Applications of pencils of conics

Keith E. Mellinger
University of Mary Washington
(joint work with Jeremy Dover, Kelly Scott, and Kenny Wantz)

May 2012

Introduction to conics

$PG(2, q)$ is the classical, or Desarguesian, finite projective plane of order q, q a prime power, and

Introduction to conics

$PG(2, q)$ is the classical, or Desarguesian, finite projective plane of order q, q a prime power, and these planes can be represented easily with a 3-dimensional vector space over a finite field.

Introduction to conics

$PG(2, q)$ is the classical, or Desarguesian, finite projective plane of order q, q a prime power, and these planes can be represented easily with a 3-dimensional vector space over a finite field.

1-dimensional subspaces $\leftrightarrow$ points

Introduction to conics

$PG(2,q)$ is the classical, or Desarguesian, finite projective plane of order q, q a prime power, and these planes can be represented easily with a 3-dimensional vector space over a finite field.

1-dimensional subspaces $\leftrightarrow$ points

2-dimensional subspaces $\leftrightarrow$ lines

quadratic forms

Just as in Euclidean geometry, we can consider the set of points whose homogeneous coordinates satisfy a “quadratic.”

quadratic forms

Just as in Euclidean geometry, we can consider the set of points whose homogeneous coordinates satisfy a "quadratic."

In this case, we use a *quadratic form* and it is not hard to show that there is precisely one non-degenerate form. Using coordinates (x, y, z), the canonical representation is

quadratic forms

Just as in Euclidean geometry, we can consider the set of points whose homogeneous coordinates satisfy a "quadratic."

In this case, we use a *quadratic form* and it is not hard to show that there is precisely one non-degenerate form. Using coordinates (x, y, z), the canonical representation is

$$y^2 = xz.$$

quadratic forms

So, a non-degenerate conic consists of the points whose homogeneous coordinates are

$$(1, x, x^2), \text{ for some } x \in GF(q)$$

or

$$(0, 0, 1).$$

quadratic forms

So, a non-degenerate conic consists of the points whose homogeneous coordinates are

$$(1, x, x^2), \text{ for some } x \in GF(q)$$

or

$$(0, 0, 1).$$

This gives a total of $q + 1$ points.

quadratic forms

So, a non-degenerate conic consists of the points whose homogeneous coordinates are

$$(1, x, x^2), \text{ for some } x \in GF(q)$$

or

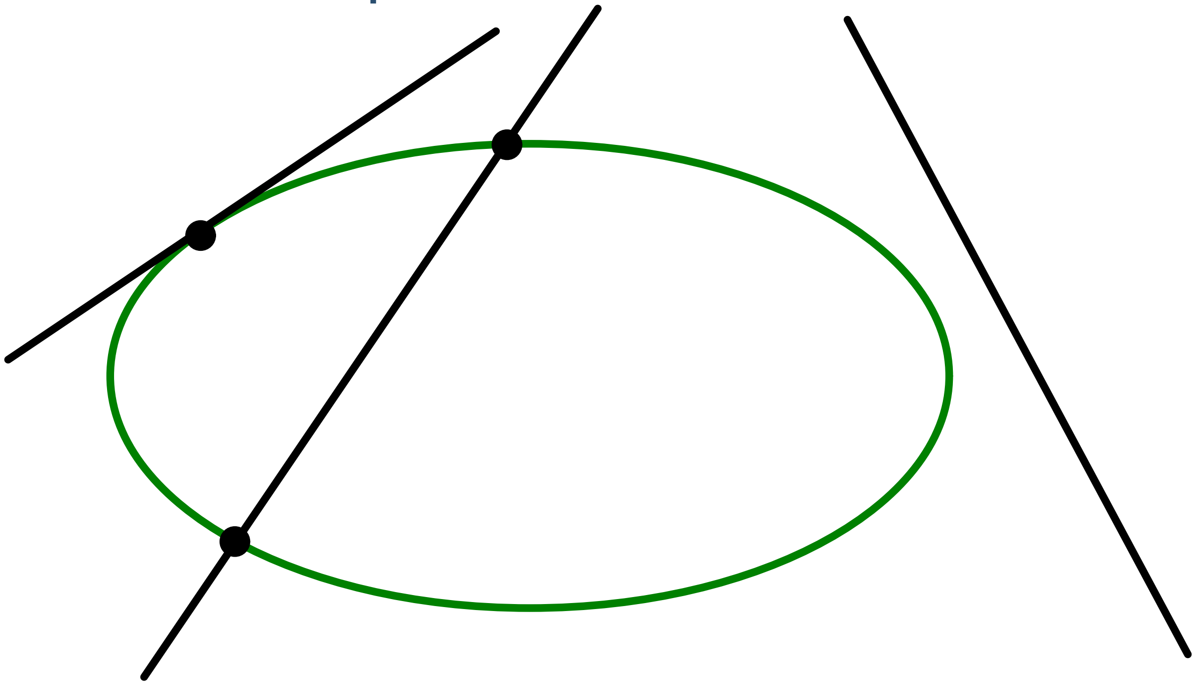
$$(0, 0, 1).$$

This gives a total of $q + 1$ points.

Every non-degenerate conic is an *arc*, a set of points, no three collinear. A famous theorem due to Segre says that when q is odd, every set of $q + 1$ points, no three collinear, is actually a conic.

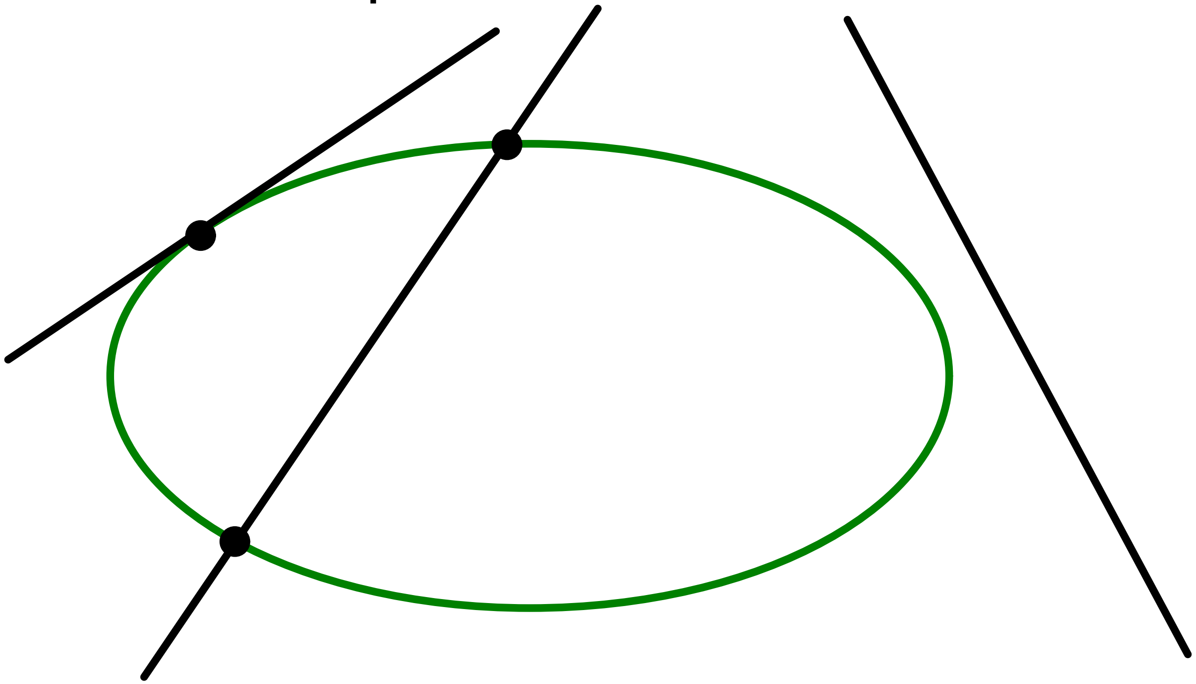
synthetic properties

Since conics form arcs, no line can meet a conic in more than 2 points.



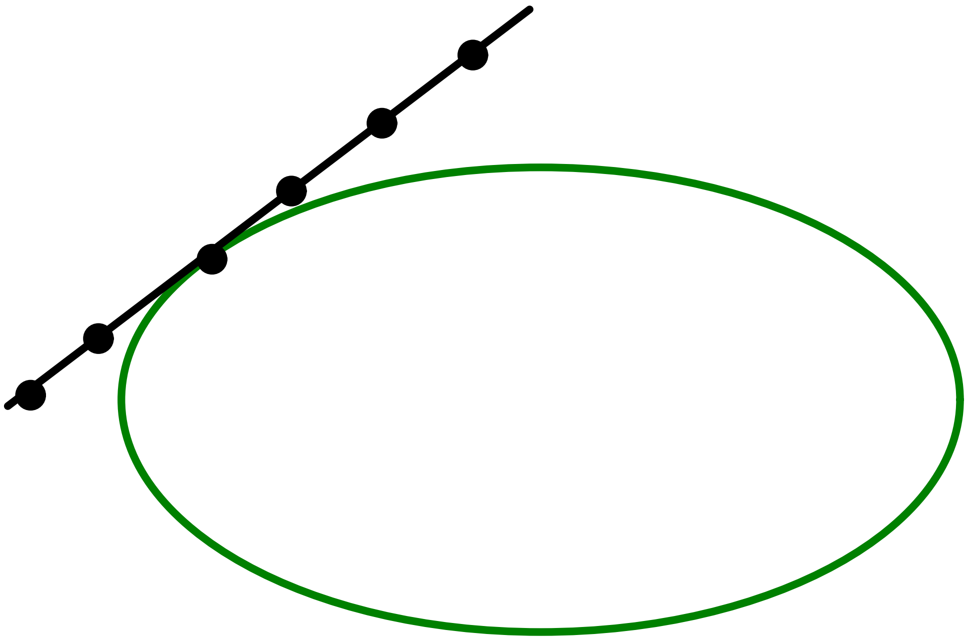
synthetic properties

Since conics form arcs, no line can meet a conic in more than 2 points.

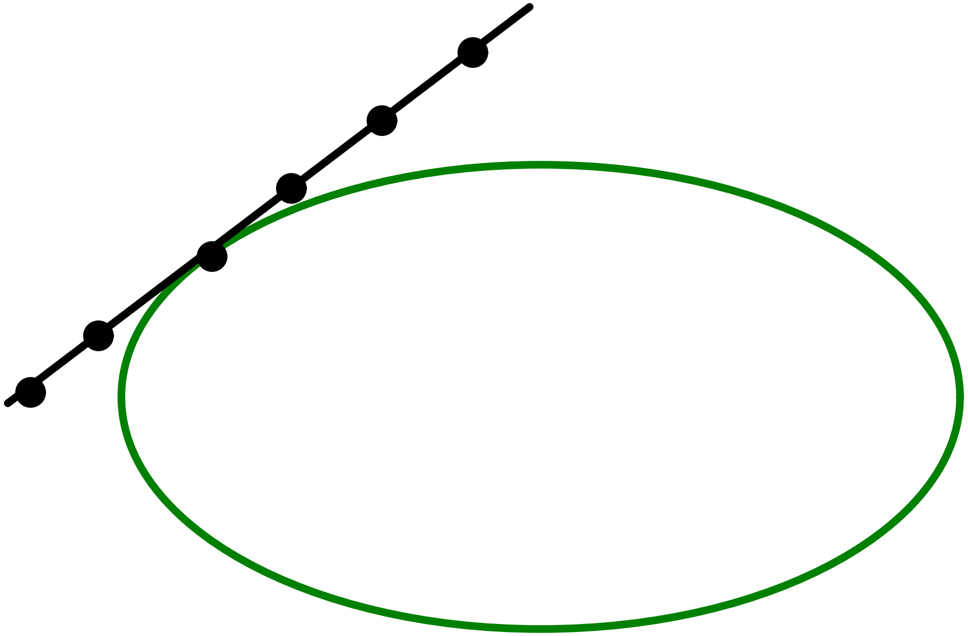


We have secant lines, tangent lines, and skew lines.

synthetic properties



synthetic properties



The *exterior* points are those that lie on tangent lines. Counting shows that about half the points off the conic are exterior. The other points are called *interior*.

pencils of conics

Let F and G be distinct quadratic forms. Then we can define the collection of quadratic forms $F + \lambda G$, $\lambda \in GF(q)$, to be the algebraic *pencil of conics* defined by F and G.

pencils of conics

Let F and G be distinct quadratic forms. Then we can define the collection of quadratic forms $F + \lambda G$, $\lambda \in GF(q)$, to be the algebraic *pencil of conics* defined by F and G.

