Colloquium on Galois Geometry

October 26, 2012

Abstracts

On rank 2 semifields of order q^6

Giuseppe Marino

Seconda Università degli Studi di Napoli, Caserta

A *semifield* is a binary algebraic structure satisfying all the axioms for a skewfield except (possibly) the associativity of multiplication. Semifields coordinatize certain translation planes (*semifield planes*) which are planes of Lenz–Barlotti class V.

A *rank 2 semifield* is a semifield 2–dimensional over at least one of its nuclei. Rank 2 semifields correspond to semifield spreads of 3–dimensional projective spaces.

L.E. Dickson in 1906 proved that all 2–dimensional semifields are fields [4]. More later, D. Knuth has shown that if two nuclei of a semifield coincide and the semifield is 2–dimensional over them, then is a Knuth semifield of type II, III or IV (see [5]). In 1977, G. Menichetti classified all 3–dimensional finite semifields proving that a semifield of order q^3, with center containing $\mathbb{F}_q$, either is a field or a Generalized Twisted Field ([7]). Later on, the same author in [8] generalized the previous result proving that a semifield of order p^n, n prime and p "large enough", is a field or a Generalized Twisted Field. Another result going in the same direction has been obtained for rank 2 commutative semifields, i.e. commutative semifields of dimension at most 2 over their middle nucleus ([3], [1], [6]). More recently, using the geometric approach of linear sets, all rank 2 semifields of order q^4 with center $\mathbb{F}_q$ have been classified ([2]).

In this conference I will give an overview on some recent classification results related to semifields 6–dimensional over the center $\mathbb{F}_q$, having at least one nucleus of order q^3 and at least one of the remaining nuclei of order q^2.

References

[1] A. Blokhuis, M. Lavrauw, and S. Ball, *On the classification of semifield flocks*, Adv. Math., 180 (2003), pp. 104–111.

[2] I. Cardinali, O. Polverino, and R. Trombetti, *Semifield planes of order q^4 with kernel F_{q^2} and center F_q*, European J. Combin., 27 (2006), pp. 940–961.

[3] S. D. Cohen and M. J. Ganley, *Commutative semifields, two-dimensional over their middle nuclei*, J. Algebra, 75 (1982), pp. 373–385.

[4] L. E. DICKSON, *On commutative linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc., 7 (1906), pp. 514–522.

[5] D. E. KNUTH, *Finite semifields and projective planes*, J. Algebra, 2 (1965), pp. 182–217.

[6] M. LAVRAUW, *Sublines of prime order contained in the set of internal points of a conic*, Des. Codes Cryptogr., 38 (2006), pp. 113–123.

[7] G. MENICHETTI, *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field*, J. Algebra, 47 (1977), pp. 400–410.

[8] ——, *n-dimensional algebras over a field with a cyclic extension of degree n*, Geom. Dedicata, 63 (1996), pp. 69–94.

Seconda Università degli Studi di Napoli, Dipartimento di Matematica
Via Vivaldi 43, 81100 Caserta
Italy

giuseppe.marino@unina2.it

Improvements of the Kramer-Mesner method for t-design constructions

Mario Osvin Pavčević

University of Zagreb, Croatia

(Joint work with Vedran Krčadinac and Anamari Nakić)

Two constructive methods have shown to be effective in explicit t-design constructions in the last 20 years, both allowing the additional assumption of an automorphism group action. We shall give a brief historic overview.

The Kramer-Mesner method, excellently implemented and successfully used for $t > 2$ by the mathematicians from the University of Bayreuth, uses a matrix which counts incidences between t-subset orbits of points and k-subset orbits of points. The other method makes use of tactical decompositions, formed by the point and block orbits of a design, which are matrices counting incidences between these two kind of orbits. Since the existence of such a tactical decomposition is necessary in case that a design exists, one may start by computing all possibilities for such matrices and then try to blow them up to full incidence matrices of t-designs. In such a way, many 2-designs were constructed, even with large parameter triples, the last unknown being 2-$(105, 40, 15)$, constructed by Z. Janko.

