Finite Geometries, Varieties and Codes

Joseph A. Thas

Abstract. In recent years there has been an increasing interest in finite projective spaces, and important applications to practical topics such as coding theory and design of experiments have made the field even more attractive. It is my intention to mention some important and elegant theorems, to say something about the used techniques and the relation with other fields, and to mention some open problems. First some characterizations of particular pointsets in the projective space $\mathrm{PG}(n,q), n \geq 2$, over $\mathrm{GF}(q)$ will be given, where, from the beginning, it is assumed that the pointset is contained in $\mathrm{PG}(n,q)$. A second approach is that where the object is described as an incidence structure satisfying certain properties; here the geometry is not a priori embedded in a projective space. This approach will be illustrated with some theorems on inversive planes, polar spaces and Shult spaces. Finally, there is a section on k-arcs in $\mathrm{PG}(n,q)$ and on linear Maximum Distance Separable codes, where the interplay between finite projective geometry, coding theory and algebraic geometry is particularly present. In an appendix an example of brand new research in the field is given.

1991 Mathematics Subject Classification: 51E15, 51E20, 51E21, 51E25, 51A50, 51B10, 05B05, 05B25, 94B27
Keywords and Phrases: Finite Geometries, Varieties, Codes, Designs, k-Arcs, Polar Spaces

1 Introduction and history

In recent years there has been an increasing interest in finite projective spaces (or Galois spaces), and important applications to practical topics such as coding theory and design of experiments have made the field even more attractive. Basic works on the subject are “Projective Geometries over Finite Fields”, “Finite Projective Spaces of Three Dimensions” and “General Galois Geometries”, the first two volumes being written by Hirschfeld [1979,1985] and the third volume by Hirschfeld and Thas [1991]; the set of three volumes was conceived as a single entity. We also mention the “Handbook of Incidence Geometry: Buildings and Foundations”, edited in 1995 by Buekenhout, which covers an enormous amount of material. In 1998 the second edition of the first volume by Hirschfeld appeared; here the author writes the following on the history of finite geometry (for bibliographical details, see Hirschfeld).

"The first actual reference or near-reference on finite geometry is von Staudt's Beiträge (1856). It contains countings of real and complex points of a projective space, as if they were points over $\mathrm{GF}(q)$ and $\mathrm{GF}(q^2)$; only dimensions two and three are considered. Then Fano (1892) defined $\mathrm{PG}(n,p)$ synthetically, while more than a decade later Hessenberg (1903) did it analytically. Next, Veblen and Bussey (1906) gave the first systematic account of $\mathrm{PG}(n,q)$ for any n and q; really, it may be noted that the group $\mathrm{PGL}(n+1,q)$ of projectivities, which is implicit in the geometry, goes back to Jordan (1870). At the same time and later, Dickson was investigating modular invariants, curves and other parts of algebraic geometry over a finite field. The link with statistics was developed by Bose (1947); earlier, Fisher (1942) had produced an experimental design from a finite plane, with Yates (1935) already having made the connection with block designs".

In his investigations on graph theory, design theory and finite projective spaces, the statistician Bose mainly used pure combinatorial arguments in combination with some linear algebra. Another great pioneer in finite projective geometry was the Italian geometer Beniamino Segre. His celebrated result of 1954 stating that in the projective plane $\mathrm{PG}(2,q)$ over the Galois field $\mathrm{GF}(q)$ with q odd, every set of $q+1$ points, no three of which are collinear, is a conic, stimulated the enthusiasm of many young geometers. The work of Segre and his followers has many links with error-correcting codes and with maximum distance separable codes, in particular. Finally, the fundamental and deep work in the last four decades on polar spaces, generalized polygons, and, more generally, incidence geometry, in the first place by Tits, but also by Shult, Buekenhout, Kantor and others, gave a new dimension to finite geometry.

Here I will state some important and elegant theorems, say something about the used techniques and the relation with other fields, and mention some open problems.

2 The geometry of $\mathrm{PG}(2,q)$

First I will consider the geometry of $\mathrm{PG}(2,q)$, that is, the projective plane over the finite field $\mathrm{GF}(q)$. To begin with, it is the purpose to show how classical algebraic curves can be characterized in pure combinatorial terms. I will illustrate this with a theorem on conics and one on Hermitian curves.