Up to isomorphism, there are only a limited number of different algebraic pencils, and they have been completely classified.

pencils of conics

Let F and G be distinct quadratic forms. Then we can define the collection of quadratic forms $F + \lambda G$, $\lambda \in GF(q)$, to be the algebraic *pencil of conics* defined by F and G.

Up to isomorphism, there are only a limited number of different algebraic pencils, and they have been completely classified.

There is a complete list in Hirschfeld's book – there are 20.

What is this talk about?

You should listen to your advisor. Sometime, he/she is right.

What is this talk about?

You should listen to your advisor. Sometime, he/she is right.

I have found multiple uses for pencils of conics.

What is this talk about?

You should listen to your advisor. Sometime, he/she is right.

I have found multiple uses for pencils of conics.

Each involves a non-trivial construction of some object in the projective plane.

Semiovals

A *semioval* is a set of points $\mathcal{S}$ such that for every point $P \in \mathcal{S}$, there exists a unique line l such that $l \cap \mathcal{S} = \{P\}$.

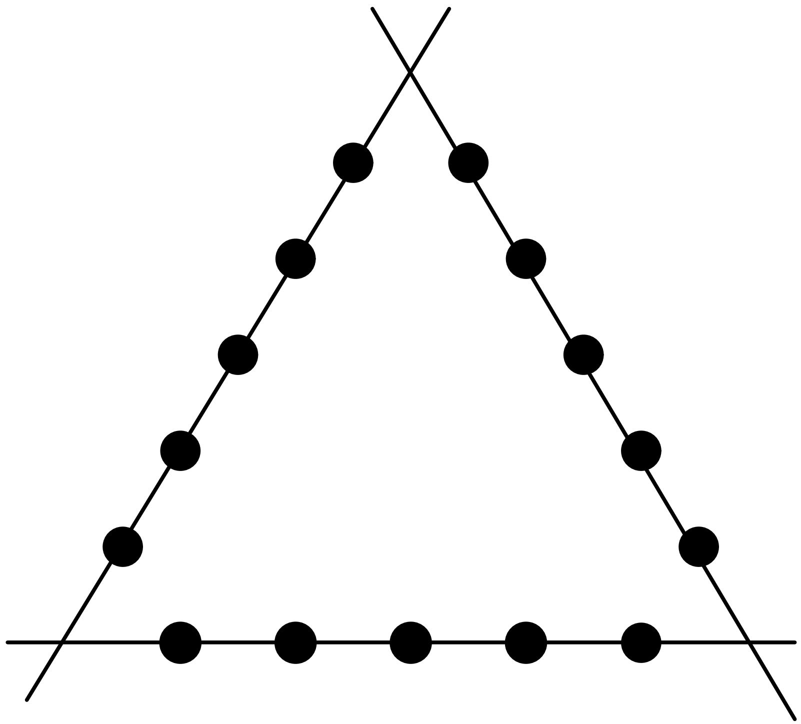
Semiovals

A *semioval* is a set of points $\mathcal{S}$ such that for every point $P \in \mathcal{S}$, there exists a unique line l such that $l \cap \mathcal{S} = \{P\}$.

