ARCS, CAPS AND CODES OLD RESULTS, NEW RESULTS, GENERALIZATIONS

J.A. THAS
GHENT UNIVERSITY

INTRODUCTION

Non-singular conic of the projective plane PG($2, q$) over the finite field GF(q) consists of $q+1$ points no three of which are collinear. Do these properties characterize non-singular conics?
For q odd, affirmatively answered by B. Segre (1954, 1955).

Generalization 1 (Segre):

Sets of k points in PG($2, q$), $k \geq 3$, no three of which are collinear, and sets of k points in PG(n, q), $k \geq n+1$, no $n+1$ of which lie in a hyperplane; the latter are k-*arcs*.

Relation between k-arcs, algebraic curves and hypersurfaces. Also, arcs and linear MDS codes of dimension at least 3 are equivalent $\Rightarrow$ new results about codes.

<u>Generalization 2 (Segre)</u> :

k-*cap* of PG$(n,q), n \geq 3$, is a set of k points no three of which are collinear.
Elliptic quadric of PG$(3,q)$ is a cap of size q^2+1.
For q odd, the converse is true (Barlotti & Panella, 1955).
Also, q^2+1 is the maximum size of a k-cap in PG$(3,q), q \neq 2$.
An *ovoid* of PG$(3,q)$ is a cap of size q^2+1 for $q \neq 2$; for $q=2$ an ovoid is cap of size 5 with no 4 points in a plane.

Ovoids of particular interest discovered by J. Tits (1962).
Ovoids $\Rightarrow$ circle geometries, projective planes, designs, generalized polygons, simple groups.

Caps $\Rightarrow$ cap-codes.

Generalization 3 (JAT, 1971):

Arcs and caps can be generalized by replacing their points with n-dimensional subspaces to obtain generalized k-arcs and generalized k-caps.

These have strong connections to generalized quadrangles, projective planes, circle geometries, flocks and other structures.

Remark on references

In a Theorem the names of the authors are in the same order as the items in the statement. Also, JAT = Thas J. A.

1. k-Arcs

1.1 Definitions

A *k-arc* in PG(n, q) is a set K of k points, with $k \geq n + 1 \geq 3$, such that no $n + 1$ of its points lie in a hyperplane.
An arc K is *complete* if it is not properly contained in a larger arc. Otherwise, if $K \cup \{P\}$ is an arc for some point P of PG(n, q), the point P *extends* K.

A *normal rational curve* (NRC) of PG(n, q), $n \geq 2$, is any set of points in PG(n, q) which is projectively equivalent to

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

A NRC contains $q + 1$ points. A NRC is a $(q + 1)$-arc.
$n = 2 \Rightarrow$ *non-singular conic*
$n = 3 \Rightarrow$ *twisted cubic*
Any $(n + 3)$-arc of PG(n, q) is contained in a unique NRC.

1.2 k-Arcs and linear MDS codes

C : *m-dimensional linear code* over GF(q) of *length k*.

If *minimum distance* $d(C)$ of C is $k-m+1 \Rightarrow$ C is *maximum distance separable code* (MDS *code*).

For $m \geq 3$, linear MDS codes and arcs are equivalent objects.

C: m-dimensional subspace of vector space $V(k,q)$.
G: $m \times k$ generator matrix for C.
Then C is MDS if and only if any m columns of G are linearly independent.
Consider the columns of G as points $P_1, P_2, ..., P_k$ of PG($m-1, q$). So C is MDS if and only if $\{P_1, P_2, ..., P_k\}$ is a k-arc of PG($m-1, q$).
This gives the relation between linear MDS codes and arcs.

1.3 The three problems of Segre

I. Given n and q, what is the maximum value of k for which a k-arc exists in PG(n, q)?

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

III. For given n and q with $q > n+1$, what are the values of k such that each k-arc of PG(n, q) is contained in a $(q+1)$-arc of PG(n, q)?

Many partial solutions.
Many results obtained by relating k-arcs to algebraic hypersurfaces and polynomials (see e.g. Thas (1968), Ball (2012), Ball & De Beule (2012), Ball & Lavrauw (2017), Bruen, Thas & Blokhuis (1988), Hirschfeld (1998), Hirschfeld, Korchmáros & Torres (2008), Hirschfeld & Storme (2001), Hirschfeld & Thas (2016)).

1.4 k-Arcs in PG$(2, q)$

Theorem

Let K be a k-arc of PG$(2, q)$. Then

(i) $k \leq q + 2$;

(ii) for q odd, $k \leq q + 1$;

(iii) any non-singular conic of PG$(2, q)$ is a $(q + 1)$-arc;

(iv) each $(q+1)$-arc of PG$(2, q)$, q even, extends to a $(q + 2)$-arc.

$(q+1)$-arcs of PG$(2, q)$ are called *ovals*; $(q+2)$-arcs of PG$(2, q)$, q even, are called *complete ovals* or *hyperovals*.

Theorem (Segre (1954, 1955))

In PG$(2, q)$, q odd, every oval is a non-singular conic.

Remark

For q even many ovals are known which are not conics.

Theorem (Segre (1967), JAT (1987))

(i) for q even, every k-arc K with

$$k > q - \sqrt{q} + 1$$

extends to a hyperoval;

(ii) for q odd, every k-arc K with

$$k > q - \frac{1}{4}\sqrt{q} + \frac{25}{16}$$

extends to a conic.

Remarks

For q an even non-square bound (i) can be improved. For most odd values of q bound (ii) can be improved. One month ago Ball & Lavrauw (2017) obtained a very good bound for all odd q, thus improving considerably previous bounds.

For q a square and $q > 4$, there exist complete $(q - \sqrt{q} + 1)$-arcs in $\mathrm{PG}(2, q)$ (see e.g. Kestenband (1981)).
In $\mathrm{PG}(2, 9)$ there exists a complete 8-arc.