A k-arc of $\mathrm{PG}(2,q)$ is a set of k points of $\mathrm{PG}(2,q)$ no three of which are collinear. Then clearly $k \leq q+2$. By Bose [1947], for q odd, $k \leq q+1$. Further, any nonsingular conic of $\mathrm{PG}(2,q)$ is a $(q+1)$-arc. It can be shown that each $(q+1)$-arc K of $\mathrm{PG}(2,q)$, q even, extends to a $(q+2)$-arc $K \cup \{x\}$ (see, e.g., Hirschfeld [1998], p.177); the point x, which is uniquely defined by K, is called the *kernel* or *nucleus* of K. The $(q+1)$-arcs of $\mathrm{PG}(2,q)$ are called *ovals.* The following celebrated theorem is due to Segre [1954].

Theorem 1. *In* $\mathrm{PG}(2,q)$, *q odd, every oval is a nonsingular conic.*

For q even, Theorem 1 is valid if and only if $q \in \{2,4\}$; see e.g., Thas [1995a].

A *Hermitian arc* or *unital* H of $\mathrm{PG}(2,q)$, with q a square, is a set of $q\sqrt{q}+1$ points of $\mathrm{PG}(2,q)$ such that any line of $\mathrm{PG}(2,q)$ intersects H in either 1 or $\sqrt{q}+1$ points. The lines intersecting H in one point are called the *tangent lines* of H. At each of its points H has a unique tangent line. Let ζ be a unitary polarity of $\mathrm{PG}(2,q)$, q a square. Then the absolute points of ζ, that is, the points x of $\mathrm{PG}(2,q)$ which lie on their image x^ζ, form a Hermitian arc. Such a Hermitian arc is called a *nonsingular Hermitian curve.* For any nonsingular Hermitian curve coordinates in $\mathrm{PG}(2,q)$ can always be chosen in such a way that it is represented by the polynomial equation

$$X_0^{\sqrt{q}+1}+X_1^{\sqrt{q}+1}+X_2^{\sqrt{q}+1}=0.$$

In 1992 the following theorem was obtained, solving a longstanding conjecture on Hermitian curves; see Thas [1992a].

Theorem 2. *In* $\mathrm{PG}(2,q)$, *q a square, a Hermitian arc H is a nonsingular Hermitian curve if and only if tangent lines of H at collinear points are concurrent.*

Theorems 1 and 2 are pure combinatorial characterizations of algebraic curves. Now we give a characterization, due to Hirschfeld, Storme, Thas and Voloch [1991], in terms of algebraic curves, that is, we will assume from the beginning that our pointset is an algebraic curve.

Theorem 3. *In* $\mathrm{PG}(2,q)$, *q a square and $q\neq 4$, any algebraic curve of degree $\sqrt{q}+1$, without linear components, and with at least $q\sqrt{q}+1$ points in* $\mathrm{PG}(2,q)$, *must be a nonsingular Hermitian curve.*

To prove the previous theorems, classical projective geometry, finite algebraic geometry, finite field theory and counting arguments were used. A proof of a completely different nature was used to solve a conjecture from 1975 on the following easily defined pointsets in $\mathrm{PG}(2,q)$.

In $\mathrm{PG}(2,q)$ any nonempty set of k points may be described as a $(k;m)$-arc, where m ($m\neq 0$) is the greatest number of collinear points in the set. For given q and m ($m\neq 0$), k can never exceed $mq-q+m$, and a $(mq-q+m;m)$-arc is called a *maximal arc*. Equivalently, a maximal arc may be defined as a nonempty set of points meeting every line in just m points or in none at all. Trivial maximal arcs are the plane $\mathrm{PG}(2,q)$ itself ($m=q+1$), the affine plane $\mathrm{AG}(2,q)$ obtained by deleting a line L from $\mathrm{PG}(2,q)$ ($m=q$), and a single point ($m=1$). If K is a $(mq-q+m;m)$-arc of $\mathrm{PG}(2,q)$, where $m\leq q$, then it is easy to show that the set

$$K'=\{\text{lines } L \text{ of } \mathrm{PG}(2,q)\ :\ L\cap K=\emptyset\}$$

is a $(q(q-m+1)/m;q/m)$-arc (i.e., a maximal arc) of the dual plane. Hence, if the plane $\mathrm{PG}(2,q)$ contains a $(mq-q+m;m)$-arc, $m\leq q$, then it also contains a $(q(q-m+1)/m;q/m)$-arc. It follows that a necessary condition for the existence of a maximal arc, with $m\leq q$, is that m should be a factor of q.