unique tangent lines

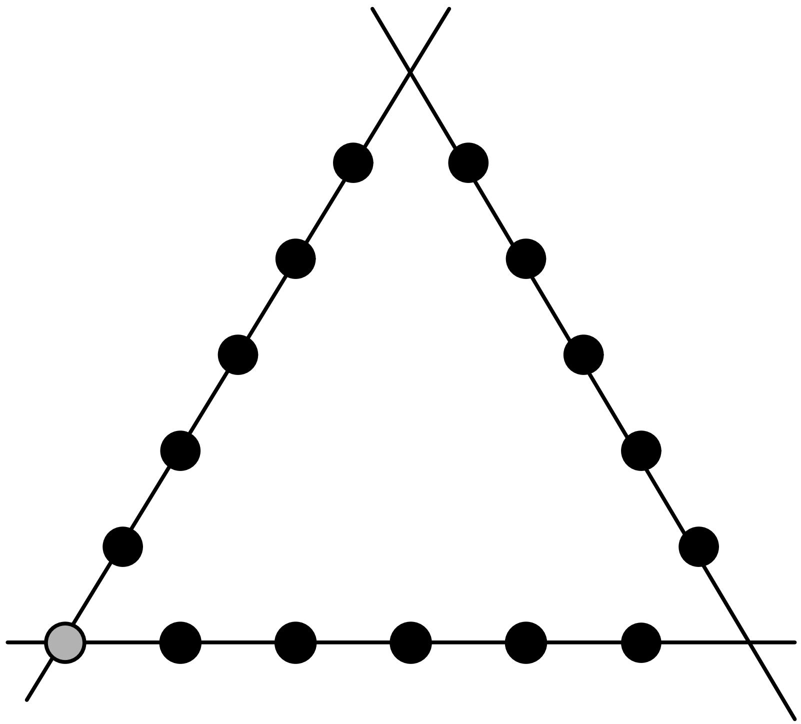
vertex-less triangle

Classic example: *the vertex-less triangle*



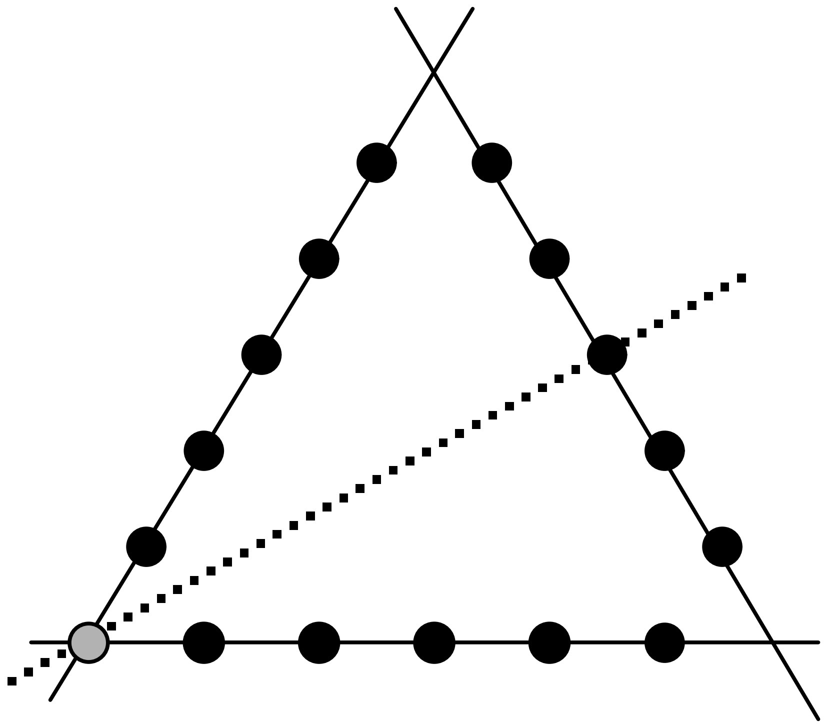
vertex-less triangle

Classic example: *the vertex-less triangle*



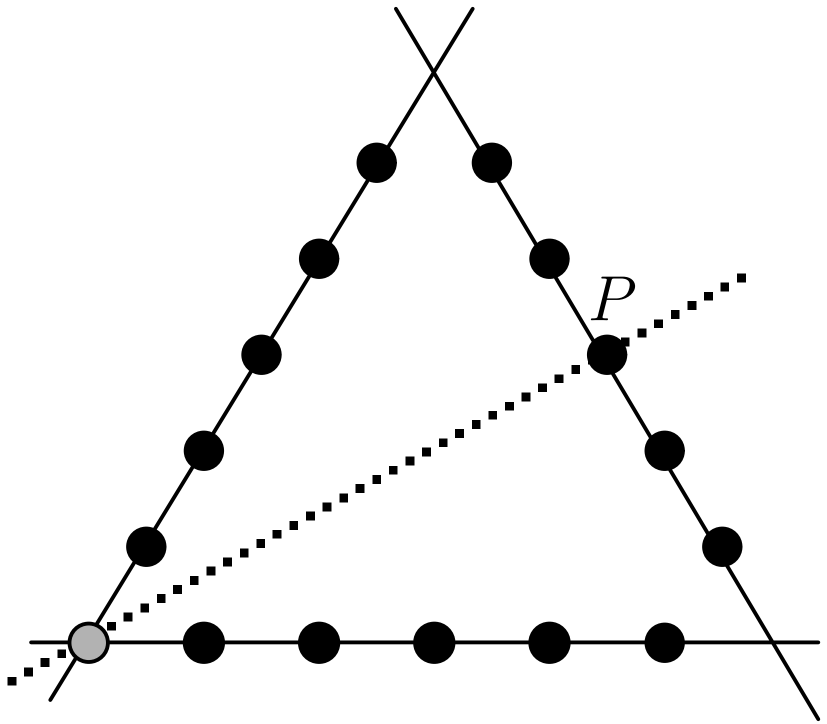
vertex-less triangle

Classic example: *the vertex-less triangle*



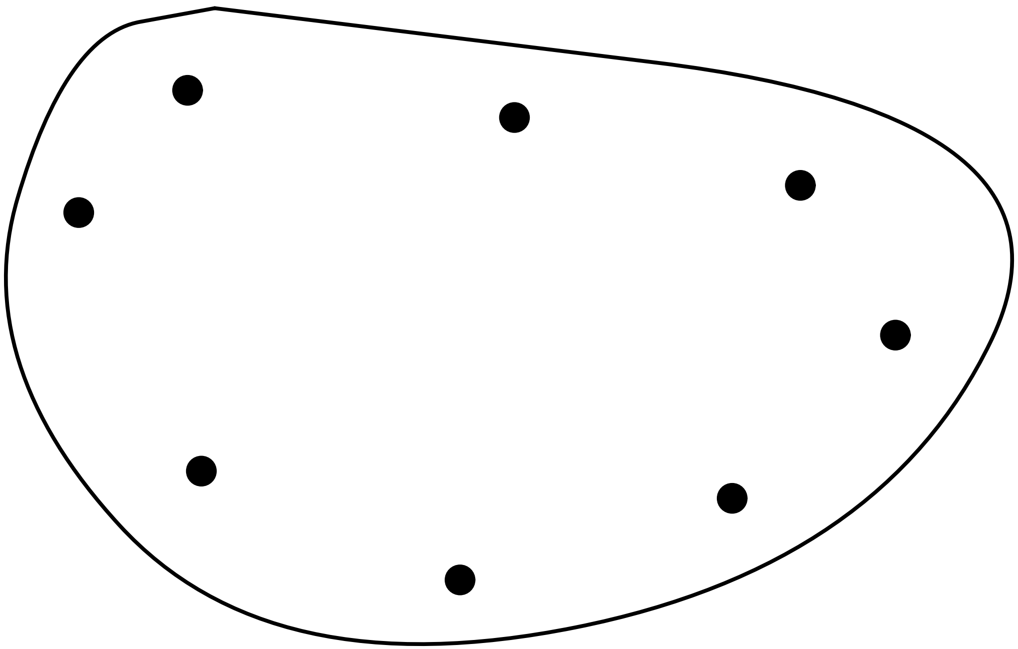
vertex-less triangle

Classic example: *the vertex-less triangle*



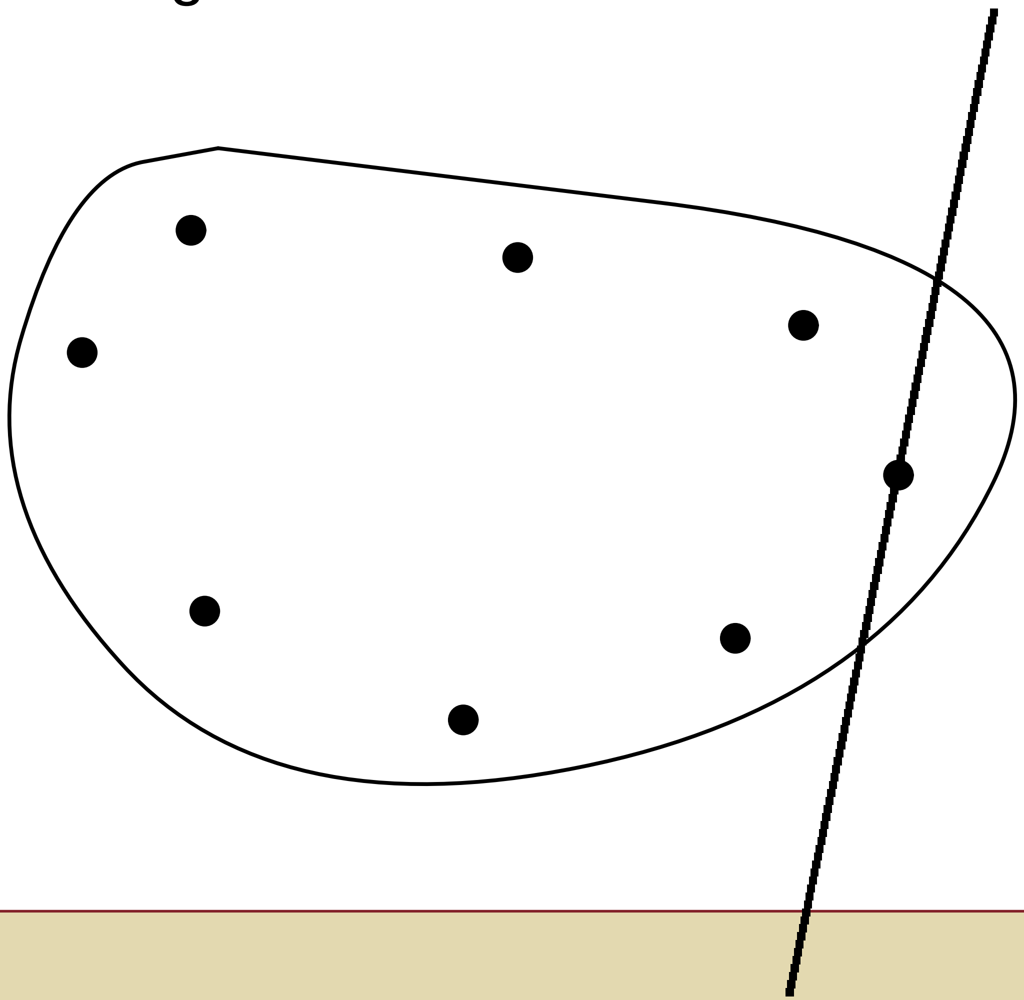
extremal in two ways

Part of the fascination with blocking semiovals is that they are extremal in two ways.
First, you can't remove any point and still have a blocking semioval.



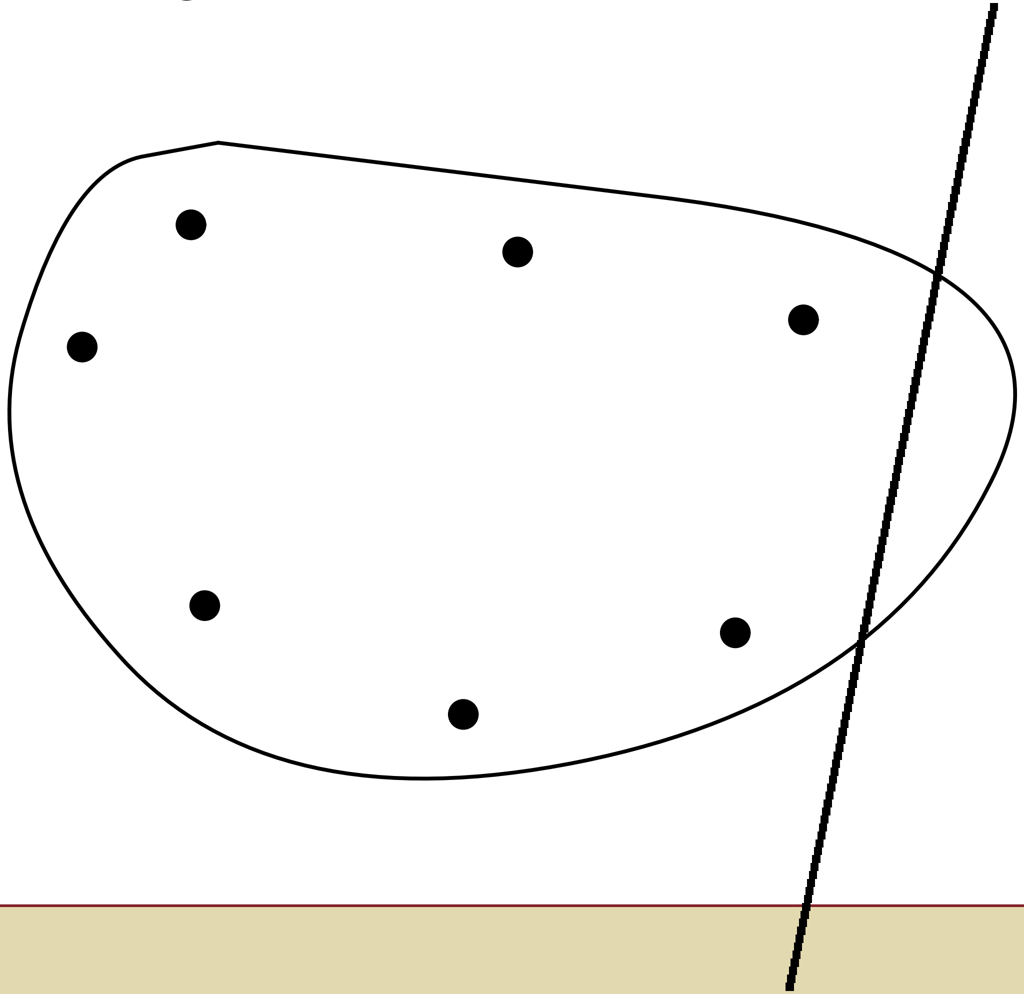
extremal in two ways

Part of the fascination with blocking semiovals is that they are extremal in two ways.
First, you can't remove any point and still have a blocking semioval.



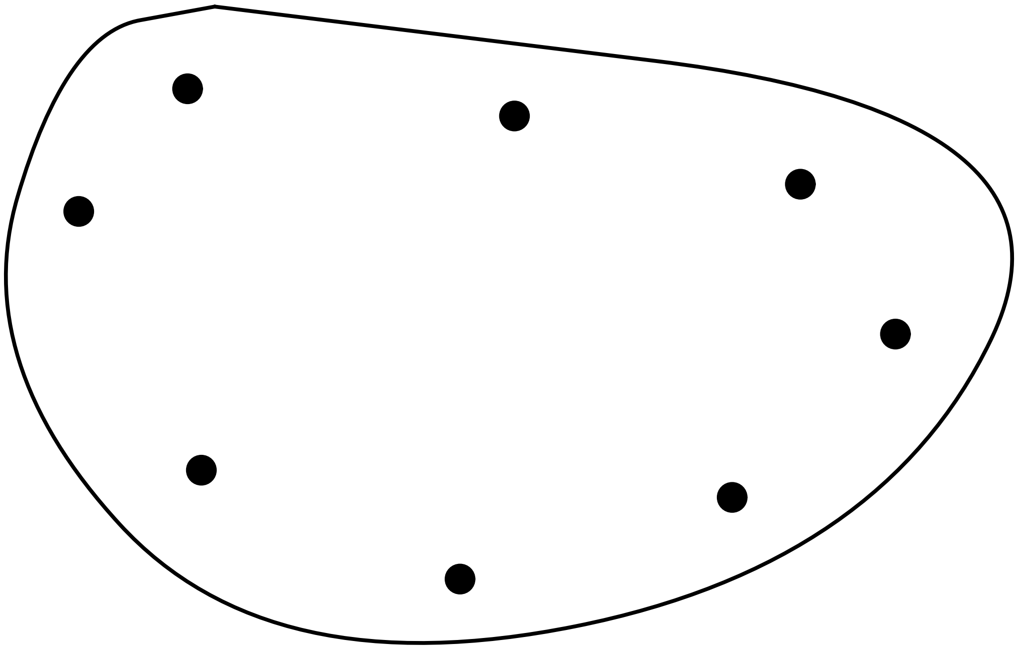
extremal in two ways

Part of the fascination with blocking semiovals is that they are extremal in two ways.
First, you can't remove any point and still have a blocking semioval.



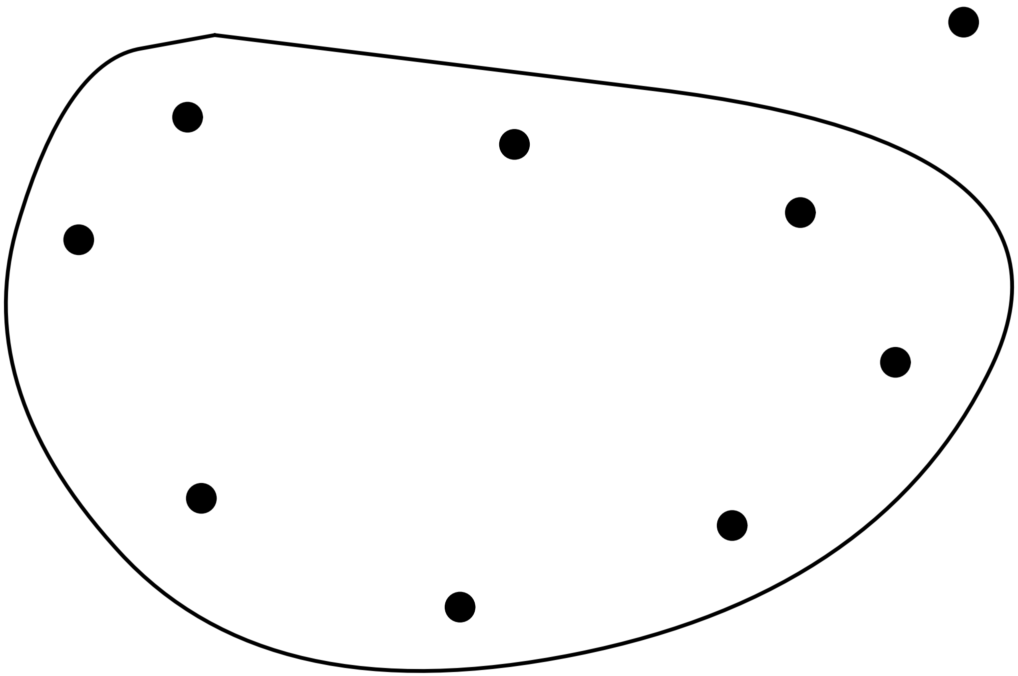
extremal in two ways

Second, you can’t add another point to your set and still have a blocking semioval.



