Abstracts for GGA09

Contents

1 Invited speakers

Galois Geometries and Coding Theory

Ivan Landjev

Institute of Mathematics and Informatics
8 Acad. G. Bonchev str., 1113 Sofia, BULGARIA
and
New Bulgarian University
21 Montevideo str., 1618 Sofia, BULGARIA

The geometric nature of certain optimality problems in coding theory has been long known. The connection between the geometry of special point sets in suitably chosen projective and affine spaces and linear codes over certain algebraic structures (finite fields, semifields, special rings) has been exploited repeatedly during the years.

In the last decade, a substantial progress has been made in the fields of finite geometry and coding theory. Yet many challenging problems remain unsolved. The goal of this talk is to state some of the basic results in both areas, to survey the recent progress and to formulate some interesting (in our view) open problems.

The talk covers the following topics:

1. Basic facts from coding theory
   - 1.1. Linear codes over finite fields and rings
   - 1.2. Equivalent codes, the automorphism group of a linear code
   - 1.3. The spectrum of a linear code. MacWilliams identities
   - 1.4. General bounds for linear codes
2. Finite geometries
   - 2.1. The projective geometries $\mathrm{PG}(V,K)$ and $\mathrm{PHG}(M_R)$
   - 2.2. Collineations in $\mathrm{PG}(V,K)$ and $\mathrm{PHG}(M_R)$
   - 2.3. Linear codes as sets of points in $\mathrm{PG}(k-1,q)$
3. Special sets of points in $\mathrm{PG}(N,q)$
   - 3.1. κ-arcs in $\mathrm{PG}(N,q)$
   - 3.2 (κ,ν)-arcs in $\mathrm{PG}(2,q)$
   - 3.3. (κ,ν)-caps in $\mathrm{PG}(N,q)$
   - 3.4. Multiple blocking sets and minihypers
4. Some special families of linear codes
   - 4.1. MDS-codes

Applications of Galois Geometry to Cryptology

Keith Martin

Information Security Group
Royal Holloway, University of London

Cryptology is the study of mathematical techniques for implementing core information security services such as confidentiality and authentication. Galois geometry has played an important role in developing the theory of cryptology in a number of different areas. We comment on the reasons why Galois geometry arises in cryptology and discuss a number of these applications.

(Almost) Perfect nonlinear functions in cryptography and geometry

Alexander Pott

Otto-von-Guericke-Universität
Magdeburg, Germany

A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called **almost perfect nonlinear** if $F(x + a) - F(x) = b$ has at most two solutions for x if $a, b \neq 0$. Recently, many new almost perfect nonlinear functions have been constructed, and new aspects on APN functions have been investigated (equivalence, automorphism groups, crookedness, connection with codes). The study of almost perfect nonlinear functions has been motivated by cryptography, in particular S-boxes.

A function $F : \mathbb{F}_q \to \mathbb{F}_q$ is called **perfect nonlinear** if $F(x + a) - F(x) = b$ has exactly one solution if $a, b \neq 0$. It is easy to see that perfect nonlinear functions cannot exist if q is even. In geometry, perfect nonlinear functions are usually called **planar**. They can be constructed from commutative semifields, but not vice versa.

In my talk, I will discuss recent results on almost perfect and perfect nonlinear functions, in particular similarities and differences between these two concepts.

Nonlinear perfect codes and their impact on designs and geometry

Mercè Villanueva

Universitat Autònoma de Barcelona

Let $\mathbb{F}_q^n$ be a vector space of dimension n over $GF(q)$. A subset C of $\mathbb{F}_q^n$ is said to be a q-ary perfect code if for some integer $r \geq 0$ every $x \in \mathbb{F}_q^n$ is within distance r from exactly one codeword of C. It is known that the only parameters for nontrivial perfect codes are those of the two Golay codes and the q-ary 1-perfect codes, where q is a prime or prime power. It is also known that the linear 1-perfect codes are unique up to equivalence. They are the well-known Hamming codes and exist for all $m \geq 2$. Nonlinear 1-perfect q-ary codes also exist for $q = 2, m \geq 4$; $q \geq 3, m \geq 3$; and for q a prime power, $q \neq 4$, $m \geq 2$.

The current main results about perfect codes will be given, as well as their connexions with design theory and projective geometry.

2 Contributed talks

Galois Geometry and Designs

Manohar Aggarwal

Department of Mathematical Sciences
The University of Memphis

Galois geometry has been extensively used for the construction of statistical designs. Bose (1939) and Bose and Nair (1939) used it for the construction of Balanced Incomplete Block Designs and Partially Balanced Incomplete Block Designs. Rao (1947) used it for the construction of Orthogonal Arrays. Bose (1947) introduced the "Packing Problem" in the context of the construction of confounded factorial experiments which is also related to Galois geometry and to Coding Theory. Most recently, some special structures of Galois geometry, e.g. Minihyper, Spreads and Partitions etc. have been used for the construction of Optimal Fractional Factorial Experiments and Supersaturated designs. In my talk, I will give a selected review of the applications of Galois geometry and some recent results.

Alternative constructions of non-classical unitals in desarguesian planes

Angela Aguglia

Politecnico di Bari
Dipartimento di Matematica
Via Re David, 70126 Bari
Italy

(Joint work with L. Giuzzi and G. Korchmáros)

We present new constructions of non-classical unitals from a classical unital $\mathcal{U}$ in $PG(2,q^2)$. The resulting non-classical unitals are either Buekenhout-Metz or Buekenhout-Tits unitals. The main idea is to find a non-standard model π of $PG(2,q^2)$ with the following three properties:

- points of π are those of $PG(2,q^2)$;
- lines of π are certain lines and conics of $PG(2,q^2)$;
- the points in $\mathcal{U}$ form a non-classical Buekenhout-Metz unital in π.

The construction also works for a Buekenhout-Tits unital, provided that conics are replaced by certain algebraic curves of higher degree.