1.5 k-Arcs in PG$(3, q)$

Theorem (Segre (1955a), Casse (1969))

(i) For any k-arc of PG(3,q), q odd and $q > 3$, we have $k \leq q+1$; any k-arc of PG$(3,3)$ has at most 5 points.

(ii) For any k-arc of PG(3,q), q even and $q > 2$, we have $k \leq q+1$; any k-arc of PG$(3,2)$ has at most 5 points.

Theorem (Segre (1955a), Casse & Glynn (1982))

(i) Any $(q+1)$-arc of PG$(3, q)$, q odd, is a twisted cubic.

(ii) Every $(q+1)$-arc of $\mathrm{PG}(3, q)$, $q = 2^h$, is projectively equivalent to

$$C = \{(1, t, t^e, t^{e+1}) | t \in \mathrm{GF}(q)\} \cup \{(0, 0, 0, 1)\},$$

where $e = 2^m$ and $(m, h) = 1$.

1.6 k-Arcs in PG$(4, q)$ and PG$(5, q)$

Theorem
(Casse (1969), Segre (1955a), Casse & Glynn (1984),Kaneta & Maruta (1989), Glynn (1986))

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

(ii) For any k-arc of PG$(4, q)$, q odd and $q \geq 5$, $k \leq q + 1$ holds; any k-arc of PG$(4, 3)$ has at most 6 points.

(iii) Any $(q + 1)$-arc of PG$(4, q)$, q even, is a NRC.

(iv) For any k-arc of PG$(5, q)$, q even and $q \geq 8$, $k \leq q + 1$ holds.

(v) In PG$(4, 9)$ there exists a 10-arc which is not a NRC; this is the so-called *10-arc of Glynn*.

Remark

Canonical form of a 10-arc of Glynn:
$\{(t^4, t^3, t^2+\sigma t^6, t, 1) | t \in \mathrm{GF}(q)\} \cup \{(1,0,0,0,0)\}$, where σ is a primitive element of GF(q) with $\sigma^2 = \sigma + 1$.

1.7 k-Arcs in $\mathrm{PG}(n,q), n \geq 3$

Theorem
(JAT (1968), Kaneta & Maruta (1989))
Let K be a k-arc of $\mathrm{PG}(n,q)$, q odd and $n \geq 3$.

(i) If
$$k > q - \frac{1}{4}\sqrt{q} + n - \frac{7}{16}$$
then K lies on a unique NRC of $\mathrm{PG}(n,q)$.

(ii) If $k = q+1$ and $q > (4n - \frac{23}{4})^2$, then K is a NRC of $\mathrm{PG}(n,q)$.

(iii) If $q > (4n - \frac{39}{4})^2$, then $k \leq q+1$ for any k-arc of $\mathrm{PG}(n,q)$.

Remark

Relying on the new bound of Ball and Lavrauw in 1.4 the results in the previous theorem can be improved considerably.

Theorem (Ball (2012), Ball & De Beule (2012))

(i) If K is a k-arc of PG(n, q), $q = p^h$, p prime, $h > 1$, $n \leq 2p - 3$, then $k \leq q + 1$.

(ii) If K is a k-arc of PG(n, p), p prime and $n \leq p - 1$, then $k \leq p + 1$.

(iii) If K is a k-arc of PG(n, q), $q = p^h$, p prime, with $q \geq n + 1 \geq p + 1 \geq 4$, then $k \leq q - p + n + 1$.

(iv) For $n \leq p - 1$ all $(q + 1)$-arcs of PG(n, q), $q = p^h$, p prime, are NRC.

Theorem (Bruen, JAT & Blokhuis (1988) + Storme & JAT (1993))

(i) If K is a k-arc of PG(n,q), q even, $q \neq 2$, $n \geq 3$, with

$$k > q - \frac{1}{2}\sqrt{q} + n - \frac{3}{4},$$

then K lies on a unique $(q+1)$-arc.

(ii) Any $(q+1)$-arc K of PG(n,q), q even and $n \geq 4$, with

$$q > (2n - \frac{7}{2})^2,$$

is a NRC.

(iii) For any k-arc K of PG(n,q), q even and $n \geq 4$, with

$$q > (2n - \frac{11}{2})^2,$$

$k \leq q+1$ holds.

1.8 Theorem (JAT (1969))

A k-arc in PG(n, q) exists if and only if a k-arc in PG$(k - n - 2, q)$ exists.

1.9 Conjecture

(i) For any k-arc K of PG(n, q), q odd and $q > n + 1$, we have $k \leq q + 1$.

(ii) For any k-arc K of PG(n, q), q even, $q > n + 1$ and $n \notin \{2, q - 2\}$, we have $k \leq q + 1$.

Remark

For any q even, $q \geq 4$, there exists a $(q+2)$-arc in PG$(q - 2, q)$.

1.10 Open problems

(a) Classify all ovals and hyperovals of PG$(2,q)$, q even.

(b) Is every k-arc of PG$(2,q)$, q odd, $q > 9$ and $k > q - \sqrt{q} + 1$ extendable?

(c) Are complete $(q - \sqrt{q} + 1)$-arcs of PG$(2,q)$ unique?

(d) Is every 6-arc of PG$(3,q)$, $q = 2^h$, $h > 2$, contained in exactly one $(q+1)$-arc projectively equivalent to

$$C = \{(1, t, t^e, t^{e+1}) | t \in \mathrm{GF}(q)\} \cup \{(0, 0, 0, 1)\},$$

with $e = 2^m$ and $(m, h) = 1$?

(e) For which values of q does there exist a complete $(q-1)$-arc in PG$(2,q)$? There are 14 open cases.
For $q \in \{4,5,8\}$ a $(q-1)$-arc is incomplete in PG$(2,q)$,
for $q \in \{7,9,11,13\}$ there exists a complete $(q-1)$-arc in PG$(2,q)$,
for $q > 13$ a $(q-1)$-arc of PG$(2,q)$ is incomplete, except possibly for
$q \in \{49,81,37,41,43,47,53,$
$59,61,67,71,73,79,83\}$.