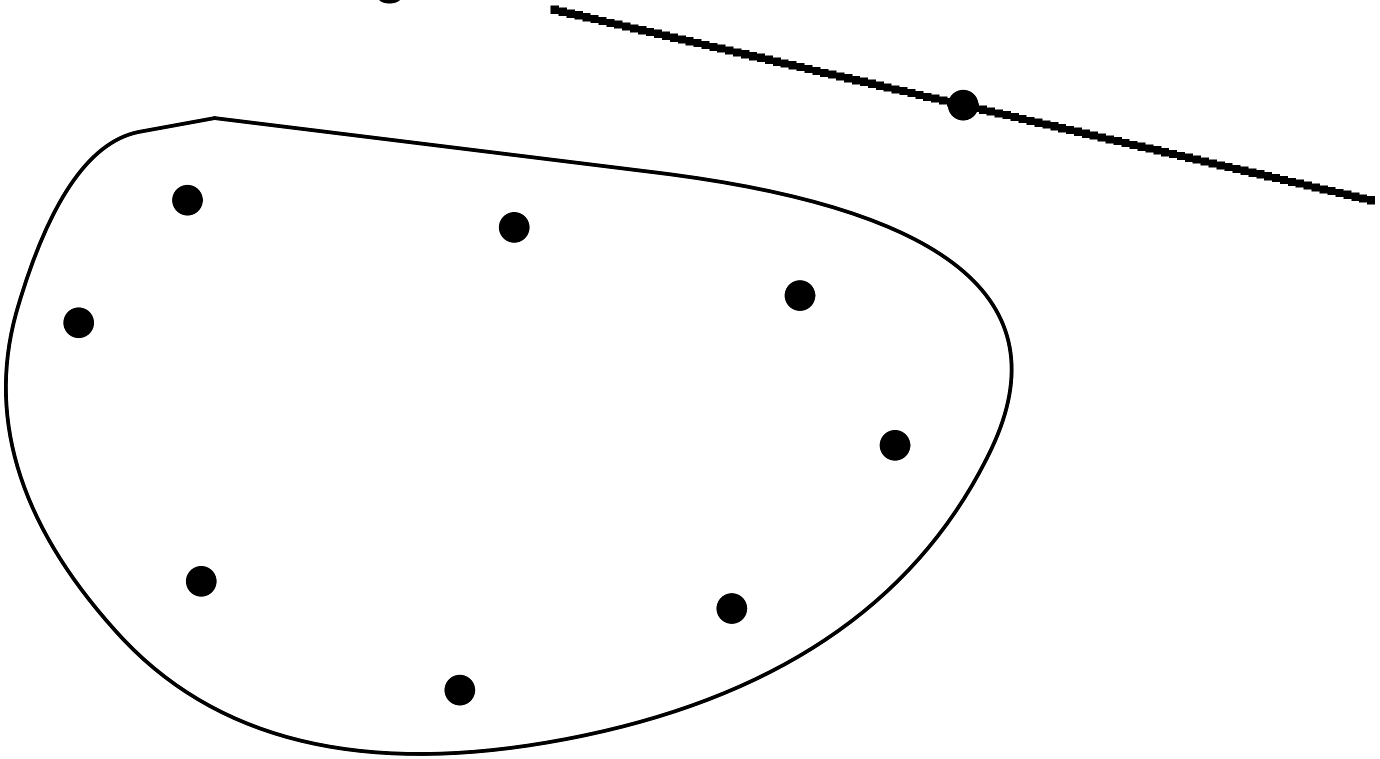
extremal in two ways

Second, you can't add another point to your set and still have a blocking semioval.



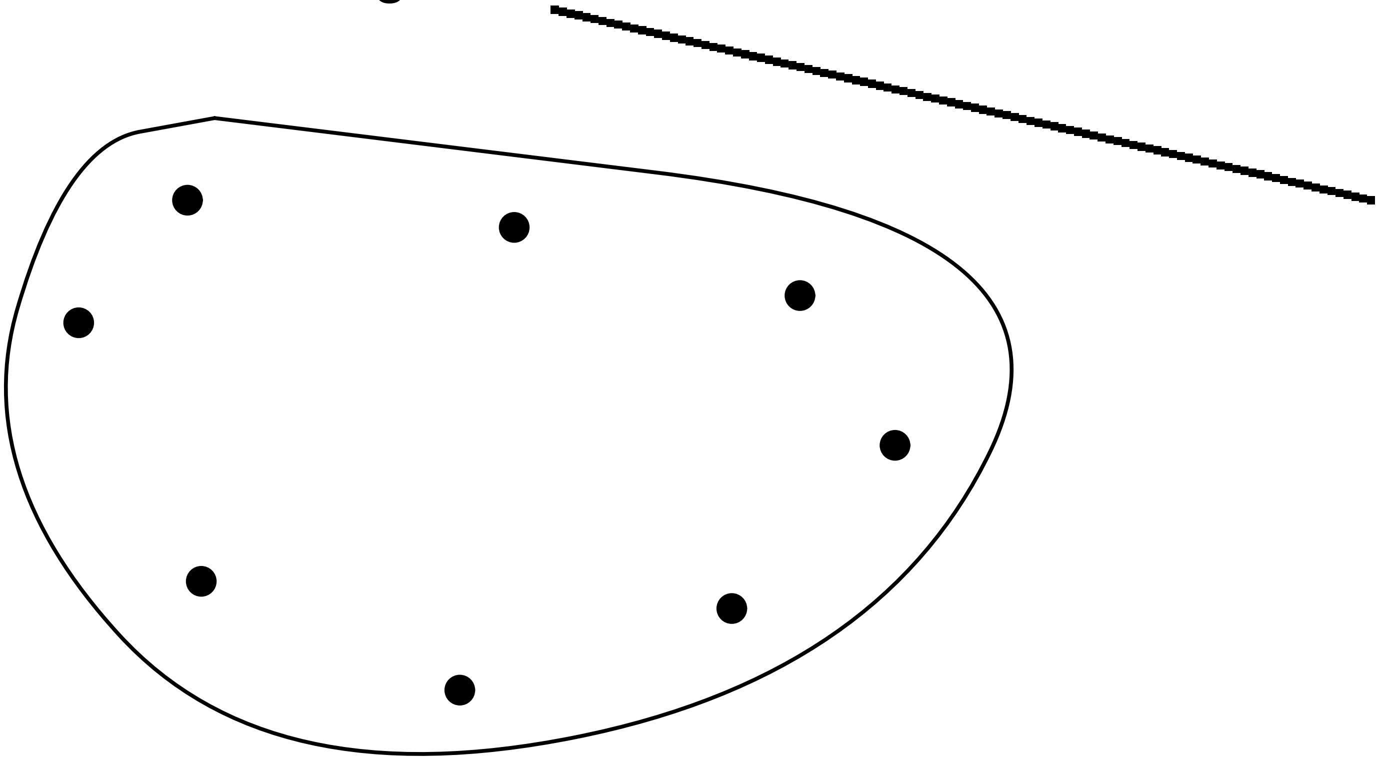
extremal in two ways

Second, you can't add another point to your set and still have a blocking semioval.



extremal in two ways

Second, you can't add another point to your set and still have a blocking semioval.



known constructions

Many of the known constructions of (blocking) semiovals contain large collinear subsets. The vertex-less triangle is one good example of this.

known constructions

Many of the known constructions of (blocking) semiovals contain large collinear subsets. The vertex-less triangle is one good example of this.

In a sense, conics are the opposite of lines. No three points of a conic are collinear. Our goal is to use conics to build semiovals (hopefully blocking).

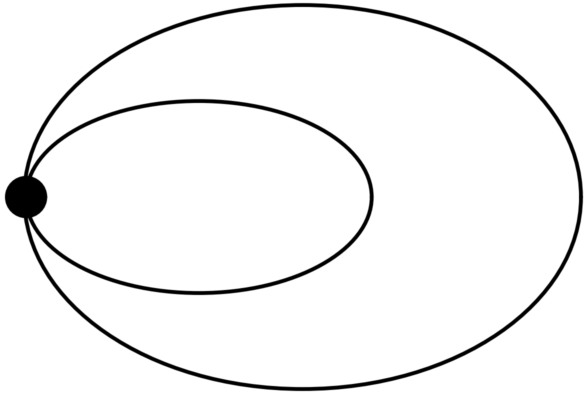
known constructions

Many of the known constructions of (blocking) semiovals contain large collinear subsets. The vertex-less triangle is one good example of this.

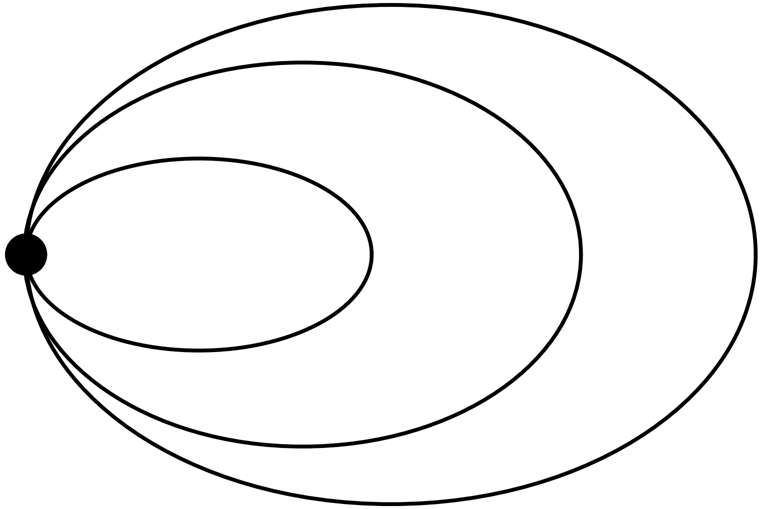
In a sense, conics are the opposite of lines. No three points of a conic are collinear. Our goal is to use conics to build semiovals (hopefully blocking).

Some of our original motivation came from a 1992 paper by Tamás Szőnyi titled “Note on the existence of large minimal blocking sets in Galois planes.”