New Quantum Caps in $PG(4,4)$

Daniele Bartoli

Dipartimento di Matematica e Informatica
Universita degli Studi di Perugia
Via Vanvitelli 1
06123 Perugia, Italy

(joint work with Stefano Marcugini and Fernanda Pambianco)

Calderbank, Rains, Shor and Sloane (see [6]) showed that error-correction is possible in the context of quantum computations. Quantum stabilizer codes are a class of additive quaternary codes in binary projective spaces, which are self-orthogonal with respect to the symplectic form. A geometric description is given in [5], where also the notion of a quantum cap is introduced. Quantum caps correspond to the special case of quantum stabilizer codes of distance $d = 4$ when the code is linear over $GF(4)$. In the present paper we review the translation from quantum error-correction to symplectic geometry and study quantum codes in $PG(4,4)$ where we construct complete quantum caps with 29, 30, 32, 33 and 34 points (see [3]). Besides we show that a 20-complete cap is quantic, where 20 is the minimum size of the complete caps in PG(4,4) (see [1], [2] and [4]).

References

[1] D. Bartoli, Quantum codes and related geometric properties, *degrees thesis 2008*.

[2] D. Bartoli, A. Davydov, S. Marcugini and F. Pambianco, The minimum order of complete quantum caps in $PG(4,4)$, *preprint.*

[3] D. Bartoli, S. Marcugini and F. Pambianco, New quantum caps in $PG(4,4)$, *preprint.*

[4] D. Bartoli, S. Marcugini and F. Pambianco, A search for small, minimal, quantum caps in $PG(4,4)$, *RAPPORTO TECNICO* N. 12 - 2008 *Dipartimento di Matematica e Informatica - Università degli Studi di Perugia.*

[5] J. Bierbrauer, G. Faina, M. Giulietti, S. Marcugini and F. Pambianco, The geometry of quantum codes. *Innov. Incidence Geom.* **6** (2007), 289-307.

[6] A. R. Calderbank, E. M. Rains, P. M. Shor and N. J. A. Sloane, Quantum error correction via codes over $GF(4)$. *IEEE Transactions on Information Theory* **44** (1998), 1369-1387.

New commutative semifields and their nuclei

Jürgen Bierbrauer

Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

In the theory of functions with maximal nonlinearity there is a sharp dichotomy between the odd characteristic and characteristic 2 cases. In characteristic 2 the motivation comes from cryptography (theory of S-boxes). We focus on quadratic PN (planar) functions in odd characteristic and APN functions in characteristic 2. The corresponding geometric objects are certain types of semibiplanes, certain generalizations of hyperovals in characteristic 2 and certain projective planes in odd characteristic. The algebraic equivalents of quadratic PN functions are commutative semifields (in odd characteristic). The classical examples are due to Dickson and Albert.

One main result is a uniform construction method for a large class of APN/PN functions in all characteristics. The semifields are constructed as cubic or biquadratic extensions. The cubic cases as well as the biquadratic examples in characteristic 2 had been considered earlier by various authors. We describe a large parametric family in the biquadratic case. The corresponding planar functions are

$$f(x) = x^{1+q'} - vx^{q^3+qq'} \text{ defined on } GF(q^4),$$

where $q = p^s, q' = p^t, 2s/\gcd(2s,d)$ odd and $ord(v) = (q^4-1)/(q-1)$. It is shown that the subcase of orders p^{4s} for odd $s > 1$ yields new planar functions. In the case of order p^{12}, the middle nucleus has order p^2 and the kernel has order p.

We also describe a general construction method for a semifield canonically associated to a given planar function and use it to determine the nuclei of certain families of new commutative semifields of dimensions 9 and 12 in arbitrary odd characteristic.

Hyperplanes of $DW(5, \mathbb{K})$ with $\mathbb{K}$ a perfect field of characteristic 2

Bart De Bruyn

Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22, 9000 Ghent
Belgium

Let $DW(5, \mathbb{K})$ denote the symplectic dual polar space of rank 3 associated with a nondegenerate alternating bilinear form of a 6-dimensional vector space V over a field $\mathbb{K}$. The dual polar space $DW(5, \mathbb{K})$ has a natural projective embedding e into the 13-dimensional projective space $\mathrm{PG}(\bigwedge^3 V)$. This embedding is called the *Grassmann embedding* of $DW(5, \mathbb{K})$. A *hyperplane* of $DW(5, \mathbb{K})$ is a proper set of points of $DW(5, \mathbb{K})$ which intersects each line in either a singleton or the whole line. If Π is a hyperplane of $\mathrm{PG}(\bigwedge^3 V)$, then the set of points of $DW(5, \mathbb{K})$ which are mapped by e into Π is a hyperplane of $DW(5, \mathbb{K})$. Each hyperplane of $DW(5, \mathbb{K})$ which can be obtained in this way is said to *arise from the Grassmann embedding*.

In the talk, we will restrict to the case that $\mathbb{K}$ is a perfect field of characteristic 2 and give a complete classification of all hyperplanes of $DW(5, \mathbb{K})$ which arise from the Grassmann embedding. For finite fields, there are 6 isomorphism classes of such hyperplanes. For infinite fields however the number of isomorphism classes depends on the structure of the field.

Some characterizations of the Split Cayley hexagon

Nicola Durante

Universitá di Napoli "Federico II"
Dipartimento di Matematica e applicazioni "R. Caccioppoli"
Complesso M. S. Angelo, via Cintia I-80126 NAPOLI
Italy

(joint work with John Bamberg)

We give two characterisations of the Split Cayley hexagon, the first of which follows a theme of Thas and Van Maldeghem (2008) on the characterisation of the Split Cayley hexagons as line sets of projective 6-space. Let $\mathcal{L}$ be a set of lines of the 6-dimensional parabolic quadric $\mathsf{Q}(6,q)$ such that on every point there are $q+1$ lines of $\mathcal{L}$ spanning a plane and $\mathcal{L}$ is connected. Then the incidence structure arising having points defined as the points of $Q(6,q)$, and with lines defined as $\mathcal{L}$, is isomorphic to a Split Cayley hexagon.
The second (related) characterization is in terms of substructures of the 3-dimensional Hermitian variety. Let π be a plane of $\mathsf{PG}(3,q^2)$ meeting $\mathsf{H}(3,q^2)$ in a non-degenerate Hermitian curve $\mathcal{O}$, and let Ω be a set of Baer subgenerators with a point in $\mathcal{O}$, such that every affine point is on $q+1$ elements of Ω spanning a Baer subplane. We show that the incidence structure Γ with points defined as the generators of $\mathsf{H}(3,q^2)$ and the affine points of $\mathsf{H}(3,q^2)\backslash\mathcal{O}$, and with lines defined as $\mathcal{O}\cup\Omega$, is isomorphic to a Split Cayley hexagon. Moreover, if we take the subgroup $\mathsf{SU}(3,q^2)$ contained in the stabiliser of $\mathcal{O}$, it has $q+1$ orbits on Baer subgenerators with a point in $\mathcal{O}$, each of which is a candidate for Ω. In this model, we give a homogeneous representation for the Fisher-Thas-Walker-Kantor generalised quadrangles.

