LE MATEMATICHE
Vol. XLVII (1992) – Fasc. II, pp. 315-328

M. D. S. CODES AND ARCS IN PROJECTIVE SPACES: A SURVEY

JOSEPH A. THAS

Let C be a code of length k over an alphabet A of size $q, q \geq 2$. Having chosen m with $2 \leq m \leq k$ we impose the following condition on C: no two words 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 (M.D.S. code). A k-arc in $PG(n, q)$ is a set K of k points with $k \geq n + 1$ such that no $n+1$ points lie in a hyperplane. It can be shown that arcs and linear M.D.S. codes are equivalent objects. Here we give a survey of important results on k-arcs, in particular we survey the answers to three fundamental problems on arcs posed by B. Segre in 1955.

1. M.D.S. codes.

1.1 M.D.S. codes.

Let C be a *code* of *lenght* k over an *alphabet* A of size $q, q \geq 2$. In other words C is simply a set of (code) words where each *word* is a k-tuple over A. 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 (=M.D.S. code)*. There is a voluminous literature on the subject. We refer to MacWilliams and Sloane [1977] for references as well as to the work of Maneri and Silverman [1971] and to the book of Hill [1986]. MacWilliams and Sloane introduce their chapter on M.D.S. codes as "one of the most fascinating in all of coding theory".

The *Hamming distance* between two code words $x = (x_1, x_2, \ldots, x_k)$ and $y = (y_1, y_2, \ldots, y_k)$ 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 defined by $\min(d(x, y) \mid x, y \in C$ and $x \neq y)$ and denoted by $d(C)$. If C is an M.D.S. code then the following interesting equality holds (see for example Hill [1986]).

Theorem 1. *For any M.D.S. code* $d(C) = k - m + 1$.

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?

1.2 The general case.
First, let $m = 2$. Then C gives a set of q^2 code words of lenght k, no two of which agree in as many as 2 positions. It is easily seen that this is equivalent to the existence of a net of order q and degree k (see Dembowski [1968], Ryser [1963]. It follows that $k \leq q + 1$, the case of equality corresponding to an affine plane of order q. From this, by an inductive argument, the following result is obtained.

Theorem 2. *For any M.D.S. code* $k \leq q + m - 1$.

The case $m = 3$ and $k = q + 2$ is equivalent to the existence of an affine plane π of order q, q even, containing an elaborate system of hyperovals. For all known examples the plane π is desarguesian and $q = 2^h$ (see Willems and Thas [1983]). For $m = 4$ and $k = q + 3$ one can only show that either $q = 2$ or 36 divides q (see Bruen and Silverman [1983]), even though (presumably) no examples with $q > 2$ exist. Accordingly, it seems that one cannot do much with the problem in its present generality.

1.3 Linear M.D.S. codes.
Now the problem will be formulated for the case when C is *linear*, that is, for the case that C is a m-dimensional subspace of the k-dimensional vector space $V(k, q)$ over $GF(q)$. It goes like this. Choose any basis for C and represent it as a $m \times k$-matrix X over $GF(q)$ of rank m. Then C is M.D.S. if and only if every set of m columns of X is linearly independent. One can multiply the columns of X by non-zero scalars and still preserve the desired property. Therefore, regard the columns of X as points $p_1, p_2, \ldots, p_k$ of $PG(m-1, q)$. From what preceeds it follows that C is M.D.S. if and only if no m points of $\{p_1, p_2, \cdots, p_k\}$ lie in a hyperplane.

1.4 Linear M.D.S. codes and k-arcs.
A k-arc in $PG(n, q)$ is a set K of k points with $k \geq n + 1$ such that no $n + 1$ points lie in a hyperplane. By 1.3 we have the following fundamental result.

Theorem 3. *Linear M.D.S. codes and arcs are equivalen objects.*

Hence all results on arcs can be translated in terms of linear M.D.S. codes, and conversaly.

2. k-arcs, normal rational curves and generalized Reed-Solomon codes.

2.1 Definition.

An arc K is *complete* if it is not properly contained in a larger arc. Otherwise, if $K \cup \{x\}$ is an arc for some point x of $PG(n,q)$ we say that x extends K.

