Constructing the Tits Ovoid from an Elliptic Quadric

Bill Cherowitzo
UCDHSC-DDC
July 1, 2006
Combinatorics 2006

Ovoids

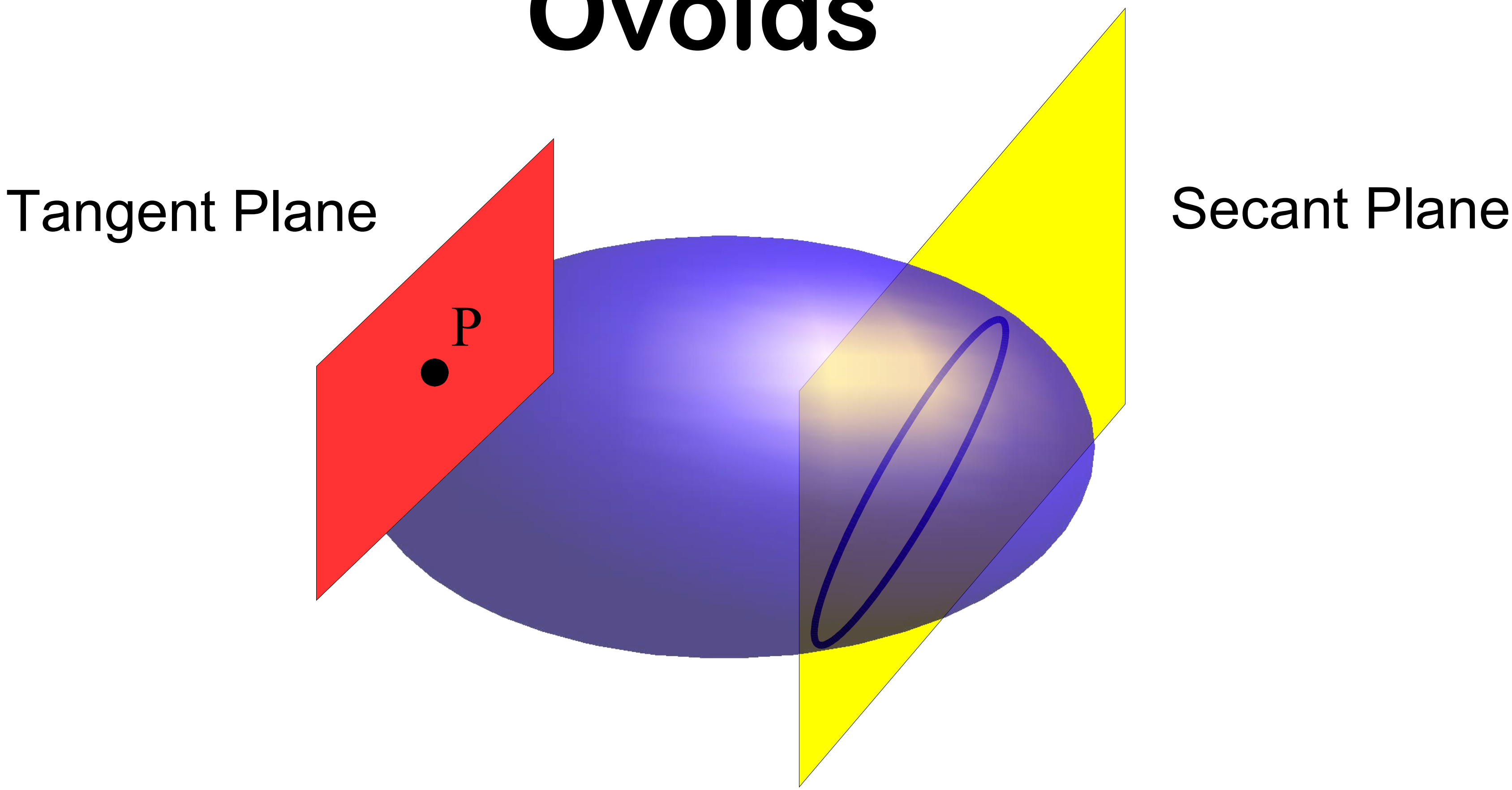
An ***ovoid*** in PG(3,q) is a set of q^2+1 points, no three of which are collinear.

- Ovoids can only exist in a 3-dimensional space.

- At each point of an ovoid, the tangent lines of the ovoid through that point lie in a plane, called the ***tangent plane*** to the ovoid at that point.

