Geometry, Combinatorial Designs and Cryptology

Fourth Pythagorean Conference

Sunday 30 May to Friday 4 June 2010

Index of Talks and Abstracts

Main talks

Short talks

9. Frank De Clerck, Intriguing sets of partial quadrangles
10. Alice Devillers, Symmetry properties of subdivision graphs
11. Dalibor Froncek, Decompositions of complete bipartite graphs into generalized prisms
12. Stelios Georgiou, Self-dual codes from circulant matrices
13. Robert Gilman, Cryptology of infinite groups
14. Otokar Grošek, The number of associative triples in a quasigroup
15. Christoph Hering, Latin squares, homologies and Euler's conjecture
16. Leanne Holder, Bilinear star flocks of arbitrary cones
17. Robert Jajcay, On the geometry of cages
18. Domenico Labbate, Classes of 2–factor isomorphic regular graphs
19. Reinhard Laue, Resolvable Steiner 3–designs
20. Michel Lavrauw, Finite semifields and linear sets in projective spaces
21. Ka Hin Leung, Weil numbers, circulant matrices and Snevily's conjecture
22. Curt Lindner, Almost resolvable 4-cycle systems
23. Giuseppe Marino, A generalization of cyclic semifields
24. Francesco Mazzocca, 3-nets embedded in a projective plane
25. Francesca Merola, Numeration systems
26. Alessandro Montinaro, On the affine planes of order 2^{3s} admitting $PSU_3(2^s)$ as a collineation group
27. Nicola Pace, On the distribution of elements of a finite group generated by random covers
28. Stanley Payne, Finite self-dual generalized quadrangles
29. Valentina Pepe, Embedding the Hermitian unital in a 7–dimensional projective space
30. Dimitris Simos, Explorations of optical orthogonal and quasi-cyclic codes from a combinatorial design perspective
31. Angelo Sonnino, k-arcs and 2-level sharing schemes
32. Rainer Steinwandt, Message authentication in the presence of key-dependent messages

33. Adriana Suárez, Attribute-based group key establishment

34. Tran van Trung and Pavol Svaba, Public key cryptosystem MST_3: cryptanalysis and realization

35. Rocco Trombetti, $\mathbf{F}_q$–pseudoreguli of $\mathrm{PG}(3, q^3)$

36. Geertrui Van de Voorde, On the linearity of higher-dimensional blocking sets

37. Alfred Wassermann, Mutually disjoint designs and new 5-designs derived from groups and codes

38. Zsuzsa Weiner, Characterizing small weight codewords of the linear code of $\mathrm{PG}(2, q)$

Adjacency matrices of polarity graphs and of other C_4–free graphs of large size

Marién Abreu

Università degli Studi della Basilicata

(Joint work with C. Balbuena and D. Labbate)

Denote by $ex(n; C_4)$ the maximum number of edges of a graph on n vertices and free of squares C_4. Brown, Erdős, Rényi and Sós were the first to consider polarity graphs in order to obtain lower bounds for $ex(n; C_4)$. Exact values for $ex(n; C_4)$ have been computed for $n \leq 31$ and the corresponding extremal graphs have been found by Clapham, Flockhart, Sheehan, Yang and Rowlinson. Moreover, Füredi has proved that $ex(q^2 + q + 1; C_4) = \frac{1}{2}q(q + 1)^2$ where q is either a power of 2 or a prime power exceeding 13.

In this talk we show a simpler method for explicitly obtaining an adjacency matrix of a polarity graph $\widehat{G}_q$ from an incidence matrix of a projective plane $PG(2, q)$, where q is a prime power. We consider the underlying simple graphs G_q and use them to obtain lower bounds on the extremal function $ex(n; C_4)$, for some $n < q^2 + q + 1$. In particular, we exhibit a C_4-free graph on $n = q^2 - \sqrt{q}$ vertices and $\frac{1}{2}q(q^2 - 1) - \frac{1}{2}\sqrt{q}(q - 1)$ edges, for a square prime power q.

On subsets of a finite vector space in which every subset of basis size is a basis

Simeon Ball

Universitat Politécnica de Catalunya

In this talk we consider sets of vectors S of the vector space $\mathbb{F}_q^k$ with the property that every subset of S of size k is a basis.

The classical example of such a set is the following.

Example (Normal Rational Curve) The set

$$S = \{(1, t, t^2, \ldots, t^{k-1}) \mid t \in \mathbb{F}_q\} \cup \{(0, \ldots, 0, 1)\},$$

is a set of size $q + 1$.

It is easily shown that S has the required property by checking that the $k \times k$ Vandermonde matrix formed by k vectors of S, has non-zero determinant.

For q even and $k = 3$, one can add the vector $(0, 1, 0)$ to S and obtain an example with $q + 2$ vectors. For these parameters, such a set of $q + 2$ vectors is called a *hyperoval*, and these have been studied extensively. There are many examples of hyperovals known which are not equivalent (up to change of basis and field automorphisms) to the example above. The only other known examples of size $q + 1$ is an example of size 10 in $\mathbb{F}_9^5$, due to Glynn, and an example in $\mathbb{F}_{2^h}^4$ due to Hirschfeld.

We shall discuss how to prove that if $|S| > (q - 1)/2 + k$ then there is a series of equations of rational functions which the vectors of S must satisfy.

We shall then consider the consequences of these equations for the following conjecture, known as the main conjecture for maximum distance separable codes.

Conjecture A set of vectors S of the vector space $\mathbb{F}_q^k$, $k \leq q - 1$, with the property that every subset of S of size k is a basis, has size at most $q + 1$, unless q is even and $k = 3$ or $k = q - 1$, in which case it has size at most $q + 2$.

We shall then consider generalisations of the following theorem of Segre.

Theorem *If $p \geq 3$ then a set S of $q + 1$ vectors of the vector space $\mathbb{F}_q^3$, with the property that every subset of S of size 3 is a basis, is equivalent to the Normal Rational Curve example, where $q = p^h$.*

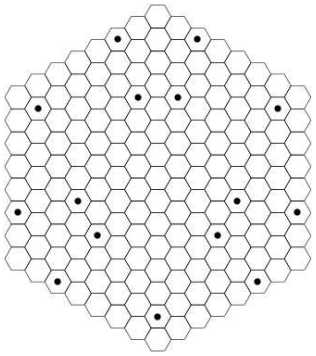
Honeycomb arrays

Simon R. Blackburn

Royal Holloway, University of London

(Joint work with Tuvi Etzion, Keith Martin, Anastasia Panoui, Maura Paterson and Doug Stinson)

Honeycomb arrays were introduced in 1984 by Golomb and Taylor as the analogue of Costas arrays in the hexagonal grid. An example is given in the figure below.



[There is exactly one dot in each 'row', where a row can lie in each of the three natural directions in the hexagonal grid; this is an analogue of the fact that a Costas array is a permutation matrix. Moreover, the $\binom{15}{2}$ vector differences between the distinct dots are all different.]

I will define honeycomb arrays precisely, and explain the recent results of [1, 2] on these arrays. I will talk about a generalisation of these arrays, a connection to cryptography, and some of the open problems in the area.

References

[1] S.R. Blackburn, T. Etzion, K.M. Martin and M.B. Paterson, Two-dimensional patterns with distinct differences – constructions, bounds, and maximal anticodes', *IEEE Trans. Inform. Theory*, to appear. `http://arxiv.org/abs/0811.3832`.

[2] S.R. Blackburn, A. Panoui, M.B. Paterson and D.R. Stinson, 'Honeycomb arrays', preprint. `http://arxiv.org/abs/0911.2384`.

Combinatorial designs via factorization of a group into subsets

Marco Buratti

University of Perugia

In the early nineties, after some improvements on some classical constructions for elementary abelian 2-designs by R.C. Bose [1] and R.M. Wilson [5], it became apparent that the basic idea was the consideration of an algebraic problem, called the *packing problem* studied in [2] in the following form:

Given a subset X of Z_n, determine whether there exists a packing of X in Z_n, namely a set of pairwise disjoint translates of X partitioning Z_n.

I spoke about this problem at several conferences on combinatorics. In particular, encouraged by Paul Erdős who heard my talk at a conference in Nasholim (Israel, 1995), I wrote another short article [3] where I proposed the same problem in an arbitrary group G. It was a surprise that this problem had been studied since 1949 in a different context. In the book [4] by S. Szabo and A.D. Sands, group theorists formulate the packing problem as follows:

Given a subset X of a group G determine whether X is a factor of G.

Here a *factor* means that there exists another subset Y of G such that any element $g \in G$ can be expressed in the form $g = x \cdot y$ for exactly one pair $(x, y) \in X \times Y$. In this case, $G = X \cdot Y$ is a *factorization* of G into the two subsets X and Y.