If a linear code has an extension, then it also has a linear extension

A. Gács

ELTE Budapest
gacs@cs.elte.hu

(joint work with T. Alderson)

For $n \geq k$, an $(n, k, d)_q$-*code* C is a collection of q^k n-tuples (often called *words* or *codewords*) over an alphabet A of size q such that the minimum (Hamming) distance between any two codewords of C is d. In general, q need not be a prime power. In the special case that $A = GF(q)$ and C is a vector space of dimension k over $GF(q)$, C is a *linear* $(n, k, d)_q$-code. In this case, the minimum distance property translates to the property that each nonzero codeword has at least d nonzero coordinates.
A code C' obtained by deleting some fixed coordinate from each codeword of C is called a *punctured code* of C. If C' is an $(n-1, k, d-1)_q$ code, then C is said to be an *extension* of C', equivalently, C' is said to be *extendable* to the code C. A code is *maximal* if it admits no extensions.

In the talk I will sketch the proof and list some consequences of the following.

Theorem 1 *[1] If a linear $(n, k, d)_q$ code can be extended to an $(n+1, k, d+1)_q$ code, then it can also be extended to a linear $(n+1, k, d+1)_q$ code.*

It is not true in general that all extensions are (equivalent to) linear. The proof is based on the so-called Bruen-Silverman model, a representation of linear codes that establishes a connection between the extensions of a linear code and the direction problem in the affine space $AG(k, q)$.

I will also discuss the possible generalisation of the result (possibly with some extra conditions on the code) to t-fold extensions. Such a result could imply that (over an alphabet of prime power size) the MDS conjectures for linear codes and for arbitrary codes are equivalent.

References

[1] T. Alderson and A. Gács, On the maximality of linear codes, submitted.

AG-codes from certain maximal curves

Massimo Giulietti

University of Perugia
Dipartimento di Matematica e Informatica
Via Vanvitelli, 1, 06123 Perugia
Italy

AG-codes are linear error-correcting codes constructed from algebraic curves. Roughly speaking, the parameters of an AG-code are good when the underlying curve has many rational points with respect to its genus. AG-codes from specific curves with many points, such as the Hermitian curve and its quotients, the Suzuki curve, and the Klein quartic, have been the object of several works. In this talk, we describe an explicit construction of one-point AG codes from the GK curves, together with some results on the permutation automorphism groups of such codes. The GK curves are defined over any finite field of order q^2 with q a perfect cube, and they are maximal curves in the sense that the number of their rational points attains the Hasse-Weil upper bound. Significantly, for $q > 8$, GK curves are the first known examples of maximal curves which are proven not to be covered by the Hermitian curve. Some of the codes constructed here have better parameters compared with the known linear error-correcting codes.

Characterization results on minihypers

A. Hallez

Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22, 9000 Ghent
Belgium

(joint work with J. De Beule and L. Storme)

Let $\mathrm{PG}(n,q)$ denote the n-dimensional projective space over $\mathrm{GF}(q)$, the finite field of order q, $q = p^h$, p prime. Denote by θ_n the size of the point set of $\mathrm{PG}(n,q)$.

Definition 2 *(Hamada and Tamari [1]) An* $\{f,m;N,q\}$-minihyper *is a pair* (F,w)*, where* F *is a subset of the point set of* $\mathrm{PG}(N,q)$ *and* w *is a weight function* $w:\mathrm{PG}(N,q)\to\mathbb{N}:P\mapsto w(P)$*, satisfying*

1. $w(P)>0\Leftrightarrow P\in F$,
2. $\sum_{P\in F} w(P)=f$, *and*
3. $\min\{\sum_{P\in H} w(P) : H \text{ is a hyperplane}\}=m$.

The weight function w determines the set F completely. When this function has only the values 0 and 1, then (F,w) is determined completely by the set F and the minihyper is denoted by F.

We present the following new result.

Theorem 3 *An* $\{\epsilon_1(q+1)+\epsilon_0,\epsilon_1;n,q\}$*-minihyper,* q *square,* $\epsilon_1+\epsilon_0<\frac{q^{7/12}}{\sqrt{2}}$ *and with at most* $\frac{q^{1/6}}{\sqrt{2}}$ *multiple points in the case* $n=3$*, is a sum of*

1. *lines*
2. $\mathrm{PG}(2,\sqrt{q})$
3. $\mathrm{PG}(3,\sqrt{q})$

References

[1] N. Hamada and T. Helleseth. Codes and minihypers. *Proceedings of the Third European Workshop on Optimal Codes and Related Topics, OC'2001, June 10-16, 2001, Sunny Beach, Bulgaria*, pages 79–84, 2001.

Constant Dimension Network Codes

Axel Kohnert

Universität Bayreuth
Mathematisches Institut
95400 Bayreuth
Germany

(joint work with Sascha Kurz)

A natural generalization of classical codes can be defined in the following way: Instead of working with the Hamming Graph $G(n, q)$ (Vertices are all possible words of length n over an alphabet with q letters. Two vertices are adjacent if they differ in only one coordinate) we look at the Hasse diagram of the linear lattice $PG(n-1, q)$. Codewords are now subspaces of $GF(q)^n$ and they build a subspace code. We call this also a q-analogue of a classical code. There is an increased interest in subspace codes in general since a paper by Kötter and Kschischang where they gave an application in network coding. There is also a connection to the theory of designs over finite fields. We modified a method of Braun, Kerber and Laue which they used for the construction of designs over finite fields to construct constant dimension codes. These are q-analogues of constant dimension codes. Using this approach we found many new constant dimension codes with a larger number of codewords than previously known codes. In this talk I will show our method of construction, and will also show what is necessary to find network codes useful for applications.