In 1969 Denniston proves that the condition $m|q$ does suffice in the case of any plane $\mathrm{PG}(2, 2^h)$, and in 1975 Thas proves that in $\mathrm{PG}(2, q)$, with $q = 3^h$ and $h > 1$, there are no $(2q+3;3)$-arcs and no $(q(q-2)/3; q/3)$-arcs. The longstanding conjecture that in $\mathrm{PG}(2, q)$, q odd, the only maximal arcs are the trivial ones, was proved just recently by Ball, Blokhuis and Mazzocca; see Ball, Blokhuis and Mazzocca [1997] and Ball and Blokhuis [1998].

Theorem 4. *In* $\mathrm{PG}(2, q)$, *q odd, there is no maximal* $(qm - q + m; m)$*-arc with* $1 < m < q$.

In the proof the point (x, y) of the affine plane $\mathrm{AG}(2, q)$ is identified with the element $x + \alpha y$ of $\mathrm{GF}(q^2) = \mathrm{GF}(q)(\alpha)$. Then, assuming the existence of a nontrivial maximal arc in $\mathrm{AG}(2, q), q$ odd, polynomials over $\mathrm{GF}(q^2)$ are defined the clever manipulation of which leads to a contradiction.

3 The geometry of $\mathrm{PG}(n, q)$, $n \geq 3$

If $\mathcal{V}$ is a "classical" algebraic variety in $\mathrm{PG}(n, q)$ (or one of its projections), $n \geq 3$, e.g., a quadric, a Hermitian variety, a Veronese variety, then a first approach is to characterize $\mathcal{V}$ either as a subset of $\mathrm{PG}(n, q)$ which intersects certain subspaces of $\mathrm{PG}(n, q)$ in sets with cardinalities in some range or as a subset of $\mathrm{PG}(n, q)$ whose points satisfy certain linear independence conditions. One characterization of the first type will be given here, while in Section 4 we will show how (subsets of) normal rational curves can be characterized by one simple independence condition on the points.

A *nonsingular Hermitian variety* H of $\mathrm{PG}(n, q)$, q a square and $n \geq 2$, is any subset of $\mathrm{PG}(n, q)$ which is equivalent under the group $\mathrm{PGL}(n+1, q)$ to the subset of $\mathrm{PG}(n, q)$ represented by the equation

$$X_0^{\sqrt{q}+1} + X_1^{\sqrt{q}+1} + \cdots + X_n^{\sqrt{q}+1} = 0.$$

A subset K of $\mathrm{PG}(n, q)$, $n \geq 2$, is of *type* $(1, m, q+1)$ if every line of $\mathrm{PG}(n, q)$ meets it in $1, m$, or $q+1$ points. A point of K is *singular* if every line through it intersects K either in 1 or $q+1$ points. Then K is called *singular* or *nonsingular* as it has singular points or not.

Theorem 5. *If K is a nonsingular set of type* $(1, m, q+1)$ *of* $\mathrm{PG}(n, q)$, *with* $3 \leq m \leq q - 1, n \geq 3$ *and* $q > 4$, *then K is either a nonsingular Hermitian variety of* $\mathrm{PG}(n, q)$ *(and then* $m = \sqrt{q} + 1$*) or the projection onto* $\mathrm{PG}(n, q)$ *of a nonsingular quadric Q of* $\mathrm{PG}(n+1, q) \supset \mathrm{PG}(n, q)$ *from a point* $x \in \mathrm{PG}(n+1, q) \setminus \mathrm{PG}(n, q)$ *other than the nucleus (or kernel) of Q in the case that n is even (and here* $m = \frac{q}{2} + 1$, *so q is even).*

For $m \neq \frac{q}{2}+1$ the result is due to Tallini Scafati [1967] and for $m = \frac{q}{2}+1, n > 3$ and part of $n = 3$, to Hirschfeld and Thas [1980a, 1980b]. The missing part in the case $m = \frac{q}{2} + 1$ and $n = 3$ was done by Glynn [1983]. Finally the case

$(q,m) = (4,3)$ was handled by Sherman [1983], see also Hirschfeld and Hubaut [1980] and Hirschfeld [1985]; it appears that here the sets K can be identified with the codewords of a *projective geometry code.*

A second approach is that where the object is described as an incidence structure satisfying certain properties; here the geometry is not a priori embedded in a projective space, even the finite field is in many cases a priori absent. Hence the finite projective space must be constructed.

