Mathematisches Forschungsinstitut Oberwolfach

Report No. 52/2001

Finite Geometries

December 2nd – December 8th, 2001

The present conference was organised by Aart Blokhuis, Dieter Jungnickel, James Hirschfeld and Jef Thas.

There were 48 participants, for many of whom it was the first visit to Oberwolfach. This included several PhD students as well as postdoctoral fellows who had recently completed their PhD's. The national distribution of the participants according to their institutions was as follows:

Australia	1
Belgium	13
Bulgaria	1
Germany	8
Hungary	4
Israel	1
Italy	6
The Netherlands	3
New Zealand	1
United Kingdom	4
United States	6

The programme consisted of 15 long talks during five mornings and 16 short talks during four afternoons. Among the highlights were talks by Simeon Ball on semifields, Matthew Brown on subquadrangles of generalized quadrangles, Roy Meshulam on expander graphs, Bernhard Schmidt on difference sets, and Koen Thas on the classification of generalized quadrangles.

On Thursday evening at a meeting of the Institute of Combinatorics and its Applications there were presentations of two medals: the 1997 Kirkman medal to Bernhard Schmidt and the 2000 Hall medal to Klaus Metsch.

A website

http://www.maths.susx.ac.uk/Staff/JWPH/OBER/oindex.html

was arranged so that abstracts could be displayed in advance of the conference. Other details as well as photographs of the conference are available there.

Abstracts

R. Ahlswede, Cone dependence – a basic combinatorial concept

S. Ball, Semifields, flocks and ovoids

T. Beth, A class of designs protecting against quantum jumps

J. Bierbrauer, Projective planes, coverings and a network problem

A. Bonisoli, Collineation groups of ovals with more than one orbit

M. Brown, Subquadrangles of generalized quadrangles of order (q, q^2)

F. Buekenhout, What is an elliptic curve?

F. De Clerck, Recent results on projective and affine full embeddings of (α, β)-geometries

G.L. Ebert, Binary codes of odd order Buekenhout–Metz unitals

Y. Edel, Extensions of generalized product caps

A. Gács, Some new results about directions

D.G. Glynn, The invariant graphs, tournaments and codes of projective planes of even order

P. Govaerts, Restrictions on the size of partial ovoids in finite classical polar spaces and in the split Cayley hexagon

N. Hamilton, New constructions of maximal arcs in Desarguesian projective planes

J. Jedwab, Designing the IEEE 802.12 transmission code

L.H. Khachatrian, Extremal problems under dimension constraints

G. Korchmáros, Transitive ovoids of the Hermitian surface

E. Kuijken, Distance-regular geometries

I.N. Landjev, On arcs in projective Hjelmslev planes over finite chain rings

D. Leemans, RWPRI and $(2T)_1$ flag-transitive linear spaces

G. Lunardon, Spreads in $H(q)$ and 1-systems of $Q(6, q)$

D. Luyckx, On 1-systems of $Q(6, q)$, q even

R. Meshulam, Group algebras and expanders

K. Metsch, Large caps of the Klein quadric

A. Pott, Cyclotomy, geometry, and perfect sequences

B. Schmidt, Asymptotic nonexistence of dihedral difference sets

L. Storme, On multiple blocking sets in Galois planes

P. Sziklai, Small multiple blocking sets in PG$(4, q^2)$ with respect to planes

K. Thas, A Lenz–Barlotti classification for finite generalized quadrangles

V.D. Tonchev, Formulas for the number of STS and SQS of low 2-rank

H. Van Maldeghem, Some remarks on Steiner systems

Cone dependence — a basic combinatorial concept

R. Ahlswede
(joint work with L.H. Khachatrian)

Definition 1. $A \subset \mathbb{E}^n$ is *cone independent* of $B \subset \mathbb{E}^n$ if no $a = (a_1, \dots, a_n) \in A$ equals a linear combination of $B \setminus \{a\}$ with non–negative coefficients.

Definition 2. If A is cone independent of A we call A a *cone independent set.*

Definition 3. Study here the case that $A, B \subset \{0,1\}^n \subset \mathbb{E}^n$ and in particular
$P(n) = \big\{A \subset \{0,1\}^n : A \text{ is cone independent}\big\}$.

Problem 1. Find $c(n) \triangleq \max\{|A| : A \in P(n)\}$.

Problem 2. Given $k, \ell, n \in \mathbb{N}$, $1 < k < \ell \leq n$. Let $A \subset V_k^n$, the set of binary sequences of length n and Hamming weight k, be such that V_ℓ^n is cone independent of A and let $P_n(k,\ell)$ be the set of all such sets. Find

$$c_n(k,\ell) = \max\nolimits_{A \in P_n(k,\ell)} |A|.$$

This is in general a very hard problem. For instance it is easily seen that in the case $\ell = k+1$ we have $c_n(k, k+1) = T(n, k, k+1)$, the Turan number ($T(n,k,\ell)$ equals the maximal cardinality of a family of sets $\mathcal{A} \subset \binom{[n]}{k}$ such that every $B \in \binom{[n]}{\ell}$ contains not more than $\binom{\ell}{k} - 1$ subsets of $\mathcal{A}$). These numbers are not even completely known for $k = 3$.

Theorem 1. *$c_n(k,n) = \binom{n-1}{k}$ if $k \mid n$ or if $k \nmid n$ and n is large.*

Theorem 2. *With $g_n(s) = \max\big\{\binom{2s-1}{2}, \binom{s-1}{2} + (s-1)(n-s)\big\}$*

$$c_n(2,\ell) = \begin{cases} g_n\left(\frac{\ell}{2}\right), & \text{if } 2 \mid \ell \\ \max\left(\left\lfloor \frac{n}{2} \right\rfloor \left\lceil \frac{n}{2} \right\rceil, g_n\left(\frac{\ell+1}{2}\right)\right), & \text{if } 2 \nmid \ell. \end{cases}$$

Conjecture 1. $c_n(k,n) = \max\limits_s |H_s|$, where, for $1 \leq s \leq k$ and $n_s = \left\lceil \frac{n \cdot s}{k} \right\rceil - 1$,

$$H_s = \Big\{v = (v_1, \dots, v_n) \in V_k^n : \sum_{i=1}^{n_s} v_i \geq s\Big\}.$$

Theorem 1 proves this for n large.

Conjecture 2. For $k \ll \ell \ll n$, the number $c_n(k,\ell)$ behaves as in the case where cone independence is replaced by linear independence.

Conjecture 3. $\lim\limits_{n\to\infty} \frac{c(n)}{2^n} < 1$.

It is known that the limit exceeds 0.55.

Semifields, flocks and ovoids

Simeon Ball
(joint work with Matthew Brown)

A *semifield* projective plane is a projective plane that is both a translation plane and a dual translation plane. A *semifield* is an algebraic structure coordinatising such a plane. Cohen and Ganley (1982) considered a particular class of commutative semifields (namely, of rank 2 over the middle nucleus) whose existence they showed was equivalent to the existence of two functions $f, g : \mathrm{GF}(q) \to \mathrm{GF}(q)$, such that both f and g are additive and $g(x)^2 + 4xf(x)$ is a non-square for all $x \in \mathrm{GF}(q) \setminus \{0\}$. For q a power of 2 Cohen and Ganley proved that the only example of such a semifield is $\mathrm{GF}(q^2)$.

By André (1954) a translation plane may be constructed from a spread of a projective space, and vice versa. A spread giving rise to a semifield translation plane is called a *semifield spread.* A *flock* of a quadratic cone $\mathcal{K}$ of $\mathrm{PG}(3,q)$ is a partition of the points of $\mathcal{K}$, minus the vertex, into plane sections. By using the Klein quadric and the Klein correspondence it is possible to construct a spread from a flock (found independently by Walker and Thas). Such a spread is a semifield spread if and only if the flock can be represented using functions f, g as in the work of Cohen and Ganley.

An ovoid of the quadric $Q(4,q)$ is a set of q^2+1 points of the quadric, no two collinear on a line of the quadric. By the Klein correspondence an ovoid of $Q(4,q)$ gives rise to a spread of $\mathrm{PG}(3,q)$. When this spread is a semifield spread the ovoid is called a *translation ovoid.* Thas (1997) gave a general geometrical correspondence between a translation ovoid of $Q(4,q)$ and a semifield flock.