References

[1] Michael Braun, Adalbert Kerber, Reinhard Laue: Systematic construction of $q-$analogues of $t-(v, k, \lambda)-$designs. Des. Codes Cryptography 34, 55–70, 2005.

[2] Ralf Kötter, F. Kschischang: Coding for errors and erasures in random network coding. IEEE Transactions on Information Theory 54, 3579–3591, 2008.

[3] Axel Kohnert, Sascha Kurz: Construction of Large Constant Dimension Codes With a Prescribed Minimum Distance, LNCS 5393, 31 – 42, 2008.

Finite semifields with a large nucleus and higher secant varieties to Segre varieties

Michel Lavrauw

Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22, 9000 Ghent
Belgium

In this talk we give a generalisation of the BEL-construction from [1] to linear sets, and then concentrate on the isotopism problem for semifields using this geometric approach.

References

[1] Ball et al: A geometric construction of finite semifields. *J. Algebra* **311** (2007), no. 1, 117–129.

On the number of abstract regular polytopes whose automorphism group is a Suzuki simple group $Sz(q)$

Dimitri Leemans

Université Libre de Bruxelles
Département de Mathématiques - C.P. 216
Boulevard du Triomphe
B-1050 Bruxelles

(joint work with Ann Kiefer)

We determine, up to isomorphism, the number of abstract regular polyhedra whose automorphism group is a Suzuki simple group $Sz(q)$ with q an odd power of 2.

On semispreads in projective spaces

Petr Lisoněk

Simon Fraser University
Department of Mathematics
8888 University Drive, Burnaby, BC
Canada V5A 1S6

The geometric structure of (partial) t-spreads and t-covers in finite projective spaces has been studied extensively, as can be seen for example in the bibliography in [2]. The following related concept is motivated by an application in the design of experiments in statistics:

Definition 4 *We say that a set $\mathcal{S}$ of t-dimensional subspaces of* $\mathrm{PG}(n,q)$ *is a* $(t;u)$-semispread of $\mathrm{PG}(n,q)$ *if the union of the elements of $\mathcal{S}$ covers all points of* $\mathrm{PG}(n,q)$ *and, moreover, the set* $\{U_1 \cap U_2 : U_1, U_2 \in \mathcal{S},\ U_1 \neq U_2\}$ *contains at most u points. If the covering condition is dropped, we say that $\mathcal{S}$ is a* partial $(t;u)$-semispread of $\mathrm{PG}(n,q)$.

Thus (partial) $(t;0)$-semispreads are exactly (partial) t-spreads. We study the known constructions of t-covers [1, 2] from the point of view of semispreads. We also discuss a computational method for the construction of (partial) $(t;u)$-semispreads. The method is based on prescribing a group of automorphisms to $\mathcal{S}$ (namely, a subgroup of the stabilizer of the intersection set). We discuss the results obtained with this method, such as a new construction of a $(2;1)$-semispread of $\mathrm{PG}(7,2)$.

References

[1] A. Beutelspacher, On t-covers in finite projective spaces. *J. Geom.* **12** (1979), 10–16.

[2] J. Eisfeld and L. Storme, (Partial) t-spreads and minimal t-covers in finite projective spaces. Lecture notes for the Socrates Intensive Course on Finite Geometry and its Applications, University of Ghent, 3–14 April 2000. Available at: `http://cage.rug.ac.be/~fdc/intensivecourse2/final.html`

New construction of some Mathon arcs

Thomas Maes

Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22, 9000 Ghent
Belgium

(joint work with Frank De Clerck and Stefaan De Winter)

In 1969, Denniston gave a construction of maximal arcs of degree n in Desarguesian projective planes of even order q, for all n dividing q. In [2], Mathon gave a construction method that generalized that of Denniston. We will use this method and a lemma from [1] to give a new construction of some of these maximal arcs. This also allows us to give a computer free counting of the number of non-isomorphic degree-8 maximal arcs in $\mathrm{PG}(2, 32)$.

References

[1] A. Aguglia, L. Giuzzi, and G. Korchmáros. Algebraic curves and maximal arcs. *J. Algebraic Combin.*, 28(4):531–544, 2008.

[2] Rudolf Mathon. New maximal arcs in Desarguesian planes. *J. Combin. Theory Ser. A*, 97(2):353–368, 2002.

On ovoidal blocking sets

Giuseppe Marino

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

Let $\mathcal{S}$ be a Desarguesian line–spread of a hyperplane $\Sigma' = PG(2n-1,q)$ of $\Sigma = PG(2n,q)$. Let P and $\bar{B}$ be, respectively, a point of a line ℓ of $\mathcal{S}$ and a minimal blocking set of a $(2(r-1)+1)$-dimensional subspace of Σ not containing P. Denote by K the cone with vertex P and base $\bar{B}$, and consider the point set B defined by

$$B = \big(K \setminus \Sigma'\big) \cup \{X \in \mathcal{S} : X \cap K \neq \emptyset\},$$

in the Barlotti–Cofman representation of $PG(n,q^2)$ in $PG(2n,q)$ associated with the line–spread $\mathcal{S}$. If $\bar{B}$ intersects the line ℓ at a point different from P, it has been proven that B is a minimal blocking set in $PG(n,q^2)$. In particular, if $\bar{B}$ is an ovoid of $PG(3,q)$ or a $Q(4,q)$ or a $Q(6,q)$, then B turns out to be a blocking set of $PG(n,q^2)$, with $3 \leq n \leq 6$, and it is called an *ovoidal blocking set* of $PG(n,q^2)$. In some cases ovoidal blocking sets of $PG(n,q^2)$ can be embedded in a Hermitian variety $H(n,q^2)$, $3 \leq n \leq 6$, as maximal partial ovoids (see [1]).

