# Recent results on $k$-arcs in Galois geometries


Angelo Sonnino

Università degli Studi della Basilicata
Potenza, Italy


Kerékjártó Geometriai Szeminárium

Szeged, 11th April 2013

# Arcs in $\mathrm{PG}(r, q)$

Let $q = p^h$ be a power of a prime integer. An arc of size $k$ (briefly a $k$-arc) in $\mathrm{PG}(r, q)$ is a set $\mathcal{K}$ consisting of $k$ points no $r + 1$ of which are contained in a hyperplane.

A $k$-arc is said to be complete if it is not contained in a (k+1)-arc.

# Motivations

- $k$-rcs in projective spaces (and planes) are interesting objects in their own right.
- $k$-arcs and linear M.D.S. codes are equivalent objects; J. A- Thas, (1992).
- Many known "good" covering codes and saturating sets arise from complete $k$-arcs; M. Giulietti and R. Vincenti (2012).
- $k$-arcs in finite projective spaces can be used in cryptography in order to produce multilevel secret sharing schemes; G. J. Simmons (1989, 1990), M. Giulietti and R. Vincenti (2012), G. Korchmáros, V. Lanzone and AS (2012).

# Arcs in $\mathrm{PG}(3, q)$

A $k$-arc in $\mathrm{PG}(3, q)$ is a set $\mathcal{K}$ consisting of $k$ points no four of which are coplanar.

- $k \leq q + 1$.

- If $k = q + 1$, then the collineation group fixing $\mathcal{K}$ contains $\mathrm{PGL}(2, q)$ and acts on its points as a 3-transitive permutation group.

- A $k$-arc whose collineation group $G$ acts transitively on its points is called a "$G$-transitive" $k$-arc.

# The problem

- Find a collineation group $G$ acting faithfully on $\mathrm{PG}(3, q)$.

- Give some sufficient condition for the orbit $P^G$ of some point $P \in \mathrm{PG}(3, q)$ to be a $k$-arc..

- In other words: does a $G$-transitive $k$-arc exist in $\mathrm{PG}(3, q)$ for a fixed $k$ and infinitely many values of $q = p^h$?

- Investigate the completeness of such $k$-arcs in view of the lower bound for the size of a complete $k$-arc in $\mathrm{PG}(3, q)$.

# Background

Previuos work in the projective plane $\mathrm{PG}(2,q)$.

- Construction of a $\mathrm{PSL}(2,7)$-transitive 24-arc in $\mathrm{PG}(2,29)$; J. M. Chao and H. Kaneta (1996).
- An infinite family of $\mathrm{PSL}(2,7)$-transitive 42-arcs in $\mathrm{PG}(2,q)$ for any $q = p^h \geq 53$ with $p \neq 7$ an odd prime, $q^3 \equiv 1 \pmod 7$, apart from finitely many values of $q$; L. Indaco and G. Korchmáros (2012).
- An infinite family of $\mathrm{A}_6$-transitive 90-arcs in either $\mathrm{PG}(2,q)$ or $\mathrm{PG}(2,q^2)$, with $q \geq 349$ and $q \neq 421$, which turn out to be complete for $q \in \{349, 409, 529, 601, 661\}$; M. Giulietti, G. Korchmáros, S. Marcugini and F. Pambianco (online 2012).

# Background

So far very little is known about $k$-arcs in $\mathrm{PG}(3,q)$.

- The maximum size for a $k$-arc in $\mathrm{PG}(3,q)$ is $q+1$.
  - If $q$ is odd and $q>4$ then any $(q+1)$-arc is projectively equivalent to a normal rational curve:

$$\{\,(t^2 : t^2 : t : 1) \mid t \in \mathbb{F}_q\,\} \cup \{(1:0:0:0)\}.$$

  - If $q=2^h$ with $h>1$ then any $(q+1)$-arc is projectively equivalent to a curve

$$\{\,(t^{2n+1} : t^{2n} : t : 1) \mid t \in \mathbb{F}_q\,\} \cup \{(1:0:0:0)\}$$

    with $\mathrm{MCD}(n,h)=1$.
- Large $k$-arcs lying on elliptic quadrics in $\mathrm{PG}(3,q)$; AS (1995, 1999).