A *normal rational curve* of $PG(n,q)$ is any set of points in $PG(n,q)$ which is projectively equivalent to $\{(t^n, t^{n-1}, \ldots, t, 1) \mid t \in GF(q)\} \cup \{(1,0,\ldots,0,0)\}$. Clearly any normal rational curve contains $q+1$ points. A normal rational curve of $PG(2,q)$ is an *irreducible conic;* a normal rational curve of $PG(3,q)$ is a *twisted cubic.* It is well-known that any $(n+3)$-arc of $PG(n,q)$ is contained in a unique normal rational curve of this space (see Hirschfeld [1985]). For $q > n+1$, the *osculating hyperplane* of the normal rational curve C at the point $x \in C$ is the unique hyperplane through x intersecting C at x with multiplicity n.

2.2 Generalized Reed-Solomon codes.

A linear code C over $GF(q)$ is called a *generalized Reed-Solomon (GRS) code* if it is represented by a matrix of the form

$$X = [g_{ij}] \quad \text{with} \quad g_{ij} = \nu_j t_j^{i-1} \quad , 1 \le i \le m, 1 \le j \le k.$$

Here $t_1, t_2, \ldots, t_k$ are distinct elements of $GF(q)$; $\nu_1, \nu_2, \ldots, \nu_k$ are nonzero (not necessarily distinct) elements of $GF(q)$. We define $0^0 = 1$. If one adds an extra column of the form $(0,0,\ldots,\nu)^T$, with $\nu \neq 0$, then the resulting linear code is called a *generalized doubly extended Reed-Solomon (GDRS) code.* It is well-known that GRS codes and GDRS codes are M.D.S. codes. From the form of the matrices immediately follows that each corresponding arc is a subset of a normal rational curve. For more details we refer to Seroussi and Roth [1986].

2.3 The three problems of B. Segre.

In 1955 Segre posed the following three fundamental problems.

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

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

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

3. k-arcs in $PG(2,q)$.

3.1 Ovals and hyperovals.

Let K be a k-arc of $PG(2,q)$. Then clearly $k \leq q+2$. By Bose [1947], for q odd, $k \leq q+1$. Further, any irreducible conic of $PG(2,q)$ is a $(q+1)$-arc. It can be shown that each $(q+1)$-arc K of $PG(2,q), q$ even, extends to a $(q+2)$-arc $K \cup \{x\}$ (see e.g. Hirschfeld [1979], p. 165); the point x, which is uniquely defined by K, is called the *kernel or nucleus* of K. The $(q+1)$-arcs of $PG(2,q)$ are called *ovals*; the $(q+2)$-arcs of $PG(2,q), q$ even, are called *complete ovals* or *hyperovals.*

The following celebrated theorem is due to Segre [1955a].

Theorem 4. *In $PG(2,q), q$ odd, every oval is an irreducible conic.*

Let $K \cup \{x\}$ be a hyperoval in $PG(2,q), q$ even, with K an irreducible conic. If $y \in K$, then $(K \setminus \{y\}) \cup \{x\} = K'$ is an oval of $PG(2,q)$. Clearly $|K \cap K'| = q$. So for $q > 4$ the oval K' cannot be an irreducible conic. Hence for $q \geq 8$, q even, the plane $PG(2,q)$ always contains ovals which are not irreducible conics. It is easy to show that for $q \in \{2,4\}$ any oval of $PG(2,q)$ is an irreducible conic. By Segre ([1957], [1962]), each hyperoval of $PG(2,8)$ is the union of a conic and its nucleus, and in $PG(2,2^h)$ with $h = 5$ and $h \geq 7$ there exist hyperovals not containing a conic as a subset. In [1958] Lunelli and Sce have shown that in $PG(2,16)$ there is a hyperoval which is not the union of a conic and its nucleus; in [1991] a similar result for $PG(2,64)$ was shown by Penttila and Pinneri.

3.2 The known hyperovals of $PG(2,q)$, $q = 2^h$.

Let $D(k)$, with $k \in \mathbb{N} \setminus \{0\}$, be the pointset

$$\{(0,1,0),(0,0,1)\} \cup \{(1,t,t^k) \mid t \in GF(q)\}.$$

Now we list all known hyperovals of $PG(2,q), q$ even.

(a) $D(2^m)$, with $(m,h) = 1$; these are due to Segre [1957]. Note that $D(2)$ gives a conic union its nucleus.

(b) $D(6)$, with h odd; these are also due to Segre [1962].