A first example concerns circle geometries and designs. A $t-(v,k,\lambda)$ *design*, with $v > k > 1, k \geq t \geq 1, \lambda > 0$, is a set P with v elements called *points*, provided with subsets of size k called *blocks*, such that any t distinct points are contained in exactly λ blocks. A $3-(n^2+1, n+1, 1)$ design is usually called an *inversive plane* or *Möbius plane* of *order* n; here the blocks are mostly called *circles.* An *ovoid* O of $\mathrm{PG}(3,q)$, $q > 2$, is a set of q^2+1 points no three of which are collinear; an *ovoid* of $\mathrm{PG}(3,2)$ is the same as a nonsingular elliptic quadric, that is, a nonsingular quadric of $\mathrm{PG}(3,2)$ containing no lines. For properties on ovoids we refer to Hirschfeld [1985]. If O is an ovoid, then O provided with all intersections $\pi \cap O$, where π is any plane containing at least 2 (and then automatically $q+1$) points of O, is an inversive plane $\mathcal{J}(O)$ of order n. An inversive plane arising from an ovoid is called *egglike.* The following famous theorem is due to Dembowski [1964].

Theorem 6. *Each (finite) inversive plane of even order is egglike.*

If the ovoid O is an elliptic quadric, then the inversive plane $\mathcal{J}(O)$ is called *classical* or *Miquelian.* Barlotti [1955] and, independently, Panella [1955] proved that for q odd any ovoid is an elliptic quadric. Hence for q odd any egglike inversive plane is Miquelian. For odd order no other inversive planes are known. To the contrary, in the even case Tits [1962] showed that for any $q = 2^{2e+1}$, with $e \geq 1$, there exists an ovoid which is not an elliptic quadric; these ovoids are called Tits ovoids and are related to the simple Suzuki groups $Sz(q)$. For even order no other nonclassical inversive planes than the ones associated to the Tits ovoids are known.

Let $\mathcal{J}$ be an inversive plane of order n. For any point x of $\mathcal{J}$, the points of $\mathcal{J}$ different from x, together with the circles containing x (minus x), form a $2-(n^2, n, 1)$ design, that is, an *affine plane* of order n. That affine plane is denoted by $\mathcal{J}_x$, and is called the *internal plane* or *derived plane* of $\mathcal{J}$ at x. For an egglike inversive plane $\mathcal{J}(O)$ of order q, each internal plane is Desarguesian, that is, is the affine plane $\mathrm{AG}(2,q)$. The following theorem, due to Thas [1994], solves a longstanding conjecture on circle geometries.

Theorem 7. *Let $\mathcal{J}$ be an inversive plane of odd order n. If for at least one point x of $\mathcal{J}$ the internal plane $\mathcal{J}_x$ is Desarguesian, then $\mathcal{J}$ is Miquelian.*

The key idea in the proof of this theorem on Möbius planes is to use a fundamental result on Minkowski planes (another type of circle geometries), which in turn depends on the classification of a particular class of quasifields. As a corollary of Theorem 7 we obtain the first computer-free proof of the uniqueness (up to isomorphism) of the inversive plane of order 7.

Another beautiful illustration of this second approach is a characterization of all polar spaces of rank at least three. Here, starting from about nothing we get everything. First, let us give Tits' axioms for a polar space of rank r, with $r \geq 3$.

A *polar space* $\mathcal{S}$ of *rank* r, with $r \geq 3$, is a set P of elements called *points*, provided with distinguished subsets called *subspaces*, such that the following properties are satisfied.

(i) Any subspace, together with the subspaces it contains, is a projective space of dimension at most $r-1$.

(ii) The intersection of any family of subspaces is a subspace.

(iii) Given a subspace π of dimension $r-1$ and a point p in $P \backslash \pi$, there exists a unique subspace π' containing p such that the dimension of $\pi \cap \pi'$ is $r-2$. Also, the subspace $\pi \cap \pi'$ is the set of all points p' of π such that p and p' are contained in some subspace of dimension one.

(iv) There exist two disjoint subspaces of dimension $r-1$.

Isomorphisms between polar spaces are defined in the usual way.