It often happens that mathematicians belonging to different areas are unaware of each other's work, even though their problems may be very closely related. Here, the idea of this talk is to spread the knowledge of the *factorization problem* among combinatorialists. A survey is also given of how this problem and some generalizations of it can be efficiently applied to the construction of some combinatorial designs.

References

[1] R.C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* **9** (1939), 353–399.

[2] M. Buratti, A packing problem and its applications to Bose's families, *J. Combin. Des.* **4** (1996), 457–472.

[3] M. Buratti, Packing the blocks of a regular structure, *Bull. Inst. Combin. Appl.* **21** (1997), 49–58.

[4] S. Szabo and A.D. Sands, Factoring groups into subsets, Lecture Notes in Pure and Applied Mathematics **257**, Chapman & Hall, 2009.

[5] R.M. Wilson, Cyclotomic and difference families in elementary abelian groups, *J. Number Theory* **4** (1972), 17–47.

Lightweight cryptographic mechanisms based on pseudorandom number generators

Mike Burmester

Florida State University

The emergence of computing environments where devices are embedded pervasively in the physical world has made possible many interesting applications and triggered new research areas. Sensor networks and radio frequency identification (RFID) systems are two such applications. Operating on a wireless medium, these systems suffer from critical security vulnerabilities for which few satisfactory solutions exist, particularly with respect to availability and privacy. In addition, existing cryptographic mechanisms may not readily be transferable to settings that involve highly constrained devices.

In this talk we focus on low cost RFID systems and consider their security in adversarial environments. Recently several lightweight RFID protocols have been proposed that are based on sharing pseudorandom number generators (PRNG) [2, 3]. With these, RFID tags get identified by drawing successive numbers from a PRNG. PRNGs can be implemented on a very small circuit footprint, and are ideally suited for such applications. Furthermore, they can be used to support resiliency in modular and concurrent deployments—the Universal Composability framework [1].

Here we discuss two innovations: (a) *refreshing* RFID tags; (b) extending the scope of PRNG applications with RFID deployments. Although the approach described above provides strong security guarantees in a theoretical framework, in practice, the seed of the PRNG is relatively short, and as numbers get drawn, the adversary will eventually succeed in distinguishing them from random and use correlation type attacks. To secure such applications one must refresh the seed of the PRNG at regular intervals, and bound the distinguishing probability below a certain threshold.

Our second contribution involves extending the scope of PRNG applications. RFID systems are not restricted to individual tag identifications. They can also be used for *group identification* [4]. There are several deployments in which group scanning is an important functionality. In such cases, the tags in the group must generate a proof of *simultaneous presence* while being scanned by an RFID reader. In general the complexity of such distributed applications can be prohibitive for most RFID deployments. However, by sharing a pseudorandom number stream, RFID tags can recognize each other's presence and produce a number that uniquely identifies the group to the Verifier.

References

[1] M. Burmester, T. Van Le, B. De Medeiros, and G. Tsudik, Universally composable RFID identification and authentication protocols. *ACM Trans. Inf. Syst. Secur. 12*, **4** (2009), 1–33.

[2] M. Burmester, B. de Medeiros, J. Munilla and A. Peinado, Secure EPC Gen2 compliant radio frequency identification, in P.M. Ruiz and J.J. Garcia-Luna-Aceves, editors, *ADHOC-NOW*, *Lecture Notes in Computer Science* **5793**, Springer, 2009, 227–240.

[3] M. Burmester and J. Munilla, Flyweight authentication with forward and backward security, WISP Summit 2009, First Workshop on Wirelessly Powered Sensor Networks and Computational RFID, Berkeley, CA, 2009.

[4] M. Burmester, B. de Medeiros and R. Motta, Provably Secure Grouping-Proofs for RFID Tags, in G. Grimaud and F-X. Standaert, editors, *CARDIS 2008*, *Lecture Notes in Computer Science* **5189**, Springer, 2008, 176–190.

Loops, neardomains, nearfields and sets of permutations

Philippe Cara

Vrije Universiteit Brussel

(Joint work with R.W. Kieboom and T. Vervloet)

Loops, nearrings and nearfields are structures in algebra which generalize groups, rings and fields, respectively. They are very useful in areas like affine and projective geometry, coding theory and cryptography. Neardomains, introduced by Karzel in 1965 and published in [1], are a weakening of nearfields in which the associativity of the addition is further relaxed.

There are well-known links between these algebraic structures and some specific sets of permutations, such as sharply 2-transitive groups. I shall report on recent work we did to describe these links in a uniform way.

The techniques are inspired by ideas from category theory. By choosing the right kind of morphisms, we can show that the category of neardomains is equivalent to the category of sharply 2-transitive groups. This equivalence nicely restricts to an equivalence of the category of nearfields and the category of sharply 2-transitive groups with an extra property.

References

[1] H. Karzel, Zusammenhänge zwischen Fastbereichen, scharf zweifach transitiven Permutationsgruppen und 2-Strukturen mit Rechteckaxiom, *Abh. Math. Sem. Univ. Hamburg* **32** (1968), 191–206.

On the structure of Weyl modules for the symplectic group

Ilaria Cardinali

University of Siena

(Joint work with A. Pasini)

Let V_k be the Weyl module of dimension $\binom{2n}{k} - \binom{2n}{k-2}$ for the group $G = \mathrm{Sp}(2n, \mathbb{F})$ arising from the k-th fundamental weight of the Lie algebra of G. Thus, V_k affords the grassmann embedding of the k-th symplectic polar grassmannian of the building associated to G. When $\mathrm{char}(\mathbb{F}) \neq 0$, it is known that the G-module V_k can be reducible.

In this talk we will investigate the structure of the module V_k mainly focusing on a geometric description of it. In particular, we will give a sufficient condition for such a module to be uniserial and a geometrical description of the composition series of that module when our condition is satisfied.

References

[1] R.J. Blok, I. Cardinali and A. Pasini, On natural representation of the symplectic group, *Bull. Belg. Math. Soc. Simon Stevin*, to appear.

[2] I. Cardinali and A. Pasini, On Weyl modules for the symplectic group, in preparation.

Parallelisms of quadrics

Bill Cherowitzo

University of Colorado Denver

(Joint work with N. Johnson)

Let K be a field and consider flocks of a quadratic cone, an elliptic quadric or a hyperbolic quadric in $PG(3, K)$. We ask whether or not there are *parallelisms* of these quadrics, which in each case means a set of mutually disjoint flocks, whose union is a complete cover of the set of conics which are the plane intersections of the quadric in question.

Surprisingly, we are able to show that all hyperbolic flocks and all conical flocks of $PG(3, K)$, for K a field admitting a quadratic extension F, may be embedded into a set of flocks that define a parallelism. In both cases, there are groups involved that essentially imply that the parallelism is a "transitive parallelism". Also we can extend the theory of parallelisms of quadratic cones to the case of the non-quadratic cones which in the finite case give rise to the *flokki* of Kantor and Penttila.

Large maximal partial ovoids of $Q^-(5,q)$

Jan De Beule

Ghent University

(Joint work with K. Metsch and K. Coolsaet)

It is easy to show that the generalized quadrangle $Q^-(5,q)$ has no ovoids, that is, no point set $\mathcal{O}$ exists for which every line of $Q^-(5,q)$ meets $\mathcal{O}$ in exactly one point. So the question how large a *partial ovoid*, that is, a set $\mathcal{K}$ of points for which every line of $Q^-(5,q)$ meets $\mathcal{K}$ in at most one point, can be, arises naturally.

We show that a partial ovoid of $Q^-(5,q)$ has size at most $\frac{1}{2}(q^3+q+2)$. This bound is sharp for $q=2,3$ ([2], [3]). Exhaustive searches using the computer have shown that this bound is not sharp for $q=4,5$. Recently, maximal partial ovoids of $Q^-(5,q)$, q odd, of size $(q+1)^2$ were found and described by Cossidente [1].

We discuss other examples of maximal partial ovoids of $Q^-(5,q)$ of size at least $(q+1)^2$. Among these, there is a family of examples for q odd, $q \equiv 3 \pmod 4$ and $q=2^h$, h even, of size $(q+1)^2$.

References

[1] A. Cossidente, Some constructions on the Hermitian surface, *Des. Codes Cryptogr.* **51** (2009), 123–129.

[2] R.H. Dye, Partitions and their stabilizers for line complexes and quadrics, *Ann. Mat. Pura Appl.* **114** (1977), 173–194.

[3] G.L. Ebert and J.W.P. Hirschfeld, Complete systems of lines on a Hermitian surface over a finite field, *Des. Codes Cryptogr.* **17** (1999), 253–268.