- All planes in PG(3,q) intersect an ovoid either in a point (the tangent planes) or in a set of q+1 points (the ***secant planes***).

Ovoids



The intersection of a secant plane and an ovoid (a ***section*** of the ovoid) is an ***oval*** of the secant plane (a set of q+1 points in a plane of order q no three of which are collinear.)

Ovoids

There are only two known families of ovoids (and *no* sporadic examples):

Elliptic Quadrics ($\exists\ \forall\ q$)

Tits Ovoids ($\exists$ iff $q = 2^{2e+1}$)

Elliptic Quadrics

An ***elliptic quadric*** in PG(3,q) is the set of points whose homogeneous coordinates satisfy a homogeneous quadratic equation and such that the set contains no line.

In terms of coordinates (x,y,z,w) of PG(3,q):

• if q is odd, the set of points satisfying $zw = x^2 + y^2$ would form an elliptic quadric, but this would not work for q even since the set would include lines in that case.

• for any q, the set of points given by:

$$\{(x, y, x^2 + xy + ay^2, 1): x,y \in GF(q)\} \cup \{(0,0,1,0)\}$$

where $t^2 + t + a$ is irreducible over GF(q), is an elliptic quadric.

A Special Automorphism

The automorphisms of GF(2^h) are the maps:

$$t \to t^{2^i}, \quad \textbf{where} \quad 0 \leqslant i \leqslant h-1.$$

When h = 2e - 1, the automorphism:

$$t \to t^{\sigma} = t^{2^e}$$

has some special properties (q = 2^h).

$$(1) \quad \sigma^2 \equiv 2 \mod (q-1)$$

$$(2) \quad \frac{1}{\sigma - 1} \equiv \sigma + 1 \mod (q-1)$$

(3) $t \to t^{\sigma+1}$ **and** $t \to t^{\sigma+2}$ **are bijections.**

The Tits Ovoid

Discovered by Jacques Tits (1962) in an examination of the Suzuki groups, these ovoids exist only in $PG(3,2^{2e-1})$ with $e \geq 2$.

These ovoids are projectively equivalent to:

$$\{(x, y, x^{\sigma} + xy + y^{\sigma+2}, 1): x,y \in GF(2^{2e-1})\} \cup \{(0,0,1,0)\}.$$

(Stan would have me say that a Tits ovoid is the set of all absolute points of a polarity of the generalized quadrangle W(q) – but I'm not going there!)

Translation Ovals & Hyperovals

An ***oval*** in a projective plane PG(2,q) is a set of q+1 points no three of which are collinear.

When q is even, there is a unique point (the ***nucleus*** or ***knot*** of the oval) which when added to the oval gives a set of q+2 points, no three collinear. Such a set of q+2 points is called the ***hyperoval*** containing the given oval.

Any line of the plane intersects a hyperoval in either 0 or 2 points and is called an ***exterior*** or ***secant*** line of the hyperoval respectively.

Translation Ovals & Hyperovals

If $q = 2^h$, a ***translation hyperoval*** is a hyperoval of PG(2,q) that is projectively equivalent to the hyperoval passing through the points (1,0,0) and (0,1,0) and whose affine points satisfy the equation $y = x^{2^i}$, where $(i,h) = 1$.

For $i = 1$ and $h-1$ the translation hyperovals are ***hyperconics*** (a conic together with its nucleus, a.k.a. a ***regular hyperoval***), but other values of i give translation hyperovals which are not projectively equivalent to hyperconics.

Translation hyperovals were first investigated by B. Segre in 1957.

Plane Sections

The sections of an elliptic quadric are all conics, and so, are projectively equivalent.

The sections of a Tits ovoid are all translation ovals, projectively equivalent to

$$\{(x, x^\sigma, 1): x \in GF(q)\} \cup \{(1,0,0)\}.$$

This uniformity of the sections of the known examples has suggested results which characterize ovoids in terms of their plane sections.

Plane Sections

Barlotti (1955) : If every plane section of an ovoid is a conic, then the ovoid is an elliptic quadric.

Segre (1959) : For $q \geq 8$, if at least $(q^3 - q^2 + 2q)/2$ plane sections are conics, the ovoid is an elliptic quadric.

Prohaska & Walker (1977) : If the plane sections of planes on a fixed secant line are conics, the ovoid is an e.q. ($q+1$).