(c) Let h be odd, $h \geq 3$. Define two automorphisms $x \mapsto x^\sigma$ and $x \mapsto x^\gamma$ of $GF(q)$ as follows:

$$\sigma = 2^{(h+1)/2},$$

$$\gamma = \begin{cases} 2^m & \text{, if } h = 4m-1 \\ 2^{3m+1} & \text{, if } h = 4m+1. \end{cases}$$

Then it was shown by Glynn [1983] that $D(\sigma+\gamma)$ and $D(3\sigma+4)$ are hyperovals.

(d) Now follows a description by Glynn [1983] of the hyperoval O of Lunelli and Sce [1958]. Consider in $PG(2,16)$ the cubics C and C' with equations $X_0^3+X_1^3+X_2^3+dX_0X_1X_2=0$ and $X_0^3+X_1^3+X_2^3+d^4X_0X_1X_2=0$, where $d\in GF(16)$, $d^5=1$ and $d\neq 1$. Then $O=(C\cup C')\setminus(C\cap C')$.

(e) Let h be odd. Define $\delta: GF(q)\to GF(q)$ by

$$\delta: x\mapsto x^{1/6}+x^{1/2}+x^{5/6}.$$

Then Payne [1985] has shown that

$$D(\delta)=\{(0,1,0),(0,0,1)\}\cup\{1,t,t^{\delta}) \mid t\in GF(q)\}$$

is a hyperoval of $PG(2,q)$.

(f) Next we describe the hyperovals of Cherowitzo [1986]. Let $h=2s+1$,

$$\sigma: GF(q)\to GF(q), \quad x\mapsto x^{2^{s+1}}$$
$$\zeta: GF(q)\to GF(q), \quad x\mapsto x^{\sigma}+x^{\sigma+2}+x^{3\sigma+4}.$$

Then $D(\zeta)=\{(0,1,0),(0,0,1)\}\cup\{(1,t,t^{\zeta}) \mid t\in GF(q)\}$ is a hyperoval for $h\leq 15$. It does not belong to the previous classes for $h\in\{5,7,9,11,13,15\}$.

(g) Finally O'Keefe and Penttila [19**] discovered a new hyperoval on $PG(2,32)$, Pentilla and Pinneri [1991] found two hyperovals in $PG(2,64)$ which are not the union of a conic and its nucleus, and Pentilla and Royle [1991] constructed a third one in $PG(2,64)$.

Note that the classes (a), (b), (c), (e) sometimes overlap for small values of q, but they are distinct for large values.

3.3 Extendable arcs.

By an ingenious trick (the lemma of tangents, see 8.2.2 in Hirschfeld [1979]), by generalizing the classical theorems of Menelaus and Ceva and by using some fundamental theorems from algebraic geometry, Segre [1967] obtained the following key result. In fact, the odd case is a slight improvement by Thas [1987] of the original inequality of Segre.

Theorem 5. *Assume that* $k>\lambda(q)$ *where*

$$\lambda(q)=\begin{cases} q-\sqrt{q}+1 & \text{for } q \text{ even} \\ q-\sqrt{q}/4+25/16 & \text{for } q \text{ odd.}\end{cases}$$

Then

(a) for q even, any k-arc K is embedded in a hyperoval which is unique except when $q = k = 2$,

(b) for q odd, any k-arc K is embedded in a unique conic.

In [1986] Fisher, Hirschfeld and Thas, and independently Boros and Szönyi [1986], construct complete $(q - \sqrt{q} + 1)$-arcs for q a square and $q > 4$; in fact these arcs were already constructed in [1981] by Kestenband, but not recognized to be complete. So for q an even square and $q \neq 4$ the bound of Segre is best possible. These $(q - \sqrt{q} + 1)$-arcs, q even or odd, can be described as follows. Let G be a cyclic group acting regularly on $PG(2, q), q$ square. Let G_1 be the subgroup of order $q - \sqrt{q} + 1$ of G. Then the orbits of G_1 are complete $(q - \sqrt{q} + 1)$-arcs when $q \geq 9$. Further, in the odd case the bound in Theorem 5 is certainly not best possible; also, examples show that the bound $q - \sqrt{q} + 1$ does not work for q an odd square (in $PG(2, 9)$ there exists a complete 8-arc, see Hirschfeld [1979]).

Further, for q an odd power of a prime ,Voloch ([1990],[1991]) was able to improve the bound in Theorem 5.