# Choose the group

If $q \equiv 1 \pmod 7$, then the projective special linear group $\mathrm{PSL}(2,7)$ can be regarded as a distinguished subgroup of $\mathrm{PGL}(4,q)$ generated by the projective collineations with matrices:

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \gamma & 0 & 0 \\ 0 & 0 & \gamma^4 & 0 \\ 0 & 0 & 0 & \gamma^4 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & \gamma^2+\gamma^5 & \gamma^3+\gamma^4 & \gamma+\gamma^6 \\ 2 & \gamma^3+\gamma^4 & \gamma+\gamma^6 & \gamma^2+\gamma^5 \\ 2 & \gamma+\gamma^6 & \gamma^2+\gamma^5 & \gamma^3+\gamma^4 \end{pmatrix},$$

with $1+\gamma+\gamma^2+\gamma^3+\gamma^4+\gamma^5+\gamma^6=0$; see Blichfeldt (1905).

# Choose the group

Let $\mathbf{S}$, $\mathbf{T}$, $\mathbf{Q}$ denote the collineations of $\mathrm{PGL}(4,q)$ associated to the matrices $S$, $T$ and $Q$. The map

$$\vartheta := \begin{cases} S \mapsto \mathbf{S} \\ T \mapsto \mathbf{T} \\ Q \mapsto \mathbf{Q} \end{cases}$$

extends to an isomorphism from $\mathrm{PSL}(2,7)$ into $\mathrm{PGL}(4,q)$. Further, the matrix $M = Q^7ST$ has projective order 4 as

$$M^4 = -7^{14}\,\mathrm{I}_4.$$

# Choose the group

Let **M** denote the collineation of $\mathrm{PGL}(4,q)$ associated to the matrix $M$. Then, a representative system of the 42 right cosets of the cyclic subgroup $\langle \mathsf{M} \rangle$ of order 4 in $\mathrm{PSL}(2,7)$ is the following:

$$\mathscr{T} = \{\, \mathsf{1},\ \mathsf{TQ},\ \mathsf{QS}^{-2},\ \mathsf{Q},\ \mathsf{TQS},\ \mathsf{QS}^{-1},\ \mathsf{QSTS},\ \mathsf{QS},\ \mathsf{QT},\ \mathsf{TQS}^2,\ \mathsf{QS}^2,\ \mathsf{S}^{-1}\mathsf{QS}^3,\ \mathsf{QS}^{-1}\mathsf{T},\ \mathsf{SQTS},\ \mathsf{QST},\ \mathsf{QSQ},\ \mathsf{QTS},\ \mathsf{QS}^{-1}\mathsf{T}^{-1},\ \mathsf{QS}^{-3},\ \mathsf{TQS}^2\mathsf{Q},\ \mathsf{QS}^3,\ \mathsf{S}^{-1}\mathsf{QST}^{-1}\mathsf{S},\ \mathsf{TS}^{-1}\mathsf{Q},\ \mathsf{S}^{-1}\mathsf{QTS}^{-1},\ \mathsf{QTS}^{-1},\ \mathsf{QST}^{-1},\ \mathsf{ST}^{-1}\mathsf{SQS},\ \mathsf{T}^{-1}\mathsf{S}^{-1}\mathsf{QTS},\ \mathsf{QSQT},\ \mathsf{SQS}^{-1}\mathsf{TQ},\ \mathsf{TS}^{-1}\mathsf{QTS},\ \mathsf{T}^{-1}\mathsf{SQST},\ \mathsf{T}^{-1}\mathsf{SQTS},\ \mathsf{T}^{-1}\mathsf{S}^{-1}\mathsf{QTS}^{-1},\ \mathsf{S}^{-2}\mathsf{QS}^2,\ \mathsf{S}^{-1},\ \mathsf{QS}^2\mathsf{QS}^{-1},\ \mathsf{QS}^2\mathsf{QS}^{-1}\mathsf{T},\ \mathsf{S}^{-1}\mathsf{QSQS}^{-1},\ \mathsf{S}^2\mathsf{QS}^{-1},\ \mathsf{S}^2\mathsf{QS}^{-1}\mathsf{T}^{-1},\ \mathsf{S}^2\mathsf{QS}^{-1}\mathsf{T}\,\},$$

where **1** denotes the identical collineation of $\mathrm{PGL}(4,q)$.

# Preliminary results

Let **M** denote the collineation of $\mathrm{PGL}(4,q)$ associated to the matrix $M$.

Proposition (AS, 2013)

*The collineation group* $\langle \mathbf{M} \rangle$ *generated by* **M** *admits four fixed points in* $\mathrm{PG}(3,q^2)$.