On extensions of hyperplanes of dual polar spaces

Bart De Bruyn

Ghent University

With every polar space Π of rank $n \geq 2$, there is associated a point-line geometry Δ which is called a *dual polar space of rank* n. The points and lines of Δ are the maximal and next-to-maximal singular subspaces of Π, and incidence is reverse containment. If F is a convex subspace of diameter $\delta \geq 2$ of Δ, then the points and lines which are contained in F define a subgeometry $\widetilde{F}$ of Δ, which is a dual polar space of rank δ. If F is a convex subspace and x a point of Δ, then F contains a unique point $\pi_F(x)$ nearest to x.

A *hyperplane* of a point-line geometry $\mathcal{S}$ is a proper subspace meeting each line. If $e : \mathcal{S} \to \Sigma$ is a full projective embedding of $\mathcal{S}$ into a projective space Σ and $\mathcal{P}$ the point set of $\mathcal{S}$, then for every hyperplane Π of Σ, the set $e^{-1}(e(\mathcal{P}) \cap \Pi)$ is a hyperplane of $\mathcal{S}$. Such a hyperplane of $\mathcal{S}$ is said to *arise from* e. If Δ is a dual polar space of rank n, if F is a convex subspace of diameter $\delta \geq 2$ of Δ, and if G is a hyperplane of $\widetilde{F}$, then the set H_G of all points at distance at most $n - \delta - 1$ from F together with all points x at distance $n - \delta$ from F for which $\pi_F(x) \in G$ is a hyperplane of Δ, called *the extension of* G.

In the talk, I will discuss several results regarding extensions of hyperplanes of dual polar spaces. In particular, I will discuss the following problem.

> Suppose the hyperplane G of the convex subspace F arises from a certain embedding of $\widetilde{F}$. Does the extension of G also arise from an embedding? And which embedding?

This discussion will allow us to prove the following result. Suppose e is the so-called absolutely universal embedding of a fully embeddable thick dual polar space Δ. If F is a convex subspace of Δ of diameter at least 2, then the embedding e will induce an embedding e_F of $\widetilde{F}$ which is isomorphic to the absolutely universal embedding of $\widetilde{F}$.

Intriguing sets of partial quadrangles

Frank De Clerck

Ghent University

(Joint work with John Bamberg and Nicola Durante)

The point-line geometry known as a *partial quadrangle*, introduced by Cameron in 1975, has the property that, for every point/line non-incident pair (P, ℓ), there is at most one line through P concurrent with ℓ. So, in particular, the well-studied objects known as *generalised quadrangles* are each partial quadrangles. An *intriguing set* of a generalised quadrangle is a set of points which induces an equitable partition of size two of the underlying strongly regular graph. We extend the theory of intriguing sets of generalised quadrangles by Bamberg, Law and Penttila to partial quadrangles, which gives insight into the structure of hemisystems and other intriguing sets of generalised quadrangles.

Symmetry properties of subdivision graphs

Alice Devillers

The University of Western Australia

(Joint work with Ashraf Daneshkhah and Cheryl E. Praeger)

The subdivision graph $\mathsf{S}(\Sigma)$ of a graph Σ is obtained from Σ by 'adding a vertex' in the middle of every edge of Σ. In other words, it is the incidence graph of Σ if Σ is seen as a vertices-edges geometry. In [1], we study various symmetry properties of $\mathsf{S}(\Sigma)$.

Let $s \geq 1$ be an integer. A graph Γ, with $G \leq \mathrm{Aut}(\Gamma)$, is said to be locally (G, s)-arc transitive if Γ contains s-arcs and, for any vertex v, the stabiliser G_v is transitive on the set of i-arcs starting at v, for all $i \leq s$; it is locally (G, s)-distance transitive if $s \leq \mathsf{diam}(\Gamma)$ and, for any vertex v, the stabiliser G_v is transitive on the set $\Gamma_i(v) = \{x \in V\Gamma \mid d(v, x) = i\}$, for all $i \leq s$. If G is also transitive on vertices, then we remove the word 'locally'.

We prove that, for a connected graph Σ, the graph $\mathsf{S}(\Sigma)$ is locally s-arc transitive if and only if Σ is $\lceil \frac{s+1}{2} \rceil$-arc transitive. The diameter of $\mathsf{S}(\Sigma)$ is $2d+\delta$, where Σ has diameter d and $0 \leqslant \delta \leqslant 2$; local s-distance transitivity of $\mathsf{S}(\Sigma)$ is defined for $1 \leqslant s \leqslant 2d+\delta$. In the general case where $s \leqslant 2d-1$, we prove that $\mathsf{S}(\Sigma)$ is locally s-distance transitive if and only if Σ is $\lceil \frac{s+1}{2} \rceil$-arc transitive. For the remaining values of s, namely $2d \leqslant s \leqslant 2d+\delta$, we classify the graphs Σ for which $\mathsf{S}(\Sigma)$ is locally s-distance transitive in the cases, $s \leqslant 5$ and $s \geqslant 15+\delta$. The remaining cases are work in progress.

References

[1] A. Daneshkhah, A. Devillers and C.E. Praeger, Symmetry properties of subdivision graphs, submitted.

Decompositions of complete bipartite graphs into generalized prisms

Dalibor Froncek

University of Minnesota Duluth

(Joint work with Sylwia Cichacz)

R. Häggkvist [3] proved that every 3-regular bipartite graph of order $2n$ with no component isomorphic to the Heawood graph decomposes the complete bipartite graph $K_{6n,6n}$.

In this talk we strengthen Häggkvist's result for a certain class of generalized prisms. Recall that a *prism* is a graph of the form $C_m \times K_2$. For j even let a $(0,j)$-*prism* of order $4n$ be a graph with two cycles $C_{2n} = v_0, v_1, \ldots, v_{2n-1}$ and $C'_{2n} = v'_0, v'_1, \ldots, v'_{2n-1}$ and $2n$ additional edges $v_1v'_1, v_3v'_3, \ldots, v_{2n-1}v'_{2n-1}$ and $v_0v'_j, v_2v'_{2+j}, \ldots, v_{2n-j}v'_0$. In our terminology a prism is a $(0,0)$-prism.

The problem of factorization of the complete bipartite graph $K_{n,n}$ into $(0,j)$-prisms with $2n$ vertices was recently completely solved by Sylwia Cichacz and DF [1].

In [2], Sylwia Cichacz, DF, and Petr Kovar proved the following theorem.

Theorem *Let $n \equiv 0 \pmod 8$, $j = a2^r$ and $n = b2^s$, for some positive integers a, b, r, s, where a, b are odd. If G is a $(0,j)$-prism of order $2n$ and $r < s$, then G decomposes $K_{\frac{3n}{2},\frac{3n}{2}}$.*

In this talk we will present some further results on decompositions of complete bipartite graphs into $(0,j)$-prisms.

References

[1] S. Cichacz and D. Froncek, Factorization of $K_{n,n}$ into $(0,j)$-prisms, *Information Processing Letters* **109** (2009), 932–934.

[2] S. Cichacz, D. Froncek and P. Kovar, Note on decomposition of $K_{n,n}$ into $(0,j)$-prisms, *IWOCA 2009*, J. Fiala, J. Kratochvil, M. Miller (Eds.), Lecture Notes in Computer Science **5874**, Springer-Verlag, Berlin, Heidelberg, 125–133.

[3] R. Häggkvist, Decompositions of complete bipartite graphs, *Surveys in Combinatorics, 1989* (Norwich, 1989), London Math. Soc. Lecture Note Ser. **141**, Cambridge Univ. Press, Cambridge, 1989, 115–147.

Self-dual codes from circulant matrices

Stelios D. Georgiou

University of the Aegean

(Joint work with Eleftherios Lappas)

Self-dual codes are an important class of linear codes due to their favorable properties; see for example [4]. The construction of self-dual codes with large minimum distance remains a challenging problem. In particular, self-dual codes over some prime fields have not been investigated thoroughly and many open cases concerning the minimum distance remain. Much work on self-dual codes has appeared in the literature; see for example [1, 2, 3, 5].

In this talk, we propose some new methods for building self-dual codes. The suggested methods use circulant matrices over prime fields in block circulant structures to construct the generator matrices. Suitable circulant matrices are chosen based on their periodic autocorrelation functions. The generator matrix, which satisfies the appropriate requirements, is described by its first row vector over $\mathbb{F}_p$. We apply these methods to investigate the minimum distance of self-dual codes. The results found are tabulated and compared with the known results in the literature.

References

[1] M. Harada, T.A. Gulliver and H. Miyabayashi, Double circulant and quasi-twisted self-dual codes over $\mathbb{F}_5$ and $\mathbb{F}_7$, *Advances Math. Communications* **1** (2007), 223–238.