Glynn (1984): If the plane sections of planes on a fixed tangent line are conics, the ovoid is an e.q. (q).

Brown (2000): If **any** section of an ovoid is a conic, the ovoid is an elliptic quadric.

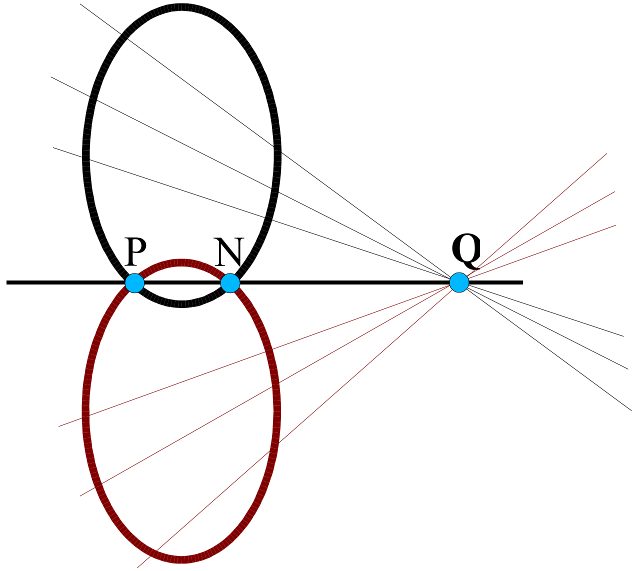
Plane Sections

Similar attempts have been made for the Tits ovoid, the best of these so far are:

O'Keefe & Penttila (1996) : An ovoid has a pencil of translation ovals as sections, if and only if, it is an elliptic quadric or a Tits ovoid.

O'Keefe & Penttila (1997) : If every section of an ovoid is contained in a translation hyperoval, then the ovoid is an elliptic quadric or a Tits ovoid.

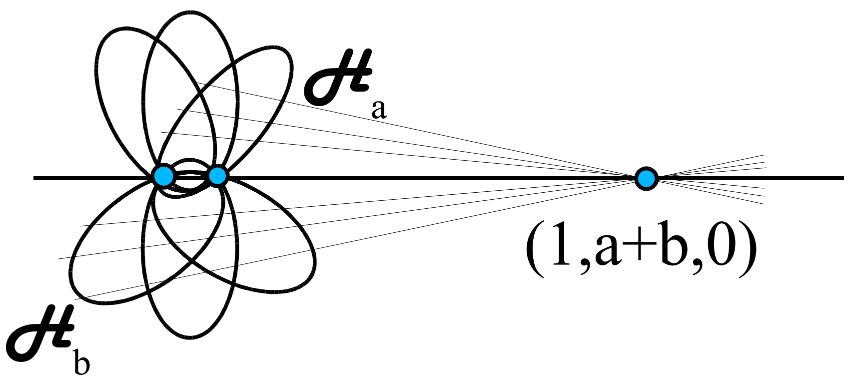
Fans of Hyperovals



Two hyperovals, $\mathcal{H}_1$ and $\mathcal{H}_2$, meeting precisely in two points N and P are said to be ***compatible*** at a point Q of the line $\mathcal{L} = \overline{NP}$, other than N or P, if all lines through Q other than $\mathcal{L}$ which are secant lines of $\mathcal{H}_1$ are exterior lines of $\mathcal{H}_2$ (and consequently, the exterior lines to $\mathcal{H}_1$ are secant lines of $\mathcal{H}_2$.)

Fans of Hyperovals

Consider a set of q hyperovals $\{\mathcal{H}_s\}$ indexed by the elements of GF(q) which mutually intersect precisely at the points (0,1,0) and (1,0,0) and for which $\mathcal{H}_a$ and $\mathcal{H}_b$ are compatible at (1,a+b,0) for all distinct a,b $\in$ GF(q).



Any set of hyperovals that are projectively equivalent to these is called a ***fan of hyperovals***.