The characteristic polynomial of $M$

$$P_m(X) = \det(M - X\mathrm{I}_4) = X^4 + 7^{14}$$

yields four distinct eigenvalues in the quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$.

# The 42-arcs

If $\lambda$ is one of these eigenvalues, then from $(M - \lambda \mathrm{I}_4) = \mathbf{0}$ we get

$$\begin{cases} (343-\lambda)x_0 + 343\gamma^2 x_1 + 343\gamma x_2 + 343\gamma^4 x_3 = 0 \\ 686x_0 + (343\gamma + 343\gamma^3 - \lambda)x_1 - (343 + 343\gamma + 343\gamma^2 \\ \qquad +343\gamma^4 + 343\gamma^5)x_2 + (343 + 343\gamma)x_3 = 0 \\ 686x_0 + (343 + 343\gamma^4)x_1 \\ \qquad +(343\gamma^4 + 343\gamma^5 - \lambda)x_2 + (343\gamma^3 + 343\gamma^5)x_3 = 0 \\ 686x_0 - (343 + 343\gamma + 343\gamma^2 + 343\gamma^3 + 343\gamma^4)x_1 \\ \qquad +(343 + 343\gamma^2)x_2 - (343 + 343\gamma + 343\gamma^3 \\ \qquad +343\gamma^4 + 343\gamma^5 + \lambda)x_3 = 0. \end{cases}$$

# The 42-arcs

For $q = p^h$, $q \geq 29$ and $q \equiv 1 \pmod 7$, set

$$\mathcal{O} = \{\, \mathbf{U}(P) \mid \mathbf{U} \in \mathscr{S} \,\} = \{P_1, \ldots, P_{42}\},$$

where $P_1 = P(1 : x_1(\gamma, \lambda) : y_1(\gamma, \lambda) : z_1(\gamma, \lambda))$ is one of the four points of $\mathrm{PG}(3, q)$ arising from the eigenvectors of $M$.

Each point of $\mathcal{O}$ can be written in terms of $\gamma$ and $\lambda$ as

$$P(1 : x_i(\gamma, \lambda) : y_i(\gamma, \lambda) : z_i(\gamma, \lambda))$$

for $1 \leq i \leq 42$.

# The $42$-arcs

Let $D_{i,j,k}$ be the determinant of the matrix whose rows are the coordinate vectors of the points $P_1$, $P_i$, $P_j$ and $P_k$, with $1 < i < j < k \leq 42$. This can be regarded as a polynomial in the indeterminates $\Gamma$ and $\Lambda$, say $D_{i,j,k}(\Gamma, \Lambda)$.
Hence a necessary condition for the points $P_1$, $P_i$, $P_j$ and $P_k$ to produce a coplanar quadruple in $\mathrm{PG}(3, q^2)$ is that the system of equations

$$\begin{cases} D_{i,j,k}(\Gamma, \Lambda) = 0 \\ \Gamma^6 + \Gamma^5 + \Gamma^4 + \Gamma^3 + \Gamma^2 + \Gamma + 1 = 0 \\ \Lambda^4 + 7^{14} = 0 \end{cases}$$

admits a solution $(\gamma, \lambda)$ in some algebraic extesion of the field $\mathbb{F}_q$.

# Existence and completeness

Proposition (AS, 2013)

*Let $q = p^n$, $q \geq 29$ and $q \equiv 1 \pmod 7$. Then the orbits of the fixed points of the collineation* $\mathbf{M}$ *associated to the matrix $M$ of projective order 4 are 42-arcs in $\mathrm{PG}(3, q^2)$ except for a finite number of values of $p$.*

Proposition (AS, 2013)

*Let $\mathcal{K}$ be a complete $k$-arc in $\mathrm{PG}(3, q^2)$. Then*

$$\binom{k}{3} > q^2.$$

# Existence and completeness

A necessary condition for a $k$-arc $\mathrm{K}$ to be complete in $\mathrm{PG}(3, q^2)$ is

$$F(k, q) = \frac{k(k-1)(k-2)}{6} - q^2 > 0.$$

Some values:

- $q = 29$ implies $F(k, 29) > 0$ when $k > 18$;
- $q = 43$ implies $F(k, 43) > 0$ when $k > 23$;
- $q = 71$ implies $F(k, 71) > 0$ when $k > 32$;
- $q = 113$ implies $F(k, 113) > 0$ when $k > 43$.

# The case $q = 29$

We noted that no 42-arc can be complete in $\mathrm{PG}(3, q^2)$ unless $q \in \{29, 43, 71\}$.