So by considering the Cohen–Ganley functions f and g, the corresponding semifield flock and translation ovoid of $Q(4,q)$ we have 3 semifield planes. These planes are not isomorphic in general, which seems to cause some confusion in the literature. To make matters worse, by the 'cubical array' method of Knuth (1965) we can construct 6 possibly non-isomorphic semifield planes from a given one.

In this lecture I will give a geometrical description of the Knuth 'cubical array' method and then explain some of the connections between the semifield planes mentioned above.

A class of designs protecting against quantum jumps

Thomas Beth

Quantum Error-Correcting Codes and their intrinsic relation to Self-Dual Codes and Finite Geometries have been known as a hot topic of research in Quantum Informatics, Combinatorics and Group Theory since 5 years; the discovery of so-called "Jump Codes", however, provides a rather new line of research in both Quantum Information Theory and Design Theory.

In our presentation we intend to give a short introduction to the concept of so-called "protected subspaces" of the Hilbert "state" space of multi-qu-bit quantum systems. From this we derive the algebraic and finite geometric conditions, under which such protected complex spaces can be generated. We shall show that in order to protect against spontaneous decay the so-called "Quantum Jumps" (which gave rise to the infamous name 100 years ago), special designs, called SEED's (spontaneous emission error designs) must be constructed. After defining the new class of t-SEED's we derive necessary conditions for their existence and construct several families of such objects based on the following result.

Theorem . *Any s-resolvable t-design $S(t,k,u)$ forms an s-SEED.*

Example 1. A 1-SEED is naturally provided by the parallel classes of an $AG(2,p)$.

Example 2. Any Kirkman System provides a 2-SEED.

The classification of SEED's seems to be a wide open problem; in the special case of SEED's with a nontrivial group action, relations to some extremal graph problems will be mentioned. Finally we give bounds for the existence of SEED's and special classes of Codes and Geometries with some exotic group actions generating such designs.

This is joint work with Gernot Alber and his group at Ulm University, Chris Charnes at University of Melbourne and Markus Grassl at Universität Karlsruhe.

Projective planes, coverings and a network problem

Jürgen Bierbrauer
(joint work with F. Pambianco and S. Marcugini)

Define a *covering* $C(n,k,r)$ to be a family of subsets (*blocks*) of an n-set, such that each block has size $\leq k$, each point is on $\leq r$ blocks and any pair of points is on a common block.

The main problem is to determine $Cov(k,r)$, the maximum n such that $C(n,k,r)$ exists. This problem arises in packet switched network design (n network sites, connected by *links* or *busses,* where each site has at most r communication ports, each link can connect at most k sites and any pair of sites appear on a common link). We think of r as fixed and $k > r$. It has been observed in the network literature that projective planes of order $q = r - 1$ can be used to construct such coverings. Charlie Colbourn (*Projective planes and congestion-free networks*, to appear in *Discrete Applied Mathematics*) formalized this and pointed out a link to (k,n)-arcs

We give a general definition of a *weighted arc* in a projective plane of order q and derive coverings from weighted arcs. Call such a covering *geometric.* It is *linear geometric* (equivalent to 3-dimensional linear codes) when the underlying plane is the Desarguesian plane $PG(2,q)$.

We use a result of Füredi's on the *fractional matching number* to determine $Cov(k,r)$ when $q = r - 1$ is a prime-power and k is large enough. In particular every $C(n,k,q+1)$, where $n > qk$, is geometric.

The case when $q = r - 1$ is not a prime-power leads to an interesting existence problem concerning a family of symmetric partially balanced designs, which in some sense are close to being projective planes. We demonstrate the method by constructing good covers $C(n,k,7)$ based on such a design on 40 points, which was constructed by Alan Ling.

Collineation groups of ovals with more than one orbit

Arrigo Bonisoli

Let π be a finite projective plane of odd order n with an oval Ω which is left invariant by a collineation group G. The most powerful results in this situation require G to act primitively or at least transitively on Ω. Much of the machinery developed to this purpose involved Hering's theory of irreducible collineation groups, that is groups fixing no point, no line and no triangle.

In recent years interesting classes of planes have been shown to possess ovals whose collineation groups have two orbits, one of which may well shrink to a single point. More generally, one might like to see what happens if the group G is intransitive on Ω and, possibly, reducible on π.

I would like to illustrate some recent contributions in this area, under the assumption that the G–orbits on Ω are precisely two and at least one of these is primitive.

Subquadrangles of generalized quadrangles of order (q, q^2)

Matthew Brown
(joint work with J. A. Thas)

A *subquadrangle* of a generalized quadrangle is a (proper) subgeometry that is also a generalized quadrangle. Many of the known generalized quadrangles of order (q, q^2) have subquadrangles of order q (that is, order (q, q)). The generalized quadrangle $Q(5, q)$ arising from a non-singular elliptic quadric $\mathcal{E}$ in $\mathrm{PG}(5, q)$ has subquadrangles isomorphic to the GQ $Q(4, q)$ given by non-singular hyperplane sections of $\mathcal{E}$. The GQ $T_3(\Omega)$ of Tits constructed from an ovoid Ω of $\mathrm{PG}(3, q)$ has subquadrangles $T_2(\mathcal{O})$, of order q, for each oval $\mathcal{O}$ that is a section of Ω.

If $\mathcal{F}$ is a flock of a quadratic cone in $\mathrm{PG}(3, q)$, then it is well-known that a GQ $\mathcal{S}(\mathcal{F})$ of order (q^2, q) (and so the dual of a GQ of order (q, q^2)) may be constructed from $\mathcal{F}$. In the case where q is even there exists a set of ovals $\{\mathcal{O}_1, \dots, \mathcal{O}_{q+1}\}$ (called a *herd*) such that $\mathcal{S}(\mathcal{F})$ has subquadrangles isomorphic to $T_2(\mathcal{O}_i)$ for $i = 1, \dots, q + 1$. This connection between flocks, GQs and herds of ovals has been an important construction method for ovals in Desarguesian planes of even order.

In this talk I will survey recent classification results on subquadrangles of order q of generalized quadrangles of order (q, q^2). I will also outline a proof of the result that when q is even a dual flock generalized quadrangle contains only the subquadrangles that are the dual of those arising from the corresponding herd ovals.

What is an elliptic curve ?

Francis Buekenhout

Is an elliptic curve the same object as a plane cubic curve without singular points over any extension of the ground field? Is it the same object as a curve defined by some simple specific equation? A lot of confusion has invaded this matter in view of its sudden popularity and the need of simple explanations.

Let me recall that there exist elliptic curves other than cubics such as a quartic with two double points and a sextic with nine cusps. The truth: every cubic without singular points is an elliptic curve. Moreover, every plane projective elliptic curve is birationally equivalent to a cubic. Where is the difference? The automorphism group of a cubic is small, it is finite of bounded order. It is by no means transitive on the points of the curve except for small cases. It is a subgroup of the collineation group of the projective plane surrounding the cubic. Every point p of the cubic determines a natural symmetry of order two but this is not an automorphism of the cubic except when p is an inflexion point. However, that symmetry is an automorphism of the elliptic curve. It is a birational automorphism. The group of birational automorphisms of an elliptic curve is transitive on its points. It preserves the elliptic curve but moves the underlying cubics. In my opinion, besides their algebraic origin and structure, cubics and elliptic curves are geometric objects that deserve an approach and characterization in the context of Incidence Geometry. Also, that structure is rich enough in order to get rid of the surrounding plane. On this conviction, I have defined a concept of GECC or Generalized Elliptic Cubic Curve. It goes along with a concept of GEC or Generalized Elliptic Curve. A GEC is a set of points equipped with a sharply transitive set of involutory transformations called symmetries. Every GECC has a canonical structure of GEC. Unlike the classical case, not every GEC is isomorphic to the GEC derived from a GECC. Every GEC equipped with a point-origin gives rise to a commutative loop. In the latter, the presence of a GECC is detected by a particular element called associative. A commutative loop with a specified associative element determines a GECC. A commutative loop with no specified element determines a GEC.