[2] S. Han and J.-L. Kim, On self-dual codes over $\mathbb{F}_5$, *Des. Codes Cryptogr.* **48** (2008), 43–58.

[3] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-correcting Codes*, North-Holland, Amsterdam, 1977.

[4] E. Rains and N.J.A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, V. Pless et al. eds., Elsevier, Amsterdam, 1998.

[5] V.D. Tonchev, Codes, in *Handbook of Combinatorial Designs, Second Edition*, C.J. Colbourn, J.H. Dinitz eds., Chapman &Hall/CRC, Boca Raton 2007, 677–702.

Cryptology of infinite groups

Robert Gilman

Stevens Insitute of Technology

It is well known that the availability of quantum computers would break public-key systems in use today. Several public-key systems based on computational problems which are not known to be efficiently solvable by quantum computers have been proposed. For such a system to be secure, the computational problem, with appropriate choice of parameters, must be difficult to solve in almost all instances; but standard complexity measures are not well adapted to verifying this criterion. We introduce generic case complexity [1, 2] and review its use in cryptanalysis of some public-key systems based on computational problems from combinatorial group theory. We also consider some new group theory problems which are suggested by the cryptanalysis.

References

[1] I. Kapovich, A. Myasnikov, P. Schupp, and V. Shpilrain, Generic-case complexity and decision problems in group theory, *J. Algebra* **264** (2003), 665–694. `http://arxiv.org/pdf/math/0203239`

[2] R. Gilman, A.G. Miasnikov, A.D. Myasnikov and A. Ushakov, Report on generic case complexity, *Herald of Omsk University*, Special Issue, 2007, 103–110. `http://www.math.stevens.edu/ rgilman/rhg/report.pdf`

The number of associative triples in a quasigroup

Otokar Grošek

Slovak University of Technology

(Joint work with P. Horák)

For a quasigroup $(Q, *)$ a triple (x, y, z), where $x, y, z \in Q$, is called associative if $(x * y) * z = x * (y * z)$. We denote by $a(Q)$ the number of associative triples in Q. In [1] the authors provide, for any $n \neq 4k + 2$, a quasigroup Q with $a(Q) = n^2$. Moreover, let

$$B(Q) = \{(x, y, z) \in Q^3 \mid x * (y * z) \neq (x * y) * z\}$$

and let $B(n) = \min\{|B(Q)|\}$, where the minimum runs over all quasigroups of order n. It is shown in [1] that $B(n) < 3n^2/32$, provided that $n > 29124$.

In our contribution we first present a lower bound on $a(Q)$ in terms of the number of idempotent elements. Let $I(Q) = \{a; a \in Q, a * a = a\}$. Then the following result holds.

Theorem 1 *Let Q be a quasigroup of order n. Then $a(Q) \geq 2n - |I(Q)|$.*

Further, we describe a construction of quasigroups having so far the smallest known number of associative triples. The starter elements for this construction have been obtained by an extensive computer search for $n \leq 7$.

Theorem 2 *There exists a sequence $\{Q_n\}_{n=1}^{\infty}$ of quasigroups so that*

(i) *the order of Q_n is 5^n and $a(Q_n) = |Q|^t$, where t is an absolute constant with*

$$t = \frac{\ln(15)}{\ln(5)} = 1.6826\cdots;$$

(ii) *the order of Q_n is 6^n and $a(Q_n) = |Q|^t$, where t is an absolute constant with*

$$t = \frac{\ln(19)}{\ln(6)} = 1.6433\cdots;$$

(iii) *the order of Q_n is 7^n and $a(Q_n) = |Q|^t$, where t is an absolute constant with*

$$t = \frac{\ln(19)}{\ln(7)} = 1.5131\cdots.$$

Some connections to cryptanalysis will be presented as well.

References

[1] J. Ježek and T. Kepka, Notes on the number of associative triples, *Acta Univ. Carolin. Math. Phys.* **31** (1990), 15–19.

Latin squares, homologies and Euler's conjecture

Christoph Hering

Universität Tübingen

(Joint work with Andreas Krebs)

We construct pairs of orthogonal Latin squares of order n by means of suitable orthomorphisms of the cyclic group of order $n-1$. These pairs always have $n-3$ confluent common transversals. They lead to partial planes of order n with $5n-2$ lines and 5 complete points. Also, we provide an easy construction of counter-examples to Euler's conjecture.

Bilinear star flocks of arbitrary cones

Leanne Holder

Rose–Hulman Institute of Technology

(Joint work with W.E. Cherowitzo)

The concept of a flock was introduced in 1968 by Dembowski to describe a partition of all but two points of a Möbius plane into circles. Shortly thereafter, the context in which the term flock was used was expanded to include partitions of quadratic sets in $\mathrm{PG}(3, q)$ into quadrics. For instance, in the case when the flock is defined over a quadratic cone, the flock is a partition of the cone, not including the vertex, into pairwise disjoint conics. Since at least the early 1970's, flocks of these quadratic sets have been studied due to their rich connection with other geometrical objects in $\mathrm{PG}(3, q)$ such as generalized quadrangles, ovals and hyperovals, translation planes, and spreads, amongst others. By the late 80's, all flocks of ovoids and hyperbolic quadrics had been classified, leaving only the classification of flocks of cones.

In the late 90's, Cherowitzo began to generalize the theory of the flocks of cones. He sought to release the flock from its reliance on the quadratic cone in $\mathrm{PG}(3, q)$. That is, by shifting the viewpoint from the conics which form a flock to the planes which determine these conics (and calling the set of planes the flock), the nature of the cone becomes irrelevant. As this definition of a flock can also be used for quadratic cones, flocks of quadratic cones will just be special cases of flocks of arbitrary cones.

A linear flock is one in which all the planes of the flock pass through a common line. Linear flocks always exist provided there is a line in $\mathrm{PG}(3,q)$ which is exterior to the cone. A bilinear flock is one in which all the planes contain at least one of two lines. The two lines are called carriers. If there is a plane in the flock which contains both carriers, then all the planes of the flock must pass through the intersection point of the carriers and thus the flock is a star flock. Thas has classified the star flocks of quadratic cones and in particular, in even characteristic, all star flocks of a quadratic cone are linear. Thus, when q is even, any bilinear flock of a quadratic cone must be linear. However, Johnson and Biliotti have shown that in the infinite case quadratic cones do admit bilinear flocks. Therefore, to find bilinear star flocks in the finite case, we must abandon quadratic cones. Cherowitzo has found some examples of these using the flokki of Kantor and Penttila.

In this talk we discuss bilinear star flocks of arbitrary cones in $\mathrm{PG}(3, q)$ and offer results leading to the existence and construction of such flocks.

On the geometry of cages

Robert Jajcay

Indiana State University

A (k, g)-cage is a k-regular graph of girth g of the smallest possible order. The usefulness of projective planes, generalized quadrangles and generalized hexagons in cage constructions is well recognized and documented, and many other less well-known constructions take further advantage of the geometric properties of these and related combinatorial structures. In our talk, we discuss some of the newer examples of such mutually beneficial connections.

Curves over finite fields, an approach from finite geometry

Gábor Korchmáros

University of Basilicata

The classical approach to the study of the number of $\mathbb{F}_q$-rational points of an algebraic curve defined over the finite field $\mathbb{F}_q$ was adapted from algebraic number theory in the 1930's. In that context, the zeta function together with character sums produced a proof of the Riemann hypothesis over a finite field; this major result, is known as the Hasse–Weil theorem.

For more recent applications to finite geometry, coding theory, correlations of shift register sequences and exponential sums, the interest is in those curves which have many $\mathbb{F}_q$-rational points. An elementary approach to the construction of large families of curves with many $\mathbb{F}_q$-rational points was developed by Garcia, Stichtenoth, van der Geer and their students. On the other hand, sophisticated methods from algebraic geometry and algebraic number theory are often effective.

In the past ten years, a team of finite geometers comprising A. Aguglia, A. Cossidente, M. Giulietti, J.W.P. Hirschfeld, myself and A. Siciliano, together with F. Torres worked out a new approach using familiar geometric objects, methods and results from finite geometry. An advantage of this approach is the possibility of a major involvement of finite group theory.

In this talk we give a survey of the known results and open problems, looking at the subject from a finite geometry point of view.

Classes of 2–factor isomorphic regular graphs

Domenico Labbate

Politecnico di Bari

(Joint work with M. Abreu and J. Sheehan)

A graph is 2–factor isomorphic if all its 2–factor are isomorphic. In this talk we present existence results for classes of 2–factor isomorphic regular graphs in the bipartite and not necessarily bipartite case. Moreover, we present constructions of infinite families of regular graphs in these classes.