Under the action of $\mathrm{PSL}(2, 7)$, the four fixed points of the collineation M describe two distinct 42-orbits which are 42-arcs in $\mathrm{PG}(3, 29^2)$.

Proposition (AS, 2013)

*The two $\mathrm{PSL}(2, 7)$-transitive 42-arcs are both complete in $\mathrm{PG}(3, 29^2)$.*

42 is a relatively small value for a complete arc when compared to $|\mathrm{PG}(3, q^2)| = 29^6 + 29^4 + 29^2 + 1 = 595531444$.

# Applications in cryptography

In a 2-level secret sharing scheme, a secret is shared among a certain number of participants distributed in two levels of privilege, with the requirement that:

- just two participants from the top level are necessary and sufficient in order to reconstruct the secret;
- $n > 2$ participants from the low level are necessary and sufficient in order to reconstruct the secret;
- the secret can be reconstructed by $n - 1$ participants from the low level if and only if they are joined by on participant from the top level.

# Secret shares with $n = 3$

Let the secret be defined at a point $P$ in a plane $\pi_d = \mathrm{PG}(2, q)$, with $q = p^h$ and $p$ a prime.

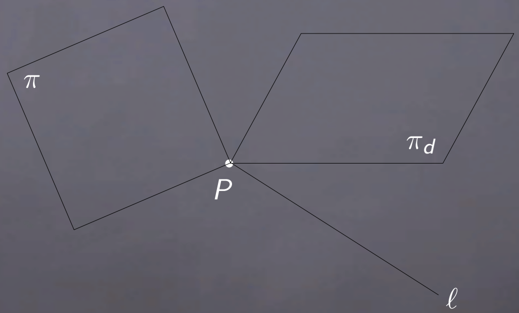
Then, in a 4-dimensional space $\mathrm{PG}(4, q)$ containing $\pi_d$:

- any pair of the private pieces of information (points) held by the members of the upper level define a line $\ell$ such that $\ell \cap \pi_d = \{P\}$;

- any three of the points held by the members of the lower level define a plane $\pi$ such that $\pi \cap \pi_d = \{P\}$.

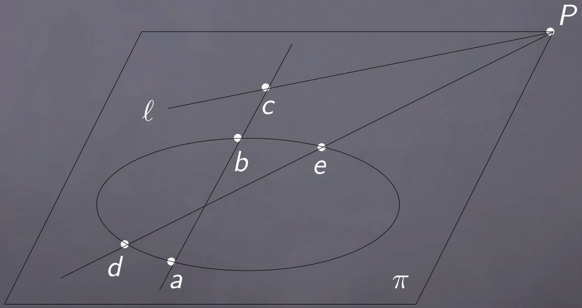
# Secret shares with $n = 3$

Representation of a two-level sharing scheme in a containing 4-dimensional space



# Further requirements

A member of the upper level and any two of the lower level should also be able to access the secret.



# Sharply focused arcs

A set $\mathcal{K}$ consisting of $k$ points in general position in the finite projective plane $\pi = \mathrm{PG}(2, q)$ is said to be sharply focused on a line $\ell$ if the $\binom{k}{2}$ distinct lines defined by pairs of points in $\mathcal{K}$ meet $\ell$ in only $k$ distinct points (G. J. Simmons, 1990).

# One step beyond: hyperfocused arcs

A $k$-arc $\mathcal{K}$ in the plane $\pi = \mathrm{PG}(2, q)$ is said to be hyperfocused on a line $\ell$ if the $\binom{k}{2}$ distinct lines through pairs of points in $\mathcal{K}$ meet $\ell$ in exactly $k-1$ distinct points.

Hyperfocused arcs can exist only when $q$ is even.

Theorem (A. Bichara, G. Korchmáros, 1987)

*Let $\mathcal{K}$ be a k-arc in $\mathrm{PG}(2, q)$ and $\mathcal{I}$ a subset of a line $\ell$ such that $\mathcal{K} \cap \ell = \emptyset$ and no secant of $\mathcal{K}$ has a point in $\mathcal{I}$. Then*

- $|\mathcal{K} \cup \mathcal{I}| \leq q+2$ *and*
- *if* $|\mathcal{K} \cup \mathcal{I}| = q+2$ *and* $|\mathcal{K}| \geq 3$ *then* $q$ *is even and* $|\mathcal{K}| \leq \frac{q}{2}$.