Solved by Ball and Lavrauw (as a corollary of their bound, see 1.4).

(f) Is conjecture 1.9 true?

(g) Solve problems I, II and III of Segre.

(h) In PG(n, q), q odd and $q \geq n$, are there $(q+1)$-arcs other than the 10-arc of Glynn which are not NRC?

(i) Is a NRC of PG(n, q), $q \geq n+1$, $2 < n < q-2$, always complete?

(j) Find the size of the second largest complete k-arc in PG$(2, q)$ for q odd and for q an even non-square.

(k) Find the size of the smallest complete k-arc in PG$(2, q)$ for all q.

2. k-Caps

2.1 Definitions

In PG(n, q), $n \geq 3$, a set K of k points no three of which are collinear is a *k-cap*.
A k-cap is complete if it is not contained in a $(k+1)$-cap . A line of PG(n, q) is a *secant*, *tangent* or *external line* as it meets K in 2,1 or 0 points.
The maximum size of a k-cap in PG(n, q) is denoted by $m_2(n, q)$.

2.2 k-Caps and cap-codes

This is entirely based on Hill (1978).

Let $K = \{P_1, P_2, ..., P_k\}$ with $P_i(a_{i0}, a_{i1}, ..., a_{in})$, be a k-cap of PG(n, q) which generates PG(n, q). Let A be the $k \times (n+1)$ matrix over GF(q) with elements a_{ij}, $i = 1, 2, ..., k$ and $j = 0, 1, ..., n$; A is called a *matrix* of K.

Let C be the linear $[k, n+1]$-code generated by the matrix A^T. Such a code is a *cap-code*.

A linear code with $(n+1) \times k$ generator matrix G is *projective* if no two columns of G represent the same point of PG(n, q). Hence cap-codes are projective.

Delete row i of the matrix A and all columns having a non-zero entry in that row $\Rightarrow$ matrix A_1. The $[k-1, n]$-code C_1 generated by A_1^T is a *residual* code of C.

Theorem

A projective code C is a cap-code iff every residual code of C is projective.

Theorem

Let K be a k-cap in PG(n, q) with code C. Then the minimum weight of C, and that of any residual, is at least $k - m_2(n-1, q)$.

Theorem

(i) $m_2(n, q) \leq q m_2(n-1, q) - (q+1)$, for $n \geq 4$;

(ii) $m_2(n, q) \leq q^{n-4} m_2(4, q) - q^{n-4} - 2\frac{q^{n-4}-1}{q-1} + 1$, $n \geq 5$.

2.3 k-Caps in PG$(3, q)$

For $q \neq 2$ $m_2(3, q) = q^2 + 1$ (Bose (1947), Qvist (1952)); $m_2(3, 2) = 8$. Each elliptic quadric of PG$(3, q)$ is a (q^2+1)-cap and any 8-cap of PG$(3, 2)$ is the complement of a plane.

A $(q^2 + 1)$-cap of PG$(3, q)$, $q \neq 2$, is an *ovoid*; the *ovoids* of PG$(3, 2)$ are its elliptic quadrics.

At each point P of an ovoid O of PG$(3, q)$, there is a unique *tangent plane* π such that $\pi \cap O = \{P\}$.
Ovoid O, π is plane which is not tangent plane $\Rightarrow \pi \cap O$ is $(q + 1)$-arc.
q is even $\Rightarrow$ the $(q^2 + 1)(q + 1)$ tangents of O are the totally isotropic lines of a symplectic polarity α of PG$(3, q)$, that is, the lines l for which $l^\alpha = l$.

Theorems (Barlotti (1955) + Panella (1955), Brown (2000))

(i) In PG$(3, q)$, q odd, every ovoid is an elliptic quadric.

(ii) In PG$(3, q)$, q even, every ovoid containing at least one conic section is an elliptic quadric.

Theorem (Tits (1962))

$W(q)$: incidence structure formed by all points and the totally isotropic lines of a symplectic polarity α of PG$(3, q)$.
Then $W(q)$ admits a polarity α' if and only if $q = 2^{2e+1}$. In that case absolute points of α' (points lying in their image lines) form an ovoid O of PG$(3, q)$; O is elliptic quadric if and only if $q = 2$.

For $q > 2$, the ovoids of the foregoing theorem are called *Tits ovoids*.
Canonical form of a Tits ovoid :

$$O = \{(1, z, y, x) | z = xy + x^{\sigma+2} + y^{\sigma}\} \cup \{(0, 1, 0, 0)\},$$

where σ is the automorphism $t \mapsto t^{2^{e+1}}$ of GF(q) with $q = 2^{2e+1}$.

The group of all projectivities of $\mathrm{PG}(3, q)$ fixing the Tits ovoid O is the Suzuki group $Sz(q)$, which acts doubly transitively on O.

For q even, no other ovoids than the elliptic quadrics and the Tits ovoids are known.

For q even and $q \leq 32$ all ovoids are known (Barlotti (1955), Fellegara (1962), O'Keefe & Penttila (1990, 1992), O'Keefe, Penttila & Royle (1994)). Finally we remark that for $q = 8$ the Tits ovoid was first discovered by Segre (1959).

2.4 Ovoids and inversive planes

Definitions

O : ovoid of PG$(3, q)$
$\mathcal{B}$: set of all intersections $\pi \cap O$,
π a non-tangent plane of O.

Then $\mathcal{I}(O) = (O, \mathcal{B}, \in)$ is a $3-(q^2+1, q+1, 1)$ design.
A $3-(n^2+1, n+1, 1)$ design $\mathcal{I} = (\mathcal{P}, \mathcal{B}, \in)$ is an *inversive plane of order* n and the elements of $\mathcal{B}$ are called *circles*.
Inversive planes arising from ovoids : *egglike*.
If the ovoid O is an elliptic quadric, then $\mathcal{I}(O)$, and any inversive plane isomorphic to it, is called *classical* or *Miquelian*.