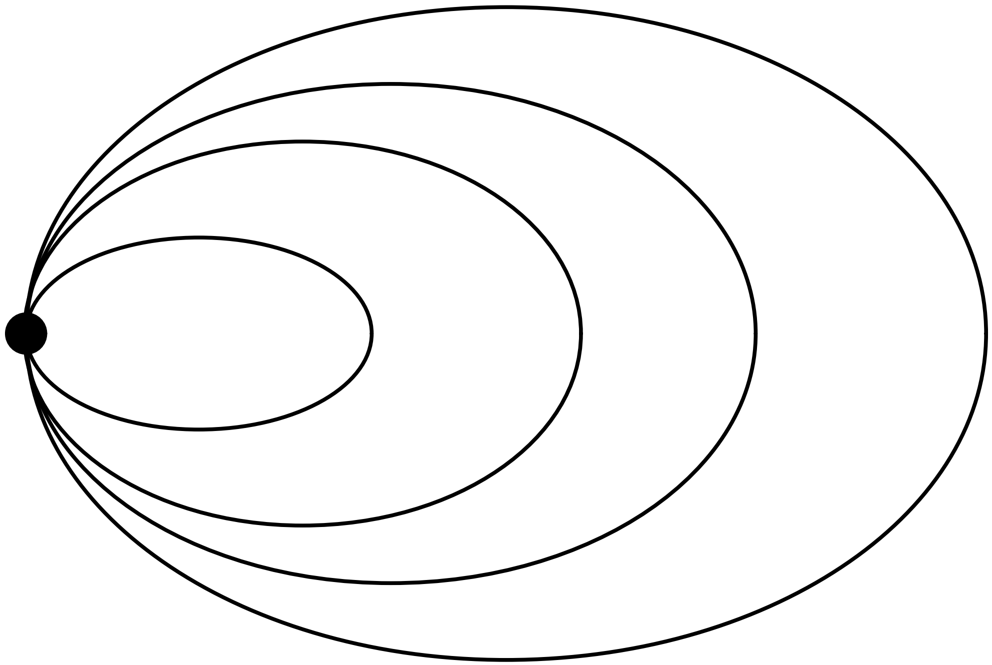
tangent pencil



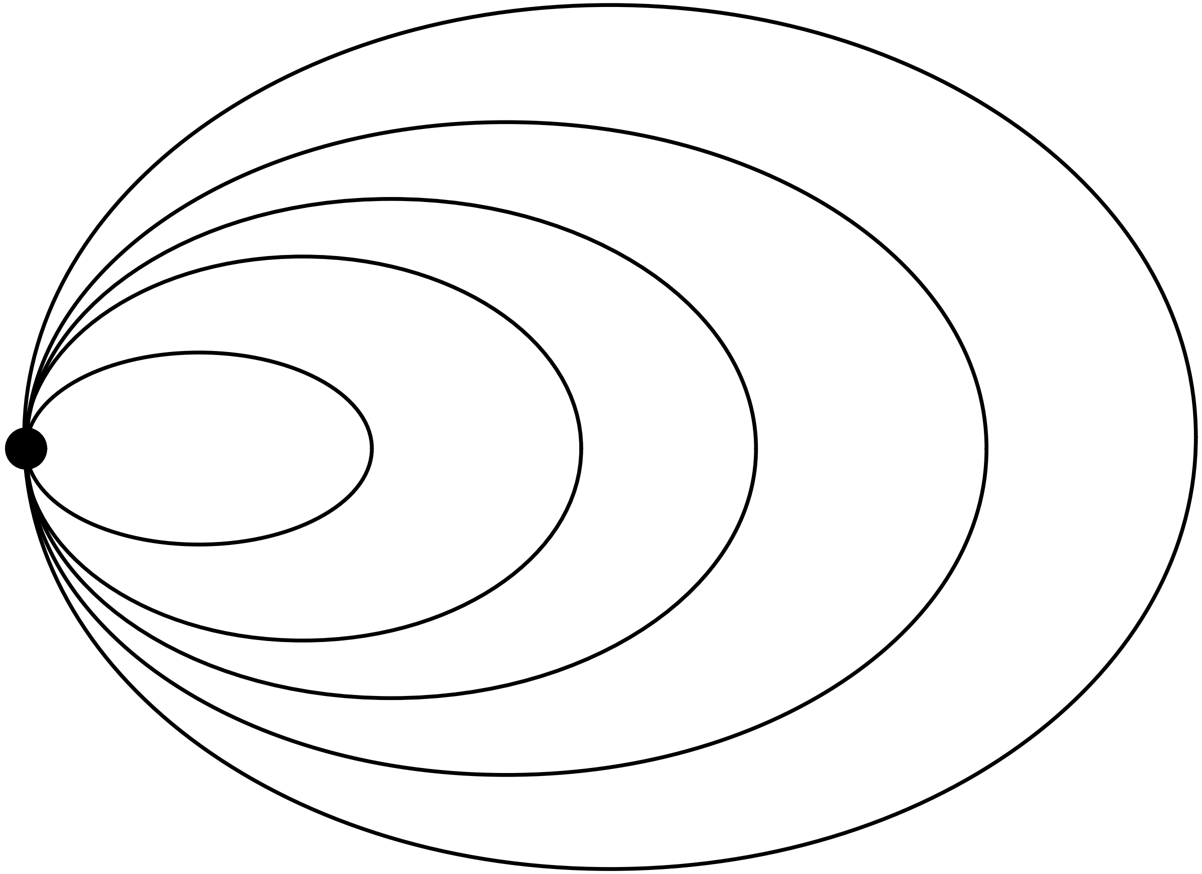
tangent pencil



tangent pencil



tangent pencil



algebraic description

Define $\mathcal{C}_0$ as the conic whose points satisfy $x^2 - yz = 0$, and $\mathcal{C}_\infty$ as satisfing $z^2 = 0$

algebraic description

Define $\mathcal{C}_0$ as the conic whose points satisfy $x^2 - yz = 0$, and $\mathcal{C}_\infty$ as satisfing $z^2 = 0$

Then, the conics in the pencil are defined by the linear combinations of these:
$\mathcal{C}_k$ is defined by $x^2 - yz + kz^2 = 0$.

algebraic description

Define $\mathcal{C}_0$ as the conic whose points satisfy $x^2 - yz = 0$, and $\mathcal{C}_\infty$ as satisfing $z^2 = 0$

Then, the conics in the pencil are defined by the linear combinations of these:
$\mathcal{C}_k$ is defined by $x^2 - yz + kz^2 = 0$.

In the arguments, Szőnyi shows that all points are “essential.” In other words, no point can be removed without destroying the blocking property. This implies that there are tangent lines at each of the points.

algebraic description

Define $\mathcal{C}_0$ as the conic whose points satisfy $x^2 - yz = 0$, and $\mathcal{C}_\infty$ as satisfing $z^2 = 0$

Then, the conics in the pencil are defined by the linear combinations of these:
$\mathcal{C}_k$ is defined by $x^2 - yz + kz^2 = 0$.

In the arguments, Szőnyi shows that all points are "essential." In other words, no point can be removed without destroying the blocking property. This implies that there are tangent lines at each of the points.

But, conics have *unique* tangents at each point. Hence, Szőnyi's set is a semioval.

algebraic description

Define $\mathcal{C}_0$ as the conic whose points satisfy $x^2 - yz = 0$, and $\mathcal{C}_\infty$ as satisfing $z^2 = 0$

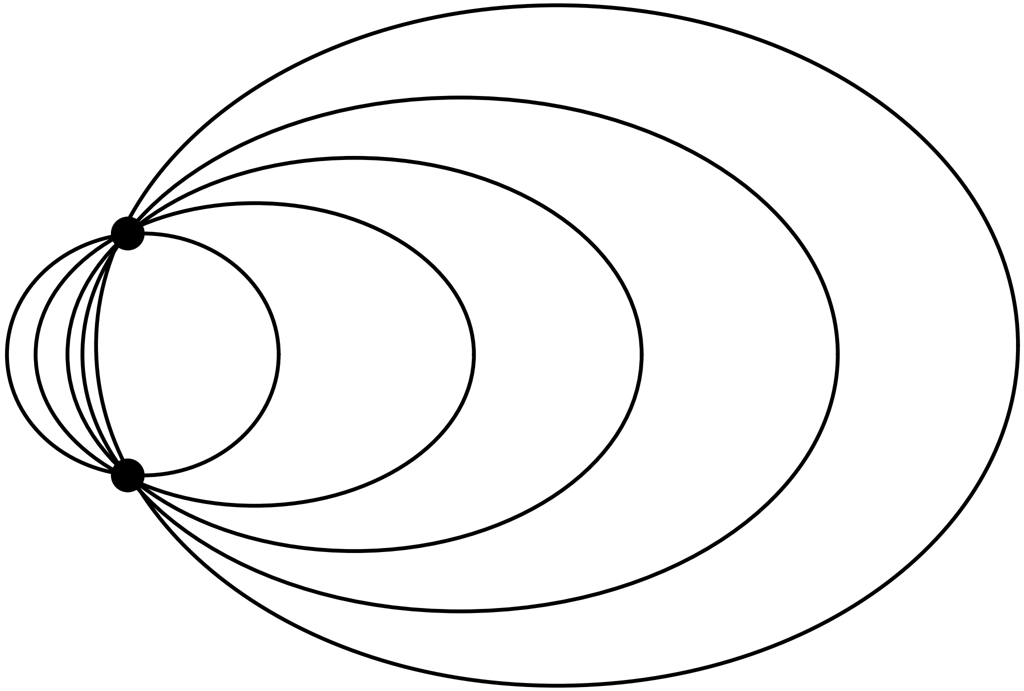
Then, the conics in the pencil are defined by the linear combinations of these:
$\mathcal{C}_k$ is defined by $x^2 - yz + kz^2 = 0$.

In the arguments, Szőnyi shows that all points are "essential." In other words, no point can be removed without destroying the blocking property. This implies that there are tangent lines at each of the points.

But, conics have *unique* tangents at each point. Hence, Szőnyi's set is a semioval.

Was there any reason to start with a pair of tangent conics?

other pencils



Our Main Result

Theorem: Let $\mathcal{B} = \bigcup_{i=1}^{k} \mathcal{C}_i$ be a semioval in $PG(2, q)$ that is the union of nondegenerate conics $\mathcal{C}_i$. Then $\mathcal{B}$ is isomorphic to one of the following sets:

- a conic (note that this is the only possibility when q is even), or
- a union of at most $\sqrt{q}$ conics all lying in a common pencil, or
- a union of at most four conics, no three in a common pencil.

Our Main Result

Theorem: Let $\mathcal{B} = \bigcup_{i=1}^{k} \mathcal{C}_i$ be a semioval in $PG(2,q)$ that is the union of nondegenerate conics $\mathcal{C}_i$. Then $\mathcal{B}$ is isomorphic to one of the following sets:

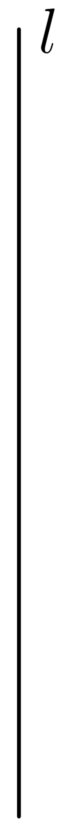
- a conic (note that this is the only possibility when q is even), or
- a union of at most $\sqrt{q}$ conics all lying in a common pencil, or
- a union of at most four conics, no three in a common pencil.

So the semiovals that can be written as a union of conics are completely classified.

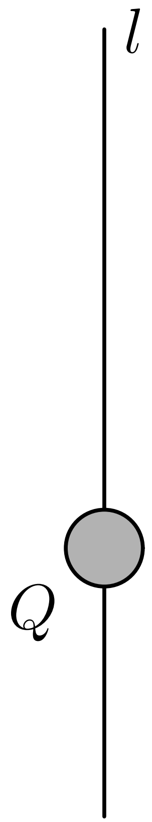
What is a blocking set?

A blocking set $\mathcal{S}$ in a projective plane π is a set of points such that every line in π contains at least one point in $\mathcal{S}$ and one point not in $\mathcal{S}$. Therefore $\mathcal{S}$ intersects every line in π but $\mathcal{S}$ contains no lines.

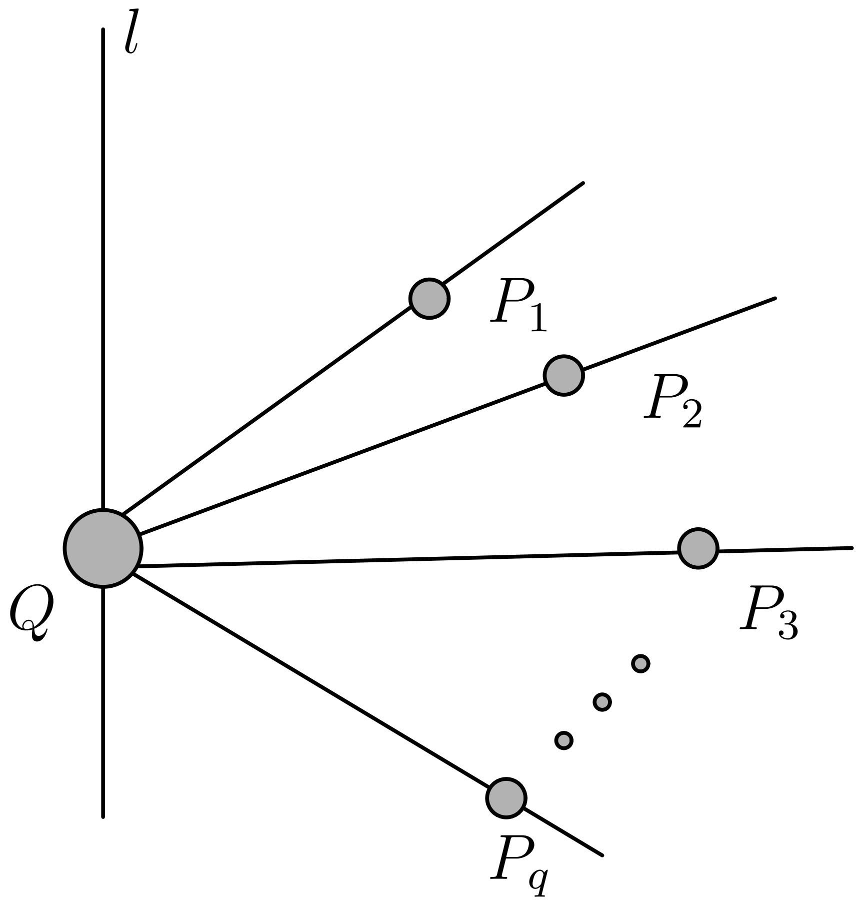
Example #1



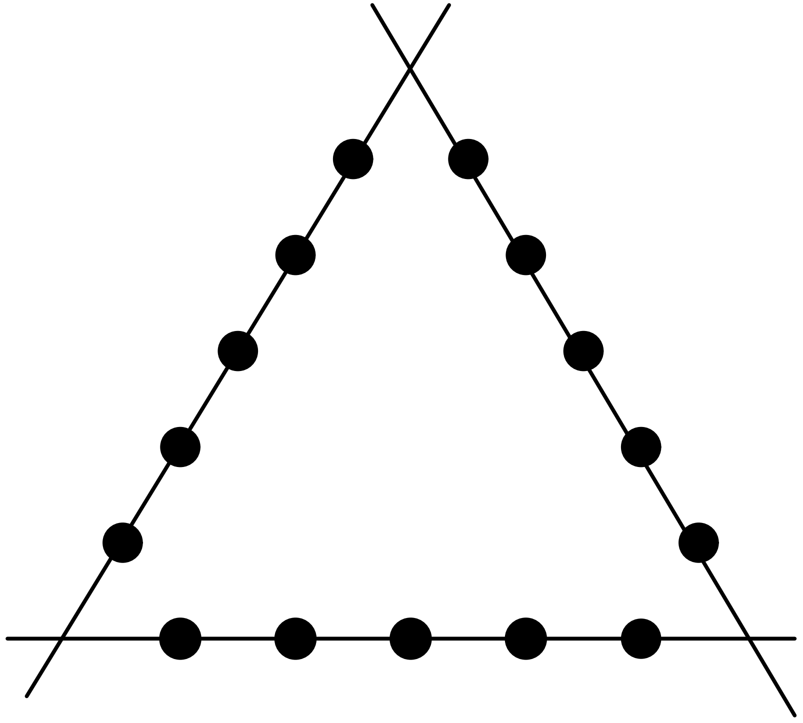
Example #1



Example #1



Example #2: Vertexless Triangle



A natural definition

Definition: An anti-blocking set $\mathcal{A}$ is a set of points such that:

A natural definition

Definition: An anti-blocking set $\mathcal{A}$ is a set of points such that:

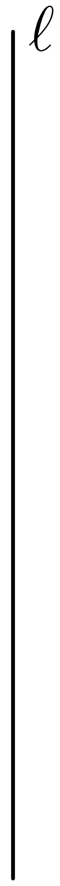
- $\mathcal{A}$ does not block all lines, and

A natural definition

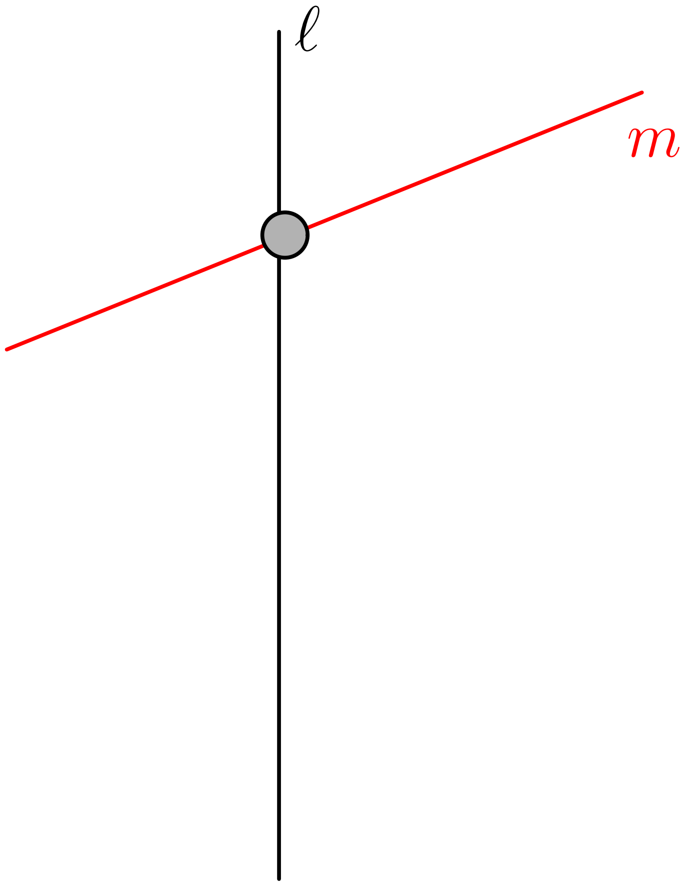
Definition: An anti-blocking set $\mathcal{A}$ is a set of points such that:

- $\mathcal{A}$ does not block all lines, and
- is not a subset of any blocking set.