Examples of finite polar spaces

(a) Let Q be a nonsingular quadric in $\mathrm{PG}(n,q)$ of rank r (that is, Q contains $(r-1)$-dimensional projective spaces, but no r-dimensional projective space), with $r \geq 3$. Then Q together with the projective spaces lying on it is a polar space of rank r.
(b) Let H be a nonsingular Hermitian variety of $\mathrm{PG}(n,q^2)$, $n \geq 5$. Then H together with the subspaces lying on it is a polar space of rank $[\frac{n+1}{2}]$ (here $[\frac{n+1}{2}]$ is the greatest integer less than or equal to $\frac{n+1}{2}$).
(c) Let ζ be a (nonsingular) symplectic polarity of $\mathrm{PG}(n,q)$, with n odd. Then $\mathrm{PG}(n,q)$ together with all absolute subspaces of ζ, is a polar space of rank $(n+1)/2$ (a projective subspace π of $\mathrm{PG}(n,q)$ is absolute for ζ if $\pi^\zeta \subseteq \pi$).

A complete classification of all polar spaces of rank at least three has been obtained by Tits [1974], building on work of Veldkamp [1959]. We state now this celebrated deep result in the finite case.

Theorem 8. *If $\mathcal{S}$ is a finite polar space of rank at least three, then $\mathcal{S}$ is isomorphic to one of (a), (b), (c).*

Polar spaces of rank 2 were also defined by Tits [1959]; these polar spaces are usually called *generalized quadrangles.* The role of generalized quadrangles in the theory of polar spaces, can be compared to the role of projective planes in the theory of projective spaces. Just as for projective planes a complete classification of all generalized quadrangles seems to be hopeless. For more on generalized quadrangles we refer to the monograph by Payne and Thas [1984] and to Thas [1995b].

Now we will describe polar spaces in an extremely simple way, just using points and lines.

A *Shult space* $\mathcal{S}$ is a nonempty set P of *points* together with distinguished subsets of cardinality at least two called *lines* such that for each line L of $\mathcal{S}$ and each point p of $P \setminus L$, the point p is collinear with either one or all points of L; here two not necessarily distinct points p_1 and p_2 are called *collinear* if there is at least one line of $\mathcal{S}$ containing these points. A Shult space is *nondegenerate* if no point of $\mathcal{S}$ is collinear with all points of $\mathcal{S}$. A *subspace* X of a Shult space $\mathcal{S}$ is a set of pairwise collinear points such that any line meeting X in more than one point is contained in X. The Shult space $\mathcal{S}$ has rank r, with $r \geq 1$, if r is the largest integer for which there is a chain

$$X_0 \subset X_1 \subset \ldots \subset X_r$$

of distinct subspaces $X_0 = \emptyset, X_1, X_2, \ldots, X_r$.

From Theorem 8 it follows that, for any finite polar space $\mathcal{S}$ of rank r, with $r \geq 3$, the pointset P together with the subspaces of dimension one is a Shult space of rank r. In fact this result also holds for infinite polar spaces. The following beautiful and extremely strong converse is due to Buekenhout and Shult [1974].

THEOREM 9. *Any nondegenerate Shult space of rank r, with $r \geq 3$, all of whose lines have cardinality at least three, together with its subspaces, is a polar space of rank r.*

We remark that Buekenhout and Shult [1974] also classified all degenerate Shult spaces; in fact, the problem is reduced to the classification of the nondegenerate ones.

Finally, let us mention that further fundamental and deep work on polar spaces, point-line geometries related to buildings, and, more generally, incidence geometry, was done in the first place by Tits, and further by Buekenhout, Cohen, Cooperstein, Kantor, Shult and others; these developments gave a new dimension to finite geometry. As excellent reference we mention the "Handbook of Incidence Geometry: Buildings and Foundations", edited by Buekenhout in 1995.

4 AN EXEMPLARY ILLUSTRATION OF THE INTERPLAY BETWEEN GALOIS GEOMETRY, CODING THEORY AND ALGEBRAIC GEOMETRY

Let C be a *code* of *length* k over an alphabet A of size q, with $q \in \mathbb{N}\setminus\{0,1\}$. In other words C is simply a set of (code) words where each word is an element of A^k. Having chosen m, with $2 \leq m \leq k$, we impose the following condition on C: no two words in C agree in as many as m positions. It then follows that $|C| \leq q^m$. If $|C| = q^m$, then C is called a *Maximum Distance Separable code (MDS code).* MDS codes are exactly the codes which meet the Singleton bound; see e.g. Hill [1986]. There is a voluminous literature on the subject; we refer e.g. to the standard work by MacWilliams and Sloane [1977] and to the book by Hill [1986]. MacWilliams and Sloane introduce their chapter on MDS codes as "*one of the most fascinating in all of coding theory".*

The *Hamming distance* between two code words $\mathbf{x} = (x_1, x_2, \ldots, x_k)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_k)$ is the number of indices i for which $x_i \neq y_i$; it is denoted by

$d(x,y)$. The *minimum Hamming distance* of C is

$$\min(d(x,y) : x, y \in C \text{ and } x \neq y)$$

and is denoted by $d(C)$. If C is an MDS code, then one easily shows that

$$d(C) = k - m + 1,$$

that is, the Singleton bound is met. One of the main problems concerning such codes is to maximize $d(C)$, and so k, for given m and q. Also, what is the structure of C in the optimal case?