Fundamental results

By 2.3 (Theorem of Barlotti & Panella) an egglike inverse plane of odd order is Miquelian. For odd order, no other inversive planes are known.

Theorem (Dembowski (1964))

Every inversive plane of even order is egglike.

Let $\mathcal{I}$ be an inversive plane of order n. For any point P of $\mathcal{I}$, the points of $\mathcal{I}$ other than P, together with the circles containing P with P removed, form a $2-(n^2, n, 1)$ design, that is, an affine plane of order n. This plane is denoted $\mathcal{I}_P$ and is called the *internal plane* or *derived plane* of $\mathcal{I}$ at P.

$\mathcal{I}(O)$ egglike $\Rightarrow \mathcal{I}_P$ Desarguesian, that is, AG$(2, q)$.

Theorem (JAT (1994))

Let $\mathcal{I}$ be an inversive plane of odd order n. If for at least one point P of $\mathcal{I}$, the internal plane $\mathcal{I}_P$ is Desarguesian, then $\mathcal{I}$ is Miquelian.

There is a unique inversive plane of order n, $n \in \{2, 3, 4, 5, 7\}$ (Witt (1938), Barlotti (1955), Chen (1972), Denniston (1973, 1973a)).
For $n = 3, 5, 7$ a computer free proof of this uniqueness is obtained as a corollary of the preceding theorem.

2.5 k-Caps in PG(n,q), $n \geq 3$

The maximum size of a k-cap in PG(n,q) is denoted by $m_2(n,q)$.

Theorem

(Bose (1947), Pellegrino (1990), Hill (1973), Edel & Bierbrauer (1999))

(i) $m_2(n,2) = 2^n$; a 2^n-cap of PG$(n,2)$ is the complement of a hyperplane;

(ii) $m_2(4,3) = 20$; there are nine projectively distinct 20-caps in PG(4,3);

(iii) $m_2(5,3) = 56$; the 56-cap in PG(5,3) is projectively unique;

(iv) $m_2(4,4) = 41$; there exist two projectively distinct 41-caps in PG(4,4).

Remark

No other values of $m_2(n, q)$, $n > 3$, are known.

Several bounds were obtained for the number k for which there exist complete k-caps in PG$(3, q)$ which are not ovoids; these bounds are used to determine bounds for $m_2(n, q)$, with $n > 3$. Here we mention just a few bounds.

Theorem (Hirschfeld (1983))

In PG$(3, q)$, q odd and $q \geq 67$, if K is a complete k-cap which is not an elliptic quadric, then

$$k < q^2 - \frac{1}{4}q^{\frac{3}{2}} + 2q.$$

Theorem (JAT (2017))

In PG$(3, q)$, q even and $q \geq 8$, if K is a complete k-cap which is not an ovoid, then

$$k < q^2 - (\sqrt{5} - 1)q + 5.$$

Remark Combining the previous theorem with the main theorem of Storme and Szőnyi (1993) there is an immediate improvement of the previous result. This important remark is due to Szőnyi.

Theorem (JAT (2017)

In PG$(3, q)$, q even and $q \geq 2048$, if K is a complete k-cap which is not an ovoid, then

$$k < q^2 - 2q + 3\sqrt{q} + 2.$$

Theorem (Meshulam (1995))

For $n \geq 4, q = p^h$ and p an odd prime,

$$m_2(n,q) \leq \frac{nh+1}{(nh)^2} q^n + m_2(n-1,q).$$

Theorem (Hirschfeld (1983))

In PG$(n,q), n \geq 4, q \geq 197$ and odd

$$m_2(n,q) < q^{n-1} - \frac{1}{4} q^{n-\frac{3}{2}} + 2q^{n-2}.$$

In fact, for $q \geq 67$ and odd,

$$m_2(n,q) < q^{n-1} - \frac{1}{4} q^{n-\frac{3}{2}} +$$

$$\frac{1}{16}(31q^{n-2} + 22q^{n-\frac{5}{2}} - 112q^{n-3} - 14q^{n-\frac{7}{2}} + 69q^{n-4})$$

$$-2(q^{n-5} + q^{n-6} + \cdots + q + 1) + 1,$$

where there is no term $-2(q^{n-5} + q^{n-6} + \cdots + 1)$ for $n = 4$.

Theorem (JAT (2017))

(i) $m_2(4,8) \le 479$;

(ii) $m_2(4,q) < q^3 - q^2 + 2\sqrt{5}q - 8$, q even, $q > 8$.

(iii) $m_2(4,q) < q^3 - 2q^2 + 3q\sqrt{q} + 8q - 9\sqrt{q} - 2$, q even, $q \ge 2048$.

Theorem (JAT (2017))

For q even, $q > 2, n \geq 5$.

(i) $m_2(n,4) \leq \frac{118}{3} 4^{n-4} + \frac{5}{3}$,

(ii) $m_2(n,8) \leq 478.8^{n-4} - 2(8^{n-5} + 8^{n-6} + \cdots + 8 + 1) + 1$,

(iii) $m_2(n,q) < q^{n-1} - q^{n-2} + 2\sqrt{5}q^{n-3} - 9q^{n-4} - 2(q^{n-5} + q^{n-6} + \cdots + q + 1) + 1$, for $q > 8$.

(iv) $m_2(n,q) < q^{n-1} - 2q^{n-2} + 3q^{n-3}\sqrt{q} + 8q^{n-3} - 9q^{n-4}\sqrt{q} - 3q^{n-4} - 2(q^{n-5} + q^{n-4} + \cdots + q + 1) + 1$, for $q \geq 2048$.