What is an elliptic curve? As a first step to the answer it is a GEC whose underlying loops are abelian. More steps remain to be made.

Recent results on projective and affine full embeddings of (α, β)-geometries

F. De Clerck

An (α, β)-geometry is a connected partial linear space $\mathcal{S}$ of order (s, t) ($s+1$ points on a line, $t+1$ lines through a point) such that for any point-line antiflag (x, L) the *incidence number* $\alpha(x, L)$, being the number of points on L and collinear with x, is equal to either α or β. If the point graph of $\mathcal{S}$ is a strongly regular graph, then $\mathcal{S}$ is called a *strongly regular (α, β)-geometry.* Well-known classes of strongly regular (α, β)-geometries are the partial geometries $\mathrm{pg}(s, t, \alpha)$ ($\alpha = \beta$, and especially the generalized quadrangles $\mathrm{GQ}(s, t)$, $\alpha = \beta = 1$) and the semipartial geometries ($\beta = 0$, and especially the partial quadrangles $\mathrm{PQ}(s, t)$, $\alpha = 1$). A semipartial geometry that is not a partial geometry is called proper. Partial geometries fully embedded in a projective space or in an affine space are completely classified. The classification of semipartial geometries embeddable in a projective space is known for $\alpha > 1$ and for $s > 2$. The classification of semipartial geometries embeddable in an affine space is known for the dimensions 2 and 3, but is open for higher dimensions.

We report on following recent results in this area.

1. On the embedding of $(0, \alpha)$-geometries in affine spaces (joint work with Matthew Brown and Mario Delanote)

1. If $\mathcal{S}$ is the dual of a proper semipartial geometry embedded in an affine space $\mathrm{AG}(n, q)$ then $\alpha = 1$.
2. Let $\mathcal{S}$ be an $\mathrm{spg}(q-1, q^2, 2, 2q(q-1))$ embedded in $\mathrm{AG}(4, q)$, then $q = 2^h$ and $\mathcal{S}$ is the Hirschfeld–Thas model of the semipartial geometry known as $TQ(4, q)$.

2. On the embedding of dual partial quadrangles in projective spaces (joint work with Nicola Durante and Jef Thas)

Let L be a line on a nonsingular Hermitian variety $\mathcal{H}$ in $\mathrm{PG}(3, q^2)$. The incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ defined by taking as point set $\mathcal{P}$ the point set of $\mathcal{H}$ not on L and as line set $\mathcal{B}$ the set of lines of $\mathcal{H}$ minus all the lines concurrent with L, is a dual partial quadrangle embedded in $\mathrm{PG}(3, q^2)$. It is a long standing conjecture that this geometry is the only proper dual partial quadrangle embedded in a projective space. We can prove this conjecture under some mild extra conditions.

3. On the embedding of (α, β)-geometries in projective spaces (joint work with Sara Cauchie and Nicholas Hamilton)

Without assuming that the (α, β)-geometry is strongly regular it is still possible to prove some classification results on such embeddable geometries. We classified (α, β)-geometries fully embedded in $\mathrm{PG}(n, q)$, for $\alpha > 1$, q odd, under the assumption that there is at least one plane of $\mathrm{PG}(n, q)$ such that the geometry induced by $\mathcal{S}$ in that plane is a partial geometry (with incidence number α or β).

Binary codes of odd order Buekenhout–Metz unitals

G. L. Ebert

(joint work with K. L. Wantz)

Treating the points and secant lines of any unital as a $2-(q^3+1, q+1, 1)$ design, one can construct the linear code spanned by the characteristic vectors of the blocks over some prime field F_p. A well-known conjecture, first suggested by B. R. Andriamanalimanana in his Ph.D. thesis at Lehigh University (1979), states that in the case when the unital is classical (Hermitian), the dimension of this code is $q^3 - q^2 + q$ for any prime p that divides $q^2 - 1$. This conjecture now has been verified by machine for $q \leq 13$, but the general result remains unproven. It appears to be a difficult problem.

In this talk we consider the case when the unital is a non-classical Buekenhout–Metz embedded in $PG(2, q^2)$ for odd q. For a given odd prime power q, there is a unique (up to projective equivalence) Buekenhout–Metz unital which can be expressed as a union of q conics in $PG(2, q^2)$, mutually tangent at some point P_∞. It is the only Buekenhout–Metz unital, including the classical unital, which contains a conic of $PG(2, q^2)$, and the presence of the above q conics makes the determination of the $2-$rank ($p = 2$) of the associated binary linear code a more tractable problem, or at least it so appears. One easily obtains an upper bound of $q^3 - q + 1$ for this $2-$rank, and we conjecture that indeed this bound is the $2-$rank. We also have a conjectured basis consisting of certain weight-2 vectors associated with the above conics, thus implying that the minimum weight of this binary code is two. It should be noted that the minimum weight in the case of the classical unital is thought to be $q + 1$. Finally, we conjecture that for all remaining non-classical Buekenhout–Metz unitals embedded in $PG(2, q^2)$ for odd q (and there are many such inequivalent unitals), the $2-$rank is q^3 and thus the binary code is simply the code of all even–weight vectors.

Extensions of generalized product caps

Yves Edel

A *k–cap K* in $PG(n, q)$ is a set of k points, no three of which are collinear. The maximum value of k for which there exists a k–cap in $PG(n, q)$ is denoted by $m_2(n, q)$. Denote by $m_2^{aff}(n, q)$ the corresponding value in $AG(n, q)$. Aside of the cases $k = 2, 3$ or $q = 2$ the precise values of the numbers $m_2(n, q)$, $m_2^{aff}(n, q)$ are known only in the following cases: $m_2(4, 3) = m_2^{aff}(4, 3) = 20$, $m_2(5, 3) = 56$, $m_2^{aff}(5, 3) = 45$, and $m_2(4, 4) = 41$. Finding the exact value for $m_2(n, q)$ or $m_2^{aff}(n, q)$, $n \geq 4$, $q > 2$ seems to be a very hard problem. As an application of our new construction we obtain improved lower bounds on some values $m_2(n, 3)$. The smallest examples are a 1216–cap in $PG(9, 3)$ and a 6464–cap in $PG(11, 3)$.

A natural asymptotic problem is the determination of

$$\mu(q) = \limsup_{n\to\infty} \frac{\log_q(m_2(n, q))}{n} = \limsup_{n\to\infty} \frac{\log_q(m_2^{aff}(n, q))}{n}.$$

It is well known that $\frac{2}{3} \leq \mu(q) \leq 1$. The affine points of a family of caps in $PG(6, q)$ from yield the slightly better bound $\mu(q) \geq \frac{1}{6}\log_q(q^4 + q^2 - 1)$. No better lower bound seems to be known for general q. Exceptions are the ternary and quaternary cases. It follows from Calderbank and Fishburn that $\mu(3) \geq 0.7218\ldots$. The 120 affine points of the cap in $PG(5, 4)$ found by Glynn show that $\mu(4) \geq 0.6906\ldots$ The construction given here can be seen as a generalization of one of the constructions of Calderbank and Fishburn.

Although the construction works for general q all our applications are in the ternary case. Our constructions of caps in ternary affine spaces lead to a better bound for $\mu(3)$. We will show that $\mu(3) \geq 0.7248\ldots$.

This leaves us with two research problems. Firstly to improve the bound on $\mu(3)$ by finding better capsets, secondly to find good caps to which we can apply the construction for $q > 3$.

More information can be found at www.mathi.uni-heidelberg.de/∼yves

Some new results about directions

András Gács

(joint work with Tamás Szőnyi)

We discuss some new results about the possible number of directions a set of q points in $AG(2,q)$ can determine. We prove that if q is the square of an odd prime p, then besides lines (determining one direction), Baer subplanes (determining $p+1$ directions) and the graph of the function $x^{(q+1)/2}$ (determining $\frac{q+3}{2}$ directions), any set determines at least $q+\frac{1}{2}p$ directions. This is sharp, the construction is due to O. Polverino, T. Szőnyi and Zs. Weiner.

