Extended field presentations of arcs and ovoids

Kanat Abdukhalikov

Dept of Mathematical Sciences, UAEU

Finite Geometries 2025
Seventh Irsee Conference
September 1–5, 2025
Irsee, Germany

Outline

"Coordinate-free" presentations of

- Hyperovals
- Segre arcs
- Maximal arcs
- Ovoids

Ovals

An k-arc in an n-dimensional projective space is a set of k points with the property that any $n+1$ of them span the whole space. An arc in a projective plane is called a planar arc.

An *oval* in projective plane $PG(2, q)$ is an a $(q+1)$-arc.

Hyperoval is a $(q+2)$-arc.

O-polynomials

$q = 2^m$

A hyperoval in $PG(2, 2^m)$ can be presented as

$$\mathcal{D}(f) = \{(1, t, f(t)) \mid t \in \mathbb{F}_{2^m}\} \cup (0, 1, 0) \cup (0, 0, 1),$$

where $f(t)$ is an o-polynomial.

Polar coordinate representation

K/F field extension of degree 2, $K = \mathbb{F}_{2^n}$, $F = \mathbb{F}_{2^m}$, $n = 2m$.

The *conjugate* of $x \in K$ over F is

$$\bar{x} = x^q.$$

Norm and *Trace* maps from K to F are

$$N(x) = x\bar{x}, \quad T = x + \bar{x}.$$

The unit circle of K is the set of elements of norm 1:

$$S = \{u \in K : N(x) = 1\}.$$

S is the multiplicative group of $(q+1)$st roots of unity in K.
Each element x of K^* has a unique representation

$$x = \lambda u$$

with $\lambda \in F$ and $u \in S$ (polar coordinate representation).

Polar coordinate representation

Consider K as $AG(2, q)$, $q = 2^m$.

Any hyperoval in K can be represented as a set

$$\left\{ \frac{u}{g(u)} : \; u \in S \right\} \cup 0 \quad \subset K$$

for some function $g : S \to F$.

Regular (hyperconic): $g(u) = 1$.

Adelaide hyperovals

Adelaide hyperoval in K:

$$g(u) = 1 + u^{(q-1)/3} + \bar{u}^{(q-1)/3}.$$

Subiaco hyperovals:

$$\begin{aligned} g(u) &= 1 + u^5 + \bar{u}^5, \\ g_1(u) &= 1 + \theta u^5 + \bar{\theta}\bar{u}^5 \quad (\text{for } m \equiv 2 \pmod 4), \end{aligned}$$

where $\langle\theta\rangle = S$.

For $q = 16$, Adelaide and Subiaco hyperovals coinside to became Lunelli-Sce hyperoval.

O-polynomials

Adelaide o-polynomials:

$$f(t) = \frac{T(b^k)}{T(b)}(t+1) + \frac{T((bt+b^q)^k)}{T(b)(t+T(b)t^{1/2}+1)^{k-1}} + t^{1/2},$$

where m even, $b \in S$, $b \neq 1$ and $k = \pm\frac{q-1}{3}$.

Subiaco o-polynomials:

$$f(t) = \frac{d^2t^4 + d^2(1+d+d^2)t^3 + d^2(1+d+d^2)t^2 + d^2t}{(t^2+dt+1)^2} + t^{1/2}$$

where $d \in F$, $tr(1/d) = 1$, and $d \notin \mathbb{F}_4$ for $m \equiv 2 \pmod 4$. This o-polynomial gives rise to two inequivalent hyperovals when $m \equiv 2 \pmod 4$ and to a unique hyperoval when $m \not\equiv 2 \pmod 4$.

Segre arcs

$F = \mathbb{F}_q$, $q = 2^m$

Any $(q+1)$-arc in $PG(3, q)$ is equivalent to one of the Segre arcs:

$$L_e = \{(1, \gamma, \gamma^{2^e}, \gamma^{2^e+1}) \mid \gamma \in F\} \cup \{(0, 0, 0, 1)\},$$

where $\gcd(e, m) = 1$.

Segre arc is cyclic.

Segre arcs

$$F = \mathbb{F}_q, \quad q = 2^m, \quad K = \mathbb{F}_{q^2}, \quad F^4 \approx K^2$$

$$S = \{u \in K \mid N(x) = 1\} = \{u \in K \mid x^{q+1} = 1\}.$$

Theorem

Let $\gcd(e, m) = 1$ *and*

$$M_e = \{(u^{2^e-1}, u^{2^e+1}) \subset K^2 \mid u \in S\}.$$

Then M_e is a Segre arc in $PG(3, F)$.

The $(q+1)$-arc M_e is clearly cyclic.

Maximal Arcs

A $\{k;t\}$-arc in $PG(2,q)$ is a set $\mathcal{K}$ of k points such that t is the maximum number of points in $\mathcal{K}$ that are collinear.

$$k \leq (q+1)(t-1)+1$$

A $\{k;t\}$-arc in $PG(2,q)$ with $k=(q+1)(t-1)+1$ is called a *maximal arc*.

If $\mathcal{K}$ is a maximal $\{k;t\}$-arc in $PG(2,q)$ and $1<t<q$ then q is even, t is a divisor of q, and every line in $PG(2,q)$ intersects $\mathcal{K}$ in 0 or t points.

The $\{q+2;2\}$-arcs in $PG(2,q)$ are hyperovals.