Now the problem will be formulated for the case when C is linear, i.e., for the case that C is an m-dimensional subspace of the k-dimensional vector space $V(k,q)$ over $\mathrm{GF}(q)$. It goes like this. Choose any basis for C and represent it as an $m \times k$-matrix A over $\mathrm{GF}(q)$ of rank m. *Then C is MDS if and only if every set of m columns of A is linearly independent.*

Next, let us turn to particular pointsets of $\mathrm{PG}(n,q)$ introduced by Segre in 1955. A *k-arc* in $\mathrm{PG}(n,q)$, with $n \geq 2$, is a set K of k points with $k \geq n+1$ such that no $n+1$ points of K lie in a hyperplane, that is, such that any $n+1$ points are linearly independent. A k-arc K is *complete* if it is not properly contained in a larger arc. Otherwise, if $K \cup \{x\}$ is a $(k+1)$-arc for some point x of $\mathrm{PG}(n,q)$ we say that *x extends K*.

A *normal rational curve* (NRC) of $\mathrm{PG}(n,q)$, with $q > n+1$, is any set of points in $\mathrm{PG}(n,q)$ which is equivalent under the group $\mathrm{PGL}(n+1,q)$ to

$$\{(t^n, t^{n-1}, \ldots, t, 1) : t \in \ \mathrm{GF}\ (q)\} \cup \{(1,0,\ldots,0,0)\}.$$

Clearly any NRC is a $(q+1)$-arc. A NRC of $\mathrm{PG}(2,q)$ is a *nonsingular conic*; a NRC of $\mathrm{PG}(3,q)$ is a *twisted cubic*.

k-Arcs were introduced by Segre [1955], who also posed the next three fundamental problems.

(a) For given n and q what is the maximum value of k for which there exist k-arcs in $\mathrm{PG}(n,q)$?

(b) For what values of n and q, with $q > n+1$, is every $(q+1)$-arc a NRC?

(c) For given n and q, with $q > n+1$, what are the values of k for which every k-arc is contained in a $(q+1)$-arc of this space?

The famous Theorem 1 of Segre gives the answer, for q odd, to Problem (b) in the twodimensional case.

Hundreds of papers were written on k-arcs, in particular on the above problems, which are now solved for "most" values of the parameters. For example, if $q > f(n)$ with f some quadratic polynomial over $\mathbb{Q}$, then $k \leq q+1$ for $n \geq 3$, and any $(q+1)$-arc in $\mathrm{PG}(n,q)$, with $n \geq 3$ and $(n,q) \neq (3,2^h)$, is a NRC; also, by

Casse and Glynn [1982] any $(q+1)$-arc of $\mathrm{PG}(3,q)$, $q=2^h$, is equivalent under $\mathrm{PGL}(4,q)$ to

$$\{(t^{2^r+1}, t^{2^r}, t, 1) : t \in \mathrm{GF}(q)\} \cup \{(1,0,0,0)\},$$

with $(r,h)=1$.

The main tool in the proofs is that with any k-arc of $\mathrm{PG}(n,q)$ there corresponds an algebraic hypersurface in the dual space of $\mathrm{PG}(n,q)$. For $n=2$ this was proved by Segre [1967] and for $n>2$ twenty years later, by Bruen, Thas and Blokhuis [1988]. Essential also are the bounds on the number of points of an algebraic curve in $\mathrm{PG}(2,q)$, particularly the Hasse-Weil bound (see, e.g., Sections 2.9 and 2.15 of Hirschfeld [1988] for references) and the Stöhr-Voloch [1986] bound.

For surveys on k-arcs we refer to Hirschfeld and Thas [1991], Thas [1992b,1995a] and Hirschfeld and Storme [1998].

The main conjecture on k-arcs is the following.

CONJECTURE. *If K is a k-arc of* $\mathrm{PG}(n,q)$, *with $q \geq n+1$, then*

(a) for q even and $n \in \{2, q-2\}$ we have $k \leq q+2$,

(b) $k \leq q+1$ in all other cases.