Theorem 6.

(a) Every k-arc K of $PG(2, p), p$ an odd prime, with $k > (44p + 40)/45$, is embedded in a unique conic.

(b) Every k-arc K of $PG(2, q), q = p^{2m+1}, m \geq 1, p$ odd, with $k > q - \sqrt{pq}/4 + 29p/16 + 1$, is embedded in a unique conic.

(c) Every k-arc K of $PG(2, q), q = 2^{2m+1}, m \geq 1$, with $k > q - \sqrt{2q} + 2$, is contained in a unique hyperoval

From Theorem 5 follows that for q even any q-arc of $PG(2, q)$ is contained in a hyperoval, and that for q odd, with $q \geq 41$, any q-arc of $PG(2, q)$ is contained in a conic. The following theorem is due to Segre [1955b] (see also Hirschfeld [1979],§8.6), but a short proof can be found in That [1987].

Theorem 7. *Any q-arc of $PG(2, q), q$ odd, is contained in a conic.*

Finally from the machinery developed by Segre [1967] (see also §10.3 and §10.4 of Hirschfeld [1979]) the following interesting result easily follows.

Theorem 8.

(a) If q is even and $k > (q + 2)/2$ then K is contained in a unique complete arc of $PG(2, q)$;

(b) if q is odd and $k > (2q + 4)/3$ then K is contained in a unique complete arc of $PG(2, q)$.

4. k-arcs in $PG(3,q)$.

4.1 $(q+1)$-arcs in $PG(3,q)$.

For $q > 2$ any twisted cubic of $PG(3,q)$ is a $(q+1)$-arc.

Theorem 9.

(a) (Segre [1955b]). For any k-arc of $PG(3,q)$, q odd and $q > 3$, $k \leq q+1$; any k-arc of $PG(3,3)$ has at most 5 points.

(b) (Casse [1969]). For any k-arc of $PG(3,q)$, q even and $q > 2$, $k \leq q+1$; any k-arc of $PG(3,2)$ has at most 5 points.

The following theorem gives the classification of all $(q+1)$-arcs of $PG(3,q)$.

Theorem 10.

(a) (Segre [1955b]). Any $(q+1)$-arc of $PG(3,q)$, q odd, is a twisted cubic.

(b) (Casse and Glynn [1982]). Every $(q+1)$-arc of $PG(3,q)$, $q = 2^h$, is projectively equivalent to $C = \{(1,t,t^e,t^{e+1}) \mid t \in GF(q)\} \cup \{(0,0,0,1\}$ where $e = 2^m$ and $(m,h) = 1$.

4.2 Extendable arcs.

In Bruen, Thas and Blokhuis [1988] the theory of Segre [1967] is generalized to $PG(3,q)$. The bounds obtained by these authors for q even were considerably improved by Storme and Thas [19**a], but again using the fundamental machinery developed by Bruen, Thas and Blokhuis [1988]. For q even, Storme and Thas [19**a] obtained the following partial answer to Problem (c) of Segre (see also Hirschfeld and Thas [1991], §27.7); part (b) was proved by Thas ([1968], [1987]) using totally different techniques.

Theorem 11.

(a) Let K be a k-arc of $PG(3,q)$, q even and $q \neq 2$. If $k > q - \sqrt{q}/2 + 9/4$, then K can be completed to a $(q+1)$-arc which is uniquely determined by K.

(b) Let K be a k-arc of $PG(3,q)$, q odd. If $k > q - \sqrt{q}/4 + 41/16$, then K is contained in a unique twisted cubic.

Finally, the following interesting result is due to Bruen, Thas and Blokhuis [1988].

Theorem 12.

(a) Any k-arc K of $PG(3,q)$, q even and $k > (q+4)/2$, is contained in a unique complete arc of $PG(3,q)$.

(b) Any k-arc K of $PG(3,q)$, q odd and $k > (2q+7)/3$, is contained in a unique complete arc of $PG(3,q)$.

5. k-arcs in $PG(n,q)$.

5.1 Solutions to the problems of Segre.

For $q \geq n$ any normal rational curve of $PG(n,q)$ is a $(q+1)$-arc.

Theorem 13. *(Kaneta and Maruta [1989]). If every $(q+1)$-arc of $PG(n,q)$, $n \geq 3$ and $q \geq n+3$, is a normal rational curve, then $q+1$ is the maximum value of k for which k-arcs exist in $PG(n+1,q)$.*

Theorem 14.