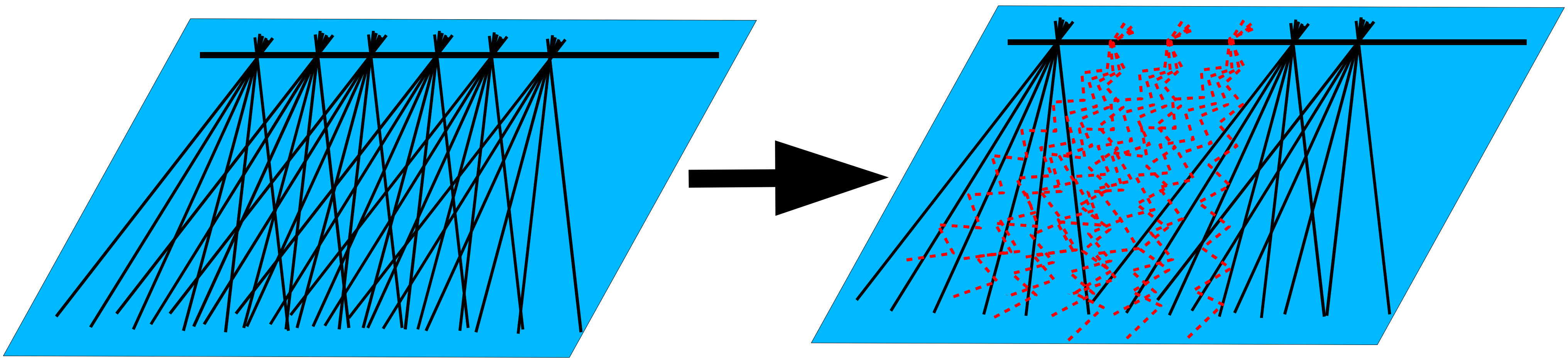
The Plane Equivalent Theorem

Glynn (1998) & Penttila (1999):

Any ovoid of $PG(3,2^h)$ is equivalent to a fan of hyperovals in a plane $PG(2,2^h)$.

The proof is constructive. Starting with the secant planes of an ovoid passing through a common tangent line of the ovoid and indexed by the elements of the field, homographies dependent on the index map each section of the ovoid into a single secant plane of this pencil. The resulting collection of ovals have a common nucleus and therefore form a fan of hyperovals. The process is reversible and the ovoid can be recovered from the fan of hyperovals.

Net Replacement



Net Replacement : A method for constructing new planes from old ones.

Oval Derivation

Oval derivation is a special type of net replacement which can be carried out when q is even.

For oval derivation the replacement net consists of the restriction to the affine plane of the set of q^2 - q translation hyperovals given by $y = mx^{2^i} + k$,$m \neq 0$, $k \in$ GF(q), (i,h) = 1, all of which pass through (1,0,0) and (0,1,0). Note that for affine points (u_1,v_1) and (u_2,v_2) with $u_1 \neq u_2$ and $v_1 \neq v_2$, the unique translation hyperoval of this set containing these points has

$$m = \frac{v_1 + v_2}{(u_1 + u_2)^{2^i}} \text{ and } k = \frac{u_1^{2^i} v_2 + u_2^{2^i} v_1}{(u_1 + u_2)^{2^i}}.$$