In other words:

- if $\mathcal{K}$ is hyperfocused on $\ell$ then $|\mathcal{I}| = q+2-k$;
- hence $|\mathcal{K} \cup \mathcal{I}| = q+2$ and the previous result applies.

# Additive arcs

In $\mathrm{PG}(2, 2^h)$ let $\Omega$ be the conic of equation

$$X^2 = YZ$$

and $\ell$ its tangent line of equation $Z = 0$.

Consider the subset $\mathcal{K}$ of $\Omega$ given by

$$\mathcal{K} = \{ (t, t^2, 1) \mid t \in A \},$$

with $A \subset \mathrm{GF}(2^h)$.

# Additive arcs

The points on $\ell$ covered by the chords of $\mathcal{K}$ are those with coordinates $(1, s, 0)$ with $s$ ranging over the set of all nonzero elements of $A$.

Theorem (W. E. Cherowitzo, L. D. Holder, 2005)
*If $A$ is a non-trivial subgroup of the additive group of $\mathrm{GF}(2^h)$ then the k-arc $\mathcal{K}$ is hyperfocused on $\ell$ and $k = |A|$.*

The hyperfocused arcs obtained by the above theorem are called "additive". Similar constructions provide "multiplicative" hyperfocused arcs as well.

# Arcs in translation ovals

In $\mathrm{PG}(2, 2^h)$ set

$$\mathcal{D}(F) = \{\, (t, F(t), 1) \mid t \in \mathrm{GF}(2^h) \,\} \cup \{(1, 0, 0)\},$$

where $F(t) \in \mathrm{GF}(2^h)[t]$ is a permutation polynomial such that

- $\deg F < 2^h$;
- $F(0) = 0$ and $F(1) = 1$;
- for each $s \in \mathrm{GF}(2^h)$,

$$G_s(X) = \begin{cases} \frac{F(X+s)+F(s)}{X} & \text{if } X \neq 0 \\ 0 & \text{if } X = 0 \end{cases}$$

  is, in turn, a permutation polynomial.

# Arcs in translation ovals

Theorem (S. E. Payne, 1971 and J. W. P. Hirschfeld, 1975)
*The set* $\mathcal{D}(F)$ *is a translation oval if and only if* $F(t) = t^{2^m}$ *with* $\gcd(m, h) = 1$.

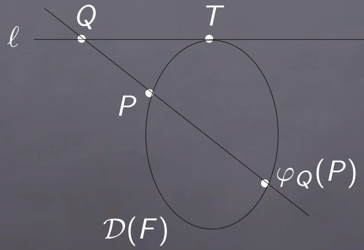
This terminology is motivated by the fact that $\mathcal{D}(F)$ is preserved by the elation defined, for $c \in \mathrm{GF}(2^h)$, by

$$\begin{cases} \rho X' = X + cZ \\ \rho Y' = Y + F(c)Z \\ \rho Z' = Z, \end{cases}$$

and in the affine plane whose ideal line has equation $Z = 0$ this mapping is a translation.

# Arcs in translation ovals

In other words, a $(2^h+1)$-arc $\mathcal{D}(F)$ in $\mathrm{PG}(2,2^h)$ is a translation oval when it has a tangent, say $\ell$, called a special tangent, such that every point $Q \in \ell$ other than the tangency point $T$ is the centre of an involutory elation $\varphi_Q$ preserving $\mathcal{D}(F)$



# Arcs in translation ovals

Let $\ell$ be the infinite line of an affine plane $\mathrm{AG}(2, 2^h)$ whose projective closure is $\mathrm{PG}(2, 2^h)$. Then the involutory elations are translations, and they are the non-trivial elements of a translation group of order $2^h$.

- $\mathcal{D}(F)$ is a conic if and only if either $m = 1$ or $m = h - 1$.
- $\mathcal{D}(F)$ is preserved by a linear collineation group $G$ fixing the point $(0, 1, 0)$ and acting 2-transitively on the affine points of $\mathcal{D}(F)$.
- The translation group of $\mathcal{D}(F)$ comprises all translations $(X, Y) \mapsto (X + a, Y + a^{2^m})$.
- The stabiliser of the origin $O(0, 0)$ in $G$ is a cyclic group consisting of all affinities $(X, Y) \mapsto (cX, c^{2^m} Y)$.

# A characterisation

Let $\Omega = \mathcal{D}(X^{2^m})$ be a translation oval in $\mathrm{PG}(2, 2^h)$ with $h \geq 3$.