(a) (Casse [1969]). For any k-arc of $PG(4,q)$, q even and $q > 4$, there holds $k \leq q+1$; any k-arc of either $PG(4,2)$ or $PG(4,4)$ has at most 6 points.

(b) (Segre [1955b]). For any k-arc of $PG(4,q)$, q odd and $q \geq 5$, there hods $k \leq q+1$; any k-arc of $PG(4,3)$ has at most 6 points.

(c) (Casse and Glynn [1984]). Any $(q+1)$-arc of $PG(4,q)$, q even, is a normal rational curve.

(d) (Kaneta and Maruta [1989]). For any k-arc of $PG(5,q)$, q even and $q \geq 8$, there holds $k \leq q+1$.

The following theorem by Thas ([1968], [1987]) gives an answer to the problems of Segre, for q odd; see also Hirschfeld and Thas [1991], §27.6.

Theorem 15.

(a) For any k-arc of $PG(n,q)$, q odd and $q > (4n-39/4)^2$, $k \leq q+1$.

(b) In $PG(n,q)$, q odd and $q > (4n-23/4)^2$, every $(q+1)$- arc is a normal rational curve.

(c) In $PG(n,q)$, q odd, every k-arc with $k > q - \sqrt{q}/4 + n - 7/16$ is contained in one and only one normal rational curve of this space.

In Bruen, Thas and Blokhuis [1988] and Blokhuis, Bruen and Thas [1990] the theory of Segre [1967] is generalized to $PG(n,q)$. For q even, the bounds obtained in Bruen, Thas and Blokhuis [1988] were considerably improved by Storme and Thas [19**a], but again using the fundamental machinery developed by Blokhuis, Bruen and Thas. See also Hirschfeld and Thas [1991], §27.7.

Theorem 16. *(Storme and Thas [19**a]).*

(a) In $PG(n,q), n \geq 4$, q even and $q > (2n-11/2)^2$, the inequality $k \leq q+1$ holds for every k-arc K.

(b) In $PG(n,q), n \geq 4$, q even and $q > (2n-7/2)^2$, every $(q+1)$-arc is a normal rational curve.

(c) *Let K be a k-arc in $PG(n,q), n \geq 4, q$ even, $q > 4$ and $k > q - \sqrt{q}/2 + n - 3/4$. Then K lies in a normal rational curve C of $PG(n,q)$. Also, C is completely determined by K.*

Finally, we mention the following interesting result which is due to Blokhuis, Bruen and Thas [1990].

Theorem 17.

(a) *Any k-arc K of $PG(n,q)$, q even and $k > (q + 2n - 2)/2$, is contained in a unique complete arc of $PG(n,q)$.*

(b) *Any k-arc K of $PG(n,q)$, q odd and $k > (2q + 3n - 2)/3$, is contained in a unique complete arc of $PG(n,q)$.*

5.2 The non-classical 10-arc of $PG(4,9)$.

By Theorem 15(b), in $PG(4,q)$, with q odd and $q \geq 107$, every $(q+1)$-arc is a normal rational curve. In Glynn [1986] a 10-arc of $PG(4,9)$ is constructed which is not a normal rational curve. This 10-arc K consists of the following points: $(0,0,0,0,1)$ and $(1,t,t^2 + mt^6, t^3, t^4)$, with $t \in GF(9)$ and m a non-square. Also, Glynn [1986] shows that, up to a projectivity, this non-classical arc together with the normal rational curve are the only 10-arcs of $PG(4,9)$. Finally it is noted that the projection of Glynn's arc K from the line p_1p_2, with $p_1, p_2 \in K$, onto a plane $PG(2,9)$ skew to p_1p_2, is the unique complete 8-arc of $PG(2,9)$ (see also §14.7 in Hirschfeld [1979]).

5.3 The nucleus or kernel of a normal rational curve, and $(q+2)$-arcs in $PG(q-2,q)$.

Theorems 18 and 19 of this section are taken from Thas [1969b].