In the second part of the talk we show that a partial spread of size k in $PG(2,q)$ is equivalent to a set of $k-1$ points in $AG(2,q^2)$ not determining a Baer subline. Using this we construct maximal partial spreads of size $nq+1$ for any n such that $3\log(q) \leq n \leq q$.

The invariant graphs, tournaments and codes of projective planes of even order

D. G. Glynn

Starting from Rota's basis conjecture about having another way of dividing n^2 points of a matroid of rank into n bases (given one way of doing it), we saw about a year ago a way to construct invariants of nets of even order using digraphs constructed from the signs of their "von Staudt" projectivities. This has now been applied to projective planes of even order, and we shall summarize some of the more important results. For example, any projective plane of order $q \equiv 0 \pmod 4$ has an invariant tournament (or 2-graph, defined up to some switchings), and every projective plane of order $q \equiv 0 \pmod 4$ has an invariant graph (2-graph, based on the points or lines). In these graphs or tournaments the neighbourhoods of vertices are codewords associated with the binary code of the plane. In the case of $q \equiv 2 \pmod 4$ quite strong things can be said about the kind of tournaments that appear: for example we know the ranks of their adjacency matrices: they generate (close to) self-dual codes reminiscent of the duadic codes. This leads to strong conjectures about certain chains of codes in the binary antiflag-space of the projective planes.

In the case of any k-net of even order q, there is a basically unique (up to complements) graph or tournament with k vertices associated with it. Quite often these graphs are non-trivial and show a great deal of structure, but a conjecture is that the graph of any translation or dual translation plane net coming from any point or line is trivial. This says something quite strong about the Latin squares of order q that can be constructed from any three concurrent lines or collinear points in such a plane of order q.

Even though the graph at any point or line of a cyclic projective plane is trivial, the graph of the whole plane is definitely not, and this could turn out to be a useful new direction for this unfinished (perhaps "never-ending"?) chapter in finite geometry.

Restrictions on the size of partial ovoids in finite classical polar spaces and in the split Cayley hexagon

P. Govaerts
(joint work with L. Storme and H. Van Maldeghem)

A *partial ovoid* O of a finite classical polar space $\mathcal{P}$ is a set of points of $\mathcal{P}$ such that no generator of $\mathcal{P}$ contains two points of O. If every generator of $\mathcal{P}$ contains one element of O, then O is called an *ovoid*. A *partial ovoid* O of the split Cayley hexagon $\mathrm{H}(q)$ is a set of mutually opposite points of $\mathrm{H}(q)$. If it has size q^3+1 then it is called an *ovoid*. In both cases, the *deficiency* of a partial ovoid is the number of points it lacks to be an ovoid.

An extendability result for partial t-spreads of finite classical polar spaces can be used to exclude the existence of maximal partial ovoids of certain sizes of the generalised hexagon $\mathrm{H}(q)$: for large maximal partial ovoids of $\mathrm{H}(q)$, the deficiency is even. It also yields an extendability result for partial ovoids of $\mathrm{H}(3,q^2)$, which can be used to prove an upper bound for the size of partial ovoids of $\mathrm{H}(4,q^2)$. This upper bound can, with a technique that works for any finite classical polar space, be lifted to an upper bound for partial ovoids of $\mathrm{H}(2n,q^2)$, $n \geq 2$.

Theorem . *Let O be a partial ovoid of $\mathrm{H}(2n,q^2)$, $n \geq 2$. Then*

$$|O| < q^{2n+1} + 1 - 2/3(q^2-1)^{n-2}(2q+1).$$

New constructions of maximal arcs in Desarguesian projective planes

Nicholas Hamilton

A *maximal $\{q(n-1)+n;n\}$-arc* in a projective plane of order q is a subset of $q(n-1)+n$ points such that every line meets the set in 0 or n points for some $2 \leq n \leq q$. For such a maximal arc n is called the *degree.* If $\mathcal{K}$ is a maximal $\{q(n-1)+n;n\}-$arc, the set of lines external to $\mathcal{K}$ is a maximal $\{q(q-n+1)/n;q/n\}-$arc in the dual plane called the *dual* of $\mathcal{K}$.

In 1997, Ball, Blokhuis and Mazzocca proved using polynomial techniques that no odd order Desarguesian projective plane contains a non-trivial maximal arc. For even order Desarguesian projective planes there are several constructions known. There are the hyperovals (degree 2) and their duals, a construction from 1969 by R.H.F. Denniston, and one from 1974 by J.A. Thas.

Since it had been over 25 years since new maximal arcs, apart from hyperovals, had been found in Desarguesian projective planes it was beginning to look like there might not be others to find. Then earlier this year R. Mathon announced a new method of construction. The idea was to take a certain set of conics on a common nucleus and to define an addition on this set. A subset of conics is then *closed* if the sum of any two elements is in the set. Mathon then showed that any closed set of conics gives rise to a maximal arc. In particular, Denniston maximal arcs may be thought of as closed sets of conics. In the paper Mathon gave a very large number of constructions of closed sets of conics in $PG(2,32)$ and $PG(2,64)$, as well as infinite families of examples. The examples have many interesting and surprising properties. Many of the maximal arcs so constructed have trivial collineation stabiliser, and the Lunelli–Sce hyperoval in $PG(2,16)$ as well as the Cherowitzo hyperoval in $PG(2,32)$ may be thought of as duals of maximal arcs arising from closed sets of conics. In a subsequent paper Mathon and myself constructed more classes of closed sets of conics as well as obtaining results on the geometric structure of the maximal arcs and their collineation stabilisers. In a further paper I gave methods for testing when a closed set of conics what not of type Denniston, and gave another construction of closed sets of conics and so maximal arcs.

In this talk I will give a survey of the recent constructions of maximal arcs and their structure.

Designing the IEEE 802.12 transmission code

Jonathan Jedwab

In 1995 the Institute of Electrical and Electronic Engineers (IEEE) approved a new international standard for the transmission of data at 100Mbit/s. This standard specified a binary code mapping that was designed to satisfy multiple constraints simultaneously. Eight years after selecting this code and presenting its properties to the IEEE I have permission to explain the principles underlying its design, which include geometrical insight, combinatorial reasoning and computer search.

Extremal problems under dimension constraints

L.H. Khachatrian

(joint work with R. Ahlswede and H. Aydinian)

Let $[n] \triangleq \{1,\dots,n\}$, $2^{[n]} \triangleq \big\{A : A \subseteq [n]\big\}$, and $\binom{[n]}{w} \triangleq \{A \in 2^{[n]} : |A| = w\}$. We associate with each subset A its characteristic $(0,1)$–vector in $\mathbb{R}^n$. The corresponding notation for $(0,1)$–vectors is the following: $E(n) \triangleq \{0,1\}^n$ and $E(n,w) \triangleq \big\{x^n \in E(n) : x^n$ has w ones$\big\}$. The set–theoretical notions like intersection, union, antichain, etc. are extended to $(0,1)$–vectors in a natural way. The dimension of $\mathcal{S} \subset \mathbb{R}^n$ is defined by $\dim(\mathcal{S}) \triangleq \dim\operatorname{span}(\mathcal{S})$.

A generic extremal problem under dimension constraint is the following. Let $\mathcal{A} \subset E(n)$ satisfy some set–theoretical properties (say antichain, pairwise non–empty intersections, etc.). In addition we require $\mathcal{A}$ to have $\dim(\mathcal{A}) = k$ $(k \le n)$ and ask for the $\mathcal{A}$ with maximum or minimum size and with the given properties.

In this talk we consider several problems, results and conjectures in this direction.

Our first result is the determination of the function

$$M(n,k,w) \triangleq \max\big\{|\mathcal{U} \cap E(n,w)| : \mathcal{U} \text{ is a } k\text{–dimensional subspace of } \mathbb{R}^n\big\}.$$

We proved that (i) $M(n,k,w) = M(n,k,n-w)$; (ii) $M(n,k,w) = \binom{n}{w}$, if $2w \le k$; (iii) $M(n,k,w) = \binom{2k-2w}{k-w}2^{2w-k}$, if $k \le 2w \le 2k-2$; (iv) $M(n,k,w) = 2^{k-1}$, if $k-1 \le w \le n/2$.

