Colloquium on Galois Geometry

Friday, December 2, 2011

Abstracts

Kramer-Mesner with Tactical Decomposition

Anamari Nakic

University of Zagreb

(Joint work with Mario-Osvin Pavcevic and Vedran Krcadinac)

A t-(v, k, λ) design is a finite incidence structure consisting of v points and a number of blocks (sets of points), such that each block contains exactly k points and every set of t distinct points is contained in exactly λ blocks. Although there are many known examples of t-designs, finite projective planes being one of them, for many parameters the question of existence remains open. In order to construct new t-(v, k, λ) designs, it is practically impossible to complete an exhaustive search because the problem is of exponential complexity. It is necessary to add constraints to the search.

We shall present a new approach in construction of t-(v, k, λ) designs. In the last few years, my supervisor Mario-Osvin Pavcevic and Vedran Krcadinac successfully combined the well known Kramer-Mesner method and tactical decomposition and *indexing* approach in order to construct new t-(v, k, λ) designs admitting an action of an automorphism group. In the past, tactical decomposition and *indexing* have been used for sporadic constructions of 2-designs. On the other hand, the Kramer-Mesner algorithm was broadly used for the construction of t-designs. It is now clear that information provided by tactical decomposition matrices can enhance the Kramer-Mesner method. This new combination of two approaches can in many cases dramatically reduce the size of the Kramer-Mesner matrix and therefore t-designs can be constructed faster and more easily. Moreover, this new method can also be used to construct other combinatorial structures with weaker properties, like symmetric configurations. We shall present an outline of this new technique as well as some new results for t-designs.

Anamari Nakic, University of Zagreb, Faculty of Electrical Engineering and Computing, Department of Applied Mathematics, Unska 3, 10000 Zagreb, Croatia
anamari.nakic@fer.hr

Exploring new directions

Marcella Takáts

Eötvös Loránd University, Budapest

(Joint work with Szabolcs Levente Fancsali and Péter Sziklai)

Let U be a point set in the n-dimensional affine space $\mathrm{AG}(n, q)$ over the finite field of q elements. We say a direction d (i.e. a point in the hyperplane at infinity H_∞) is determined by U if there is a line with the ideal point d containing at least two points of U. Let D be the set of directions determined by U. If $|U| > q^{n-1}$ then it is clear from the pigeon hole principle that all the directions are determined. The most studied case is the extremal case when $|U| = q^{n-1}$.

First we give a summary of the history and the most important results of the direction problem in the plane. Rédei and Megyesi proved that in $\mathrm{AG}(2, p)$, p prime, if $|U| = p$, then U determines at least $\frac{p+3}{2}$ directions. Blokhuis, Ball, Brouwer, Storme and Szőnyi (BBBSz) completely characterized the case when $U \subset \mathrm{AG}(2, q)$, $|U| = q$, $q = p^h$. Let $s = p^e$ be the largest power of p such that each secant meets U in a multiple of s points. They proved that then one of the following holds:

(i) $s = 1$ *and* $\frac{q+3}{2} \leq |D| \leq q + 1$;
(ii) $\mathrm{GF}(s)$ *is a subfield of* $\mathrm{GF}(q)$ *and* $\frac{q}{s} + 1 \leq |D| \leq \frac{q-1}{s-1}$;
(iii) $s = q$ *and* $|D| = 1$.

Moreover, if $s \geq 3$ *then* U *is* $\mathrm{GF}(s)$*-linear.*

Tamás Szőnyi proved that in $\mathrm{AG}(2, p)$, if $|U| = k < p$, then U determines at least $\frac{k+3}{2}$ directions, and he also proved a stability theorem if $|U| = q - \varepsilon$.

In the second part of the talk we examine directions determined by less then q points. Trying to find an analogue with the theorem of BBBSSz lead us to describe the possible number of determined directions. We give an outline of affine and projective linear sets, and consider projective linear sets as direction sets. Then we sketch the method using the Rédei-polynomial of U, where $t = p^h$ is a well defined parameter. We prove the following theorem:

THEOREM. **(Fancsali, Sziklai, T.)** *Let* $k \leq q$, $U \subset \mathrm{AG}(2, q)$ *be a point set,* $|U| = k$. *Let* D *be the set of directions determined by* U. *Then one of the following holds:*
(i) $s = 1$ *and* $\frac{k+3}{2} \leq |D| \leq q + 1$;
(ii) $|D| > 1$ *and* $\frac{k-1}{t+1} + 2 \leq |D| \leq \frac{k-1}{s-1}$ *and* $s \leq t < q$;

(iii) $|D| = 1$ *and* $s \leq t = q$.