In this talk, we will further investigate the construction of ovoidal blocking sets of $PG(n,q^2)$, $3 \leq n \leq 6$, up to isomorphism. Moreover we will establish the geometric conditions assuring that an ovoidal blocking set can be embedded in a Hermitian variety.

References

[1] F. Mazzocca, L. Storme and O. Polverino: Blocking sets in $PG(r,q^n)$, *Des. Codes Cryptogr.*, **44** (2007), 97–113.

h-Blocking sets in $\mathbf{PG}(r, q^n)$

Francesco Mazzocca

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

Generalizing a construction in [1], new classes and new sizes of minimal blocking sets in finite projective spaces $\mathrm{PG}(r, q^n)$ of non-prime order were recently found in [2] ($r = 2$) and [4] ($r > 2$).

In this talk, I will show a natural generalization of the main constructions in [2] and [4] in order to get new families of h-blocking sets in $\mathrm{PG}(r, q^n)$ ([3]).

References

[1] A.Cossidente, A.Gács, C.Mengyán, A.Siciliano, T.Szőnyi and Zs. Weiner: On large minimal blocking sets in $\mathrm{PG}(2, q)$, *J. Combin. Des.*, **13** n.1 (2005), 25-41.

[2] F. Mazzocca and O. Polverino: Blocking sets in $\mathrm{PG}(2, q^n)$ from cones of $\mathrm{PG}(2n, q)$, *J. Algebraic Combin.*, **24** (2006), 61-81.

[3] F. Mazzocca and O. Polverino: h-Blocking sets in $\mathrm{PG}(r, q^n)$, to appear.

[4] F. Mazzocca, L. Storme and O. Polverino: Blocking sets in $\mathrm{PG}(r, q^n)$, *Des. Codes Cryptogr.*, **44** (2007), 97-113.

On the spectrum of maximal partial ovoids of the generalized quadrangle $\mathcal{Q}(4,q)$, q odd

Valentina Pepe

Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22, 9000 Ghent
Belgium

(joint work with C. Rößing and L. Storme)

Let $\mathcal{Q}(4,q)$ be the parabolic quadric of $PG(4,q)$. A *partial ovoid* $\mathcal{O}$ of $\mathcal{Q}(4,q)$ is a set of points such that every line of $\mathcal{Q}(4,q)$ contains at most one point of $\mathcal{O}$ and $\mathcal{O}$ is called *maximal* if it is not contained in a larger partial ovoid.

An *ovoid* $\mathcal{O}$ of $\mathcal{Q}(4,q)$ is a set of points such that every line of $\mathcal{Q}(4,q)$ contains exactly one point of $\mathcal{O}$ and it is well known that $\mathcal{O}$ has q^2+1 points.

In the last years, the sizes of the largest ([1]) and the smallest ([2]) maximal partial ovoids of $\mathcal{Q}(4,q)$ has been investigated and in a recent paper ([3]), the authors prove a spectrum result on the size of maximal partial ovoids of $\mathcal{Q}(4,q)$, for even q, that is for every integer k in a given interval, there exists a maximal partial ovoid of size k. We prove a similar result for the maximal partial ovoids of $\mathcal{Q}(4,q)$, q odd.

References

[1] M.R. Brown, J. De Beule and L. Storme, Maximal partial spreads of $T_2(O)$ and $T_3(O)$. *European J. Combin.*, **24** (2003), 73–84.

[2] M. Cimráková, S. De Winter, V. Fack and L. Storme, On the smallest partial ovoids and spreads of the generalized quadrangles $\mathcal{W}(q)$ and $\mathcal{Q}(4,q)$. *European J. Combin.*, **28** (2007), 1934–1942.

[3] C. Rößing and L. Storme, A spectrum result on maximal partial ovoids of the generalized quadrangle $\mathcal{Q}(4,q)$, q even. *European J. Combin.*, to appear.

[4] V. Pepe, C. Rößing and L. Storme, A spectrum result on maximal partial ovoids of the generalized quadrangle $\mathcal{Q}(4,q)$, q odd. preprint.

Inversive Spaces, 0-1-Geometries, and Low-Density Parity-Check Codes

Cornelia Rößing

School of Mathematical Sciences
University College Dublin
Belfield, Dublin 4, Ireland

LDPC codes have been attracting attention over the recent decade. Originally introduced in the seminal work of Gallager in the sixties, they were (re)discovered soon after the famous TURBO codes. This talk will describe a family of LDPC codes that are derived from what are called 0-1-geometries which we have found in a geometric structure called inversive space. We will briefly discuss basic properties and show some performance diagrams. These diagrams suggest that these codes might be useful in various applications like general communications as well as data storage.

Complete Set of Homogeneous Polynomials in $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ reaching the maximum number of zeros

Adnen Sboui

Middle East Technical University
Department of Mathematics and Institute of Applied Mathematics
İnönü Bulvarı, 06531, Ankara, Turkey

(joint work with Ferruh Özbudak)

The geometric configuration of maximal hypersurfaces of degree d in the n-dimensional projective space over a Galois field $GF(q)$, is described only in the case $d \leq q$ by Serre [4] giving a proof to a conjecture of Tsfasman, which says that a maximal hypersurface is a union of d hyperplanes meeting in a common linear subvariety of codimension 2. An important application of such results is the computation of the number of minimum weight codewords in the generalized Reed-Muller codes.

In the affine case, the minimum distance of the generalized Reed-Muller codes has been determined by Kasami, Lin and Peterson [2]. Moreover the list of all polynomials reaching the maximal number of zeros is given, and the corresponding maximal hypersurfaces are characterized for all $d < n(q-1)$, by Delsarte, Goethals and Mac Williams [1]. Therefore the number of codewords reaching the minimum distance was computed.

In the projective case, the performance of the generalized Reed-Muller codes is viewed relatively better compared to the affine case by some arguments given by Lachaud [3]. There are some results of the analogous problems in the projective case. The minimum distance of the generalized projective Reed-Muller codes has been determined by Sørensen [5] in the case $d < n(q-1)$. For the case $d \leq q$, the same result was been proven independently by Serre [4].