The antichain problem under dimension constraint is to determine

$$A_k(n) \triangleq \max\big\{|\mathcal{F}| : \mathcal{F} \subset E(n), \dim(\mathcal{F}) \le k, \mathcal{F} \text{ is an antichain}\big\}.$$

Our conjecture, that $A_k(n) = M\left(n,k,\lfloor \frac{n}{2} \rfloor\right)$, is proved for $n \ge 2k-2$ or $k = n-1$.

The intersection problems are to determine $J_k(n,t) \triangleq \max\{|\mathcal{A}| : \mathcal{A} \subset E(n), \mathcal{A}$ is t–intersecting, $\dim(\mathcal{A}) = k\}$ and $J_k(n,w,t)$ (the same function when $\mathcal{A} \subset E(n,w)$). Let $\mathcal{K}(n,t) \subset 2^{[n]}$ denote the Katona set.

We conjecture that, for $t > n-k+1$,

$$J_k(n,t) = |\mathcal{K}(k-1, t-(n-k+1))| + |\mathcal{K}(k-1, t+(n-k+1))|,$$

if $2|(n+t)$ and

$$J_k(n,t) = 2|\mathcal{K}(k-2, t-(n-k+1))| + 2|\mathcal{K}(k-2, t+(n-k+1))|,$$

if $2 \nmid (n+t)$.

We show that (i) $J_k(n,t) = 2^{k-1}$, for $t \leq n-k+1$; (ii) $J_k(n,t) = 2^{k-2}$ for $n \geq \frac{3}{2}k - 1$, $t = n-k+2$; (iii) the conjecture holds for the cases (a) $t \geq 2(n-k)-1$, (b) $k \leq n \leq k+3$, (c) $n \geq k\sqrt{k}/\sqrt{2}$.

For $J_k(n,w,1)$ with $w \leq n/2$ we conjecture that $J_k(n,w,1) = M(n-1,k,w-1)$ and prove this when $k \leq w$ or $k < 2w \leq 2k-2$.

Transitive ovoids of the Hermitian surface

Gábor Korchmáros

(joint work with Antonello Cossidente)

Let $\mathcal{H}(3,q^2)$ be the (non–degenerate) Hermitian surface in PG$(3,q^2)$, and let $G \cong PGU(4,q^2)$ be the linear collineation group preserving $\mathcal{H}(3,q^2)$. An *ovoid* of $\mathcal{H}(3,q^2)$ is a set of point on $\mathcal{H}(3,q^2)$ which has exactly one common point with every generator of $\mathcal{H}(3,q^2)$. Every ovoid consists of q^3+1 pairwise non–conjugate points of $\mathcal{H}(3,q^2)$. An ovoid $\mathcal{O}$ is called *transitive* if the subgroup H of G preserving $\mathcal{O}$ acts transitively on the point–set of $\mathcal{O}$. A known example of a transitive ovoid is the *classical* ovoid consisting of all points in the intersection of $\mathcal{H}(3,q^2)$ with a non-tangent plane. The existence of many non–classical ovoids was pointed out by Payne and Thas. Nevertheless, transitive non–classical ovoids are known to exist only for q even. The following classification theorem was announced on the occasion of the 18^{th} British Combinatorial Conference held at the University of Sussex, 1 to 6 July, 2001.

Theorem . *For q even, there are exactly two projectively non–equivalent transitive ovoids of $\mathcal{H}(3,q^2)$.*

The theorem depends on both combinatorial results from finite geometry and deep theorems from finite group theory. The aim of the present talk is to outline of the proof.

Distance-regular geometries

Elisabeth Kuijken

(joint work with F. De Clerck)

A distance-regular geometry is a partial linear space of order (s,t) satisfying the following axioms, where d is the diameter of the point graph.

- There exist constants α_{2i-1}, $1 \leq i \leq d$, such that for any point-line pair (p,L) at mutual distance $2i-1$ in the incidence graph there are exactly α_{2i-1} points on L which are at distance $2i-2$ from p.

- There exist constants t_{2i}, $1 \leq i \leq d$, such that for any two points p and q at mutual distance $2i$ in the incidence graph there are exactly $t_{2i}+1$ lines through p which are at distance $2i-1$ from q.

Distance-regular geometries are generalizations of both (semi)partial geometries ($d=2$) and regular near-polygons ($\alpha_{2i-1}=1$ for all i, $1 \leq i \leq d$), and their point graphs are distance-regular. We discuss some infinite classes of proper distance-regular geometries, which are neither (semi)partial geometries nor regular near-polygons. Characterizations of these geometries follow from characterizations of their point graphs. Finally it is proved that the dual of a semipartial geometry $\mathrm{spg}(s,t,\alpha,\mu)$ with $t>s$ and $\mu=\alpha^2$ is a distance-regular geometry with $d=3$. As the only known examples of semipartial geometries with a distance-regular dual have $\mu=\alpha^2$, it is conjectured that this is a necessary condition as well.

On arcs in projective Hjelmslev planes over finite chain rings

Ivan N. Landjev

Let Π be a projective Hjelmslev plane over a chain ring R of cardinality q^2 and nilpotency index 2, that is, a ring with $R > \operatorname{Rad} R > (0)$ and $R/\operatorname{Rad} R \simeq \mathbb{F}_q$. A $(k,2)$-arc in Π is a set of points no three of which are collinear. Denote by $m_2(\Pi)$ the maximum possible cardinality of such arcs. It is known that

$$m_2(\Pi) \leq \begin{cases} q^2+q+1 & \text{for } q \text{ even;} \\ q^2 & \text{for } q \text{ odd .} \end{cases}$$

We prove, using Witt vectors, that $(4^\ell+2^\ell+1,2)$-arcs do exist in projective Hjelmslev planes over Galois rings of order 4^l and characteristic 4. Further, we prove that such arcs do not exist for chain rings of characteristic 2.

RWPRI and $(2T)_1$ flag-transitive linear spaces

Dimitri Leemans

(joint work with Francis Buekenhout and Paul-Olivier Dehaye)

The classification of finite flag-transitive linear spaces is almost complete. For the thick case, this result was announced by Buekenhout, Delandtsheer, Doyen, Kleidman, Liebeck and Saxl, and in the thin case (where the lines have 2 points), it amounts to the classification of 2-transitive groups, which is generally considered to follow from the classification of finite simple groups. These two classifications actually leave an open case, which is the so-called 1-*dimensional* case. In this talk, we work with two additional assumptions. These two conditions, namely $(2T)_1$ and Rwpri, are taken from another field of study in Incidence Geometry and allow us to obtain a complete classification. In particular, for the 1-dimensional case, we show that the only $(2T)_1$ flag-transitive linear spaces are $AG(2,2)$ and $AG(2,4)$, with $A\Gamma L(1,4)$ and $A\Gamma L(1,16)$ as respective automorphism groups.

Spreads in $H(q)$ and $1-$systems of $Q(6,q)$

G. Lunardon

(joint work with I. Cardinali, O. Polverino and R. Trombetti)

In this paper we prove that the projections along reguli of a translation spread of the classical generalized hexagon $H(q)$ are translation ovoids of $Q(4,q)$. As translation ovoids of $Q(4,q),\ q=2^r$, are elliptic quadrics, this forces that all translation spreads of $H(q), q=2^r$, are semi-classical. By representing $H(q)$ as a coset geometry, we obtain a characterization of a translation spread in terms of a set of points of $PG(3,q)$ which belong to imaginary chords of a twisted cubic and we construct a new example of semi-classical spread of $H(q), q=2^r$. Finally, we give a canonical construction of semi-classical locally Hermitian $1-$systems of $Q(6,q)$ which are spreads of $Q^-(5,q)$, proving that there exist semi-classical non-Hermitian locally Hermitian spreads of $Q^-(5,q)$.