Resolvable Steiner 3–designs

Reinhard Laue

Universität Bayreuth

The existence problem of resolvable Steiner t–$(v, k, 1)$ systems with $t > 2$ has been solved by Hartman [2] for Steiner Quadruple Systems, that is for $t = 3$ and $k = 4$, up to 23 cases which have been settled by Ji and Zhu [3]. Further sporadic examples of resolvable Steiner systems are the Witt designs with parameters 5–$(12, 6, 1)$, 5–$(24, 8, 1)$ and a 5–$(48, 6, 1)$ design, see [4]. Recently, Masanori Sawa asked for resolvable Steiner 3–designs with $k > 4$. From an analysis of the 3–$(q^n + 1, q + 1, 1)$ designs admitting $\mathrm{PGL}(2, q^n)$ as a group of automorphisms the following result is obtained.

Theorem *Let $q > 2$ be a prime power, $q + 1$ not a power of 2, and n a positive integer. Then there exists a resolvable 3–$(q^{3^n} + 1, q + 1, 1)$ design.*

It is not clear whether it is necessary to assume that $q + 1$ is not a power of 2. At least for $q = 7$ and $q = 31$ the designs are resolvable, as computations with MAGMA [1] show. It is conceivable that the result would hold for all parameters 3–$(q^n + 1, q + 1, 1)$ where n is odd.

The resolvable 3–designs presented, together with other series from [4], can be used for a construction of other families of 3–designs; see van Tran [5]. They will be used for further work with Masanori Sawa et al. to construct other families of 3–designs.

References

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

[2] A. Hartman, The existence of resolvable Steiner quadruple systems, *J. Combin. Theory Ser. A* **44** (1987), 182–206.

[3] L. Ji and L. Zhu, Resolvable Steiner quadruple systems for the last 23 orders, *SIAM J. Discrete Math.* **19** (2005), 420–430.

[4] R. Laue, Resolvable t–designs, *Des. Codes Cryptogr.* **32** (2004), 277–301.

[5] T. van Trung, Recursive constructions for 3-designs and resolvable 3-designs, *J. Statist. Plann. Inference* **95** (2001), 341–358.

Finite semifields and linear sets in projective spaces

Michel Lavrauw

Ghent University

In this talk, we will explain the notion of a linear set in a projective space over a finite field, and elaborate on their use in the theory of finite semifields.

References

[1] M. Lavrauw and O. Polverino, Finite semifields, in *Current Research Topics in Galois Geometries*, edited by J. De Beule and L. Storme, Nova Academic Publishers, to appear.

Weil numbers, circulant matrices and Snevily's conjecture

Ka Hin Leung

National University of Singapore

(Joint work with B. Schmidt)

In the study of Weil numbers and circulant matrices, we often need to consider the following interesting situation:

Let G be a cyclic group. There exists a subset $\{x_1, \ldots, x_n\}$ in G such that every difference $x_i - x_j$ can be represented as $x_{i'} - x_{j'}$ with $(i, j) \neq (i', j')$.

For instance, if a circulant weighing matrix D is expressed as the condition that $\sum a_g g \in \mathbb{Z}[G]$ such that all $a_g = 0$ or ± 1, then the support of D satisfies this condition. The same situation also arises when we study the existence of Weil numbers. A Weil number is an algebraic integer z of the form $\sum a_i \zeta^i$, where ζ is an m-th root of unity and $|z\bar{z}| = n$ is an integer. The existence of Weil numbers is related to the problem of the existence of difference sets. While studying Weil numbers, Kedlaya showed the following result.

Theorem 1 *Given a prime p, if there exists a set $X = \{x_1, \ldots, x_n\}$ in G such that every difference $x_i - x_j$ can be represented as $x_{i'} - x_{j'}$ with $(i, j) \neq (i', j')$, then $p \leq \sqrt{6}^n$.*

It follows from this theorem that, if z is Weil number in $\mathbb{Z}[\zeta_p]$ and $|z\bar{z}| = n$, then $p \leq \sqrt{6}^n$. Another immediate application on circulant matrices will be presented by B. Schmidt in another talk. However, in order to obtain more general results, it is not sufficient to consider only the prime case. Also, instead of studying the differences of one set, it might be better to study sums of two sets.

Theorem 2 *Let G be a cyclic group and A, B be subsets of G that contain 0. Suppose for any $a \in A, b \in B$, there exist $a \neq a' \in A, b' \neq b \in B$ such that $a + b = a' + b'$. If $\langle A \rangle = G$ or $\langle B \rangle = G$ and $|G| \geq 2^{|A|+|B|-2}$, then there exist proper subsets $A' \subset A$ and $B' \subset B$ such that, if $a \in A', b \in B'$, $a' \in A, b' \in B$, then $a + b = a' + b'$ implies $a' \in A'$ and $b' \in B'$.*

In this talk, I will mainly discuss how Theorem 2 can be applied to problems on Weil numbers and circulant matrices. For instance, we obtain a similar result on Weil numbers in $\mathbb{Z}[\zeta_{p^r}]$ instead of $\mathbb{Z}[\zeta_p]$. It seems that Theorem 2 can also be applied to get an improved F-bound. As for the case of circulant matrices, a significant improvement on earlier results is obtained. Lastly, Theorem 2 can be applied to solve some special cases of Snevily's Conjecture, a problem in additive number theory.

Almost resolvable 4-cycle systems

Curt Lindner

Auburn University

A 4-cycle system of order n is a pair (X, C), where C is a collection of edge disjoint 4-cycles which partitions the edge set of K_n with vertex set C. It is well-known that the spectrum for 4-cycle systems is precisely the set of all $n \equiv 1 \pmod 8$ and that if (X, C) is a 4-cycle system of order n, $|C| = n(n-1)/8$. An almost parallel class of a 4-cycle system of order n is a collection of $(n-1)/4$ vertex disjoint 4-cycles. An *almost resolvable* 4-cycle system of order n is a partition of C into $(n-1)/2$ almost parallel classes and a half parallel class consisting of $(n-1)/8$ vertex disjoint 4-cycles. One can show using various brute force arguments that an almost resolvable 4-cycle system of order 9 *does not* exist. However, there does exist an almost resolvable 4-cycle systems for all other orders $n \equiv 1 \pmod 8 \geq 17$. The construction is pretty easy; and that's exactly what this talk is all about: a transparently easy construction of almost resolvable 4-cycle systems of every order $n \equiv 1 \pmod 8 \geq 17$.

A generalization of cyclic semifields

Giuseppe Marino

Seconda Università degli Studi di Napoli

Suppose that W is a finite n–dimensional vector space, $n > 1$, over a field F and assume that $T \in GL(W, K)$, where K is a proper subfield of F. If $T \in \Gamma L(W, F) \setminus GL(W, F)$ is F–irreducible, then viewing T and $f \in F$ as elements of $GL(W, K)$, the set

$$\Delta(T, F) = \{\mathbf{1}\alpha_0 + T\alpha_1 + ... + T^{n-1}\alpha_{n-1}); \, \alpha_i \in F, \;\; i = 0, 1, ..., n-1\}$$

is an additive spread set over the field K, and so it yields a semifield which is called *cyclic semifield*. This construction generalizes that of Sandler [5] and is due to Jha and Johnson [1], [2].

In [3], all the cyclic semifields of order q^6 that are of dimension 6 over the associated centers and have right and middle nucleus isomorphic to $\mathbb{F}_{q^2}$ and left nucleus isomorphic to $\mathbb{F}_{q^3}$ have been determined and it has been proven that any semifield of order q^6 with left nucleus isomorphic to $\mathbb{F}_{q^3}$, middle and right nuclei both isomorphic to $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$ is isotopic to a cyclic semifield. In [4], a new construction is given of cyclic semifields of orders q^{2n}, n odd with kernel (left nucleus) $\mathbb{F}_{q^n}$ and right and middle nuclei isomorphic to $\mathbb{F}_{q^2}$, and the isotopism classes are determined. Also, this construction is generalized to produce potentially new semifields of the same general type that are not isotopic to cyclic semifield. In particular, a new semifield plane of order 4^5 and new semifield planes of order 16^5 are constructed by this method.

References

[1] V. Jha and N.L. Johnson, An analog of the Albert–Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem, *Algebras Groups Geom.* **6** (1989), 1–35.

[2] V. Jha and N.L. Johnson, Translation planes of large dimension admitting nonsolvable groups, *J. Geom.* **45** (1992), 87–104.

[3] N.L. Johnson, G. Marino, O. Polverino and R. Trombetti, Semifields of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$, *Finite Fields Appl.* **14** (2008), 456–469.

[4] N.L. Johnson, G. Marino, O. Polverino and R. Trombetti, On a generalization of cyclic semifields, *J. Algebraic Combin.* **26** (2009), 1–34.