In this paper we give the list of all homogeneous polynomials in $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h$ reaching the maximum number of zeros, and we characterize the corresponding maximal hypersurfaces for all $d < n(q-1)$. Therefore we determine the number of minimum weight codewords of the generalized projective Reed-Muller codes. For our proofs we use some geometric arguments, which also give some information regarding weights of the codewords of the generalized projective Reed-Muller codes above the minimum distance.

References

[1] P. Delsarte, J.M. Goethals, and F.J. Mac Williams: On generalized Reed-Muller codes and their relatives, Inform. Control **16** (1970).

[2] T. Kasami, S. Lin, and W. Peterson: New Generalizations of the Reed-Muller codes. I. primitive codes, IEEE Trans. Inform. Theory **IT-14**, N. 2 (1968),

[3] G. Lachaud: The parameters of projective Reed-Muller codes, Discrete Math. 81, no. 2 (1990), 217–221.

[4] J.-P. Serre: Lettre à M. Tsfasman du 24 Juillet 1989, in journées Arithmétiques de Luminy 17-21 Juillet 1989, Astérisque **198-199-200** (1991).

[5] A. B. Sørensen: Projective Reed-Muller codes, IEEE Transactions on Information Theory, Vol **37**, No. 6, November 1991,

On translation ovoids of unitary polar spaces

Alessandro Siciliano

Università degli Studi della Basilicata
Dipartimento di Matematica e Informatica
Via dell'Ateneo Lucano, 85100 Potenza
Italy

In the projective space $\mathrm{PG}(n, q)$ coordinatized by the finite field $\mathrm{GF}(q)$ let $\mathcal{P}$ denote a classical polar space. The *generators* of $\mathcal{P}$ are the subspaces of maximal dimension contained in it.

An *ovoid* of $\mathcal{P}$ is a set of points having exactly one common point with every generator. An ovoid $\mathcal{O}$ of $\mathcal{P}$ is a *translation ovoid* with respect to a point P of $\mathcal{O}$ if there is a collineation group of $\mathcal{P}$ fixing all lines of $\mathcal{P}$ through P and acting regularly on points of the ovoid but not P.

Examples of translation ovoids of $Q^+(3, q)$ are non-degenerate conics contained in it. In $Q^+(5, q)$, translation ovoids are equivalent to semifield spreads and translation ovoids of $Q(4, q)$ correspond to symplectic semifield spreads.

In the paper [2] it was shown that these are the only orthogonal finite polar spaces having translation ovoids.

In [1] several infinite families of translation ovoids of the unitary polar space $H(3, q^2)$ are constructed. In the talk we will present results on the existence of translation ovoids in unitary polar spaces $H(2n + 1, q^2)$.

References

[1] A. Cossidente, G.L. Ebert, G. Marino and A. Siciliano, Shult sets and translation ovoids of the Hermitian surface, *Adv. Geom.* **6** (2006), 523–542.

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

A full classification of the complete k-arcs in $\mathrm{PG}(2, 27)$

H. Sticker

Ghent University
Department of Applied Mathematics and Computer Science
Krijgslaan 281-S9, 9000 Ghent
Belgium

(joint work with K. Coolsaet)

Recently, we obtained a full classification (up to equivalence) of all complete k-arcs in the Desarguesian projective plane of order 27. This was done by computer and took only 33 days. As far as we know, we are the first to do this. The algorithm used is an application of isomorph-free backtracking using canonical augmentation, as introduced by B. McKay [1], which we have adapted to the case of subset generation in Desarguesian projective planes [2]. For each of the complete arcs in $\mathrm{PG}(2, 27)$ we computed the automorphism group and the type of algebraic curve into which it can be embedded.

The largest complete arc is of course the conic. The second largest complete arc has size 22 and has a large intersection (14 points) with a conic. 7 of the other points are external to this conic, 1 is internal. $\mathrm{PG}(2, 27)$ also has an arc of size 18 containing 15 points on a conic and 3 points external to this conic. Another complete arc is one of size 19 that can be embedded onto an irreducible cubic curve with equation $x_2^2x_1 + x_0^3 - \alpha^5x_0^2x_1 + \alpha^2x_1^3 = 0$. We also mention an arc of size 12 with automorphism group isomorphic to the symmetric group on 4 elements. This arc can easily be generalized to other q.

References

[1] McKay B. D., *Isomorph-Free exhaustive Generation*, J. Algorithms, **26** (1998), 306–324.

[2] Coolsaet K. and Sticker H., *A full classification of the complete k-arcs in $PG(2, 23)$ and $PG(2, 25)$*, Journal of Combinatorial Designs, to appear.

Structure and stability

Peter Sziklai

Eötvös University, Budapest
Department of Computer Science
Pázmany P. s. 1/c, 1117 Budapest
Hungary

Structure and stability theorems appear already among the first results of finite geometry over Galois fields. Two theorems of Segre form a pair like this: the first states that in $\mathrm{PG}(2,q)$, q odd, every oval (i.e. $(q+1)$-arc) is a conic, while the second shows the stability of the structure determined in the first: a $(q+1-\varepsilon)$-arc is always extendible to an oval (hence to a conic), if ε is small enough. It means that there are no "nice structures" "close" to the conic, except the perturbed (i.e. truncated) conic itself.

For introducing the main concepts and for further applications first we deal with partitions of the plane.

Question (structure). Let $\mathcal{S}$ be a class of plane "curves". Suppose that $S \subset \mathcal{S}$ partitions the plane $\mathrm{AG}(2,q)$ or $\mathrm{PG}(2,q)$. What is the "structure" of S like?

(For short I use the word "curve" for any nice pointset.) The difficulty of this question depends on the choice of the class $\mathcal{S}$. The corresponding stability problem is the following:

Question (stability). Let $\mathcal{S}$ be a class of plane curves. Suppose that $S \subset \mathcal{S}$ "almost partitions" the plane $\mathrm{AG}(2,q)$ (or $\mathrm{PG}(2,q)$), i.e. the curves in S are pairwise disjoint and $|\mathrm{AG}(2,q) \setminus \big(\bigcup_{s\in S} s\big)|$ is "small". Is S extendible to a partition, i.e. is there a partition S', $S \subset S' \subset \mathcal{S}$?