On 1-systems of $Q(6,q)$, q even

Deirdre Luyckx

(joint work with J. A. Thas)

A 1-system $\mathcal{M}$ of the parabolic quadric $Q(6,q)$ in $\mathsf{PG}(6,q)$ is a set $\{L_0, L_1, \ldots, L_{q^3}\}$ consisting of q^3+1 lines on $Q(6,q)$ having the property that the tangent space of $Q(6,q)$ at L_i has no point in common with $(L_0 \cup L_1 \cup \ldots \cup L_{q^3}) \setminus L_i$, $i=0,1,\ldots,q^3$. We will discuss a method to construct new locally hermitian 1-systems of $Q(6,q)$, q even; for q odd, this was already done in previous work. One of these 1-systems is the spread $\mathcal{S}_{[\delta]}$ of the hexagon $\mathsf{H}(q)$, $q=2^{2e}$, which was discovered independently by A. Offer and G. Lunardon and our method yields a geometric way to construct $\mathcal{S}_{[\delta]}$. Also, we can classify these new 1-systems as the only ones on $Q(6,q)$ which are locally hermitian and semiclassical, but not contained in a 5-dimensional subspace.

Our class of new 1-systems has beautiful applications in a wide range of fields. By projection from the nucleus of $Q(6,q)$ onto a $\mathsf{PG}(5,q)$ not containing the nucleus, every 1-system of $Q(6,q)$, q even, yields a 1-system of $W_5(q)$. Thus we have found a new class of 1-systems of $W_5(q)$. It is known that the set of points on the lines of a 1-system of $W_5(q)$ has two intersection numbers with respect to hyperplanes and consequently every such 1-system defines a two-weight code and a strongly regular graph. It has also been shown that every 1-system of $W_5(q)$ is an SPG-regulus and hence yields a semipartial geometry. So our class of 1-systems provides us with examples of two-weight codes, strongly regular graphs and semipartial geometries. Concerning the semipartial geometries, we can show that some of them are new, but for the two-weight codes and the strongly regular graphs, this question has to be investigated further.

Group algebras and expanders

R. Meshulam

(joint work with A. Wigderson)

Expander graphs are essential tools in a variety of combinatorial, algorithmic and coding theoretic problems. We discuss constructions of expanders which utilize certain group algebras over finite fields.

Let G be a finite group and let p be a prime such that $(p, |G|) = 1$. A subset A of the group algebra $\mathbb{F}_p[G]$ is *$\delta-$balanced* if all non-trivial Fourier coefficients of A are bounded by $1 - \delta$.

We give a (nearly sharp) representation theoretic condition which guarantees that $\mathbb{F}_p[G]$ has a few G-orbits whose union A is δ-balanced. Let $r_d(G; \mathbb{F})$ denote the number of irreducible representations of G over $\mathbb{F}$ of dimension at most d and let

$$m(G; \mathbb{F}) = \max_{d \geq 1}(\log_2 r_d(G; \mathbb{F}))/d \ .$$

Theorem 1. *For any $\delta < \frac{1}{2}$, there exist $s = O(\frac{1}{(1-2\delta)^2}(m(G; \mathbb{F}_p) + \log p))$ elements $h_1, \ldots ,$ $h_s \in \mathbb{F}_p[G]$ such that the multiset $A = \cup_{i=1}^{s} Gh_i \subset F_p[G]$ is δ-balanced.*

One consequence of Theorem 1 is a simple construction of asymptotically good codes which uses relatively few randomized bits. For other applications we need an exponential bound on the number of $d-$dimensional representations in terms of the Kazhdan Constant κ of a generating set $S \subset G$.

Theorem 2. *If G is an M_ℓ-group, that is, any complex irreducible representation of G is induced from a representation of dimension at most ℓ of some subgroup of G, then*

$$r_d(G; \mathbb{C}) \leq \left(\frac{1}{\kappa}\right)^{O(\ell|S|d)} .$$

Our main application of Theorems 1 and 2 is a new iterative construction of expanding Cayley graphs of nearly constant degree.

Large caps of the Klein quadric

Klaus Metsch

A cap of a point line incidence structure $\mathcal{I}$ is a set of points no three of which are collinear in $\mathcal{I}$. The talk discusses large caps of the Klein quadric $Q^+(5, q)$. If one considers $Q^+(5, q)$ embedded in $PG(5, q)$, then a cap of $Q^+(5, q)$ is also a cap of $PG(5, q)$, since the lines of $PG(5, q)$ that do not belong to $Q^+(5, q)$ meet $Q^+(5, q)$ in at most two points.

An easy counting argument shows that every cap of $Q^+(5, q)$ satisfies $|C| \leq (q^2+1)(q+1)$ for odd q, and $|C| \leq (q^2 + 1)(q + 2)$ for even q.

Glynn constructed in 1988 caps of size $(q^2 + 1)(q + 1)$ of $Q^+(5, q)$ for all q. While this answers the question of the cardinality of a largest cap for odd q, it is not known whether $Q^+(5, q)$, q even, has a cap of size $(q^2 + 1)(q + 1)$. Ebert, Szőnyi and Metsch constructed caps of size $(q^2 + 1)(q + 2) - q - 1$ of $Q^+(5, q)$ for even q. They also showed for even q that every cap of C of $Q^+(5, q)$ with $|C| > (q^2 + 1)(q + 2) - q - 1$ is contained in a cap of size $(q^2 + 1)(q + 2)$.

The talk presents these examples and results as well as the following new results for caps of $Q^+(5, q)$ for odd q: Every cap C with $|C| > q^3 + q^2 + 2$ is contained in a cap of size $(q^2 + 1)(q + 1)$. Also, there exists caps of size $q^3 + q^2 + 1$ that are not contained in larger caps. The existence of a cap of size $q^3 + q^2 + 2$ of $Q^+(5, q)$, q odd, that is not contained in a larger cap of $Q^+(5, q)$ is an open problem.

Cyclotomy, geometry, and perfect sequences

Alexander Pott

(joint work with Gohar Kyureghyan)

Let

$$a = (a_i)_{i=0}^{N-1}$$

be a ±1-vector. We define the correlation coefficients

$$C_t(a) := \sum_{i=0}^{N-1} a_i a_{i+t}$$

where the indices are taken modulo N. We consider the problem to construct vectors where

$$\max_{t \in \{1,\dots,N-1\}} |C_t(a)| \qquad (*)$$

is small. It is well known that the correlation coefficients translate into intersection properties of the sets

$$D := \{i : a_i = 1\}$$

and

$$D + t := \{i + t : i \in D\}.$$

More precisely,

$$C_t(a) = N - 4(|D| - |D \cap (D+t)|).$$

In the talk, we will discuss sequences where the maximum in $(*)$ is ≤ 4 (*perfect sequences*). In particular, we discuss new constructions using *cyclotomy* and constructions related to classical difference sets, hence classical *geometry.*

Asymptotic nonexistence of dihedral difference sets

Bernhard Schmidt

(joint work with Ka Hin Leung)

Difference sets in *cyclic* groups exist in abundance, for instance, Singer, quadratic residue, and twin prime difference sets. Remarkably, the situation changes dramatically if the group structure is changed a little: It is conjectured that no nontrivial difference sets exist in *dihedral* groups. In this talk, the following asymptotic result will be explained.

For any primes $p_1, \dots, p_s$ there are only finitely many products of powers of the p_i which can be orders of dihedral difference sets.

The main difficulty of the proof is that it has to work for all possible parameters of dihedral difference sets. At the end, it boils down to making an apparently completely intractable number–theoretic condition made tractable by complementary combinatorial arguments.

On multiple blocking sets in Galois planes

L. Storme

(joint work with A. Blokhuis and T. Szőnyi)

A *t-fold blocking set* B in $\mathrm{PG}(2,q)$ is a set of points such that every line of $\mathrm{PG}(2,q)$ intersects B in at least t points.

In $\mathrm{PG}(2,q)$, q square, the Baer subplanes are the smallest 1-fold blocking sets not containing a line, and in $\mathrm{PG}(2,q)$, q a cube (but not a square) power, the two smallest 1-fold blocking sets, not containing a line, are projected subgeometries $\mathrm{PG}(3,q^{1/3})$.

In 1999, the authors studied t-fold blocking sets in $\mathrm{PG}(2,q)$, q square, of cardinality $t(q+1)+c$, where $t < q^{1/4}/2$ and where $c < q^{2/3}$. It was proved that such t-fold blocking sets contain t pairwise disjoint Baer subplanes.