Remark

In PG$(3, q)$, our bound is better than the bound $k \leq q^2 - q + 5$ (q even and $q \geq 8$) of J. M. Chao (1999). In 2014, J. M. Cao and L. Ou (2014) published the bound $k \leq q^2 - 2q + 8$ (q even and $q \geq 128$), which is better than ours. However I did not understand some reasoning in their proof, so I sent two mails to one of the authors explaining why I think part of the proof is not correct. I never received an answer.

2.6 Open problems

(a) In PG$(3,q)$, $q \neq 2$, what is the maximum size of a complete k-cap with $k < q^2+1$?

(b) Classify all ovoids of PG$(3,q)$, for q even.

(c) Is every inversive plane of odd order Miquelian?

(d) Determine $m_2(n,q)$ or upper bounds of $m_2(n,q)$ for $n \geq 4, q \neq 2$.

3. Generalized ovals and ovoids

3.1 Introduction

Arcs and caps can be generalized by replacing their points with $(n-1)$-dimensional subspaces, $n \geq 1$, to obtain *generalized k-arcs* and *generalized k-caps*.

We will focus on generalized ovals and generalized ovoids.

Strong connections to: generalized quadrangles, projective planes, circle geometries, flocks, strongly regular graphs, two-weight codes and other structures.

3.2 Generalized k-arcs and generalized k-caps

Definitions

(1) A *generalized k-arc* of $\mathrm{PG}(mn+n-1,q)$, $k \geq m+1 \geq 3$: set K of k $(n-1)$-dimensional subspaces such that no $m+1$ of its elements lie in a hyperplane. A generalized arc K is *complete* if it is not properly contained in a larger generalized arc. Otherwise, if $K \cup \{\pi\}$ is an arc for some $(n-1)$-dimensional subspace π of $\mathrm{PG}(mn+n-1,q)$, the space π *extends* K.

(2) A *generalized k-cap* of $\mathrm{PG}(l,q)$: set K of k $(n-1)$-dimensional subspaces, $k \geq 3$, no three of which are linearly dependent.

Theorem (JAT (1971))

(i) For every generalized k-arc of PG$(3n-1,q)$ we have $k \leq q^n+2$; for q odd we always have $k \leq q^n+1$.

(ii) In PG$(3n-1,q)$ there exist generalized (q^n+1)-arcs; for q even there exist generalized (q^n+2)-arcs in PG$(3n-1,q)$.

(iii) If O is a generalized (q^n+1)-arc of PG$(3n-1,q)$, then each element π_i of O is contained in exactly one $(2n-1)$-dimensional subspace τ_i which is disjoint from all elements of $O \setminus \{\pi_i\}$; τ_i is the *tangent space* of O at π_i.

(iv) For q even all tangent spaces of a generalized (q^n+1)-arc O of PG$(3n-1,q)$ contain a common $(n-1)$-dimensional subspace π; π is the *nucleus* of O. Hence O is incomplete and extends to a $(q^n + 2)$-arc by adding to O its nucleus.

3.3 Generalized ovals and ovoids

Definitions

In Ω = PG$(2n + m - 1, q)$ define a set $O = O(n, m, q)$ of subspaces as follows: O is a set of $(n - 1)$-dimensional subspaces π^i_{n-1}, with $|O| = q^m + 1$, such that

(i) every three generate a PG$(3n - 1, q)$;

(ii) for every $i = 0, 1, ..., q^m$, there is a subspace τ_i of Ω of dimension $m+n-1$ which contains π^i_{n-1} and is disjoint from π^j_{n-1} for $j \neq i$.

(1) If $m = n$, O is a *pseudo-oval* or *generalized oval* or $[n - 1]$-*oval* of PG$(3n - 1, q)$.

For $m = 1$, a [0]-oval is just an oval of $\mathrm{PG}(2, q)$. By 3.2 each generalized (q^n+1)-arc of $\mathrm{PG}(3n-1, q)$ is a pseudo-oval.

(2) For $n \neq m$, the set O is a *pseudo-ovoid* or *generalized ovoid* or $[n-1]$-*ovoid* or *egg* of $\mathrm{PG}(2n+m-1, q)$. A [0]-ovoid is just an ovoid of $\mathrm{PG}(3, q)$.

(3) The space τ_i is the *tangent space* of O at π^i_{n-1}; it is uniquely determined by O and π^i_{n-1}.

<u>Theorem (Payne & JAT (1984, 2009))</u>

(i) For any $O(n, m, q)$, $n \leq m \leq 2n$ holds;

(ii) Either $n = m$ or $n(a+1) = ma$ with $a \in \mathbf{N_0}$ and a odd.

Theorem (Payne & JAT (1984, 2009))

(i) Each hyperplane of PG$(2n+m-1,q)$ not containing a tangent space of $O(n,m,q)$, contains either 0 or $1+q^{m-n}$ elements of $O(n,m,q)$. If $m=2n$, then each such hyperplane contains exactly $1+q^n$ elements of $O(n,2n,q)$. If $m \neq 2n$, then there are hyperplanes which contain no element of $O(n,m,q)$.

(ii) If $n=m$ with q odd or if $n \neq m$, then each point of PG$(2n+m-1,q)$ which is not contained in an element of $O(n,m,q)$ belongs to either 0 or $q^{m-n}+1$ tangent spaces of $O(n,m,q)$. If $m=2n$ then each such point belongs to exactly q^n+1 tangent spaces of the egg. If $m \neq 2n$, then there are points contained in no tangent space of $O(n,m,q)$.

(iii) For any $O(n,m,q)$, q even, we have

$$m \in \{n, 2n\}.$$

Corollary

Let $\widetilde{O}$ be the union of all elements of any $O(n,2n,q)$ in PG$(4n-1,q)$ and let π be any hyperplane. Then $|\widetilde{O} \cap \pi| \in \{\gamma_1, \gamma_2\}$, with

$$\gamma_1 = \frac{(q^n-1)(q^{2n-1}+1)}{q-1}, \gamma_1 - \gamma_2 = q^{2n-1}.$$

Hence $\widetilde{O}$ defines a linear projective two-weight code and a strongly regular graph.