In the talk we will consider several problems of this type and we will discuss some applications as well. We are going to speak about the "classical" direction problem in the plane, with its generalizations as well. Also an interesting "one dimensional stability result" will be mentioned.

References

[1] P. Sziklai, Partial flocks of the quadratic cone, *J. Combin. Th. Ser. A*, **113** (2006), 698-702.

[2] P. Sziklai, Flocks of cones of higher degree, *J. Algebraic Combin.*, **25** (2007), 233–238.

Vandermonde sets and super-Vandermonde sets

Marcella Takats

Eötvös University, Budapest
Department of Computer Science
Pázmany P. s. 1/c, 1117 Budapest
Hungary

(joint work with Peter Sziklai)

Given a set $T \subseteq \mathrm{GF}(q)$, $|T| = t$, w_T is defined as the smallest positive integer k for which $\sum_{y \in T} y^k \neq 0$. It can be shown that $w_T \leq t$ always and $w_T \leq t-1$ if the characteristic p divides t. T is called a *Vandermonde* set if $w_T \geq t-1$ and a *super-Vandermonde* set if $w_T = t$. This notion was first defined and used (in a slightly different form) by Gács and Weiner [1]. This (extremal) algebraic property is interesting for its own right, but the original motivation comes from finite geometries as many nice pointsets of a projective or affine plane correspond to Vandermonde sets. In this talk we classify small and large super-Vandermonde sets.

References

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

[2] P. Sziklai, M. Takats, Vandermonde sets and super-Vandermonde sets, Finite Fields Appl., **14** (2008), 1056-1067.

Singer quadrangles

Koen Thas

Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S25, 9000 Ghent
Belgium

(joint work with Stefaan De Winter and Ernie Shult)

In recent years there has been quite some interest in developing a Singer (group) theory for other types of geometries than projective planes, especially for generalized quadrangles (GQs) — in the finite case one of the central classes of Lie type geometries.

In my talk I will report on recent work that explains which of the known finite GQs actually admit a Singer group. I will also discuss related results.

Slices of the unitary spread

Rocco Trombetti

Universitá di Napoli Federico II
Dipartimento di Matematica e Applicazioni "R. Caccioppoli"
Via Cintia, 80126 Napoli
Italia

(joint work with G. Lunardon, L. Parlato, and V. Pepe)

The unitary spread and the unitary ovoid are strictly related geometric objects contained in the hyperbolic quadric $\mathcal{Q}^+(7,q)$ of $PG(7,q)$, if $q \equiv 2 \pmod 3$ and in the parabolic quadric $\mathcal{Q}(6,q)$ of $PG(6,q)$, if $q \equiv 0 \pmod 3$. These were introduced by W.M. Kantor in [5] although, for $q = 3^{2h+1}$, unitary spread already appeared in [3]. We prove that the slices of the unitary spread of $\mathcal{Q}^+(7,q)$, $q \equiv 2 \pmod 3$, can be partitioned into five classes. Slices belonging to different classes are non–equivalent under the action of the subgroup of $P\Gamma O^+(8,q)$ fixing the unitary spread. When q is even, there is a connection between spreads of $\mathcal{Q}^+(7,q)$ and symplectic 2–spreads of $PG(5,q)$ (see [1] and [2]). We determine all possible non–equivalent symplectic 2–spreads arising from the unitary spread of $\mathcal{Q}^+(7,q)$, $q = 2^{2h+1}$. Some of these were already discovered in [5]. When $q = 3^h$, the slices of the unitary ovoid of $\mathcal{Q}(6,q)$ with respect to singular hyperplanes and hyperplanes intersecting $\mathcal{Q}(6,q)$ in a hyperbolic quadric were studied in [4]. Here, we complete this study by classifying, up to the action of the subgroup of $P\Gamma O(7,q)$ fixing the unitary ovoid, all slices of the unitary ovoid of $\mathcal{Q}(6,q)$ with respect to non–singular hyperplanes. In particular we focus on slices of the unitary ovoid and of the unitary spread with respect to hyperplanes intersecting $Q(6,q)$ in elliptic quadrics.

References

[1] J.F. Dillon, Elementary Hadamard difference sets, Ph.D thesis, Univ. of Meryland, College Park, (1974).

[2] R. Dye, Partitions and their stabilizers for line complexes and quadrics, Ann. Mat. (4), (114) (1977).

[3] J.A. Thas, Polar spaces, generalized hexagons and perfect codes, *J. Combin. Theory (A)*, 29 (1980).

[4] W.M. Kantor, Ovoids and translation planes, *Canad. J. Math.*, 36 (5) (1982).

[5] W.M. Kantor, Spreads, translation planes and Kerdock sets I, *SIAM J. Alg. Disc. Meth.*, 3 (2) (1982).

The dual code of $\mathcal{Q}(4,q)$ and $\mathcal{Q}^+(5,q)$

Geertrui Van de Voorde

Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22, 9000 Ghent
Belgium
(joint work with Valentina Pepe and Leo Storme)

Let $\mathcal{Q}(4,q)$, resp. $\mathcal{Q}^+(5,q)$, be the parabolic quadric in $\mathrm{PG}(4,q)$, resp. the hyperbolic quadric in $\mathrm{PG}(5,q)$. In [1], the codewords of small weight in the dual code (or *LDPC-code*) of points and lines of $\mathcal{Q}(4,q)$ are characterised. In this talk, I will characterise the small weight codewords of the dual code of points and generators of $\mathcal{Q}^+(5,q)$, using purely geometrical arguments.

After that, I will investigate the codewords with the largest weight in these two codes for q even. In particular, for $\mathcal{Q}(4,q)$, q even, I will show that there is an empty interval in the weight distribution of the dual of the code of $\mathcal{Q}(4,q)$. To prove this, we show that a blocking set of $\mathcal{Q}(4,q)$, q even, of size q^2+1+r, where $0 < r < (q+4)/6$, contains an ovoid of $\mathcal{Q}(4,q)$, improving on [2, Theorem 9].

