combinatorial structures invariant under some subgroups of $S(6,2)$

Andrea Švob

Department of Mathematics
University of Rijeka, Croatia
asvob@math.uniri.hr

In [1] we introduced the method for constructing transitive 1-designs from finite groups. Using the method, other combinatorial structures such as strongly regular graphs can be constructed. We will apply the method for obtaining results from the symplectic group $S(6,2)$. Transitive combinatorial structures will be constructed on the conjugacy classes of the maximal and second maximal subgroups under the action of some of $S(6,2)$ subgroups. In this talk, the constructed structures will be described.

This is a joint work with Dean Crnković and Vedrana Mikulić Crnković.

References

[1] D. Crnković, V. Mikulić, A. Švob, On some transitive combinatorial structures constructed from the unitary group $U(3,3)$, Journal of Statistical Planning and Inference 144 (2014), 19-40.

Norm invariance method and application

Kristijan Tabak

Rochester Institute of Technology
D. T. Gavrana 15
10 000 Zagreb
Croatia

We develop norm invariance approach to offer one way to deal with 2-groups which may posses a difference set. As an example of a method we deal with two infinite classes of 2-groups.

List of participants

Adachi, Tomoko (Toho University)
Bachoc, Christine (Universite de Bordeaux)
Bartoli, Daniele (Department of Mathematics, Ghent University)
Blackburn, Simon (Royal Holloway University of London)
Braic, Snjezana (Department of Mathematics, Faculty of Science, University of Split, Croatia)
Braun, Michael (University of Applied Science Darmstadt)
Buratti, Marco (Università di Perugia)
Byrne, Eimear (University College Dublin)
Cardinali, Ilaria (University of Siena)
Castoldi, André (University of Ottawa / Universidade Estadual de Maringá)
Claridge, Jessica (Royal Holloway, University of London)
Climent, Joan-Josep (Universitat d'Alacant)
Creedon, Leo (Institute of Technology Sligo)
Crnkovic, Dean (Department of Mathematics, University of Rijeka, Croatia)
D. Cardell, Sara (University of Alicante)
De Beule, Jan (Ghent University)
de la Cruz, Javier (Universidad del Norte, Barranquilla, Colombia)
Doyen, Jean (University of Brussels)
Draziotis, Kostantinos (Aristotle University of Thessaloniki)
Dumicic Danilovic, Doris (Department of mathematics, University of Rijeka)
Elia, Michele (Politecnico di Torino)
Etzion, Tuvi (Computer Science Dept., Technion, Haifa)
Farkas, Peter (Slovak University of Technology and Pan-European University in Bratislava)
Freij, Ragnar (Aalto University)
Giuzzi, Luca (Universita' di Brescia)
Gluesing-Luerssen, Heide (University of Kentucky)
Gnilke, Oliver (Aalto University)
Golemac, Anka (University of Split, Faculty of Science)
Grassl, Markus (Universität Erlangen-Nürnberg & Max-Planck-Institut für die Physik des Lichts)
Greferath, Marcus (Aalto University)
Gropp, Harald (University of Heidelberg)
Heinlein, Daniel (University of Bayreuth)
Helleseth, Tor (University of Bergen)
Honold, Thomas (Zhejiang University)
Hu, Sihuang (RWTH Aachen)
Jedwab, Jonathan (Simon Fraser University)
Jimbo, Masakazu (Nagoya University)
Jurrius, Relinde (University of Neuchâtel)
Karabulut Kurt, Gunes (Istanbul Technical University)
Kerber, Adalbert (Universität Bayreuth, Germany)
Kiermaier, Michael (Universität Bayreuth, Germany)
Kokkala, Janne (Aalto University)
Kovacevic, Mladen (University of Novi Sad)
Krčadinac, Vedran (University of Zagreb)
Krotov, Denis (Sobolev Institute of Mathematics)
Kurz, Sascha (University of Bayreuth)
Kusejko, Katharina (ETH Zurich)
Landjev, Ivan (New Bulgarian University)
Laue, Reinhard (Universität Bayreuth, Germany)
Li, Na (University College Dublin)
Mandic, Josko (Department of Mathematics, University of Split)
Manini, Daniele (University of Torino - Computer Science Department)
Maruta, Tatsuya (Osaka Prefecture University)
Metsch, Klaus (Justus-Liebig-Universität Gießen)
Miao, Ying (University of Tsukuba)
Mikulić Crnković, Vedrana (Department of Mathematics, University of Rijeka)
Monteiro, Francisco (University Institute of Lisbon)
Moura, Lucia (University of Ottawa)
Moustrou, Philippe (IMB - University of Bordeaux)
Nagy, Gábor P. (University of Szeged)
Nakic, Anamari (University of Zagreb)
Nebe, Gabriele (RWTH Aachen)
Olmez, Oktay (Ankara Unversity)
Östergård, Patric (Aalto University)
Otal, Kamil (Middle East Technical University)
Özbudak, Ferruh (Middle East Technical University)
Pacher, Christoph (AIT Austrian Institute of Technology, Digital Safety & Security Department)
Panario, Daniel (Carleton University)
Pavcevic, Mario Osvin (University of Zagreb)
Pavese, Francesco (University of Basilicata)
Pott, Alexander (Otto-von-Guericke-University Magdeburg)
Raviv, Netanel (Technion)
Riet, Ago-Erik (University of Tartu)
Rodrigues, Bernardo (University of KwaZulu-Natal)
Rosenthal, Joachim (University of Zurich)
Rousseva, Assia (Sofia University)
Rößing, Cornelia (University College Dublin)
Rukavina, Sanja (Department of Mathematics, University of Rijeka)
Ryoh, Fuji-Hara (University of Tsukuba)
Schmidt, Kai-Uwe (Otto-von-Guericke University)
Sheekey, John (Universiteit Gent)
Simos, Dimitris (SBA Research)
Solov'eva, Faina (Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk)
Stokes, Klara (University of Skövde)
Storme, Leo (Ghent University)
Šubašić, Aljoša (PMF, Split, Croatia)
Svob, Andrea (Department of Mathematics, University of Rijeka, Croatia)
Tabak, Kristijan (Rochester Institute of Technology)
Tekin, Eda (METU)
Touserkani, Rouzbeh (Assistant Professor at IPM, Tehran)
Tran van Trung (University of Duisburg-Essen)
Trautmann, Anna-Lena (University of Zurich)
Um, Laurence (Universitat Politècnica de Catalunya)
Ustimenko, Vasyl (Institute of Mathematics, University of Maria Curie Sklodowska)
Vasil'eva, Anastasia (Sobolev Institute of Mathematics)
Vazquez Castro, Maria Angeles (Telecommunications and

Systems Engineering, Autonomous University of Barcelona, Spain)
Villar, Darwin (Lehrstuhl D für Mathematik, RWTH Aachen)
Vucicic, Tanja (Department of Mathematics, Faculty of Science, University of Split, Croatia)
Vukobratovic, Dejan (University of Novi Sad)
Wassermann, Alfred (Universität Bayreuth, Germany)
Westerbäck, Thomas (Aalto University)
Willems, Wolfgang (Department of Mathematics, Otto-von-Guericke-University Magdeburg)
Zumbrägel, Jens (TU Dresden)

List of speakers