Theorem (G. Korchmáros, V. Lanzone, AS, 2012)

*Let $\mathcal{K}$ be a k-arc contained in $\Omega$ which is hyperfocused on a special tangent of $\Omega$. Then $\mathcal{K}$ is additive. In particular, $k = 2^d$ with $2 \leq d \leq h$.*

# Extendable arcs

Let $\mathcal{K}$ be a sharply focused arc contained in a translation oval $\Omega$, with focus set $\mathcal{F}$ contained in a special tangent $\ell$ of $\Omega$.

- Since $k = |\mathcal{F}|$, through every point of $\mathcal{K}$ there is a 1-secant to $\mathcal{K}$ (an $\mathcal{F}$-tangent) which meets $\ell$ at a focus.
- $\mathcal{K}$ has exactly $k$ such $\mathcal{F}$-tangents.
- If the $\mathcal{F}$ tangents are concurrent at a point $U \in \Omega$, then:
    - the $(k+1)$-arc $\mathcal{K} \cup \{U\}$ is hyperfocused on $\ell$ with the same focus set $\mathcal{F}$;
    - we call $\mathcal{K}$ an extendable sharply focused arc.

# Extendable arcs

Let $\mathcal{K}$ be a $k$-arc contained in a translation oval $\Omega$, with focus set $\mathcal{F}$ contained in a special tangent $\ell$ of $\Omega$.

Theorem (G. Korchmáros, V. Lanzone, AS, 2012)
*If $\mathcal{K}$ is sharply focused on $\ell$ then $\mathcal{K}$ is extendable.*

Theorem (G. Korchmáros, V. Lanzone, AS, 2012)
*If $\mathcal{K}$ has as many as $k+1$ focuses on $\ell$ then $\mathcal{K}$ is 2-extendable.*

# A new description of the scheme

The secret is a point $X$ contained in a line $s$ in $\mathrm{PG}(4, q)$ so that planes and lines of a three-dimensional subspace $\mathrm{PG}(3, q)$ not containing $s$ can be used to describe the scheme.

Let $\ell$ be a line of $\mathrm{PG}(3, q)$ through $X$. The set of shadows (pieces of information given to the participants) is:

- a subset $\mathcal{I}$ of points on $\ell$ in case of participants of the top level;
- a subset $\mathcal{K}$ of points in $\mathrm{PG}(3, q)$ in case of participants of the lower level.

# A new description of the scheme

Now $\mathcal{K}$ must be chosen in such a way that

- no point of $\mathcal{K}$ lies on $\ell$;
- no four points in $\mathcal{K}$ are coplanar;
- no three points in $\mathcal{K}$ are coplanar with a point in $\mathcal{I} \cup \{X\}$.

In other words, $\mathcal{K}$ is a $k$-arc in $\mathrm{PG}(3, q)$ disjoint from $\ell$ such that no point from $\mathcal{I} \cup \{X\}$ is cut out by the plane determined by a triangle inscribed in $\mathcal{K}$.

# A new description of the scheme

Points on $\ell$ which are coplanar with triplets of points on $\mathcal{K}$ are called focuses and the set $\mathcal{F}$ consisting of all focuses is called the focus set.

The trivial lower bound on $\mathcal{F}$ is

$$|\mathcal{F}| \geq k-2,$$

and when the equality holds $\mathcal{K}$ is called a spatial hyperfocused arc.

In the next cases, if $|\mathcal{F}| = k-1$ then the arc $\mathcal{K}$ is called a spatial sharply focused arc, while if $|\mathcal{F}| = k$ then it is called a spatial equifocused arc.

# Classification and symmetry

Up to a projectivity, any $(2^h+1)$ arc $\Gamma$ in $\mathrm{PG}(3,2^h)$ is a set of points with coordinates $(X,Y,Z,T)$ defined as follows:

$$\Gamma = \{\,(t, F(t), tF(t), 1) \mid t \in \mathrm{GF}(2^h)\,\} \cup \{Z_\infty\},$$

with $F(t) = t^{2^m}$, $\gcd(m,h)=1$, and $Z_\infty$ the point with projective coordinates $(0,0,1,0)$.

$\Gamma$ is a twisted cubic if and only if either $m=1$ or $m=h-1$.

$\Gamma$ is contained in the hyperbolic quadric $\mathcal{Q}$ of equation

$$XY + ZT = 0.$$

# Classification and symmetry

The projection of $\Gamma$ from its point $Z_\infty$ onto the plane $\pi$ of equation $Z = 0$ is a translation oval $\Omega$ minus its infinite point.