Theorem 18. *Let C be a normal rational curve of $PG(2^s - 2, q)$, with $q = 2^h$ and $h \geq s \geq 3$. Then the intersection of the $q+1$ osculating hyperplanes of C is a $PG(2^{s-1} - 2, q)$. Also, each of the $q+1$ tangents of the algebraic curve C has a point in common with $PG(2^{s-1} - 2, q)$. Finally, these $q+1$ points of $PG(2^{s-1} - 2, q)$ form a normal rational curve C_1 of this space.*

Definitions. The curve C_1 of Theorem 18 will be called the *tangent curve* of C. The tangent curve $(C_1)_1$ of C_1 will also be denoted by C_2, etc. The curve C_{s-2} is an irreducibile conic of $PG(2,q)$. The nucleus of C_{s-2} will be called the *nucleus* or *kernel* of the normal rational curve C.

Theorem 19. *Let C be a normal rational curve of $PG(q-2,q)$, $q = 2^h$, with nucleus x. Then $C \cup \{x\}$ is a $(q+2)$-arc of $PG(q-2,q)$.*

Conjecture. For $q \geq n + 1 (q+2)$-arcs in $PG(n,q)$ are only possible for q even with $n = 2$ or $n = q - 2$.

6. The duality principle for k-arcs.

6.1 The duality principle.

This section is taken from Thas [1969a].

Let K be a k-arc of $PG(n,q)$, $n \geq 2$ and $k \geq n+4$, and let K consist of the points

$$p_i(y_0^{(i)}, y_1^{(i)}), \ldots, y_n^{(i)}) \quad , \; i = 0, 1, \ldots, k-1.$$

Then each submatrix of order $n+1$ of the $k \times (n+1)$-matrix $\left[y_j^{(i)}\right]$ is non singular. Consider now the $n+1$ hyperplanes of $PG(k-1,q)$ with equations

$$y_j^{(0)} X_0 + y_j^{(1)} X_1 + \cdots + y_j^{(k-1)} X_{k-1} = 0, \quad j = 0, 1, \ldots, n.$$

These hyperplanes are linearly independent, and so they intersect in a $PG(k-n-2,q)$. Now take $k-n-1$ linearly independent points of $PG(k-1,q)$ in this $PG(k-n-2,q)$:

$$q_i(z_0^{(i)}, z_1^{(i)}, \ldots, z_{k-1}^{(i)}), \; i = 0, 1, \ldots, k-n-2.$$

Now consider the following k points of $PG(k-n-2,q)$:

$$p'_j(z_j^{(0)}, z_j^{(1)}, \ldots, z_j^{(k-n-2)}) \; , \; j = 0, 1, \ldots, k-1.$$

Then it can be shown that each submatrix of order $k-n-1$ of the $k \times (k-n-1)$-matrix $\left[z_j^{(i)}\right]$ is non-singular. Hence $\{p'_0, p'_1, \ldots, p'_k\}$ is a k-arc of $PG(k-n-2,q)$.

In particular, if

$$\left[y_j^{(i)}\right] = \begin{bmatrix} I_{n+1} \\ Y \end{bmatrix},$$

with I_{n+1} the identity matrix of order $n+1$ and Y a $(k-n-1) \times (n+1)$-matrix, then one can put

$$\left[z_j^{(i)}\right]^T = \begin{bmatrix} -Y & I_{k-n-1} \end{bmatrix}.$$

Theorem 20. *(The duality principle for k-arcs)*

A k-arc of $PG(n,q)$, $n \geq 2$ and $k \geq n+4$, exists if and only if a k-arc of $PG(k-n-2,q)$ exists. Further, for $q \geq \max(n+2, k-n)$, $n \geq 2$ and $k \geq n+4$,

$$\frac{\textit{number of } k\textit{-arcs of } PG(n,q)}{\textit{number of } k\textit{-arcs of } PG(k-n-2,q)} =$$

$$= \frac{\textit{number of normal rational curves of } PG(n,q)}{\textit{number of normal rational curves of } PG(k-n-2,q)}.$$

6.2 Applications.
This *duality* can be applied onto the results of the preceding sections. Two examples will be given:

(i) Since $(q+2)$-arcs exist in $PG(2,q)$, q even, $(q+2)$-arcs also exist in $PG(q-2,q)$.