Our intention was to combine these two methods. To be able to do that, equations for tactical decomposition coefficients had to be computed for t-designs for $t > 2$. The combined method makes use of the generality of the Kramer-Mesner attempt and uses tactical decomposition equations as necessary existence conditions. By help of them we are able to reduce the size of the Kramer-Mesner matrix and to achieve a linear system of appropriate size to be solved by efficient computer algorithms in reasonable time.

The GAP platform has been used in order to simplify the construction procedure for other users. The idea is to add a package with which t-designs will be constructed easily and faster than before. We shall support our ideas by examples such as inversive planes and other interesting series of t-designs.

The future work should involve the application of this combined construction method for q-ary designs, combinatorial structures of great interest for coding theory, since they are immediately leading to optimal codes.

University of Zagreb, Faculty of electrical engineering and computing, Depart-

ment of applied mathematics, Unska 3, 10000 Zagreb, Croatia
mario.pavcevic@fer.hr

Contributions to pure and applicable Galois geometry

Cornelia Rößing

University College Dublin, Ireland

The first part presents spectrum results for maximal partial ovoids and maximal partial spreads of generalised quadrangles and minimal blocking sets with respect to planes in PG(3,q). For a spectrum result we prove that there exists such a substructure for every cardinality within the interval of the spectrum. The focus of the second section of the talk is on inversive planes, also called Möbius-planes. We characterise the subplanes of Miquelian inversive planes and develop a bound for the cardinality of a blocking set (with respect to the circles) of an inversive plane. In the last part we introduce an application of generalised quadrangles and inversive planes in coding theory. We give a construction for LDPC codes based on these geometries and show the performance of a code developed from an inversive plane in a waterfall diagram.

University College Dublin, School of Mathematical Sciences, Belfield, Dublin 4, Ireland
roessing@maths.ucd.ie

Transitive designs constructed from finite groups

Andrea Švob

University of Rijeka, Croatia

(Joint work with Dean Crnković and Vedrana Mikulić Crnković)

The main subject of the talk is construction of transitive designs from finite groups. In the talk I will introduce the construction method of the combinatorial structures, which is based on the construction of transitive 1-designs and regular graphs constructed from finite groups. Comparison with previous methods of the construction of combinatorial structures from primitive groups will show that the introduced method is their generalization. Besides the construction of primitive designs, for which the methods are previously known, the developed method also includes transitive designs. The method will be applied on the construction of 2-designs and strongly regular graphs. The structures will be defined on the conjugacy classes of the maximal and second maximal subgroups under the action of finite groups or their maximal subgroups. Constructed structures and their automorphism groups will be described.

University of Rijeka, Department of Mathematics, Radmile Matejcic 2, The University Campus Trsat, 51000 Rijeka, Croatia
asvob@math.uniri.hr

On colourings of projective planes

Tamás Szőnyi

Eötvös Loránd University, Budapest, Hungary

(Joint work with Gábor Bacsó, Tamás Héger)

The chromatic number of a hypergraph is the smallest number of colours needed to colour the points so that no edge is monochromatic. Projective planes of order greater than 2 have chromatic number 2. This simply means that projective planes of order greater than 2 have non-trivial blocking sets. We shall discuss general results on 2-colourability of n-uniform hypergraphs and their consequences for projective spaces. The 2-colouring can also be described by a function $f : V \to \{-1, +1\}$, where V is the ground set and the discrepancy of an edge E is just $|\sum_{x \in E} f(x)|$. Intuitively, this measures the difference of the sizes of the two colour classes along E. The discrepancy of a hypergraph is the maximum discrepancy of its edges. To determine the discrepancy of a projective plane is not trivial at all. Standard equations for one colour class give that it is at least $\sqrt{q}$ and Spencer proved in 1989 that this is the right order of magnitude. We will discuss other interesting questions (with some old answers) about 2-colourings of projective planes.