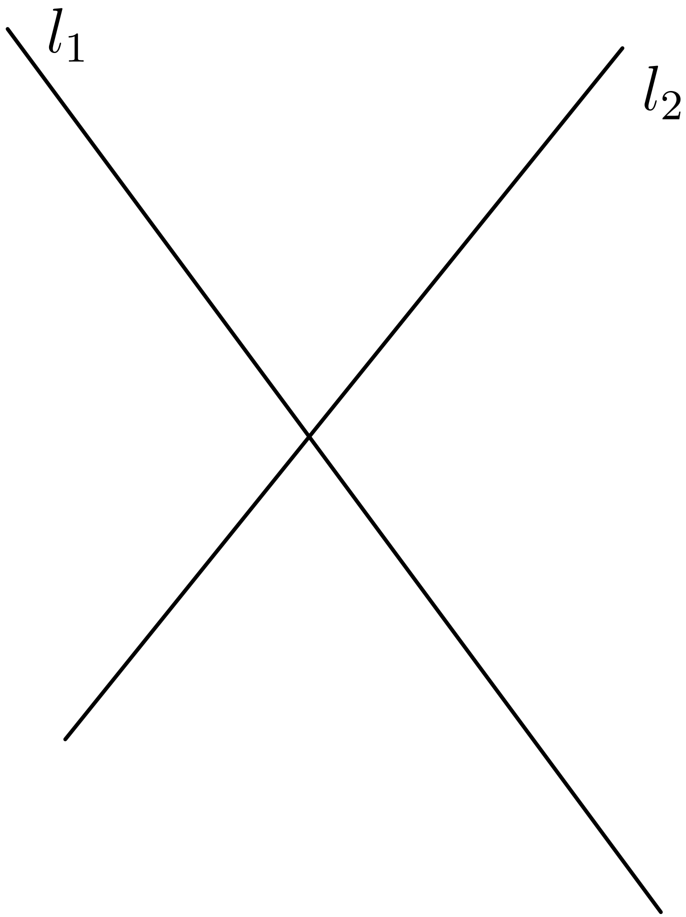
Example #1: Complement of a Line



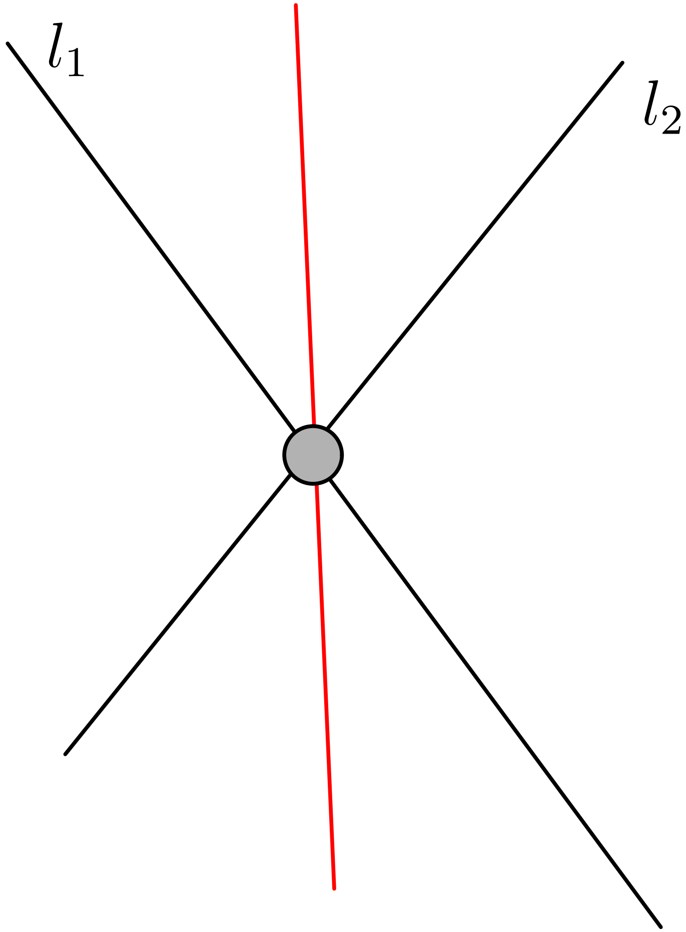
Example #1: Complement of a Line



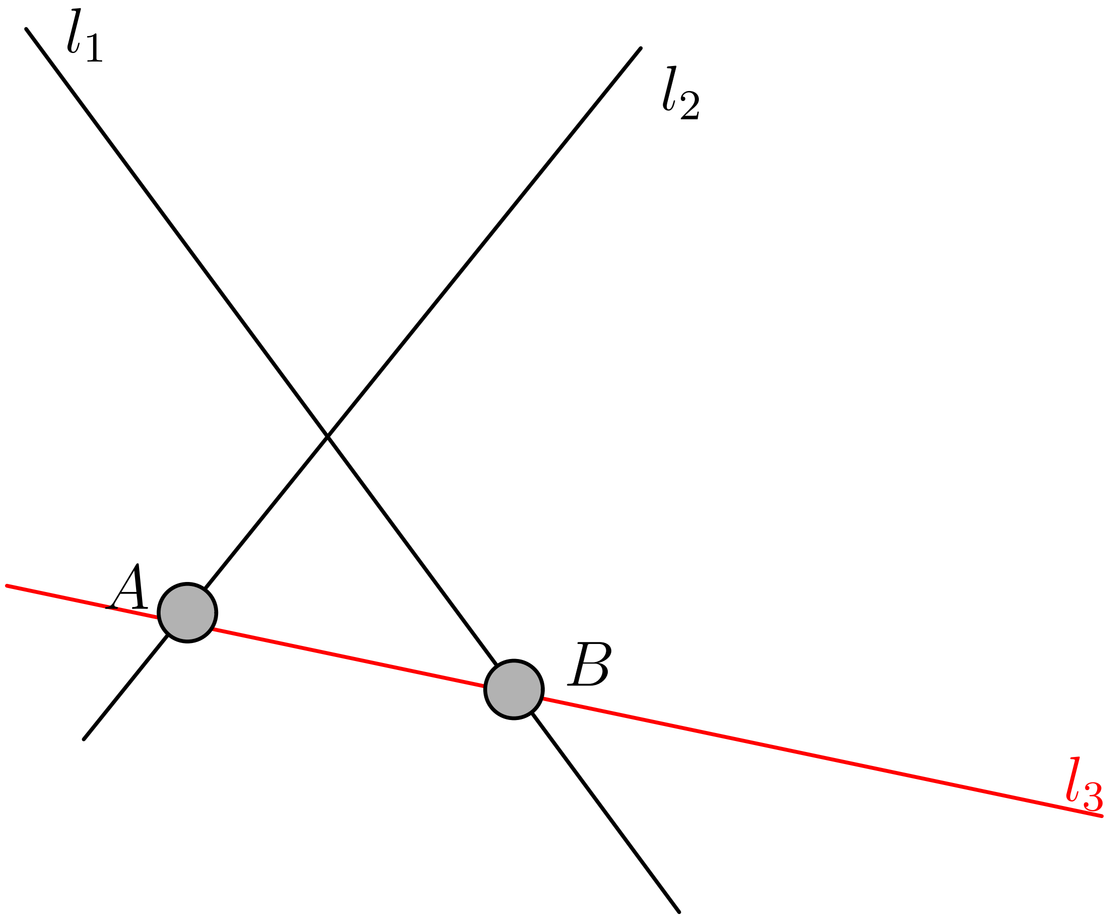
Example #2: Complement of 2 Lines



Example #2: Complement of 2 Lines



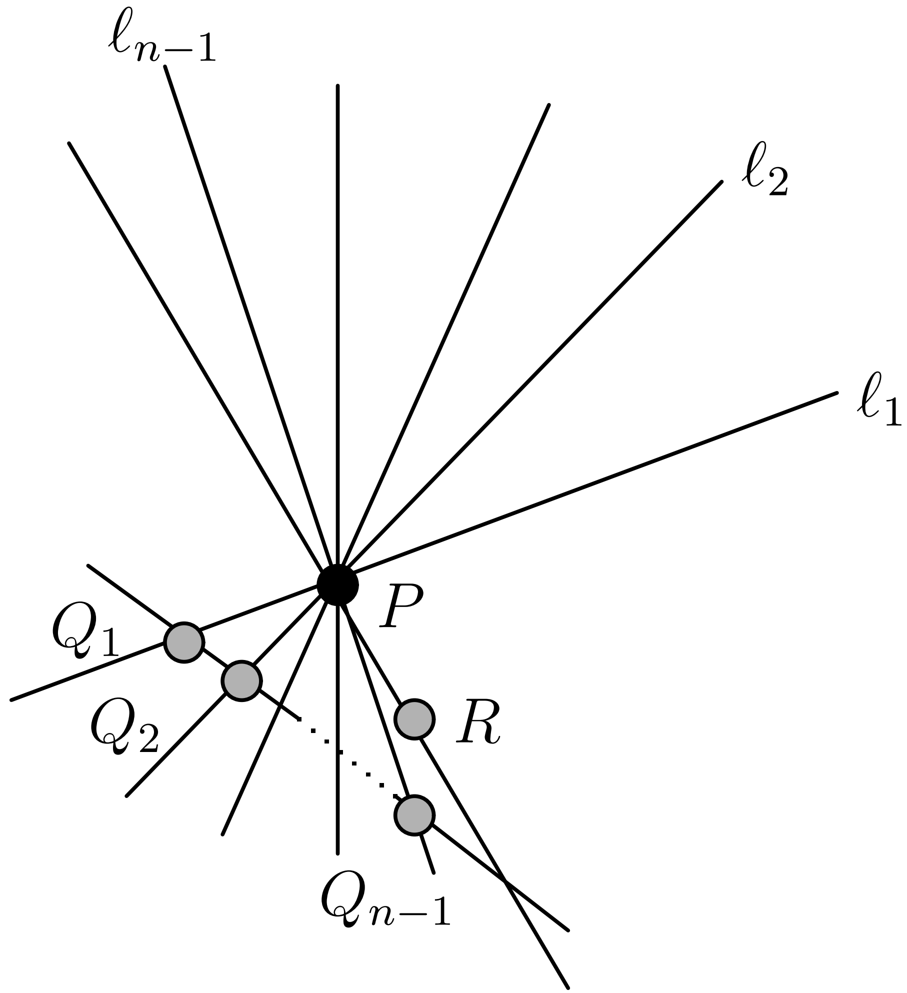
Example #2: Complement of 2 Lines

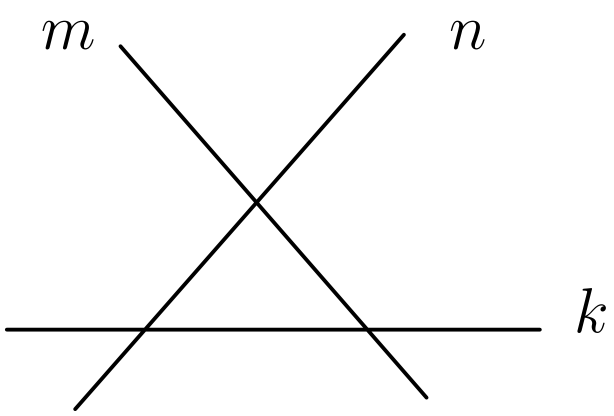


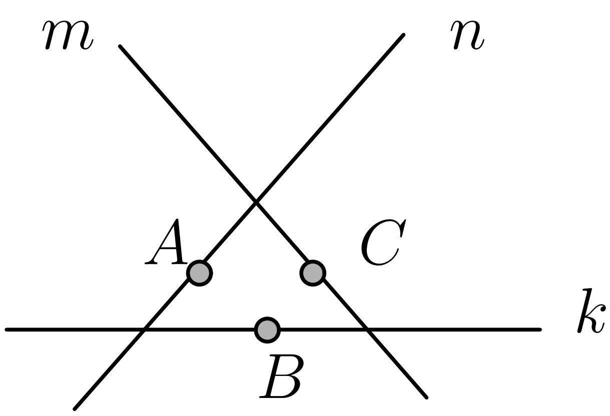
Results

Theorem Let $\mathcal{A}$ be an anti-blocking set and $\mathcal{L}$ the set of all lines that do not contain a point of $\mathcal{A}$. Then $|\mathcal{L}| \leq 2$.

By way of contradiction, suppose $|\mathcal{L}| \not\leq 2$ so that $|\mathcal{L}| \geq 3$. We show that points can be added to $\mathcal{A}$ in such a way as to build a blocking set. Therefore, $\mathcal{A}$ is in fact a subset of a blocking set and so is not an anti-blocking set. This will prove our result.

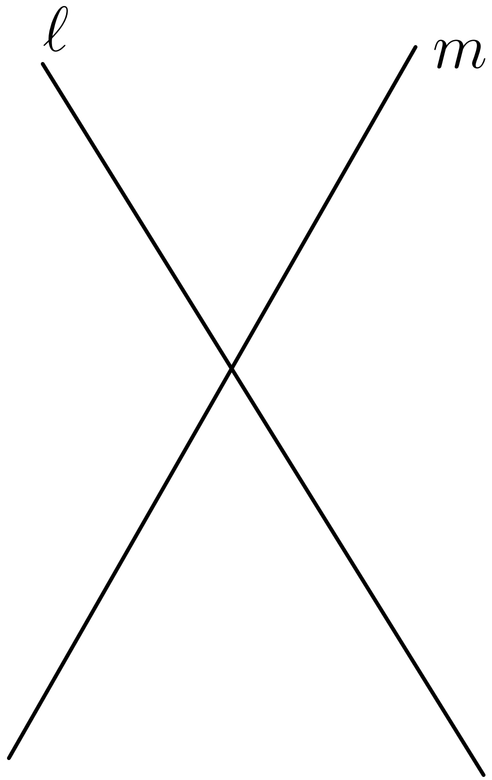

ℓ_{n-1}
ℓ_2
ℓ_1
P
Q_1
Q_2
R
Q_{n-1}


m
n
k


m
n
A
C
k
B

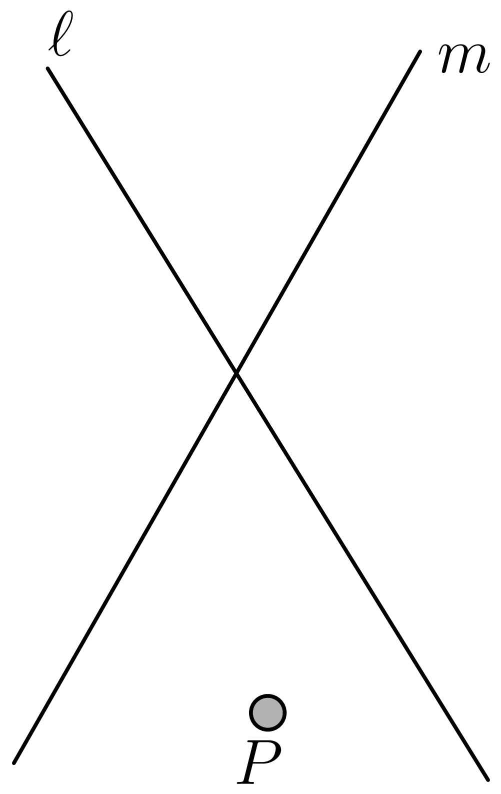
Results

Theorem Let $\mathcal{A}$ be an anti-blocking set. If $\mathcal{A}$ is a subset of the complement of two lines, then $\mathcal{A}$ is exactly equal to the complement of two lines.



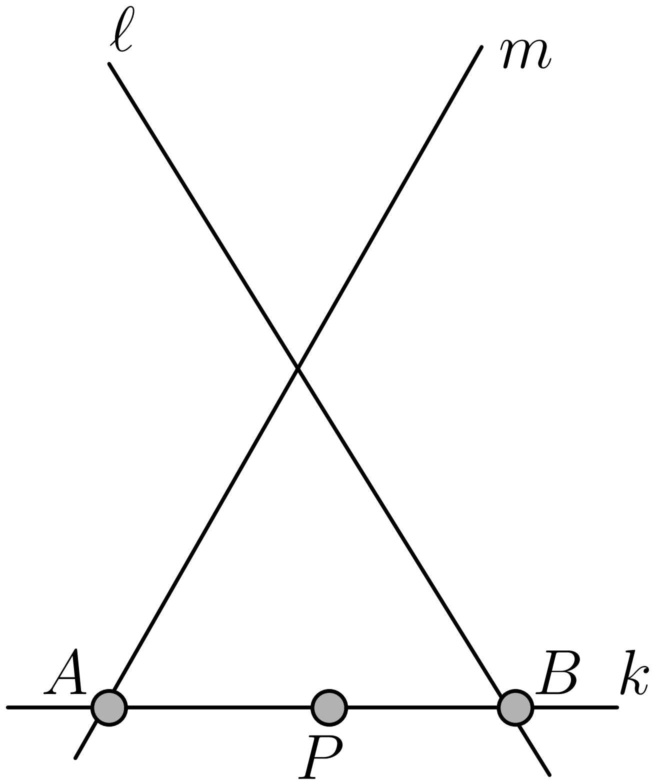
Results

Theorem Let $\mathcal{A}$ be an anti-blocking set. If $\mathcal{A}$ is a subset of the complement of two lines, then $\mathcal{A}$ is exactly equal to the complement of two lines.



Results

Theorem Let $\mathcal{A}$ be an anti-blocking set. If $\mathcal{A}$ is a subset of the complement of two lines, then $\mathcal{A}$ is exactly equal to the complement of two lines.



A characterization

Naturally, we wish to use a pencil of conics to construct an anti-blocking set.

A characterization

Naturally, we wish to use a pencil of conics to construct an anti-blocking set.

Our construction relies on a characterization of anti-blocking sets:

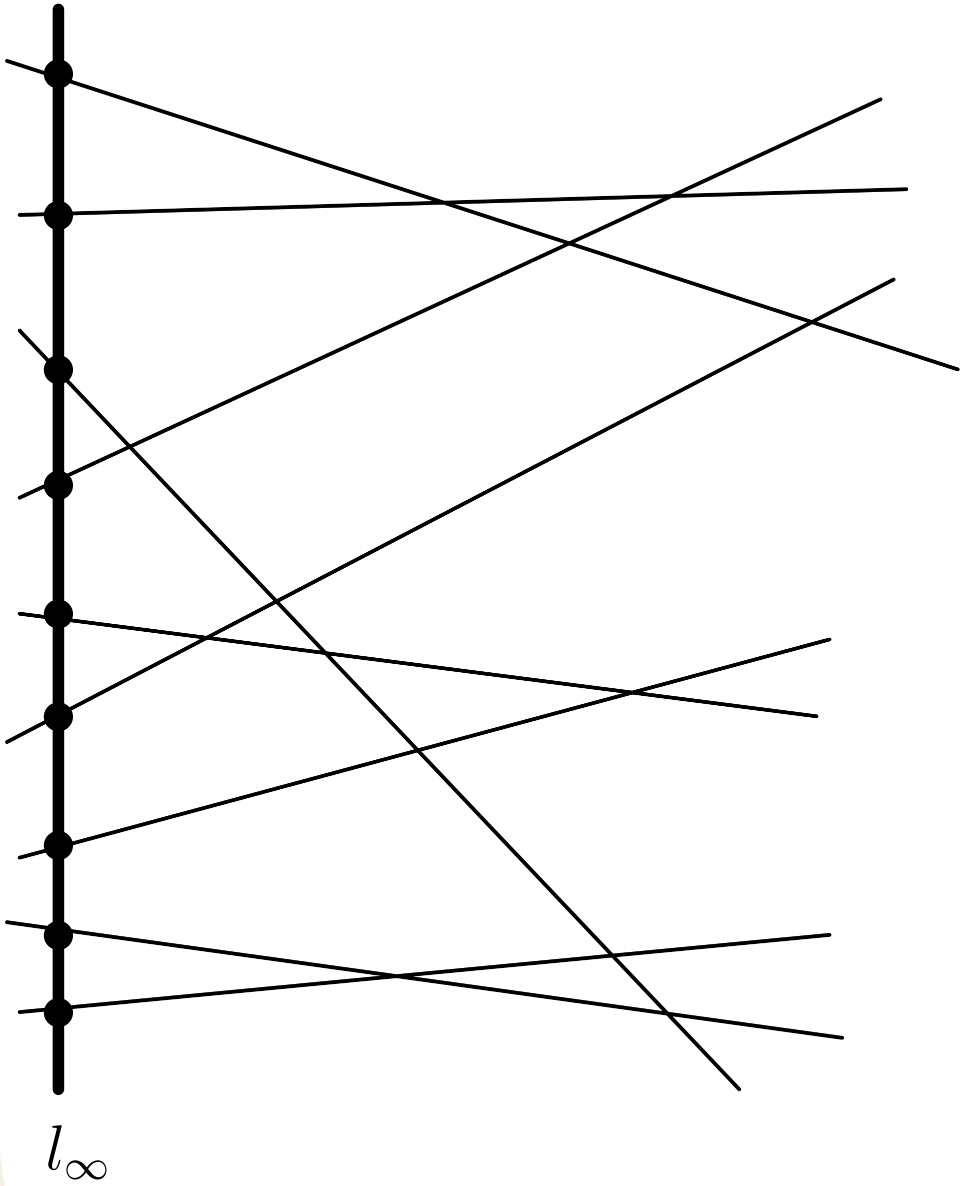
A characterization

Naturally, we wish to use a pencil of conics to construct an anti-blocking set.