3.4 Regular pseudo-ovals and pseudo-ovoids

In the extension PG$(2n+m-1, q^n)$ of the space PG$(2n+m-1, q)$, with $m \in \{n, 2n\}$, consider n subspaces $\xi_i, i = 1, 2, ..., n$, each a PG$(\frac{m}{n}+1, q^n)$, that are conjugate in the extension GF(q^n) of GF(q) and which span PG$(2n+m-1, q^n)$. This means that they form an orbit of the Galois group corresponding to this extension and that they span PG$(2n+m-1, q^n)$.

In ξ_1, consider an oval O_1 for $n = m$ and an ovoid O_1 for $m = 2n$.Further, define $O_1 = \{x_0^{(1)}, x_1^{(1)}, ..., x_{q^m}^{(1)}\}$. Next, let $x_i^{(1)}, x_i^{(2)}, ..., x_i^{(n)}$, with $i = 0, 1, ..., q^m$, be conjugate in GF(q^n) over GF(q). The points $x_i^{(1)}, ..., x_i^{(n)}$ define an $(n-1)$-dimensional subspace π_i over GF(q) for $i = 0, 1, ..., q^m$. Then, $O = \{\pi_0, \pi_1, ..., \pi_{q^m}\}$ is a generalized oval of PG$(3n-1, q)$ for $n = m$

and a generalized ovoid of $\mathrm{PG}(4n-1,q)$ for $m=2n$. These objects are the *regular* or *elementary pseudo-ovals* and the *regular* or *elementary pseudo-ovoids*.

Every known pseudo-oval is regular and, for q even, every known pseudo-ovoid is regular. For q odd there are pseudo-ovoids which are not regular.

3.5 Translation duals

Theorem (Payne & JAT (1984, 2009))

(i) For q odd, the tangent spaces of a pseudo-oval $O(n, n, q)$ form a pseudo-oval $O^*(n, n, q)$ in the dual space of PG$(3n - 1, q)$.

(ii) The tangent spaces of an egg $O(n, m, q)$ in PG$(2n + m - 1, q)$ form an egg $O^*(n, m, q)$ in the dual space of PG$(2n + m - 1, q)$.

Definition

(1) The pseudo-oval $O^*(n, n, q)$ is the *translation dual* of the pseudo-oval $O(n, n, q)$.

(2) The egg $O^*(n, m, q)$ is the *translation dual* of the egg $O(n, m, q)$.

3.6 Characterizations

Let $O = O(n, n, q) = \{\pi_0, ..., \pi_{q^n}\}$ be a pseudo-oval in $\mathrm{PG}(3n-1, q)$. The tangent space of O at π_i is τ_i. Choose $\pi_i, i \in \{0, 1, ..., q^n\}$, and let $\mathrm{PG}(2n-1, q) \subseteq \mathrm{PG}(3n-1, q)$ be skew to π_i. Further, let $\tau_i \cap$ $\mathrm{PG}(2n-1, q) = \eta_i$ and $\langle \pi_i, \pi_j \rangle \cap$ $\mathrm{PG}(2n-1, q) = \eta_j$, with $j \neq i$. Then $\{\eta_0, \eta_1, ..., \eta_{q^n}\} = \Delta_i$ is an $(n-1)$-spread of $\mathrm{PG}(2n-1, q)$.

Now, let q be even and let π be the nucleus of O. Let $\mathrm{PG}(2n-1, q) \subseteq \mathrm{PG}(3n-1, q)$ be skew to π. If $\zeta_j = \mathrm{PG}(2n-1, q) \cap \langle \pi, \pi_j \rangle$, then $\{\zeta_0, \zeta_1, ..., \zeta_{q^n}\} = \Delta$ is an $(n-1)$-spread of $\mathrm{PG}(2n-1, q)$.

Next, let q be odd. Choose $\tau_i, i \in \{0, 1, ..., q^n\}$. If $\tau_i \cap \tau_j = \delta_j$, with $j \neq i$, then

$$\{\delta_0, \delta_1, ..., \delta_{i-1}, \pi_i, \delta_{i+1}, ..., \delta_{q^n}\} = \Delta_i^*$$

is an $(n-1)$-spread of τ_i.

Theorem (Casse, JAT & Wild (1985))

Consider a pseudo-oval O with q odd. Then at least one of the $(n-1)$-spreads

$$\Delta_0, \Delta_1, ..., \Delta_{q^n}, \Delta_0^*, \Delta_1^*, ..., \Delta_{q^n}^*$$

is regular iff they all are regular iff the pseudo-oval O is regular.

Theorem (Rottey & Van de Voorde (2015))

Consider a pseudo-oval O of $\mathrm{PG}(3n-1, q)$, with $q = 2^h, h > 1, n$ prime. Then all $(n-1)$-spreads $\Delta_0, \Delta_1, ..., \Delta_{q^n}$ are regular iff the pseudo-oval O is regular.

An alternative shorter proof and a slightly stronger result is contained in JAT (2017a)

In PG$(3n-1,q)$ let π_1, π_2, π_3 be mutually skew $(n-1)$-dimensional subspaces, further let τ_i be a $(2n-1)$-dimensional space containing π_i but skew to π_j and π_k, with $\{i,j,k\} = \{1,2,3\}$, and let $\tau_i \cap \tau_j = \eta_k$, with $\{i,j,k\} = \{1,2,3\}$. The space generated by η_i and π_i will be denoted by ζ_i, with $i = 1,2,3$. If the $(2n-1)$-dimensional spaces $\zeta_1, \zeta_2, \zeta_3$ have a $(n-1)$-dimensional space in common, then $\{\pi_1, \pi_2, \pi_3\}$ and $\{\tau_1, \tau_2, \tau_3\}$ are in *perspective*.