[5] R. Sandler, A note on some new finite division ring planes, *Trans. Amer. Math. Soc.* **104** (1962), 528–531.

3-nets embedded in a projective plane

Francesco Mazzocca

Seconda Universitá degli Studi di Napoli

(Joint work with G.Korchmáros and A.Blokhuis)

A 3-*net of order* n is a point-line incidence structure consisting of n^2 points together with three classes of lines each consisting of n lines such that

(i) any two lines from different classes are incident;

(ii) no two lines from the same class are incident;

(iii) any point is incident with exactly one line from each class.

We investigate [1] finite 3-nets embedded in a projective plane over a (finite or infinite) field of any characteristic p. Such an embedding is *regular* when each of the three classes of the 3-net comprises concurrent lines, and *irregular* otherwise. It is *completely irregular* when no class of the 3-net consists of concurrent lines. We are interested in embeddings of 3-nets which are irregular but the lines of one class are concurrent.

For an irregular embedding of a 3-net of order $n \geq 5$ we prove that, if all lines from two classes are tangent to the same irreducible conic, then all lines from the third class are concurrent. We also prove the converse provided that the order n of the 3-net is smaller than p.

In the complex plane, apart from a sporadic example of order $n = 5$ due to Stipins [2], each known irregularly embedded 3-net has the property that all its lines are tangent to a plane cubic curve. Actually, we show that the procedure of constructing irregular 3-nets with this property works over any field. Moreover, in positive characteristic, we present some more examples for $n \geq 5$ and give a complete classification for $n = 4$.

References

[1] A. Blokhuis, G. Korchmáros and F. Mazzocca, 3-nets embedded in a projective plane, 2009, arXiv:0911.4100.

[2] J. Stipins, Old and new examples of k-nets in $\mathbb{P}^2$, arXiv:math/0701046.

Numeration systems

Francesca Merola

Università di Roma Tre

It is known that it is possible to write each natural number as a sum of distinct non-consecutive Fibonacci numbers: in a sense, then, the Fibonacci sequence can be thought as a base for a numeration system. More generally, a linear numeration system uses as a base a sequence obtained from a recurrence relation: to obtain a unique expression for a number in such a numeration system a greedy procedure is normally used. I shall discuss some combinatorial problems that arise in this setting - in particular, a connection between greedy expessions for numbers and words with some forbidden substring - and look at possible applications.

On the affine planes of order 2^{3s} admitting $PSU_3(2^s)$ as a collineation group

Alessandro Montinaro

Università del Salento

(Joint work with M. Biliotti)

Collineation groups of finite projective planes and their geometries have been studied systematically since the beginning of the twentieth century. Special attention is devoted to collineation groups G of a finite projective plane Π that fix a line l and act on it with some transitivity properties. The case when G is 2-transitive on l has been completely solved throughout the years mainly by Cofman, Schulz , Czerwinski, Kallaher, Biliotti and Korchmáros and more recently by Biliotti and Francot [1].

When we consider groups G with some transitivity properties on l, the most natural generalization of 2-transitivity is primitivity and ultimately transitivity. The problem increases in difficulty, but Biliotti and Montinaro [2] provide an essentially complete solution when G is almost simple and, more generally, when G has a faithful and transitive action on l. In particular, when G is an almost simple group, then G is 2-transitive on l and one of the following occurs:

1. $n = 2^s$, $\Pi \cong PG_2(2^s)$, and $Soc(G) \cong PSL_2(2^s)$;

2. $n = 2^{2s}$, s odd, and $Soc(G) \cong Sz(2^s)$;

3. $n = 2^{3s}$, s even, and $Soc(G) \cong PSU_3(2^s)$.

The first two cases do occur, whereas the third is still open. The present talk focuses mainly on the latter case. If the plane exists, it must be the joint embedding of a resolvable 2-$(q\,(q^3 - q^2 + 1)\,, q, 1)$ design $\mathcal{D}_1$ and the dual of a resolvable 2-$(q^2(q^3 + 1), q^2, 1)$ design $\mathcal{D}_2$, both invariant under G. Such resolvable designs do exist independently of the plane Π and none of them is embeddable in $PG_k(q)$.

In particular, we show that, for $q = 4$, the design $\mathcal{D}_1$ admits a unique hyperresolution that is compatible with the tactical decomposition of Π. Hence, a new partial geometry $pg(12740, 48, 60, 45)$ is obtained. Since the hyperresolution yields only *non-linear* ovoids in the partial geometry, then the plane Π does not exist for $q = 4$.

References

[1] M. Biliotti and E. Francot, Two-transitive orbits in finite projective planes, *J. Geom.* **82** (2005), 1–24.

[2] M. Biliotti and A. Montinaro, Affine planes admitting a collineation group with a transitive action on the line at infinity, *J. Algebra*, to appear.

On the distribution of elements of a finite group generated by random covers

Nicola Pace

Florida Atlantic University

Random covers for finite groups were introduced by Magliveras et al. in [3] and used for designing public key cryptosystems. In a recent paper [1], Klingler et al. define a multiset $\mathcal{S}_k$, which can be considered as a particular type of random cover, and formulate a generalization of the traditional discrete logarithm problem from cyclic to arbitrary finite groups. In this talk, we consider a more general type of random cover and extend a result, proved in [1], on the distribution of elements generated by random covers. We consider the particular instance analyzed in [1] for the groups $\mathrm{PSL}(2, \mathrm{p})$. For the case where α and β are two non-commuting generators of order p, we provide a closed-form formula for the multiplicities of elements of $\mathrm{PSL}(2, \mathrm{p})$ in $\mathcal{S}_k(\alpha, \beta)$ and consequently a best possible estimation for the distribution of group elements in $\mathcal{S}_k(\alpha, \beta)$.

References

[1] L.C. Klingler, S.S. Magliveras, F. Richman and M. Sramka, Discrete logarithms for finite groups, *Computing* **85** (2009), 3–19.

[2] W. Lempken, S.S. Magliveras, Tran van Trung and W. Wei, A public key cryptosystem based on non-abelian finite groups, *J. Cryptol.* **22** (2009), 62–74.

[3] S.S. Magliveras, D.R. Stinson and Tran van Trung, New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups, *J. Cryptol.* **15** (2002), 285–297.

Finite self-dual generalized quadrangles

Stanley Payne

University of Colorado Denver

(Joint work with J. A. Thas)

Let $\mathcal{S}$ be a finite self-dual generalized quadrangle (GQ) of order s. We start by collecting the known results for such GQ and examining them for the known examples. Among the known finite GQ a self-dual $\mathcal{S}$ must be of the form $T_2(\mathcal{O})$ (first constructed by J. Tits) where $\mathcal{O}$ is a translation oval. A problem of central interest is to determine the number of absolute points of a duality. One curious consequence of a theorem in the recent Ph.D. thesis of B. Temmermans [1] is the following: if $\mathcal{O}$ is a translation oval in $PG(2,q)$ where $q = 2^e$, $e \equiv 2 \pmod 4$, and if θ is a certain one of the known dualities of $T_2(\mathcal{O})$, then θ must have exactly $1 + q$ absolute points. This example leads to the following result.

Theorem *Let $q = 2^e$ where $e \equiv 2 \ (mod\ 4)$. Let α be an automorphism that generates the Galois group of the of the Galois field F_q. Then there must be exactly $q/2$ values of $x \in F_q$ for which the absolute trace of $x(x + x^\alpha)$ is zero.*

There is something special about the case $e \equiv 2 \pmod 4$, since this result fails in general, in particular when $q = 16$, where the number of such field elements x (with $\alpha = 2$) is $12 > 16/2$.

References

[1] B. Temmermans, *Dualities and Collineations of Projective and Polar Spaces and of Related Geometries*, Ph.D. Thesis, Ghent University, 2010.

Embedding the Hermitian unital in a 7–dimensional projective space

Valentina Pepe

University of Ghent

(Joint work with H. Van Maldeghem)

Let $\mathcal{U}$ be a Hermitian unital of $PG(2, \mathbb{L})$, where $\mathbb{L}$ is the quadratic Galois extension of the field $\mathbb{K}$, and consider it as a point–block geometry, where the blocks are the Baer sublines contained in the unital. The Veronesean embedding α of the linear space $\mathcal{U}$ in $PG(7, \mathbb{K})$ is such that the image of a block is a conic of a plane of $PG(7, \mathbb{K})$ and $\mathcal{U}^\alpha$ is a suitable hyperplane section of the Hermitian Veronesean of $PG(2, \mathbb{L})$; for more details about this embedding, see [1].