In 1997, Lovász and Szőnyi proved that minimal t-fold blocking sets in $\mathrm{PG}(2,q)$, $q=p^h$, p prime, of size $t(q+1)+c$ with t and c satisfying some conditions, intersect every line in $t \pmod{p}$ points.

Using this latter result, for t-fold blocking sets in $\mathrm{PG}(2,q)$, q square, whose cardinality satisfies a certain upper bound, we prove that they contain t pairwise disjoint Baer subplanes, or $t-1$ pairwise disjoint Baer subplanes and one projected $\mathrm{PG}(3,q^{1/3})$. For t-fold blocking sets whose cardinality satisfies a larger upper bound, we prove that they are the disjoint union of a number t_0 of Baer subplanes and a $(t-t_0)$-fold blocking set, with $0 \leq t_0 < t$.

Small multiple blocking sets in PG$(4,q^2)$ with respect to planes

Peter Sziklai

(joint work with S. Ferret, L. Storme and Zs. Weiner)

The smallest 1-fold blocking sets in $\mathrm{PG}(4,q^2)$, with respect to planes, are well-known already: planes; cones with a Baer-subplane as a base and a point as vertex, contained in a 3-subspace; subgeometries PG(4,q). Our result extends this classification for t-fold blocking sets (t small), which, under some bound, happen to be disjoint unions of the previous examples. To achieving this we had to generalize previous theorems on planar blocking sets (in the general form multiple points are allowed as well) and also to extend the result about $\equiv 1 \pmod{p}$ -intersections of 1-fold blocking sets (with respect to k-dimensional subspaces in $\mathrm{PG}(n,q)$), by T. Szőnyi and Zs. Weiner.

A Lenz–Barlotti classification for finite generalized quadrangles

Koen Thas

In *Finite Geometries*, P. Dembowski wrote that an alternative approach to the study of projective planes began with the paper *Homogeneity of projective planes* by R. Baer (1942), in which the close relationship between Desargues' theorem and the existence of central collineations was pointed out. Baer's notion of (p,L)-transitivity, corresponding to this relationship, proved to be extremely fruitful; it provided a better understanding of coordinate structures and it led eventually to the only coordinate-free classification of projective planes existing today, namely the classification by H. Lenz in *Kleiner Desarguesscher Satz und Dualität in projektiven Ebenen* (1954) and A. Barlotti in *Sulle possibili configurazioni del sistema delle coppie punto-retta* $(A,\,a)$ *per cui un piano grafico risulta* $(A,\,a)$*-transitivo* (1958). Due to deep discoveries in finite group theory, the analysis of this classification has been particularly penetrating for finite projective planes in recent years.

For generalized quadrangles (GQ's), J.A. Thas and H. Van Maldeghem gave a (first) definition of Desargues configurations and proved a result analogous to the theorem of Baer for projective planes. Then H. Van Maldeghem, J.A. Thas and S.E. Payne gave a second approach to the problem by introducing the notion of (p,L)*-transitivity* (with pIL)

for GQ's. They then proved that a GQ is Moufang if and only if it is (p, L)-transitive for all flags (p, L). As a geometrical counterpart to (p, L)-transitivity, they introduced the notion of a (p, L)-*Desarguesian generalized quadrangle*, and they proved that a finite generalized quadrangle is (p, L)-Desarguesian if and only if it is (p, L)-transitive. Also, by a celebrated theorem of J.A. Thas, S.E. Payne and H. Van Maldeghem, every half Moufang GQ is automatically Moufang, and hence classical by the deep group-theoretical result(s) of P. Fong and G.M. Seitz.

However, despite these promising results, a 'good' classification based on subconfigurations of flags (p, L), respectively panels (p, L, q), for which the generalized quadrangle is (p, L)-transitive, respectively (p, L, q)-transitive (which is defined in a similar way as (p, L)-transitivity), seems (quite) far away and would yield many open classes very hard to deal with. We present the following alternative.

A line L of a generalized quadrangle $\mathcal{S}$ is an *axis of symmetry* if it is regular, and if there is a pair of distinct points (p, q) both incident with L for which the generalized quadrangle is (p, L, q)-transitive. In our talk, we discuss a classification of generalized quadrangles based on the possible subconfigurations of axes of symmetry.

As an application of the classification presented here, we were able to solve a recent conjecture of W.M. Kantor.

Formulas for the number of Steiner triple and quadruple systems of low 2-rank

Vladimir D. Tonchev

Doyen, Hubaut, and Vandensavel used methods from finite geometry to derive a lower bound on the 2-rank of a Steiner triple system and proved that the classical Steiner triple system of the lines in binary projective space is the unique (up to isomorphism) system of minimum 2-rank. Teirlinck proved a similar bound for Steiner quadruple systems, in which case the classical system of the planes in a binary affine space is the only one of minimum 2-rank. The results of Doyen, Hubaut, Vandensavel and Teirlinck were extended by Assmus, who proved that all Steiner triple or quadruple systems with the same number of points and the same 2-rank span equivalent binary codes. In addition, Assmus gave an explicit description of the code for any given rank, and determined its automorphism group. Using these results, the author found recently an explicit formula for the total number of distinct Steiner triple systems on $2^n - 1$ whose 2-rank is greater by one than the the minimum $2^n - n - 1$, as well as a formula for the number of distinct Steiner quadruple systems on 2^n points of 2-rank $2^n - n$. Namely, the number of distinct Steiner triple systems on $2^n - 1$ points of 2-rank $2^n - n$ is given by the formula

$$\frac{(2^n-1)!(2^{\frac{(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^{n-1}-n})}{2^{2^{n-1}-1}(2^{n-1}-1)(2^{n-1}-2)\dots(2^{n-1}-2^{n-2})},$$

while the total number of Steiner quadruple systems on 2^n points of 2-rank $2^n - n$ is given by the formula

$$\frac{(2^n)!(2^{\frac{2^{n-3}(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^{n-1}-n})}{2^{2^{n-1}+\frac{n(n-1)}{2}}(2^{n-1}-1)(2^{n-2}-1)\dots(2^2-1)}.$$

Apart from the classical Steiner triple and quadruple systems of minimum 2-rank and their counterparts at the other end of geometric dimension, namely the designs of the hyperplanes in a binary projective or affine space, where the designs are known to be unique, this appears to be the first occasion where a formula for the exact number of all designs belonging to an infinite family is known. These formulas resemble the formula for the number of all k-dimensional subspaces of a given n-dimensional space over a finite field, or the number of isotropic subspaces of given dimension. The latter formula has been widely used for the classification of self-dual codes in coding theory. The formulas for the number of Steiner triple and quadruple systems can be used for the classification of Steiner systems up to isomorphism. As an illustration, the classification of Steiner quadruple systems on 16 points and 2-rank 12 will be given. The formulas can be used also for deriving bounds on the number of isomorphism classes of Steiner systems of the given rank. In particular, it is shown that the number of non-isomorphic Steiner triple or quadruple systems of 2-rank $2^n - n$ grows exponentially.

Some remarks on Steiner systems

HENDRIK VAN MALDEGHEM

I will make three remarks on Steiner systems, based on Table A5.1 in Beth, Jungnickel and Lenz, Design Theory, Volume 2, second edition (1999). First, I will extend and refine the class KW, also bringing automorphisms into play; then I will embed the classical hexagons of order (q,q) into new Steiner systems and show that for one class of these, the automorphism group is precisely the group $\mathrm{Aut}G_2(q)$ (I will mention an application of this). I also discuss the question whether it is possible to embed the dual split Cayley hexagons into Steiner systems such that the blocks of the systems are all traces of points in the hexagon (this gives rise to nontrivial geometric questions in Galois spaces). Finally, I will state a general construction method for Steiner systems out of old ones and give some examples.