Theorem (JAT (2011))

Assume that $O = \{\pi_0, \pi_1, ..., \pi_{q^n}\}$ is a pseudo-oval of PG$(3n-1,q)$, q odd, and let τ_i be the tangent space of O at π_i, with $i = 0,1,...,q^n$. If for any three distinct $i,j,k \in \{0,1,...,q^n\}$ the triples $\{\pi_i, \pi_j, \pi_k\}$ and $\{\tau_i, \tau_j, \tau_k\}$ are in perspective, then O is regular. The converse also holds.

Theorem (Payne & JAT (1984, 2009))

The egg $O(n, 2n, q)$ is regular iff one of the following holds.

(i) For any point z not contained in an element of $O(n, 2n, q)$, the $q^n + 1$ tangent spaces containing z have exactly $(q^n - 1)/(q - 1)$ points in common.

(ii) Each PG$(3n - 1, q)$ which contains at least three elements of $O(n, 2n, q)$, contains exactly $q^n + 1$ elements of $O(n, 2n, q)$.

Remark

For more on generalized ovals and generalized ovoids we refer to THAS & PAYNE (1984, 2009), and THAS, THAS & VAN MALDEGHEM (2006).

3.7 Open problems

(a) What is the maximium number of elements of a generalized k-arc in PG$(mn+n-1, q)$?

(b) What is the maximum number of elements of a generalized k-cap in PG(l, q)?

(c) Is $q^{2n}+1$ the maximum number of elements of a generalized k-cap in PG$(4n-1, q)$, with $m > 1$?

(d) A *weak generalized ovoid* is a generalized $(q^{2n}+1)$-cap in PG$(4n-1, q)$. Is every weak generalized ovoid a generalized ovoid?

(e) Does there exist an egg $O(n, m, q)$ for q odd and $m \notin \{n, 2n\}$?

(f) Is every pseudo-oval regular?

(g) For q even, is every generalized ovoid $O(n, 2n, q)$ regular?

(h) Is $O(n, n, q)$, with q odd, always isomorphic to its translation dual?

(i) For q even, is every $O(n, 2n, q)$ always isomorphic to its translation dual?
In the odd case there are counterexamples.

(j) Is a pseudo-oval $O(n, n, 2)$ regular if all spreads $\Delta_0, \Delta_1, ..., \Delta_{2^n}$ are regular?

(k) Consider a pseudo-oval $O(n, n, q)$, with $q = 2^h, h > 1$, and n prime. Is $O(n, n, q)$ regular if at least one of the spreads $\Delta_0, \Delta_1, ..., \Delta_{q^n}$ is regular?

(l) Consider a pseudo-oval $O(n, n, q)$, with $q = 2^h, h > 1$, and n not prime. Is $O(n, n, q)$ regular if all spreads $\Delta_0, \Delta_1, ..., \Delta_{q^n}$ are regular?

REFERENCES

BALL, S (2012) On sets of vectors of a finite vector space in which every subset of basis size is a basis, *J. Eur. Math. Soc*. 14, 733-748.

BALL, S and DE BEULE, J (2012) On sets of vectors of a finite vector space in which every subset of basis size is a basis II, *Des. Codes Cryptogr.* 65, 5-14.

BALL, S and LAVRAUW, M (2017) Planar arcs, *Arxiv* 1705.10940v2 [math. CO].

BARLOTTI, A (1955) Un' estensione del teorema di Segre-Kustaanheime, *Boll. Unione Mat. Ital.* 10, 96-98.

BLOKHUIS, A, BRUEN, A. A. and THAS, J. A (1990) Arcs in $PG(n, q)$, MDS-codes and three fundamental problems of B. Segre - some extensions, *Geom. Dedic.* 35, 1-11.

BOSE, R. C. (1947) Mathematical theory of the symmetrical factorial design, *Sankhya* 8,

107-166.
BROWN, M. R. (2000) Ovoids of $PG(3,q)$, q even, with a conic section, *J. Lond. Math. Soc.* 62, 569-582.
BRUEN, A. A., THAS, J. A. and BLOKHUIS, A. (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, 441-459.
CAO, J. M. and OU, L (2014) Caps in $PG(n,q)$ with q even and $n \geq 3$, *Discrete Math.* 326, 61-65.
CASSE, L. R. A. (1969) A solution to Beniamino Segre's 'Problem $I_{r,q}$' for q even, *Atti Accad. Naz. Lincei Rend* 46, 13-20.
CASSE, L. R. A. and GLYNN, D. G. (1982) The solution to Beniamino Segre's problem $I_{r,q}, r = 3, q = 2^h$, *Geom. Dedic.* 13, 157-164.
CASSE, L. R. A. and GLYNN, D. G. (1984) On the uniqueness of $(q+1)_4$-arcs of $PG(4,q), q =$

$2^h, h \geq 3$, *Discrete Math.* 48, 173-186.
CASSE, L. R. A., THAS, J. A. and WILD, P. R. (1985) (q^n+1)-sets of $PG(3n-1, q)$, generalized quadrangles and Laguerre planes, *Simon Stevin* 59, 21-42.
CHAO, J. M. (1999) On the size of a cap in $PG(n, q)$ with q even and $n \geq 3$, *Geom. Dedic.* 74, 91-94.
CHEN, Y (1972) The Steiner systems $S(3, 6, 26)$, *J. Geom.* 2, 7-28.
DEMBOWSKI, P. (1968) *Finite Geometries*, Springer, New York, 375 pp.
DENNISTON, R. H. F. (1973) Uniqueness of the inversive plane of order 5, *Manuscr. Math.* 8, 11-19.
DENNISTON, R. H. F. (1973a) Uniqueness of the inversive plane of order 7, *Manuscr. Math.* 8, 21-23.
EDEL, Y. and BIERBRAUER, J. (1999) 41 is the largest size of a cap in $PG(4, 4)$, *Des. Codes Cryptogr.* 16, 151-160.