We remark that $(q+2)$-arcs exist in $\mathrm{PG}(2,q)$ and $\mathrm{PG}(q-2,q), q=2^h$ and $h \geq 2$; see Hirschfeld and Thas [1991].

As already mentioned, a linear code C of length k and dimension m, with $2 \leq m \leq k$, over $\mathrm{GF}(q)$ is MDS if and only if it is generated by the rows of an $m \times k$-matrix A over $\mathrm{GF}(q)$ for which every set of m columns is linearly independent. Now we regard the columns of A as points $p_1, p_2, \ldots, p_k$ of $\mathrm{PG}(m-1,q)$. Then, for a linear MDS code, no m of these points lie in a hyperplane, that is, for $m \geq 3$ these points form a k-arc of $\mathrm{PG}(m-1,q)$. Conversely, with any k-arc of $\mathrm{PG}(m-1,q), m \geq 3$, there corresponds a linear MDS code. Remark that the linear MDS codes of dimension two are known and are quite trivial. So we have the following theorem.

THEOREM 10. *Linear* MDS *codes of dimension at least three and k-arcs are equivalent objects.*

So each result on linear MDS codes of dimension at least three can be tranlated into a result on k-arcs, and conversely. This way a lot of new fundamental results on linear MDS codes were obtained. Many of these translated results on k-arcs were proved long before the relation with coding theory was discovered. This is indeed a beautiful example of interrelationship between pure finite geometry and coding theory.

5 APPENDIX: RECENT RESEARCH IN FINITE GEOMETRIES

In this appendix I will give an example of brand new research in the field.

Let P and B be disjoint sets, each consisting of q^2+q+1 lines of $\mathrm{PG}(n,q)$. An element L of P and an element M of B are called incident if and only if $L \cap M \neq \emptyset$. Now assume that the point-line incidence structure with pointset P, lineset B and the given incidence is a projective plane $\mathcal{P}$ of order q. Finally, we suppose that for any incident point-line pair (L,M) of $\mathcal{P}$, all points and lines of $\mathcal{P}$ incident either with L or with M are contained in a common hyperplane of $\mathrm{PG}(n,q)$. Then the author and Van Maldeghem just proved that the plane $\mathcal{P}$ is Desarguesian, that $n \in \{6,7,8\}$, that for $n=6$ q is a power of 3 and that, up to isomorphism, there is a unique example in $\mathrm{PG}(6,q)$ for any such $q=3^h$. Also, they already handled large part of the remaining cases $n=7,8$, and the complete classification normally should be finished by the beginning of the conference.

The solution of this problem is a key step in the determination of all dual classical generalized hexagons with $q+1$ points on any line, whose points are points of $\mathrm{PG}(n,q)$ and whose lines are lines of $\mathrm{PG}(n,q)$; see Thas [1995b] for the definition of generalized hexagon.

References

S. Ball and A. Blokhuis [1998]. An easier proof of the maximal arcs conjecture. *Proc. Amer. Math. Soc.*, to appear.

S. Ball, A. Blokhuis, and F. Mazzocca [1997]. Maximal arcs in desarguesian planes of odd order do not exist. *Combinatorica*, 17:31-47.

A. Barlotti [1955]. Un 'estensione del teorema di Segre-Kustaanheimo. *Boll. Un. Mat. Ital.*, 10:96-98.

R.C. Bose [1947]. Mathematical theory of the symmetrical factorial design. *Sankhyā*, 8:107-166.

A.A. Bruen, J.A. Thas and A. Blokhuis [1988]. On M.D.S. codes, arcs in $\mathrm{PG}(n,q)$ with q even, and a solution of three fundamental problems of B. Segre. *Invent. Math.*, 92:441-459.

F. Buekenhout (editor) [1995]. *Handbook of Incidence Geometry: Buildings and Foundations.* North-Holland, Amsterdam.

F. Buekenhout and E.E. Shult [1974]. On the foundations of polar geometry. *Geom. Dedicata*, 3:155-170.

L.R.A. Casse and D.G. Glynn [1982]. The solution to Beniamo Segre's problem $I_{r,q}$, $r=3, q=2^h$. *Geom. Dedicata* 13:157-164.

P. Dembowski [1964]. Möbiusebenen gerader Ordnung, *Math. Ann.*, 157: 179-205.

R.H.F. Denniston [1969]. Some maximal arcs in finite projective planes. *J. Combin. Theory*, 6:317-319.

D.G. Glynn [1983]. On the characterization of certain sets of points in finite projective geometry of dimension three. *Bull. London Math. Soc.*, 15:31-34.