In the third part of the talk we extend the definition of determining directions to determining subspaces at infinity.

Definition *Let* $U \subset \mathrm{AG}(n, q) \subset \mathrm{PG}(n, q)$*, and* k *be a fixed integer,* $0 \leq k \leq n-2$*. We say a subspace* S_k *of dimension* k *in* H_∞ is determined *by* U *if there is an affine subspace* T_{k+1} *of dimension* $k+1$*, having* S_k *as its hyperplane at infinity, containing at least* $k+2$ *affinely independent points of* U *(i.e. spanning* T_{k+1}*).*

If $|U| > q^{n-1}$ then it is clear again that all the k-subspaces of H_∞ are determined. We examine the extremal case $|U| = q^{n-1}$. We show a hierarchy of the determined subspaces of a given point set. On the other hand, we classify point sets *not* determining every k-subspace in certain cases. For 3 dimensions and $k = 1$, i.e. determining lines, the following theorem holds.

THEOREM. **(Sziklai, T.)** *Let* $U \subset \mathrm{AG}(3,q) \subset \mathrm{PG}(3,q)$*,* $|U| = q^2$*. Let* N *be the set of lines in* H_∞ *non-determined by* U*. Then one of the following holds:*

1. $|N| = 0$*, i.e.* U *determines all the lines of* H_∞*;*
2. $|N| = 1$ *and then there is a parallel class of affine planes such that* U *contains one "arbitrary" complete line in each of its planes;*
3. $|N| = 2$ *and then* U *together with the two undetermined lines in* H_∞ *form a hyperbolic quadric or* U *contains* q *parallel lines;*
4. $|N| \geq 3$ *and then* U *contains* q *parallel lines (*U *is a cylinder).*

References

[1] SZ. L. FANCSALI, P. SZIKLAI, M. TAKÁTS, *The number of directions determined by less than* q *points.* submitted.

[2] P. SZIKLAI, M. TAKÁTS, *An extension of the direction problem.* submitted.

Marcella Takáts, Eötvös Loránd University, 1117 Budapest, Pázmány P. s. 1/c, Hungary
takats@cs.elte.hu

Subspaces of matrices with restricted rank

John Sheekey

University College Dublin

(Joint work with Rod Gow and Jean-Guillaume Dumas)

Subspaces of matrices, in which the rank of the contained non-zero elements is restricted in some way, have many applications in coding theory and geometry.

A subspace of $M_n(\mathbb{F}_q)$ defines a “rank metric code”: a linear code whose elements are matrices, where the weight of a codeword is taken to be the rank of the matrix. A subspace of symmetric or hermitian matrices defines a code in another way; via their connection with quadratic and hermitian forms. The weight function for these codes is the hamming weight, and the weight of a codeword is a function of the rank of the corresponding matrix.

Constant rank subspaces have connections to finite geometry. An n-dimensional constant rank n subspace of $M_n(\mathbb{F}_q)$ defines a *semifield*, and vice-versa. Such a subspace may be used to find a *spread* in $\mathbb{F}_q^{2n}$, and large constant rank subspaces can lead to similar geometric structures.

In this talk we discuss the general problem of finding large subspaces of matrices with restricted rank, with particular focus on constant rank subspaces of symmetric and hermitian matrices. These subspaces have connections to contant weight or two-weight codes. We present new sharp upper bounds for constant rank subspaces of hermitian matrices, and constant odd rank subspaces of symmetric matrices.

John Sheekey, University College Dublin, Belfield, Dublin, Ireland
johnsheekey@gmail.com

The numerical semigroup of combinatorial configurations

Klara Stokes

Universitat Rovira i Virgili, Tarragona, Spain

(Joint work with Maria Bras-Amorós)

A combinatorial (r, k)-configuration is an incidence structure such that there are r lines through any point, k points on any line and through any pair of points there is at most one line or, equivalently, any pair of lines meet in at most one point. Combinatorial configurations are also called partial linear spaces.

