# ARCS, CAPS AND CODES

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).

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.

Generalization 2 (Segre) :

$k$-*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 and 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, finite simple groups.

## 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

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

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 $P_1, P_2, \cdots, P_k$ of PG($m - 1, q$). So $C$ is MDS if and only if $\{P_1, P_2, \cdots, P_k\}$ 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. For given $n$ and $q$, what is the maximum value of $k$ such that 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 (Segre, Bruen, Blokhuis, Thas)

## 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)

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, Thas)

(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 many particular values of $q$ the bounds in the previous theorem can be improved.

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

In PG$(2, 9)$ there exists a complete 8-arc.

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

**Theorem (Segre, Casse)**

(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, Casse & Glynn)**

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

(ii) Every $(q+1)$-arc of 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, Segre, Casse & Glynn, Kaneta & Maruta, Glynn)

(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*.

## 1.7 $k$-Arcs in PG$(n,q), n \geq 3$

Theorem (Thas, Kaneta & Maruta)

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

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

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

## Theorem (Blokhuis, Bruen, Thas, Storme)

(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 (Thas)

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) 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 $(m, h) = 1$?

(d) For which values of $q$ does there exist a complete $(q-1)$-arc in PG$(2, q)$? there are 14 open cases.

(e) Is conjecture 1.9 true?

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

(g) 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?

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

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

(j) Find the size of the smallest complete $k$-arc in $\mathrm{PG}(2, q)$ 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 in PG$(3, q)$

For $q \neq 2$ $m_2(3, q) = q^2 + 1$ (Bose, Qvist); $m_2(3, 2) = 8$. 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 $\mathrm{PG}(3,q)$, $q \neq 2$, is an *ovoid*; the *ovoids* of $\mathrm{PG}(3,2)$ are its elliptic quadrics.

At each point $P$ of an ovoid $O$ of $\mathrm{PG}(3,q)$, there is a unique *tangent plane* $\pi$ such that $\pi \cap O = \{P\}$.
Ovoid $O$, $\pi$ 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 $\alpha$ of $\mathrm{PG}(3,q)$, that is, the lines $l$ for which $l^\alpha = l$.

Theorems (Barlotti & Panella, Brown)

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

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

Theorem (Tits)

$W(q)$ : incidence structure formed by all points and the totally isotropic lines of a symplectic polarity $\alpha$ of PG$(3,q)$.
Then $W(q)$ admits a polarity $\alpha'$ if and only if $q = 2^{2e+1}$. In that case absolute points of $\alpha'$ (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 $\sigma$ is the automorphism $t \mapsto t^{2^{e+1}}$ of GF$(q)$ with $q = 2^{2e+1}$.

The group of all projectivities of 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, Fellegara, O'Keefe, Penttila, Royle). Finally we remark that for $q = 8$ the Tits ovoid was first discovered by Segre.

## 2.3 Ovoids and inversive planes

### Definitions

$O$ : ovoid of PG$(3, q)$
$\mathcal{B}$ : set of all intersections $\pi \cap O$,
$\pi$ 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 2.2 (Theorem of Barlotti & Panella) an egglike inverse plane of odd order is Miquelian. For odd order, no other inversive planes are known.

Theorem (Dembowski)

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 (Thas)

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 $n$, $n \in \{2, 3, 4, 5, 7\}$ (Chen, Denniston, Witt).
For $n = 3, 5, 7$ a computer free proof of this uniqueness is obtained as a corollary of the preceding theorem.

## 2.4 Open problems

(a) In PG$(3, q)$, $q \neq 2$, what is the maximum size of a complete $k$-cap with $k < q^2 + 1$? Partial results are known, e.g. : in PG$(3, q)$, $q$ odd and $q \geq 67$, if $K$ is a complete $k$-cap which is not an elliptic quadric, then

$$k < q^2 - \frac{1}{4}q^{3/2} + 2q \text{ (Hirschfeld);}$$

in PG$(3, q)$, $q$ even and $q \geq 128$, if $K$ is a complete $k$-cap which is not an ovoid, then

$$k \leq q^2 - 2q + 8 \text{ (Cao and Ou).}$$

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

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

(d) Determine $m_2(n, q)$ for $n \geq 4$. Many partial results are known :
$m_2(n, 2) = 2^n, m_2(4, 3) = 20$ (Pellegrino),
$m_2(5, 3) = 56$ (Hill), $m_2(4, 4) = 41$ (Edel & Bierbrauer);
several bounds for $m_2(n, q)$ are known.