Given an embedding $\alpha : \mathcal{U} \longrightarrow PG(7, \mathbb{F})$, with $\mathbb{F}$ any field, such that the image of a block is a point–set generating a plane of $PG(7, \mathbb{F})$, we investigate under which conditions α turns out to be the Veronesean embedding of $\mathcal{U}$, and hence $\mathbb{K}$ is isomorphic to a subfield of $\mathbb{F}$.

References

[1] A. De Wispelaere, J. Huizinga and H. Van Maldeghem, Veronesean embeddings of Hermitian unitals, *European J. Combin.*, to appear.

Basic pregeometries

Cheryl Praeger

University of Western Australia

(Joint work with Michael Giudici and Geoffrey Pearce)

I will report on a study of finite pregeometries $\Gamma = (X, *, t)$ with connected rank 2 truncations and admitting a group G of automorphisms transitive on the set X_i of elements of X of each given type i.

Considering two different notions of degeneracy led, via a combination of quotient reduction, decomposition and application of a certain generic construction, to two families of basic pregeometries in this family such that each pregeometry is associated with at least one basic pregeometry. The basic pregeometries involve either faithful primitive actions on each X_i, or faithful and quaisprimitive actions on the X_i, respectively.

Analysing the basic pregeometries admitting each kind of primitive or quasiprimitive permutation group, according to the O'Nan-Scott categories of such groups, led to constructions of basic pregeometries (which are in fact thick geometries) of arbitrarily large rank for all but one kind of primitive group. The question of bounding the rank remains open for that kind of group - essentially a product of two isomorphic simple groups.

References

[1] M. Giudici, C. E. Praeger and G. Pearce, Basic pregeometries and degeneracy, in preparation.

Finiteness of circulant weighing matrices of fixed weight

Bernhard Schmidt

Nanyang Technological University, Singapore

(Joint work with Ka Hin Leung)

A *circulant weighing matrix* is a circulant matrix A with entries $-1, 0, 1$ such that $AA^T = nI$. The integer n is called the *weight* of the matrix. We show that, for fixed n, there are essentially only finitely many circulant weighing matrices of weight n. More precisely, all such matrices arise from a finite set of objects which we call *irreducible orthogonal families of weight* n.

Explorations of optical orthogonal and quasi-cyclic codes from a combinatorial design perspective

Dimitris E. Simos

National Technical University of Athens

(Joint work with Christos Koukouvinos)

Optical orthogonal codes (OOC) and quasi-cyclic (QC) codes are of great importance in the field of coding theory. The notion of OOCs was first conceived by Salehi [2], in order to model the ability of a fiber optic channel to be shared simultaneously by multiple users without interference. Combinatorial design theory plays an important role in the construction of OOCs; difference families over cyclic groups construct OOCs, cyclic difference sets give sequences with low autocorrelation and recursive constructions of optimal OOCs have emerged from regular cyclic packings. In addition to wide-band multiple access system, OOCs also find applications in mobile radio, spread-sprectrum communications and radar signal.

QC codes form an important class of linear codes, which contains the well-known class of cyclic codes. These codes are a natural generalization of the cyclic codes. Many of the best known block codes, including the Reed–Muller codes and the $[24, 12]$ Golay code, are quasi-cyclic. Furthermore, it has been shown that the minimum distance of QC codes meets a modified version of the Gilbert–Varshamov bound [1].

We give an overview of these constructions for OOCs and QC codes from a combinatorial design point of view. We enrich the available methodologies for the design of OOCs by presenting a new formalism for the properties of an OOC using traditional tools of computer algebra and symbolic computation. Moreover, a connection between cyclic-structured designs and QC codes is given and the possible interaction between OOC and QC codes is explored.

References

[1] T. Kasami, A Gilbert–Varshamov bound for quasi-cyclic codes of rate 1/2, *IEEE Trans. Inform. Theory* **20** (1974), 679.

[2] J.A. Salehi, Code division multiple-access techniques in optical fiber networks-Part I: Fundamental principles, *IEEE Trans. Commun.* **37** (1989), 824–833.

k-arcs and 2-level sharing schemes

Angelo Sonnino

Università della Basilicata

(Joint work with G. Korchmáros and V. Lanzone)

Motivated by applications to 2-level secret sharing schemes, we investigate k-arcs contained in a $(q+1)$-arc Γ of $\mathrm{PG}(3,q)$, q even, which have only a small number of focuses on a real axis of Γ. Doing so, we also investigate hyperfocused and sharply focused arcs contained in a translation oval of $\mathrm{PG}(2,q)$.

Message authentication in the presence of key-dependent messages

Rainer Steinwandt

Florida Atlantic University

(Joint work with M. González Muñiz)

Standard notions for defining the security of encryption, signature, or message authentication schemes, such as IND-CCA or EUF-CMA, do not consider scenarios where (plaintext) messages depend on secret key material. Such scenarios are of interest in connection with hard disk encryption, for instance, or when side channel information is to be taken into account. Over the last years, significant progress has been made in understanding key-dependent encryption, and also results for key-dependent signing and signcryption are available by now.

This talk discusses the security of message authentication codes (MACs) in a scenario where an adversary has access to a tag generation oracle that accepts efficiently computable functions of the secret key as input. This enables the modelling of, for example, the computation of a tag for a hard disk backup with the MAC key being stored on the hard disk itself. In combination with a verification oracle, such an "enhanced" tag generation oracle turns out to be a powerful tool for an adversary; existential unforgeability is impossible to achieve for any stateless scheme, even in the random oracle model.

The talk presents, in the random oracle model, a (stateful) message authentication code that achieves existential unforgeability in the above scenario.

Multicollision attacks on iterated hash functions

Douglas Stinson

University of Waterloo

(Joint work with M. Nandi and J. Upadhyay)

Let $h : X \to Y$ be a hash function. An *s-multicollision* is a set of s distinct elements $x_1, \ldots, x_s \in X$ such that $h(x_1) = \cdots = h(x_s)$. When $s = 2$ this is just termed a *collision*.

In 2004, Joux discovered a method of constructing 2^r-multicollisions for iterated hash functions that is substantially faster than an exhaustive search. Subsequently, some generalizations of Joux's attacks were presented by Nandi and Stinson, as well as by Hoch and Shamir.

A different kind of multicollision attack, called a *herding attack*, was proposed by Kelsey and Kohno in 2006. This attack is based on a so-called *diamond structure*. A recent analysis of the complexity of constructing diamond structures was given by Stinson and Upadhyay, in which the problem is modelled using random graph theory.

In this talk, we survey the attacks mentioned above. In particular, we point out some interesting applications of combinatorial techniques in the design and analysis of these attacks.

References

[1] M. Nandi and D.R. Stinson. Multicollision attacks on some generalized sequential hash functions. *IEEE Trans. Inform. Theory* **53** (2007), 759–767.

[2] D.R. Stinson and J. Upadhyay, On the complexity of the herding attack and some related attacks on hash functions, preprint.

Attribute-based group key establishment

Adriana Suárez Corona

University of Oviedo

(joint work with R. Steinwandt)

We propose a formalization of *attribute-based group key establishment*, a cryptographic primitive enabling parties to establish a common session key based on the possession of certain attributes. In addition to a security model, a two-round protocol providing the desired security guarantees is presented. As main technical tool, we introduce a notion of *attribute-based signcryption*, which may be of independent interest. A corresponding security model is presented, and we show that secure attribute-based signcryption can be obtained by means of the *encrypt-then-sign* paradigm.

The security proof of the two-round key establishment presented is in the random oracle model and relies on the Computational Diffie–Hellman assumption and the security of the underlying attribute-based signcryption scheme. We also address additional properties of the proposed protocol, such as deniability and privacy.

Public key cryptosystem MST_3: cryptanalysis and realization

Tran van Trung [1] **and Pavol Svaba** [2]

Universität Duisburg-Essen

The public key cryptosystem MST_3 has been developed on the basis of group factorization by using logarithmic signatures (LS) and random covers [1]. LS are the basis for the public key cryptosystem MST_1 and random covers for the public key cryptosystem MST_2. In [1] lower bounds for the work effort required to launch a direct attack and a chosen plaintext attack against MST_3 have been determined. By exploiting the characteristic of the multiplication in the Suzuki 2-groups, a further analysis [2] provides a stronger result which shows, in particular, that the class of "transversal LS" are unfit to use for a realization of MST_3.

The aim of this talk is to present a strengthened version of MST_3, its cryptanalysis and its realization [3]. We first show a method how to improve the generic scheme MST_3 on the basis of Suzuki 2-groups. We then present our results of a thorough cryptanalysis of the new improved scheme. More precisely, using heuristic and algebraic methods we establish lower bounds for the workload of conceivable direct attacks on the private keys. We further develop a powerful chosen plaintext attack which allows us to rule out the usage of a certain class of LS. Consequently, classes of LS withstanding this attack can be identified and thus to our knowledge they could be used in the realization of the scheme. Finally, we describe and discuss the implementation issues of the scheme and show data of its performance obtained from an experimental result.