A numerical semigroup is a subset S of the natural numbers $\mathbb{N} \cup \{0\}$, such that S is closed under addition, the 0 is in S and the complement $(\mathbb{N} \cup \{0\}) \setminus S$ is finite. For example, the set of all sums whose terms are either multiples of 3 or multiples of 4 forms a numerical semigroup.

Fixing r and k we can prove that the set of parameters for which there exist combinatorial (r, k)-configurations forms a numerical semigroup. From this result we can deduce corollaries on the existence of combinatorial configurations. In particular, the existence of a conductor for a numerical semigroup implies that there is a number N such that there always exists a combinatorial configuration of size n for n greater than N, assuming that the necessary conditions for existence are satisfied.

A triangle in a combinatorial configuration is a set of three distinct points p_1, p_2, p_3 and three distinct blocks l_1, l_2, l_3, such that there is the incidence relation $p_1 l_1 p_2 l_2 p_3 l_3 p_1$. We restrict to consider the set of parameters for which there exist combinatorial configurations without triangles. We can prove that also this set forms a numerical semigroup. Also in this case we get interesting corollaries, now on the existence of triangle-free combinatorial configurations.

Finally, I will describe an application of combinatorial configurations to a protocol that preserves the privacy of the users of search engines.

Klara Stokes, Universitat Rovira i Virgili, Departament d'enginyeria informàtica i matemàtiques, Av. Països Catalans, 26, Campus Sescelades, 43007 Tarragona, Spain
klara.stokes@urv.cat

On geometry and distance-regular graphs

Frédéric Vanhove

Ghent University

A finite, connected graph Γ with diameter d, without loops or multiple edges, is said to be *distance-regular* if for any two vertices x and y at distance k in Γ, the number of vertices z at distance i from x and at distance j from y is a constant p^k_{ij}, only depending on k, i and j (see [2]). Many concepts and results in the theory of such graphs rely heavily on the eigenvalues and eigenspaces of the adjacency matrices. Very well known examples include the Johnson graphs $J(n, d)$ (from design theory), the Hamming graphs $H(d, q)$ (from coding theory) and the Grassmann graphs $J_q(n, d)$ (from projective geometry). In general, many distance-regular graphs are linked in some way to (Galois) geometries.

A *code* in a distance-regular graph is simply a non-empty subset of vertices. One often wants properties of codes under certain restrictions, regarding their size or regularity in some way. A general theory developed for distance-regular graphs, including Delsarte theory [3], sometimes turns out to be very useful here.

Another very broad project aims to classify all distance-regular graphs with certain properties (of the eigenvalues, eigenspaces, diameter,...). Bannai and Ito [1] proposed the problem of classifying all distance-regular graphs with the *Q-polynomial* property, roughly speaking with a “meaningful” ordering of the eigenspaces.

The goal of this talk is to consider the interaction between these concepts, to mention a few old and a few new results, and to discuss some important problems still to be solved.

References

[1] E. Bannai and T. Ito, *Algebraic combinatorics I: Association schemes*, Benjamin/ Cummings, Menlo Park, CA, 1984.

[2] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-regular graphs*, Springer-Verlag, Berlin, 1989.

[3] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res Rep Suppl 10 (1973), 1–97.

Frédéric Vanhove, Ghent University, Department of Mathematics, Krijgslaan 281-S22, 9000 Ghent, Belgium
fvanhove@cage.ugent.be URL: `http://cage.ugent.be/~fvanhove/`

Additive Combinatorics in vector spaces over large finite fields

Jan-Christoph Schlage-Puchta

Universiteit Gent

(Partly joint work with G. Bhowmik, I. Halupczok, and W. Schmid)

Additive combinatorics studies the behaviour of sets of elements in an algebraic structure with respect to the algebraic operations. Typical questions are "Given sets A, B, what can one say about $\{a + b : a \in A, b \in B\}$?", or "Which conditions on a set A imply that there exists a subset B, such that $\sum_{b \in B} b = 0$?". In this talk I will describe a method to translate such questions into problems in combinatorial geometry, and give some results obtained by this approach.

Jan-Christoph Schlage-Puchta, Ghent University, Department of Mathematics,
Krijgslaan 281-S22, 9000 Ghent, Belgium
jcsp@cage.ugent.be