(ii) Duality applied to Theorem 16 gives:
   (a) In $PG(n,q)$, $q-4 \geq n > q-\sqrt{q}/2-11/4$ and $q=2^h$, every k-arc K satisfies $k \leq q+1$.
   (b) In $PG(n,q)$, $q-5 \geq n > q-\sqrt{q}/2-11/4$ and $q=2^h$, every $(q+1)$-arc is a normal rational curve.
   (c) Let K be a k-arc in $PG(n,q)$, $n > q-\sqrt{q}/2-11/4$,$q=2^h$, $h>2$ and $k \geq n+6$. Then K lies in a normal rational curve C of $PG(n,q)$. Also, C is completely determined by K.

6.3 Linear M.D.S. codes and duality.
Let K be a k-arc of $PG(m-1,q)$, with $3 \leq m \leq k-3$, and let K' be a k-arc of $PG(k-m-1,q)$ obtained from K by duality. If C is the linear M.D.S. code corresponding to K and C' is the linear M.D.S. code corresponding to K', then each vector of C is orthogonal to each vector of C'. Since $\dim C' = k-m = k-\dim C$, it follows that $C' = C^{\perp}$, that is, C' is the *dual code* of C. This also gives a proof, for $3 \leq m \leq k-3$, of the following theorem; see also Hill [1986].

Theorem 21. *For $2 \leq m \leq k-2$ the dual of a linear M.D.S. code is again a linear M.D.S. code.*

7. The completeness of normal rational curves.

The following interesting theorem on normal rational curves is due to Seroussi and Roth [1986].

Theorem 22. *For $n \geq 2$, and $n \neq 2$ if q is even, a k-arc in $PG(n,q)$ not contained in a normal rational curve has at most $(q+2n-1)/2$ points in common with a normal rational curve.*

As a direct corollary we have the following result.

Theorem 23. *For q even, $n \geq 3$, $q > 2n-4$ and q odd, $n \geq 2$, $q > 2n-3$, any normal rational curve of $PG(n,q)$ is complete.*

Considerable improvements of Theorem 23 are contained in Storme and Thas [19**b] and in Storme [19**]. In Storme [19**] the following theorem is proved.

Theorem 24. *Any normal rational curve of $PG(n,q)$ is complete whenever q is prime with $q \geq p_0$ or $q = p^{2h+1}$, $h \geq 1$, with p an odd prime and $p \geq p_0(h)$.*

REFERENCES

[1] A. Blokhuis, A.A. Bruen, and J.A. Thas (1990), *Arcs in $PG(n,q)$, M.D.S. codes and three fundamental problems of B. Segre-some extensions,* Geom. Dedicata, 35 (1990), pp. 1-11.

[2] E. Boros and T. Szönyi,(1986), *On the sharpness of a theorem of B. Segre,* Combinatorica, 6 (1986), pp. 261-268.

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

[4] A.A. Bruen and R. Silverman (1983), *On the non-existence of certain M.D.S. codes and projective planes,* Math. Z., 183 (1983), pp. 171-175.

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

[6] L.R.A. Casse (1969), *A solution to Beniamino Segre's 'Problem $I_{r,q}$' for q even,* Atti Accad. Naz. Lincei Rend., 46 (1969), pp. 13-20.

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

[8] L.R.A. Casse and G.G. Glynn (1984), *On the uniqueness of $(q+1)_4$-arcs of $PG(4,q)$, $q = 2^h$, $h \geq 3$,* Discrete Math., 48 (1984), pp. 173-186.

[9] W.E. Cherowitzo (1986), *Hyperovals in Desarguesian planes of even order,* Ann. Discrete Math., 37 (1986), pp. 87-94.

[10] P. Dembowski (1968), *Finite geometries,* Springer, Berlin, 1968.

[11] J.C. Fischer - J.W.P. Hirschfeld and J.A. Thas (1986), *Complete arcs in planes of square order,* Ann. Discrete Math., 30 (1986), pp. 243-250.

[12] D.G. Glynn (1983), *Two new sequences of ovals in finite Desarguesian planes of even order,* Volume 1036 of Lecture Notes in Math., Springer, Berlin, (1983), pp. 217-229.

[13] D.G. Glynn (1986), *The non-classical 10-arc of $PG(4,9)$,* Discrete Math., 59 (1986), pp. 43-51.

[14] R. Hill (1986), *A first course in coding theory,* Oxford University Press, Oxford, 1986.

[15] J.W.P. Hirschfeld (1979), *Projective geometries over finite fields,* Oxford University Press, Oxford, 1979.

[16] J.W.P. Hirschfeld (1985), *Finite projective spaces of three dimensions,* Oxford University Press, Oxford, 1985.