FELLEGARA, G. (1962) Gli ovaloidi di uno spazio tridimensionale di Galois di ordine 8, *Atti Accad Naz. Lincei Rend.* 32, 170-176.
HILL, R. (1973) On the largest size of cap in $S_{5,3}$, *Atti Accad. Naz. Lincei Rend.* 54, 378-384.
HILL, R. (1978) Caps and codes, *Discrete Math.* 22, 111-137.
HIRSCHFELD, J. W. P. (1998) *Projective Geometries over Finite Fields*, second edition, Oxford University Press, xiv + 555 pp.
HIRSCHFELD, J. W. P. (1983) Caps in elliptic quadrics, *Ann. Discrete Math.* 18, 449-466.
HIRSCHFELD, J. W. P. , KORCHMÁROS, G. and TORRES, F. (2008) *Algebraic Curves over a Finite Field*, Princeton University Press, Princeton, xxii + 696 pp.
HIRSCHFELD, J. W. P. and STORME, L. (2001) The packing problem in statistics, coding theory and finite projective spaces: update 2001, in *Finite Geometries, Developments in*

Mathematics, Kluwer, Boston, pp. 201-246.
HIRSCHFELD, J. W. P. and THAS, J. A. (2016) *General Galois Geometries*, second edition, Springer, London, xvi + 409 pp.
KANETA, H. and MARUTA, T. (1989) An elementary proof and extension of Thas' theorem on k-arcs, *Math. Proc. Camb. Philos. Soc.* 105, 459-462.
KESTENBAND, B. C. (1981) Unital intersections in finite projective planes, *Geom. Dedic.* 11, 107-117.
MESHULAM, R. (1995) On subsets of finite abelian groups with no 3-term arithmetic progression, *J. Combin. Theory, Ser. A* 71, 168-172.
O' KEEFE, C. M. and PENTTILA, T. (1990) Ovoids of $PG(3,16)$ are elliptic quadrics, *J. Geom.* 38, 95-106.
O' KEEFE, C. M. and PENTTILA, T. (1992) Ovoids of $PG(3,16)$ are elliptic quadrics. II, *J. Geom.* 44, 140-159.

O'KEEFE, C. M., PENTTILA, T. and ROYLE, G. F. (1994) Classification of ovoids in $PG(3, 32)$, *J. Geom.* 50, 143-150.
PANELLA, G. (1955) Caratterizzazione delle quadriche di uno spazio (tri-dimensionale) lineare sopra un corpo finito, *Boll. Unione Mat. Ital.* 10, 507-513.
PAYNE, S. E. and THAS, J. A. (1984) *Finite Generalized Quadrangles*, Pitman, London, 312 pp.
PAYNE, S. E. and THAS, J. A. (2009) *Finite Generalized Quadrangles*, second edition, European Mathematical Society, Zurich, xii + 287 pp.
PELLEGRINO, G. (1970) Sul massimo ordine delle calotte in $S_{4,3}$, *Matematice (Catania)* 25, 1-9.
QVIST, B. (1952) Some remarks concerning curves of the second degree in a finite plane, *Ann. Acad. Sci. Fenn., Ser. A* 134, 1-27.
ROTTEY, S. and VAN DE VOORDE, G. (2015)

Pseudo-ovals in even characteristic and ovoidal Laguerre planes, *J. Combin. Theory, Ser. A* 129, 105-121.
SEGRE, B. (1954) Sulle ovali nei piani lineari finiti, *Atti Accad. Naz. Lincei Rend.* 17, 1-2.
SEGRE, B. (1955) Ovals in a finite projective plane, *Can. J. Math.* 7, 414-416.
SEGRE, B. (1955a) Curve razionali normali e k-archi negli spazi finiti, *Ann. Mat. Pura Appl.* 39, 357-379.
SEGRE, B. (1959) On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two, *Acta Arith.* 5, 315-332.
SEGRE, B. (1967) Introduction to Galois Geometries, *Atti Accad. Naz. Lincei Mem.* 8, 133-236 (edited by J. W. P. Hirschfeld).
STORME, L. and THAS, J. A. (1993) 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* 62, 139-154.

STORME, L. and SZŐNYI, T. (1993) Caps in $PG(n,q)$, q even, $n \geq 3$, *Geom. Dedic.* 45, 163-169.

THAS, J. A. (1968) Normal rational curves and k-arcs in Galois spaces, *Rend. Mat.* 1, 331-334.

THAS, J. A. (1969) 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, 121-134.

THAS, J. A. (1971) The m-dimensional projective space $S_m(M_n(GF(q)))$ over the total matrix algebra $M_n(GF(q))$ of the $(n\times n)$-matrices with elements in the Galois field $GF(q)$, *Rend. Mat.* 4, 459-532.

THAS, J. A. (1987) Complete arcs and algebraic curves in $PG(2,q)$, *J. Algebra* 106, 451-464.

THAS, J. A. (1994) The affine plane $AG(2,q)$, q odd, has a unique one point extension, *Invent. Math.* 118, 133-139.

THAS, J. A. (2011) Generalized ovals in $PG(3n-1, q)$, with q odd, *Pure Appl. Math. Q.* 7, 1007-1035 (Special Issue: in honor of Jacques Tits).
THAS, J. A. (2017) On k-caps in $PG(n, q)$, with q even and $n \geq 3$, *Discrete Math.*, to appear.
THAS, J. A. (2017a) Regular pseudo-hyperovals and regular pseudo-ovals in even characteristic, submitted, Arxiv 1702.01097.
THAS, J. A., THAS, K. and VAN MALDEGHEM, H. (2006) *Translation Generalized Quadrangles*, Ser. Pure Math., vol. 6, World Sci. Publ., Hackensack, xxx + 345 pp.
TITS, J. (1962) Ovoides et groupes de Suzuki, *Arch. Math.* 13, 187-198.
WITT, E. (1938) Über Steinersche Systeme, *Abh. Math. Sem. Hamburg* 12, 265-275.

J. A. THAS, Ghent University