R. Hill [1986]. *A First Course in Coding Theory.* Oxford University Press, Oxford.

J.W.P. Hirschfeld [1985]. *Finite Projective Spaces of Three Dimensions.* Oxford Univerity Press, Oxford.

J.W.P. Hirschfeld [1998]. *Projective Geometries over Finite Fields.* Oxford University Press, Oxford; first edition, 1979.

J.W.P. Hirschfeld and X. Hubaut [1980]. Sets of even type in $\mathrm{PG}(3,q)$ alias the binary (85,24) projective code. *J. Combin. Theory Ser. A*, 29:101-112.

J.W.P. Hirschfeld and L. Storme [1998]. The packing problem in statistics, coding theory and finite projective spaces. *J. Statist. Plann. Inference*, to appear.

J.W.P. Hirschfeld, L. Storme, J.A. Thas, and J.F. Voloch [1991]. A characterization of Hermitian curves. *J. Geom.*, 41:72-78.

J.W.P. Hirschfeld and J.A. Thas [1980a]. The characterization of projections of quadrics over finite fields of even order. *J. London Math. Soc.*, 22:226-238.

J.W.P. Hirschfeld and J.A. Thas [1980b]. Sets of type $(1,n,q+1)$ in $\mathrm{PG}(d,q)$. *Proc. London Math. Soc.*, 41:254-278.

J.W.P. Hirschfeld and J.A. Thas [1991]. *General Galois Geometries.* Oxford University Press, Oxford.

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

G. Panella [1955]. Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito. *Boll. Un. Mat. Ital.*, 10:507-513.

S.E. Payne and J.A. Thas [1984]. *Finite Generalized Quadrangles.* Pitman, London.

B. Segre [1954]. Sulle ovali nei piani lineari finiti. *Atti Accad. Naz. Lincei Rend.*, 17:1-2.

B. Segre [1955]. Curve razionali normali e k-archi negli spazi finiti. *Ann. Mat. Pura Appl.*, 39:357-379.

B. Segre [1967]. Introduction to Galois Geometries (edited by J.W.P. Hirschfeld). *Atti Accad. Naz. Lincei Mem.*, 8:133-236.

B.F. Sherman [1983]. On sets with only odd secants in geometries over GF(4). *J. London Math. Soc.*, 27:539-551.

K.O. Stöhr and J.F. Voloch [1986]. Weierstrass points and curves over finite fields. *Proc. London Math. Soc.*, 52:1-19.

M. Tallini Scafati [1967]. Caratterizzazione grafica delle forme hermitiane di un $S_{r,q}$. *Rend. Mat. e Appl.*, 26:273-303.

J.A. Thas [1975]. Some results concerning $\{(q+1)(n-1);n\}$-arcs and $\{(q+1)(n-1)+1;n\}$-arcs in finite projective planes of order q. *J. Combin. Theory Ser. A*, 19:228-232.

J.A. Thas [1992a]. A combinatorial characterization of Hermitian curves. *J. Algebraic Combin.*, 1:97-102.

J.A. Thas [1992b]. M.D.S. codes and arcs in projective spaces: a survey. *Matematiche (Catania)*, 47:315-328.

J.A. Thas [1994]. The affine plane $\mathrm{AG}(2,q)$, q odd, has a unique one point extension. *Invent. Math.*, 118:133-139.

J.A. Thas [1995a]. Projective geometry over a finite field. In *Handbook of Incidence Geometry: Buildings and Foundations*, pages 295-347. North-Holland, Amsterdam.

J.A. Thas [1995b]. Generalized polygons. In *Handbook of Incidence Geometry: Buildings and Foundations*, pages 383-431. North-Holland, Amsterdam.

J. Tits [1959]. Sur la trialité et certains groupes qui s'en déduisent. *Inst. Hautes Etudes Sci. Publ. Math.,* 2:13-60.

J. Tits [1962]. Ovoïdes et groupes de Suzuki. *Arch. Math.*, 13:187-198.

J. Tits [1974]. *Buildings of Spherical Type and Finite BN-Pairs.* Lecture Notes in Math. 386, Springer, Berlin.

F.D. Veldkamp [1959]. Polar geometry I-IV. *Indag. Math.*, 21:512-551.

Joseph A. Thas
University of Ghent,
Department of Pure Mathematics
and Computer Algebra,
Krijgslaan 281,
B-9000 Gent, Belgium,
jat@cage.rug.ac.be