References

[1] J.L. Kim, K. Mellinger, and L. Storme, Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles, *Des. Codes Cryptogr.*, **42(1)** (2007), 73–92.

[2] J. Eisfeld, L. Storme, T. Szőnyi, and P. Sziklai, Covers and blocking sets of classical generalized quadrangles. *Discrete Math.,* **238** (2001), 35–51.

Algebraic combinatorics applied to projective spaces

Frédéric Vanhove

Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22, 9000 Ghent
Belgium

(joint work with Frank De Clerck and John Bamberg)

Consider the automorphism group $\mathsf{PGL}(n+1,q)$ of a projective space $\mathrm{PG}(n,q)$, which acts generously transitively on the set of a-spaces, for every $a \in \{0,\ldots,n-1\}$. Two pairs of a-spaces (π_1,π_2) and (π_1',π_2') will be in the same orbit on pairs if and only if $\pi_1 \cap \pi_2$ and $\pi_1' \cap \pi_2'$ have the same dimension. These orbits on pairs define a set of symmetric relations on the a-spaces, giving an association scheme.

In this talk, I will discuss how the eigenspaces of the association schemes on a-spaces are linked to each other. It turns out that certain properties of sets of subspaces can be expressed in an algebraic way, by considering the minimal idempotents vanishing on the characteristic vector of such a set of a-spaces. This leads to some non-existence results, and to theorems on linked geometric properties of sets of subspaces.

An Axiomatic Approach to Semiaffine Spaces

Hendrik Van Maldeghem

Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22, 9000 Ghent
Belgium

In 1995, Beutelspacher, De Vito and Lo Re classify finite linear spaces all planes of which are semiaffine. In short, these spaces are unions of affine spaces that lie between some affine spaces and its projective completion. They also provide an axiom system for such spaces, using the notion of weak parallelism of lines, and a rather strong condition on this weak parallelism.

In this talk, we show that one can delete the latter strong condition, and obtain the same spaces, even deleting the finiteness assumption (and hence we do not use the classification of finite semiaffine planes by Kuiper and Dembowski).

We place our result in the bigger framework of axiomatic projective, polar and gamma spaces, and of the classification of spherical buildings of rank at least 3 using the Moufang condition.

Characterizing small weight codewords of the linear code of $\mathbf{PG}(2, q)$

Zsuzsa Weiner

Computer and Automation Research Institute of the Hungarian Academy of Sciences
H-1111 Budapest, Lágymányosi út 11, HUNGARY
weiner@sztaki.hu

(joint work with Tamás Szőnyi and András Gács)

Let $C_1(2, q)$ be the p-ary linear code defined by the lines of $\mathrm{PG}(2, q)$, $q = p^h$, where p is a prime; that is the linear combination of lines of $\mathrm{PG}(2, q)$ over the finite field $\mathrm{GF}(p)$ with p elements. In this talk we show that a codeword c with weight $(w(c))$ less than $[\sqrt{q}]q + 1 + (q - [\sqrt{q}]^2)$ 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 obviously 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 up certain values $(q + 1, 2q, 2q + 1, \dots)$ and there are lots of relatively large empty intervals. When q is even, this is in an earlier result with Szőnyi (see [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 $]q + 1, 2q[$. Furthermore, they also extended this result to codes generated by the k-dimensional subspaces of $\mathrm{PG}(n, q)$, see [2].

References

[1] A. Blokhuis, A. Brouwer, H. Wilbrink, Hermitian unitals are code words, *Discrete Math.* **97** (1991), no. 1-3, 63–68.

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

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

Some geometric approaches to APN functions

Satoshi Yoshiara

Tokyo Woman's Christian University
Department of Mathematics
Suginami-ku, Tokyo 167-8585
Japan

I will report several results obtained by investigating (universal) geometric objects associated with almost perfect nonlinear (APN) functions on a finite field $GF(q)$, $q = 2^n$.

The first geometric object we consider is the incidence graph of a semibiplane. From each APN function f on $GF(q)$, we construct such a graph Γ_f with $2q^2$ vertices, consisting of two bipartite halves corresponding to q^2 points and q^2 blocks. The graph Γ_f is covered by the incidence graph $\tilde{\Gamma}$ of a semibiplane, obtained as a certain truncation of the Coxeter complex of type D_q. The graph $\tilde{\Gamma}$ (independent of f) can be thought of as the graph defined on the set of vectors in $GF(2)^q$, where two vectors v and w are incident whenever $v + w$ has weight 1, and the bipartite half containing v is determined by its weight.

Examining covering maps, we can establish that two APN functions f and g on $GF(q)$ are CCZ-equivalent if and only if the graphs Γ_f and Γ_g are isomorphic. Moreover, we find strong restrictions on the structure of the automorphism group of Γ_f. We can also show that Γ_f is a distance-regular graph of diameter 4, if n is odd.

The second geometric object is defined only when an APN function f on $GF(q)$ is quadratic. In this case with $n \geq 2$, we can construct an $(n-1)$-dimensional dual hyperoval $\mathcal{S}^n[f]$ over $GF(2)$ with ambient space $GF(q) \oplus GF(q)$, a collection of $(d+1)$-dimensional subspaces of $GF(q) \oplus GF(q)$ with certain intersection properties. Its universal cover is the so called Huybrechts dual hyperoval with ambient space $GF(q) \oplus (GF(q) \wedge GF(q))$.

Examining a covering map, we find a canonical form of f as the image of a (universal) APN function on $GF(q) \wedge GF(q)$. This shows that quadratic APN functions on $GF(q)$ (up to extended affine equivalence) correspond to the subspaces of the vector space of alternating bilinear forms on $GF(q)$ with minimum distance 2, where the distance of two forms f and g is given by (the rank of $f+g)/2$. Thus we are naturally led to the investigation of "codes" with a specified minimum weight in a class of association schemes. Furthermore, we can show that two quadratic APN functions f and g on $GF(q)$ are extended affine equivalent if and only if the associated dimensional dual hyperovals $\mathcal{S}^n[f]$ and $\mathcal{S}^n[g]$ are isomorphic.