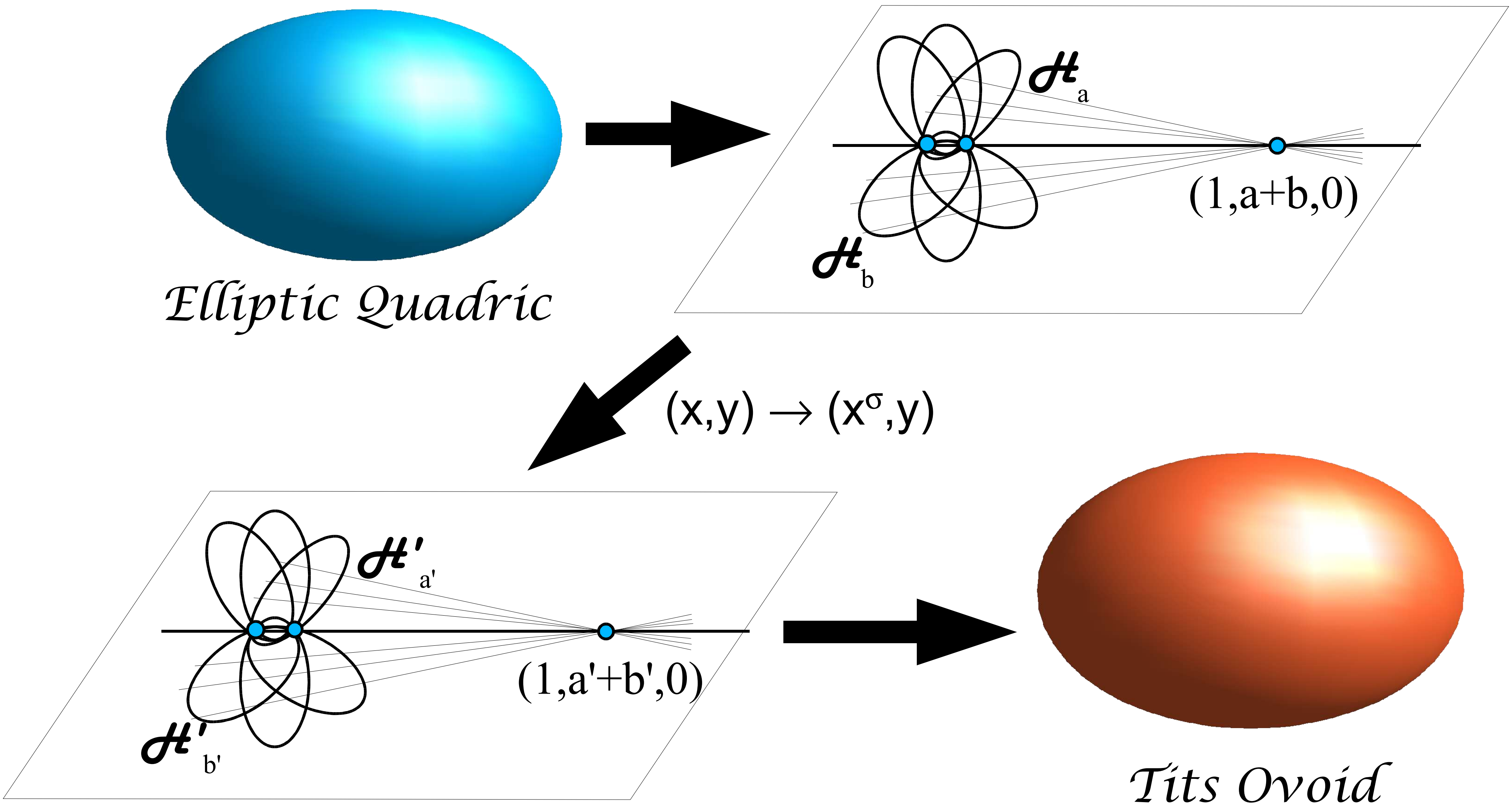
Oval Derivation

The result of performing oval derivation is a plane isomorphic to the original plane (this is not true for more general net replacements).

Oval derivation is equivalent to applying the point map

$$(x, y) \rightarrow (x^{2^{-i}}, y).$$

The Construction



The Algebra

As there is a single orbit of elliptic quadrics under PGL(4,q) we can take as our starting point the quadric Ω whose point set is:

$\Omega := \{(s,t,t^2 + st + \eta s^2,1): s,t \in GF(q)\} \cup \{(0,0,1,0)\}$,

where $\eta \in GF(q)$ is a fixed element of absolute trace 1. The line ℓ_∞ given by $x_0 = x_3 = 0$ is tangent to Ω at the point Q_∞ = (0,0,1,0). The secant planes of Ω through ℓ_∞ will be denoted by $\pi_\alpha : x_0 = \alpha x_3$ for $\alpha \in GF(q)$. Furthermore, we define the conic sections $\mathcal{O}_\alpha := \pi_\alpha \cap \Omega$. By the Plane Equivalent Theorem we obtain a fan of conics in π_0 all passing through Q_∞ and having common nucleus (0,1,0,0). The q conics are:

$\mathcal{F}_\alpha = \{(0,t,t^2 + \eta \alpha^2, 1): t \in GF(q)\} \cup (0,0,1,0)$, for $\alpha \in GF(q)$.

The Algebra

Let σ be the automorphism of $GF(2^{2e-1})$ given by $x \to x^\sigma = x^{2^e}$.

We now perform oval derivation on the affine plane $\pi_0 \setminus \ell_\infty$ using the transformation $(0,x,y,1) \to (0,x^\sigma,y,1)$. Denote the projective completion of the derived plane by π_0'.