Denniston Maximal Arcs

Choose $\delta \in F = \mathbb{F}_q$ such that the polynomial $X^2 + \delta X + 1$ is irreducible over F. For each $\lambda \in F$ consider the quadratic curve D_λ in $AG(2, q)$ defined by the equation $X^2 + \delta XY + Y^2 = \lambda$.

If $\lambda \neq 0$ then D_λ is a conic and its nucleus is the point $(0, 0)$.
If $\lambda = 0$ then D_λ consists of the single point $(0, 0)$.

Let $\Delta \subseteq F$. Then the set

$$D = \bigcup_{\lambda \in \Delta} D_\lambda \tag{1}$$

is a maximal arc in $AG(2, q)$ if and only if Δ is a subgroup of the additive group of F.
In this case D is a maximal $\{qt - q + t; t\}$-arc with $t = |\Delta|$.

Denniston Maximal Arcs

The next theorem shows that in terms of polar coordinates the Denniston maximal arcs can be expressed in a very simple way.

Theorem

The Denniston maximal arcs can be expressed as

$$D = \bigcup_{\lambda \in \Lambda} \lambda S \subset K,$$

where Λ is a subgroup of the additive group of the field F and S is the unit circle of K.

Ovoids

In the projective space $PG(3, q)$ with $q > 2$, an *ovoid* is a set of $q^2 + 1$ points meeting every line in at most 2 points.

There are two known ovoids in $PG(3, q)$, $q = 2^m$:

elliptic quadric and *Suzuki-Tits* ovoid.

Suzuki-Tits ovoids were first described by Tits and they are stabilized by the Suzuki groups Sz(q).

Suzuki groups Sz(q) also known as the twisted Chevalley groups of type ${}^2B_2(q)$.

Ovoids

Let Q be a non-degenerate quadratic form on 4-dimensional vector space V over F.

The set of singular points of Q defines either *hyperbolic* or *elliptic* quadric in $PG(3, q)$.

The elliptic quadric in $PG(3, q)$ is an ovoid (contains $q^2 + 1$ points).

Ovoids

The next theorem provides a coordinate-free presentation of the elliptic quadric in $PG(3, q)$.

Theorem

Let $E \supset K \supset F$ be a chain of finite fields, $|E| = q^4$, $|K| = q^2$, $|F| = q$, $q = 2^m$. Then

$$Q(x) = Tr_{K/F}(N_{E/K}(x))$$

is a non-degenerate quadratic form on 4-dimensional vector space E over F. Moreover, the set

$$\mathcal{O} = \{u \in E \mid N_{E/K}(u) = 1\} = \{u \in E \mid u^{q^2+1} = 1\}$$

determines an elliptic quadric in $PG(3, q)$.

K. A., D. Ho

Suzuki-Tits ovoids

Let $q = 2^m$, where $m \geq 3$ is odd.

Let $\sigma = 2^{(m+1)/2}$.

Suzuki-Tits ovoids:

$$\{(1, x, y, xy + x^{\sigma+2} + y^{\sigma}) \mid x, y \in \mathbb{F}_q\} \cup \{(0, 0, 0, 1)\}.$$

Suzuki-Tits ovoids

Let $q = 2^m$, where $m \geq 3$ is odd.

Let $s = q - \sqrt{2q} + 1$, $t = q + \sqrt{2q} + 1$. Then $q^2 + 1 = st$.

$$\mathcal{O}_s := \{x \in E \mid x^s = 1\},$$

$$\mathcal{O}_t := \{x \in E \mid x^t = 1\},$$

$$\mathcal{O} = \{u \in E \mid N_{E/K}(u) = 1\} = \{u \in E \mid u^{q^2+1} = 1\}.$$

Then

$$\mathcal{O} = \mathcal{O}_s\mathcal{O}_t$$

Suzuki-Tits ovoids

Let

$$\mathcal{T}_0 := \mathcal{O}_s \cup \left\{ \left(v^{q-1} + \frac{1}{v^{q-1}} \right)^{q-1} uv \mid u \in \mathcal{O}_s, v \in \mathcal{O}_t \backslash \{1\} \right\},$$

Theorem

1) The set $\mathcal{T}_0$ is a Suzuki-Tits ovoid.
2) The set $\mathcal{T}_0$ is the set of solutions of the equation $Q_0(x) = 0$, where

$$Q_0(x) = x^{q^2+1} + x^{s(\sqrt{2q}+1)} + x^s + 1.$$

K. A., S. Ball, D. Ho, T. Popatia

Suzuki-Tits ovoids

Let

$$\mathcal{T}_1 := \mathcal{O}_t \cup \left\{ \left(u^{q-1} + \frac{1}{u^{q-1}} \right)^{q-1} uv \mid u \in \mathcal{O}_s \setminus \{1\}, v \in \mathcal{O}_t \right\},$$

Theorem

1) The set $\mathcal{T}_1$ is a Suzuki-Tits ovoid.
2) The set $\mathcal{T}_1$ is the set of solutions of the equation $Q_1(x) = 0$, where

$$Q_1(x) = x^{q^2+1} + 1 + x^t \left(\frac{1 + x^{\sqrt{2q}t(\sqrt{q/2}-1)}}{1 + x^{\sqrt{2q}t}} \right) + \\ + x^t \sum_{j=0}^{\log \sqrt{q/2}-1} x^{2^j(\sqrt{2q}-2)t}(1 + x^{\sqrt{2q}t})^{2^j-1}.$$

K. A., S. Ball, D. Ho, T. Popatia

Thank you very much for your attention!