Let $G$ be the symmetry group of $\Gamma$, that is, the linear collineation group of $\mathrm{PG}(3, 2^h)$ preserving $\Gamma$.

- $G$ has order $2^h(2^{2h} - 1)$;
- $G$ is isomorphic to the projective linear group $\mathrm{PGL}(2, 2^h)$;
- $G$ acts on $\Gamma$ as $\mathrm{PGL}(2, 2^h)$ on the projective line $\mathrm{PG}(1, 2^h)$ in its natural sharply 3-transitive permutation representation.

# The focus line

Let $r$ be a real axis of $\Gamma$, that is, $r$ is the meet of two tangent planes of $\Gamma$. Then dual line $r^\perp$ of $r$ is a chord of $\Gamma$.

- Let $\Gamma \cap r^\perp = \{P, Q\}$.
- There exists $g \in G$ such that $g(P) = O(0,0,0,1)$ and $g(Q) = Z_\infty(0,0,1,0)$.
- Take $\ell = g(r)$.

Henceforth, the line $\ell$ will be our choice for the focus sets of $k$-arcs $\mathcal{K}$ contained $\Gamma$.

# The focus set on $\ell$

Lemma (G. Korchmáros, V. Lanzone, AS, 2012)

*For three pairwise distinct points in* $\Gamma$ *with homogeneous coordinates* $P_u(u, u^{2^m}, u^{2^m+1}, 1)$, $P_v(v, v^{2^m}, v^{2^m+1}, 1)$ *and* $P_w(w, w^{2^m}, w^{2^m+1}, 1)$, *the plane determined by them cuts out on* $\ell$ *the point with homogeneous coordinates*

$$\left(1, \frac{(uv)^{2^m}(u+v) + (uw)^{2^m}(u+w) + (vw)^{2^m}(v+w)}{uv(u+v)^{2^m} + uw(u+w)^{2^m} + vw(v+w)^{2^m}}, 0, 0\right).$$

# The stabiliser of a line

- The subgroup $H$ of $G$ which preserves $\ell$ is a dihedral group of order $2(2^h - 1)$.

- $H_{O,Z_\infty}$ is a cyclic group of order $2^h - 1$ acting on $\Gamma \setminus \{O, Z_\infty\}$ as a sharply transitive permutation group.

If $\mathcal{K}$ is a $k$-arc contained in $\Gamma$ such that $O, Z_\infty \in \mathcal{K}$, then up to a symmetry in $H$ it contains the point $P_1$ with homogeneous coordinates $(1, 1, 1, 1)$.

# Spatial hyperfocused arcs

Lemma (G. Korchmáros, V. Lanzone, AS, 2012)
*Let $\mathcal{K}$ be a k-arc contained in $\Gamma$ which is spatial hyperfocused on the line $\ell_\infty$ of equations $Z = T = 0$. Assume that $O, P_1, Z_\infty \in \mathcal{K}$. The projection of $\mathcal{K}$ from $Z_\infty$ onto the plane of equation $Z = 0$ is a hyperfocused $(k-1)$-arc $\mathcal{K}'$ on $\ell_\infty$ which belongs to the family of additive hyperfocused arcs as seen before.*

Lemma (G. Korchmáros, V. Lanzone, AS, 2012)
*Let $\mathcal{K}$ be a k-arc as as in the previous theorem. Then some triangle inscribed in $\mathcal{K}$ with vertex $P_1$ determines a plane that passes through the point $X_\infty$; the same holds for $Y_\infty$.*

# Spatial hyperfocused arcs

Theorem (G. Korchmáros, V. Lanzone, AS, 2012)

*Let $\mathcal{K}$ be a k-arc contained in $\Gamma$. Let $\ell$ be a real axis of $\Gamma$ whose dual line $\ell^{\perp}$ contains two points of $\mathcal{K}$. Then $\mathcal{K}$ is not a spatial hyperfocused arc on $\ell$.*

The existence of spatial hyperfocused arcs in $\mathrm{PG}(3, 2^h)$ is yet an open problem.

# Spatial sharply focused arcs

From the previous theorem the question arises whether such an arc $\mathcal{K}$ may at least be spatial sharply focused.