In the second part of the talk we shall discuss results about the upper chromatic number of projective planes. The notion comes from Voloshin's work on colourings of mixed hypergraphs. For a finite plane Π, the upper chromatic number $\overline{\chi}(\Pi)$ denotes the maximum number of colours in a colouring of the points such that each line has at least two points of the same colour. So, instead of excluding monochromatic lines we exclude "rainbow" ones. Few results are known for general planes, mainly due to Bacsó and Tuza. In the talk we focus on determining or bounding the upper chromatic number of $\mathrm{PG}(2, q)$. The following construction relates the upper chromatic number and the minimum size of a double blocking set: take a double blocking set and colour all of its points red. The remaining points get pairwise different colours. This shows that $\overline{\chi}(\Pi) \geq v - \tau_2(\Pi) + 1$, where v denotes the number of points and τ_2 is the minimum size of a double blocking set. In several cases we could prove that we actually have equality in this bound.

Eötvös Loránd University, Institute of Mathematics, H-1117 Budapest, Pázmány Péter s. 1/c Hungary
szonyi@cs.elte.hu

Subplanes of a translation plane

Rocco Trombetti

University of Naples

The subplane dimension question for an affine (projective) plane π of order n, consists of asking if the existence of a subplane, say π_0, of π of order k forces the dimension of π with respect to π_0 (i.e., $log_k n$) to be a positive integer. Such a problem has been deeply studied as proving that the question has a negative answer. Different authors, in fact, have found examples of planes with trascendental or fractional dimensions. The former examples are translation planes or planes coordinatized by so called nearfields while the great part of the latter are semifield planes (i.e., planes coordinatized by semifields) and these are shown to be fractional dimensional with respect to subplanes which still are coordinatized by semifields (in fact, by finite fields) and are in *canonical position* with respect to the starting plane.

In the first part of this talk we will overview some of the techniques which leaded to the detection of such examples and will describe the state of the art on this topic. Nevertheless, it seems that the integer dimensional case has been not yet investigated properly. For instance, it is not clear, in general, under which assumptions a translation plane may contain a Baer subplane. We will face with this problem in the second part of the talk, by showing a sufficient and necessary condition for a translation plane in order to contain a subplane which is not necessarily in canonical position. This relies on the geometric structure of the *rational partial spread* contained in the spread associated with the translation plane. Then, we will exhibit a geometric procedure to obtain, starting from a Baer subplane π_0 (not necessarily a quasifield plane and not necessarily in canonical position) of an affine translation plane π, a Baer subplane π_0' of the transpose plane π^t of π which is, in general, not isomorphic to the transpose π_0^t of π_0. As a first application of this geometric procedure we prove that the transpose semifield planes of some planes recently discovered in [1], admit a GTF-plane as a Baer subplane in canonical position. By further exploiting the procedure in the semifield case, it is possible to construct six Baer subplanes contained in the Knuth derivatives of π, starting from a Baer subplane of π in canonical position. We will show that the relevant chain and the one determined by π_0 by means of the Knuth operations are, in general, different. Finally, we will argue on some implications of these results in the setting of derivation theory, proving that the existence of Baer subplanes in the planes coordinatized by a derivative of BH-semifields, implies that this plane is, in fact, derivable.

References

[1] L. BUDAGHYAN AND T. HELLESETH, *New perfect nonlinear multinomials over* $\mathbf{F}_{p^{2k}}$ *for any odd prime* p, in Sequences and their applications—SETA 2008, vol. 5203 of Lecture Notes in Comput. Sci., Springer, Berlin, 2008, pp. 403–414.

Dipartimento di Matematica e Applicazioni Caccioppoli,
Università degli Studi di Napoli "Federico II", Complesso di Monte S. Angelo–Edificio T.,
via Cintia, I–80126 Napoli
rtrombet@unina.it