References

[1] W. Lempken, S.S. Magliveras, Tran van Trung and W. Wei, A public key cryptosystem based on non-abelian finite groups, *J. Cryptology* **22** (2009), 62–74.

[2] S.S. Magliveras, P. Svaba, Tran van Trung and P. Zajac, On the security of a realization of cryptosystem MST_3, *Tatra Mt. Math. Publ.* **41** (2008), 1–13.

[3] P. Svaba and Tran van Trung, Public key cryptosystem MST_3: cryptanalysis and realization, Preprint No. 2 (2010), IEM.

[1] first speaker

[2] second speaker

$\mathbb{F}_q$–pseudoreguli of $\mathrm{PG}(3, q^3)$

Rocco Trombetti

Universitá degli Studi di Napoli Federico II

In [1], J.W. Freeman introduced certain partial spreads of $\mathrm{PG}(3, q^2)$ called *pseudoreguli*. These arise from regular spreads of a canonical subgeometry $\mathrm{PG}(3, q)$ of $\mathrm{PG}(3, q^2)$. Pseudoreguli are of interest because, when q is odd, they are related to the derivation set of a class of translation planes of order q^4.

In [2], the authors constructed an analog in $\mathbb{P} = \mathrm{PG}(3, q^3)$ of a pseudoregulus by projecting a Desarguesian 2–spread of a 5–dimensional projective space $\mathrm{PG}(5, q)$ embedded in $\mathrm{PG}(5, q^3)$ as a canonical subgeometry; this analog is a $\mathbb{F}_q$–*pseudoregulus* of $\mathbb{P}$. Also, there is a connection between $\mathbb{F}_q$–pseudoreguli of $\mathbb{P}$ and some rank–2 semifields of order q^6 with center $\mathbb{F}_q$. The relevant semifields are called semifields of *scattered type*.

So far, the known examples of semifields of scattered type are some Knuth semifields and some generalized twisted fields. In [2], Knuth semifields and generalized twisted fields of order q^6, two-dimensional over their left nucleus and with center $\mathbb{F}_q$, are characterized in terms of the associated $\mathbb{F}_q$–pseudoreguli. In this talk, starting from an $\mathbb{F}_q$–pseudoregulus of $\mathbb{P}$ and exploiting this connection, we derive, up to the isotopy relation, the multiplication rule of some rank–2 semifields of scattered type. We present several computer-generated examples of new such semifields. Finally, we are able to generalize some of these to an infinite family, which turns out to be a new infinite family of scattered semifields.

References

[1] J.W. Freeman, Reguli and pseudoreguli in PG(3, s^2), *Geom. Dedicata* **9** (1980), 267–280.

[2] G. Marino, O. Polverino and R. Trombetti, On $\mathbb{F}_q$-linear sets of $\mathrm{PG}(3, q^3)$ and semifields, *J. Combin. Theory Ser. A* **114** (2007), 769–788.

On the linearity of higher-dimensional blocking sets

Geertrui Van de Voorde

Ghent University

A *small minimal k-blocking set* B in $\mathrm{PG}(n,q)$ is a set of points of cardinality less than $3(q^k+1)/2$, intersecting every $(n-k)$-space, such that no proper subspace of B has this property. *Linear sets*, introduced by Lunardon [2], gave rise to the first examples of small minimal blocking sets that were not of Rédei type [3], disproving the wide-spread belief that all small minimal blocking sets were of Rédei type. This construction led to the *linearity conjecture* for blocking sets, stating that every small minimal k-blocking set is linear; see [4].

In this talk, we show that if the linearity conjecture holds for blocking sets in the plane, that is, for 1-blocking sets in $\mathrm{PG}(2,q)$, then it also holds for k-blocking sets in $\mathrm{PG}(n,p^h)$, where p is relatively large with respect to h. We will explain how this bound on p arises by relating the problem to the intersection problem for a subline and a linear set, which was solved in [1].

This result shows that, to prove the linearity conjecture for k-blocking sets in $\mathrm{PG}(n,q)$ for large q, it is sufficient to deal with the planar case.

References

[1] M. Lavrauw and G. Van de Voorde, On linear sets on a projective line, *Des. Codes Cryptogr.*, to appear.

[2] G. Lunardon, Normal spreads, *Geom. Dedicata* **75** (1999), 245–261.

[3] P. Polito and O. Polverino, On small blocking sets, *Combinatorica* **18** (1998), 133–137.

[4] P. Sziklai, On small blocking sets and their linearity. *J. Combin. Theory Ser. A* **115** (2008), 1167–1182.

Mutually disjoint designs and new 5-designs derived from groups and codes

Alfred Wassermann

University of Bayreuth

(Joint work with Makoto Araya, Masaaki Harada, and Vladimir D. Tonchev)

Constructions of disjoint 5-designs obtained from permutation groups and extremal self-dual codes are presented. Several new simple 5-designs are found with parameters that were left open in the table of 5-designs given in [3], namely, 5-(v, k, λ) designs with

$$\begin{aligned}
(v, k, \lambda) &= (18, 8, 2m), \quad m = 6, 9; \\
&= (19, 9, 7m), \quad m = 6, 9; \\
&= (24, 9, 6m), \quad m = 3, 4, 5; \\
&= (25, 9, 30); \\
&= (25, 10, 24m), \quad m = 4, 5; \\
&= (26, 10, 126); \\
&= (30, 12, 440); \\
&= (32, 6, 3m), \quad m = 2, 3, 4; \\
&= (33, 7, 84); \\
&= (36, 12, 45n), \quad 2 \leq n \leq 17.
\end{aligned}$$

These results imply that a simple 5-(v, k, λ) design with $(v, k) = (24, 9)$, $(25, 9)$, $(26, 10)$, $(32, 6)$, or $(33, 7)$ exists for all admissible values of λ. The computations were done using DISCRETA [1] and MAGMA [2].

References

[1] A. Betten, E. Haberberger, R. Laue and A. Wasserman, DISCRETA - a program to construct t-designs with prescribed automorphism group, Lehrstuhl II für Mathematik, Universität Bayreuth, Available online at `http://www.mathe2.uni-bayreuth.de/discreta/`

[2] W. Bosma and J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, Available online at `http://magma.maths.usyd.edu.au/magma/`.

[3] G.B. Khosrovshahi and R. Laue, t-Designs with $t \geq 3$, in *Handbook of Combinatorial Designs*, (2nd edition), C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2007, 79–101.

Characterizing small weight codewords of the linear code of PG$(2, q)$

Zsuzsa Weiner

Prezi.com

(Joint work with András Gács and Tamás Szőnyi)

For $q = p^h$, where p is a prime, let $C_1(2, q)$ be the p-ary linear code defined by the lines of PG$(2, q)$, that is, the linear combination of lines of PG$(2, q)$ over the finite field GF(p) with p elements. In this talk, we show that a codeword c with weight $w(c)$ less than $\lfloor\sqrt{q}\rfloor\, q + 1 + (q - \lfloor\sqrt{q}\rfloor^2)$ is "trivial"; that is, it is the linear combination of $\lceil \frac{w(c)}{q+1} \rceil$ lines, when q is large and $h > 2$. For the case $h = 1, 2$, we have partial results only. Blokhuis, Brouwer and Wilbrink [1] showed that the classical unital is a codeword and so it must be the linear combination of at least $q - \sqrt{q}$ lines, which shows that the above result is sharp when q is a square. This characterization yields that the weight of such codewords can only take certain values $(q + 1, 2q, 2q + 1, \dots)$ and there are many relatively-large, empty intervals. When q is even, this is in an earlier result with Szőnyi [3] in a different context, that is, the stability of sets of even type. A minor alteration of that proof yields the general case. It was shown earlier by Lavrauw, Storme, Sziklai and Van de Voorde that the weights of $C_1(2, q)$ cannot lie in the interval $q + 1 < w(c) < 2q$. They also extended this result to codes generated by the k-dimensional subspaces of PG(n, q); see [2].

References

[1] A. Blokhuis, A. Brouwer and H. Wilbrink, Hermitian unitals are code words, *Discrete Math.* **97** (1991), 63–68.

[2] M. Lavrauw, L. Storme, P. Sziklai and G. Van de Voorde, An empty interval in the spectrum of small weight codewords in the code from points and k-subspaces of PG(n, q), *J. Combin. Theory, Ser. A*, to appear.

[3] T. Szőnyi and Zs. Weiner, On stability results in finite geometry, http://www.cs.elte.hu/∼weiner/stab.pdf.