Lemma (G. Korchmáros, V. Lanzone, AS, 2012)

*Let $\mathcal{K}$ be a k-arc contained in $\Gamma$ which is spatial sharply focused on the line $\ell_\infty$ of equations $X_3 = X_4 = 0$. Assume that $O, P_1, Z_\infty \in \mathcal{K}$. Then the projection of $\mathcal{K}$ from $Z_\infty$ onto the plane of equation $X_3 = 0$ is either a hyperfocused $(k-1)$-arc or it is 1-extendable to a hyperfocused arc on the line $\ell_\infty$ of equations $X_3 = X_4 = 0$. Such hyperfocused arcs belong to the family of additive arcs with $A$ the additive group of a subfield of $\mathrm{GF}(2^h)$.*

# Spatial sharply focused arcs

Lemma (G. Korchmáros, V. Lanzone, AS, 2012)

*Let $\mathcal{K}$ be a k-arc contained in $\Gamma$ which is spatial sharply focused on the line $\ell_\infty$ of equations $X_3 = X_4 = 0$. Assume that $O, P_1, Z_\infty \in \mathcal{K}$. Then some triangle inscribed in $\mathcal{K}$ determines a plane that passes through the point $X_\infty$; the same holds for $Y_\infty$.*

Theorem (G. Korchmáros, V. Lanzone, AS, 2012)

*Let $\mathcal{K}$ be a k-arc contained in $\Gamma$. Let $\ell$ be a real axis of $\Gamma$ whose dual line $\ell^\perp$ contains two points of $\mathcal{K}$. Then $\mathcal{K}$ is not a spatial sharply focused arc on $\ell$.*

As for the spatial hyperfocused arcs, the existence of spatial sharply focused arcs in $\mathrm{PG}(3, 2^h)$ is yet an open problem.

# Spatial equifocused arcs

Set $\mathcal{K} = \Gamma$ and let $\ell$ be a line whose dual line $\ell^\perp$ is a chord of $\mathcal{K}$. Then $\mathcal{K}$ itself is equifocused on $\ell$ in the following sense.

- Since $\mathcal{K}$ is complete, every point outside $\mathcal{K}$ (in particular, each point on $\ell$) is coplanar to some triplet of pairwise distinct points of $\mathcal{K}$.
- Embed $\mathrm{PG}(3, 2^h)$ into $\mathrm{PG}(3, 2^{nh})$, with $\gcd(m, n) = 1$.
- In $\mathrm{PG}(3, 2^{nh})$ the set $\mathcal{K}$ is a $(2^h + 1)$-arc contained in a $(2^{nh} + 1)$-arc $\gamma'$.
- $\ell$ viewed as a line of $\mathrm{PG}(3, 2^{nh})$ is a real axis of $\Gamma'$.
- $\mathcal{K}$ embedded in $\mathrm{PG}(3, 2^{nh})$ is a spatial equifocused $(2^h + 1)$-arc on $\ell$.

Spatial equifocused arcs obtained that way are said to be of subfield type.

# A classification theorem

Theorem (G. Korchmáros, V. Lanzone, AS, 2012)
*Let $\mathcal{K}$ be a k-arc in $\mathrm{PG}(3, 2^h)$ contained in a $(2^h + 1)$-arc $\Gamma$. Let $\ell$ be a real axis of $\Gamma$ whose dual line $\ell^\perp$ contains two points of $\mathcal{K}$. If $\mathcal{K}$ is a spatial equifocused arc on $\ell$ then it is of subfield type.*

Lemma (G. Korchmáros, V. Lanzone, AS, 2012)
*For an additive subgroup $A$ of $\mathrm{GF}(2^h)$ with $h \geq 4$ let $B$ be a set of non-zero elements $b \in A$ whose inverse $b^{-1}$ is also in $A$. If $|B| \geq |A| - 2$ then $A = B \cup \{0\}$ and $A$ is the additive group of a subfield of $\mathrm{GF}(2^h)$.*

# A dynamic system

Recall that the symmetry group $G$ of $\Gamma$ admits a subgroup $H$ which is is a dihecral group of order $2(2^h - 1)$.

If $g \in H$, the image $g(\mathcal{K})$ of $\mathcal{K}$ also satisfies the following conditions:

- no point of $g(\mathcal{K})$ lies on $\ell$;
- no four points in $g(\mathcal{K})$ are coplanar;
- no three points in $g(\mathcal{K})$ are coplanar with a point in $\mathcal{I} = \ell \setminus g(\mathcal{F})$, with $g(\mathcal{F})$ the focus set of $g(\mathcal{K})$ on $\ell$.

In this version, Simmons' model becomes "dynamic" in the sense that a random choice of the set of shares distributed to the participants enables to increase the security of the whole system.