[17] J.W.P. Hirschfeld and J.A. Thas (1991), *General Galois geometries,* Oxford Universuty Press, Oxford, 1991.

[18] H. Kaneta and T. Maruta (1989), *An elementary proof and extension of Thas' theorem on k-arcs,* Math. Proc. Cambridge Philos. Soc., 105 (1989), pp. 459-462.

[19] B. Kestenband (1981), *Unital intersections in finite projective planes,* Geom. Dedicata, 11 (1981), pp. 107-117.

[20] L. Lunelli and M. Sce (1958), *k-archi completi nei piani proiettivi desarguesiani di rango 8 e 16,* Technical Report, Centro di Calcoli Numerici, Politecnico di Milano, 1958.

[21] F.J. MacWilliams and N.J.A. Sloane (1977), *The theory of error-correcting codes,* North-Holland, Amsterdam, 1977.

[22] C. Maneri and R. Siverman (1971), *A combinatorial problem with applications to geometry,* J. Combin. Theory Ser. A, 11 (1971), pp. 118-121.

[23] C. O'Keefe, T. Penttila (19**), *A new hyperoval in $PG(2,32)$,* 19**. To appear.

[24] S.E. Payne (1985), *A new family of generalized quadrangles,* Congress. Numer., 49 (1985), pp. 115-128.

[25] T. Penttila and I. Pinneri (1991), *Private communication,* 1991.

[26] T. Penttila and G. Royle (1991), *Private communication,* 1991.

[27] H.J. Ryser (1963), *Combinatorial mathematics,* Wiley, New York, 1963.

[28] B. Segre (1955a), *Ovals in a finite projective plane,* Canad. J. Math., 7 (1955), pp. 414-416.

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

[30] B. Segre (1957), *Sui k archi nei piani finiti di caratteristica due,* Rev. Math. Pures Appl., 2 (1957), pp. 289-300.

[31] B. Segre (1962), *Ovali e curve σ nei piani di Galois di caratteristica due,* Atti Accad. Naz. Lincei Rend., 32 (1962), pp. 785-790.

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

[33] G. Seroussi and R.M. Roth (1986), *On MDS extension of generalized Reed-Solomon codes,* IEEE Trans. Infor. Theory, IT-32 (1986), pp. 349-354.

[34] L. Storme (19**), *Completeness of normal rational curves 19***, To appear.

[35] L. Storme and J.A. Thas (19**a), *M.D.S. codes and arcs in $PG(n,q)$ with q even: An improvement of the bounds of Bruen, Thas and Blokhuis,* J. Combin. Theory Ser. A, 19**. To appear.

[36] L. Storme and J.A. Thas (19**b), *Generalized Reed-Solomon codes and normal rational curves: An improvement of results by Seroussi and Roth,* In Advances in Finite Geometries and Designs, (1991), Oxford University Press, Oxford pp. 369-389.

[37] J.A. Thas (1968), *Normal rational curves and k-arcs in Galois spaces,* Rend. Mat., 1 (1968), pp. 331-334.

[38] J.A. Thas (1969a), *Connection between the Grassmannian $G_{k-1;n}$ and the set of the k-arcs of the Galois space $S_{n,q}$,* Rend. Mat., 2 (1969), pp. 121-134.

[39] J.A. Thas (1969b), *Normal rational curves and $(q+2)$-arcs in a Galois space $S_{q-2,q}(q=2^h)$,* Atti Accad. Naz. Lincei Rend., 47 (1969), pp. 249-252.

[40] J.A. Thas (1987), *Complete arcs and algebraic curves in $PG(2,q)$,* J. Algebra, 106 (1987), pp. 451-464.

[41] J.F. Voloch (1990), *Arcs in projective planes over prime fields,* J. Geom., 38 (1990), pp. 198-200.

[42] J.F. Voloch (1991), *Complete arcs in Galois planes of non-square order,* In Advances in Finite Geometries and Designs, 1991, Oxford University Press, Oxford, pp. 401-406.

[43] M.L.H. Willems and J.A. Thas (1983), *A notte on the existence of special Laguerre i-structures and optimal codes,* European J. Combin., 4 (1983), pp. 93-96.

Seminar of Geometry and Combinatorics
University of Gent
Krijgslaan 281, B-9000 Gent, Belgium