Edited by J.W. P. Hirschfeld

Participants

Prof. Dr. Rudolf Ahlswede
ahlswede@mathematik.uni-bielefeld.de
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld

Prof. Dr. Laura Bader
laura.bader@dma.unina.it
Dipartimento di Matematica e Appl.
Universita di Napoli
Complesso Monte S. Angelo
Via Cintia
I-80126 Napoli

Dr. Simeon Ball
simeon@maths.qmw.ac.uk
simeonsan@hotmail.com
School of Mathematical Sciences
Queen Mary College
University of London
Mile End Road
GB-London, E1 4NS

Prof. Dr. Thomas Beth
eiss_office@ira.uka.de
Institut für Algorithmen und
Kognitive Systeme
Universität Karlsruhe
Am Fasanengarten 5, Geb. 5034
76131 Karlsruhe

Dr. Jürgen Bierbrauer
jbierbra@mtu.edu
Dept. of Math. Sciences
Michigan Technological University
1400 Townsend Drive
Houghton, MI 49931
USA

Prof. Dr. Aart Blokhuis
aartb@win.tue.nl
Department of Mathematics
Technische Universiteit Eindhoven
Postbus 513
NL-5600 MB Eindhoven

Prof. Dr. Arrigo Bonisoli
bonisoli.arrigo@unimo.it
Dip. di Scienze Soc. Cogn. Quant.
Universita degli Studi di Modena
e Reggio Emilia
Via Giglioli Valle
I-42100 Reggio Emilia

Prof. Dr. Andries E. Brouwer
aeb@cwi.nl
Department of Mathematics
Technische Universiteit Eindhoven
Postbus 513
NL-5600 MB Eindhoven

Prof. Dr. Matthew Brown
mbrown@cage.rug.ac.be
Dept. of Pure Mathematics and
Computer Algebra
Ghent University
Krijgslaan 281
B-9000 Gent

Prof. Dr. Francis Buekenhout
fbueken@ulb.ac.be
Dept. de Mathematiques
Universite Libre de Bruxelles
CP 216 Campus Plaine
Bd. du Triomphe
B-1050 Bruxelles

Prof. Dr. Frank De Clerck
fdc@cage.rug.ac.be
Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

Prof. Dr. Jean Doyen
jdoyen@ulb.ac.be
Dept. de Mathematiques
Universite Libre de Bruxelles
CP 216 Campus Plaine
Bd. du Triomphe
B-1050 Bruxelles

Prof. Dr. Gary Ebert
ebert@math.udel.edu
Department of Mathematical Sciences
University of Delaware
501 Ewing Hall
Newark, DE 19716-2553
USA

Dr. Yves Edel
y.edel@mathi.uni-heidelberg.de
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg

Prof. Dr. Andras Gacs
gacs@cs.elte.hu
Department of Computer Science
Eötvös University
Pazmany Peter setany 1/C
H-1117 Budapest

Prof. Dr. David Glynn
d.glynn@math.canterbury.ac.nz
Dept. of Mathematics and Statistics
University of Canterbury
Private Bag 4800
Christchurch 1
NEW ZEALAND

Patrick Govaerts
pg@cage.rug.ac.be
Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

Dr. W. Willem H. Haemers
haemers@kub.nl
Department of Econometrics
Tilburg University
P. O. Box 90153
NL-5000 LE Tilburg

Prof. Dr. Nicholas Hamilton
nick@cage.rug.ac.be
Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

Prof. Dr. Raymond Hill
r.hill@salford.ac.uk
Dept. of Mathematics
University of Salford
GB-Salford M5 4WT

Prof. Dr. James W.P. Hirschfeld
jwph@sussex.ac.uk
School of Mathematical Sciences
University of Sussex
GB-Brighton BN1 9QH

Dr. Jonathan Jedwab
jonathan-jedwab@yahoo.co.uk
c/o 5 Shamrock Way
Southgate
GB-London N14 5SB

Prof. Dr. Dieter Jungnickel
jungnickel@math.uni-augsburg.de
Institut für Mathematik
Universität Augsburg
86135 Augsburg

Prof. William M. Kantor
kantor@math.uoregon.edu
Dept. of Mathematics
University of Oregon
Eugene, OR 97403-1222
USA

Prof. Dr. Jennifer D. Key
keyj@math.clemson.edu
Dept. of Mathematical Sciences
Clemson University
Martin Hall
Clemson, SC 29634-0975
USA

Prof. Dr. Levon H. Khachatrian
lk@mathematik.uni-bielefeld.de
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33501 Bielefeld

Prof. Dr. Gabor Korchmaros
korchmaros@unibas.it
Dipartimento di Matematica
Universita degli Studi
della Basilicata
Contrada Macchia Romana
I-85100 Potenza

Elisabeth Kuijken
ekuijken@cage.rug.ac.be
Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

Prof. Dr. Ivan Landjev
ivan@moi.math.bas.bg
Institute of Mathematics
ul. Acad. G. Bonchev
block 8
1113 Sofia
BULGARIA

Dr. Michel Lavrauw
lavrauw@win.tue.nl
Dept. of Pure Mathematics and
Computer Algebra
Ghent University
Krijgslaan 281
B-9000 Gent

Dr. Dimitri Leemans
dleemans@ulb.ac.be
Dept. de Mathematiques
Universite Libre de Bruxelles
CP 216 Campus Plaine
Bd. du Triomphe
B-1050 Bruxelles

Prof. Dr. Guglielmo Lunardon
lunardon@unina.it
Dipartimento di Matematica e Appl.
Universita di Napoli
Complesso Monte S. Angelo
Via Cintia
I-80126 Napoli

Deirdre Luyckx
dluyckx@cage.rug.ac.be
Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

Prof. Dr. Hendrik Van Maldeghem
`huv@cage.rug.ac.be`
Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

Dr. Roy Meshulam
`meshulam@math.technion.ac.il`
Department of Mathematics
Technion
Israel Institute of Technology
Haifa 32000
ISRAEL

Dr. Klaus Metsch
`klaus.metsch@math.uni-giessen.de`
Mathematisches Institut
Universität Gießen
Arndtstr. 2
35392 Gießen

Prof. Dr. Stanley E. Payne
`spayne@carbon.cudenver.edu`
Department of Mathematics
University of Colorado at Denver
P.O.Box 173364; Campus Box 170
1250 14th St., Ste. 600
Denver, CO 80217-3364
USA

Prof. Dr. Tim Penttila
`penttila@maths.uwa.edu.au`
Department of Mathematics & Stat.
University of Western Australia
35 Stirling Highway
Crawley, WA 6009
AUSTRALIA

Prof. Dr. Alexander Pott
`alexander.pott@mathematik.uni-magdeburg.de`
Fakultät für Mathematik
Otto-von-Guericke-Universität
Magdeburg
Postfach 4120
39016 Magdeburg

Prof. Dr. Marialuisa J. de Resmini
`resmini@mat.uniroma1.it`
Dipartimento di Matematica
Universita degli Studi di Roma I
"La Sapienza"
Piazzale Aldo Moro, 2
I-00185 Roma

Dr. Bernhard Schmidt
`bernhard.schmidt@math.uni-augsburg.de`
Institut für
Angewandte Mathematik II
Universität Augsburg
86135 Augsburg

Prof. Dr. Leo Storme
`ls@cage.rug.ac.be`
Dept. of Pure Mathematics and
Computer Algebra
Ghent University
Krijgslaan 281
B-9000 Gent

Dr. Peter Sziklai
`sziklai@cs.elte.hu`
Department of Computer Science
Eötvös University
Pazmany Peter setany 1/C
H-1117 Budapest

Prof. Dr. Tamas Szönyi
`szonyi@cs.elte.hu`
Department of Computer Science
Eötvös University
Pazmany Peter setany 1/C
H-1117 Budapest

Prof. Dr. Joseph A. Thas
jat@cage.rug.ac.be
Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

Koen Thas
kthas@cage.rug.ac.be
Department of Pure Mathematics and
Computer Algebra
Ghent University
Galglaan 2
B-9000 Gent

Prof. Dr. Vladimir D. Tonchev
tonchev@mtu.edu
Dept. of Math. Sciences
Michigan Technological University
1400 Townsend Drive
Houghton, MI 49931
USA

Zsuzsa Weiner
weiner@cs.elte.hu
Department of Computer Science
Eötvös University
Pazmany Peter setany 1/C
H-1117 Budapest