Observe that the point $(0,t,t^2+\eta\alpha^2,1)$ of π_0 is transformed to $(0,u, u^\sigma+\eta\alpha^2,1)$ of π_0'. Since $x \to x^{\sigma+2}$ is a permutation of GF(q), to each α of GF(q) we can associate a $\beta \in$ GF(q) such that

$$\beta^{\sigma+2} = \eta\alpha^2.$$

We now see that this oval derivation transforms

$$\mathcal{F}_\alpha \to \mathcal{F}_\beta' = \{(0,u,u^\sigma + \beta^{\sigma+2},1): u \in GF(q)\} \cup (0,0,1,0).$$

The Algebra

Proposition: The translation ovals $\mathcal{F}_c'$ and $\mathcal{F}_d'$ $(c \neq d)$, where $\mathcal{F}_\beta' = \{(u, u^\sigma + \beta^{\sigma+2}, 1) : u \in GF(q)\} \cup (0,1,0)$, are compatible at the point $(1, c+d, 0)$.

Proof: A line other than ℓ_∞ through $(1, c+d, 0)$ is a secant (resp. exterior) line of $\mathcal{F}_\beta'$ provided the equation

$$u^\sigma + (c+d)u + k + \beta^{\sigma+2} = 0$$

has 2 (resp. 0) solutions with $k \in GF(q)$. This equation has 2 (resp. 0) solutions provided

$$\mathbf{tr}\left(\frac{k+\beta^{\sigma+2}}{(c+d)^{\frac{\sigma}{\sigma-1}}}\right)$$

is 0 (resp. 1), where tr is the absolute trace function of GF(q).

The Algebra

Proposition: The translation ovals $\mathcal{F}_c'$ and $\mathcal{F}_d'$ ($c \neq d$), where $\mathcal{F}_\beta' = \{(u, u^\sigma + \beta^{\sigma+2}, 1) : u \in GF(q)\} \cup (0,1,0)$, are compatible at the point (1,c+d,0).

Proof (cont): For any k we have

$$\mathbf{tr}\left(\frac{k+c^{\sigma+2}}{(c+d)^{\frac{\sigma}{\sigma-1}}}\right)+\mathbf{tr}\left(\frac{k+d^{\sigma+2}}{(c+d)^{\frac{\sigma}{\sigma-1}}}\right) = \mathbf{tr}\left(\frac{c^{\sigma+2}+d^{\sigma+2}}{(c+d)^{\frac{\sigma}{\sigma-1}}}\right) = \mathbf{tr}\left(\frac{c^{\sigma+1}+d^{\sigma+1}}{(c+d)^{\sigma+1}}\right) = 1.$$

The penultimate simplification uses the invariance of trace under an automorphism and the relation $\frac{1}{\sigma-1} \equiv \sigma+1 \mod(q-1)$.
Therefore,

$$\mathbf{tr}\left(\frac{k+c^{\sigma+2}}{(c+d)^{\frac{\sigma}{\sigma-1}}}\right) \neq \mathbf{tr}\left(\frac{k+d^{\sigma+2}}{(c+d)^{\frac{\sigma}{\sigma-1}}}\right)$$

and each line other than ℓ_∞ through (1,c+d,0) is a secant to one and exterior to the other of $\mathcal{F}_c'$ and $\mathcal{F}_d'$.

Where do we go from here?

The complete classification of ovoids in PG(3,q) is a long standing open problem.

- If q is odd, then it has been known since 1955 that every ovoid of PG(3,q) is an elliptic quadric.

- If q = 4 or 16, then every ovoid of PG(3,q) is an e.q.

- If q = 8 or 32 then every ovoid is either an elliptic quadric or a Tits ovoid.

- It is widely conjectured that these are the *only* families of ovoids in PG(3,q), but the classification for even q has only been achieved for $q \leq 32$.

Where do we go from here?

As an intermediate step towards this classification, we would like to settle the following:

Conjecture: In $PG(3,2^{2e+1})$ an ovoid with translation oval section is either an elliptic quadric or a Tits ovoid.

This is of course the natural extension of Brown's result and our plan of attack on this conjecture would use Brown's result.

Where do we go from here?

Specifically:

Start with an unkown ovoid having a translation oval as a section.

This is equivalent to a fan of hyperovals with one of the hyperovals being the given section.

Apply the inverse of the oval derivation we have used in this lecture. This converts the given section to a conic.

Show that the fan of hyperovals is converted to a fan of hyperovals.

This new fan gives an ovoid containing a conic as a section ... so by Brown's result this is an elliptic quadric.

Reverse the construction and our result shows that the unknown ovoid is a Tits ovoid.