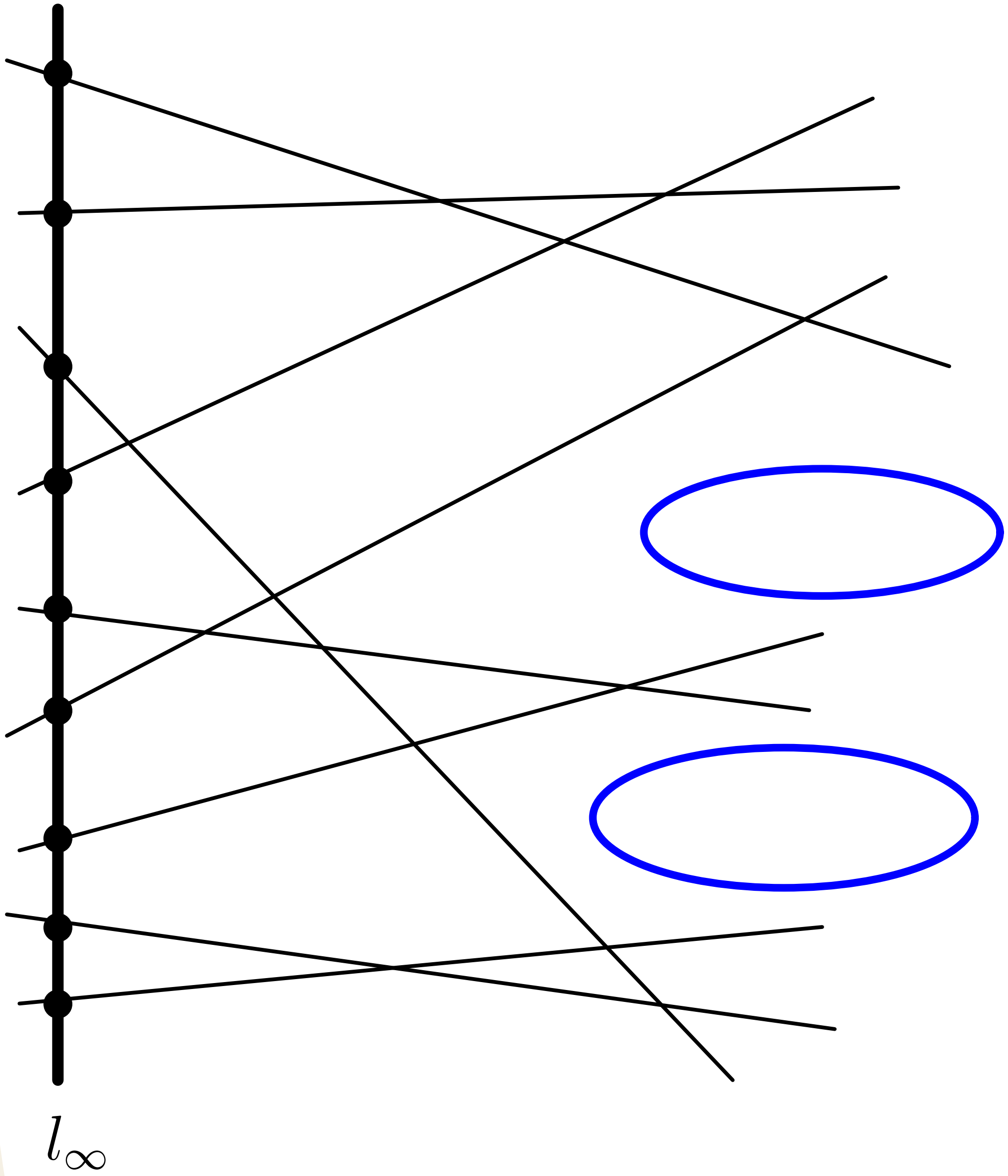
Our construction relies on a characterization of anti-blocking sets:

Theorem: Let ℓ_∞ be a line of the projective plane π. Suppose $\mathcal{A} \subseteq (\pi \setminus \ell_\infty)$, and $\mathcal{A}$ is not the complement of two lines. Then, $\mathcal{A}$ is an anti-blocking set if and only if for every point $P \in \ell_\infty$, there is a line ℓ ($\neq \ell_\infty$) through P such that $(\ell \setminus \{P\}) \subset \mathcal{A}$.

A characterization



Remove conics?

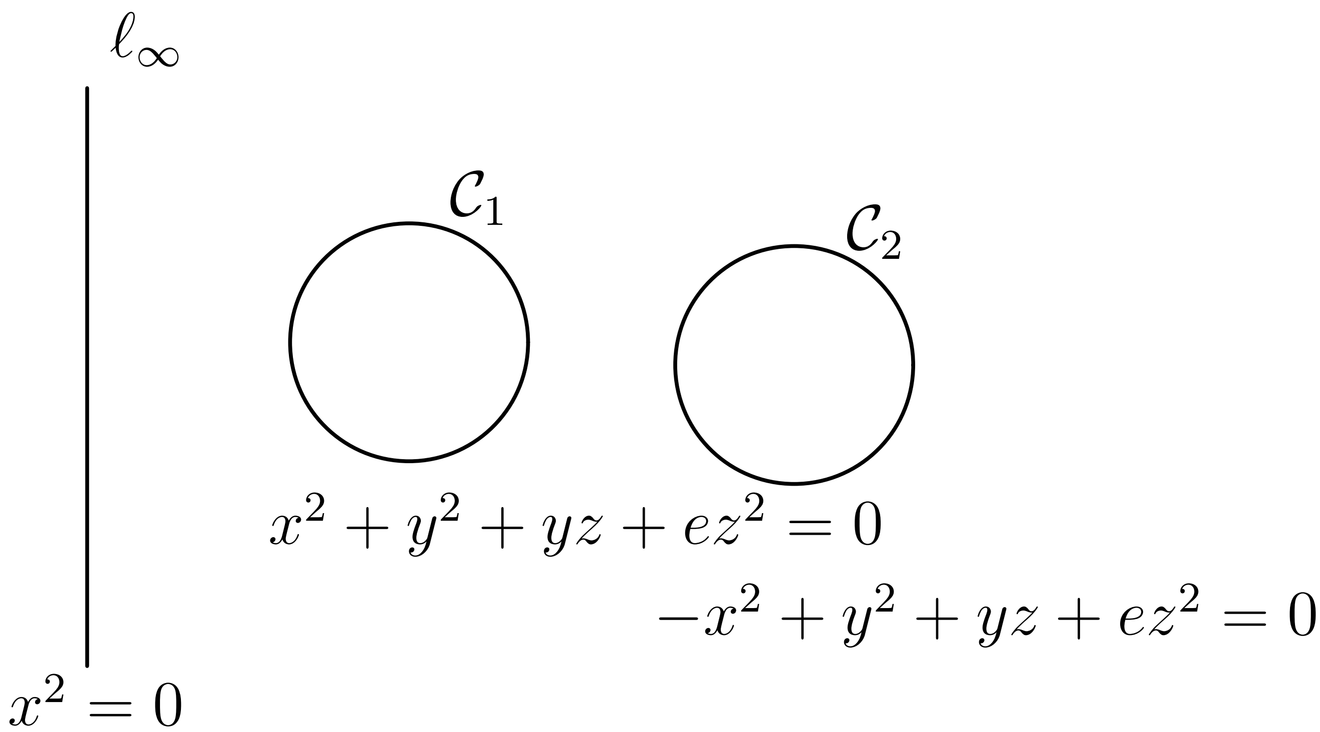


Remove conics?

It turns out that we can, again, use the algebraic pencils to describe precisely when one can select conics that satisfy the conditions to form an anti-blocking set.

Remove conics?

It turns out that we can, again, use the algebraic pencils to describe precisely when one can select conics that satisfy the conditions to form an anti-blocking set.



An anti-blocking sets from a pencil

Theorem: Let $\pi = PG(2,q)$ where $q \equiv 1 \pmod 4$. Then there exists an anti-blocking set of π of size $\frac{3q^2+1}{4}$.

An anti-blocking sets from a pencil

Theorem: Let $\pi = PG(2,q)$ where $q \equiv 1 \pmod 4$. Then there exists an anti-blocking set of π of size $\frac{3q^2+1}{4}$.

We argue that one can select $\frac{q-1}{4}$ conics from an algebraic pencil, remove them from the point-set of $\pi \setminus \ell_\infty$, and be left with a collection of points forming an anti-blocking set.

An anti-blocking sets from a pencil

If $P = (0, a, b)$ and $a^2 + ab + eb^2$ is a non-square, the special line is

$$\ell = \langle (0, a, b), (1, 0, 0) \rangle$$

If $P = (0, a, b)$ and $a^2 + ab + eb^2$ is a square, we have two lines:

$$\ell_+ = \langle (0, a, b), (1, 0, c) \rangle, \ell_- = \langle (0, a, b), (1, 0, -c) \rangle$$

An anti-blocking sets from a pencil

If $P = (0, a, b)$ and $a^2 + ab + eb^2$ is a non-square, the special line is

$$\ell = \langle (0, a, b), (1, 0, 0) \rangle$$

If $P = (0, a, b)$ and $a^2 + ab + eb^2$ is a square, we have two lines:

$$\ell_+ = \langle (0, a, b), (1, 0, c) \rangle, \ell_- = \langle (0, a, b), (1, 0, -c) \rangle$$

The technique is all algebraic. We use the face that -1 is a square, and we select λ to have certain properties (which is guaranteed by the cyclotomic numbers of order 2).

What is a cap?

A *cap* in a projective or affine geometry is a set of points with the property that no line meets the set in more than two points.

What is a cap?

A *cap* in a projective or affine geometry is a set of points with the property that no line meets the set in more than two points.

In a projective or affine plane of order q, the maximal size of a cap is bounded by $q+1$ if q is odd, or $q+2$ if q is even. These bounds are achieved in the Desarguesian and many other planes, though there do exist planes where the maximal cap is smaller than these bounds, for example the dual derived semifield plane of order 16.

Some bounds

There exist bounds on the maximal size of a cap in higher-dimensional geometries as well, but exact values are known in only a very few small cases.

Some bounds

There exist bounds on the maximal size of a cap in higher-dimensional geometries as well, but exact values are known in only a very few small cases.

In $AG(4, q)$ or $PG(4, q)$, the maximal size of a cap is $\mathcal{O}(q^3)$. If $q \geq 8$ is even, the maximal size of a cap in $PG(4, q)$ is less than or equal to $q^3 - q^2 + 6q - 3$.

Some bounds

There exist bounds on the maximal size of a cap in higher-dimensional geometries as well, but exact values are known in only a very few small cases.

In $AG(4, q)$ or $PG(4, q)$, the maximal size of a cap is $\mathcal{O}(q^3)$. If $q \geq 8$ is even, the maximal size of a cap in $PG(4, q)$ is less than or equal to $q^3 - q^2 + 6q - 3$.

These bounds are non-constructive, and the best-known caps are significantly smaller than these bounds. In $AG(4, q)$, q even, the best known construction is due to Edel and Bierbrauer and yields a $(3q^2 + 4)$-cap.

The Pellegrino cap

One celebrated result on caps is due to Pellegrino who showed that the maximal size of a cap in both $AG(4,3)$ and $PG(4,3)$ is 20.

The Pellegrino cap

One celebrated result on caps is due to Pellegrino who showed that the maximal size of a cap in both $AG(4,3)$ and $PG(4,3)$ is 20.

As part of an undergraduate research project, Tucker provides an interesting analysis of Pellegrino's cap in $AG(4,3)$. Viewing $GF(9)$ as a two-dimensional vector space over $GF(3)$ with basis $\{1,\epsilon\}$, there is a natural bijection between the points of $AG(4,3)$ and the points of $AG(2,9)$, via $(a,b,c,d) \leftrightarrow (a+b\epsilon, c+d\epsilon)$.

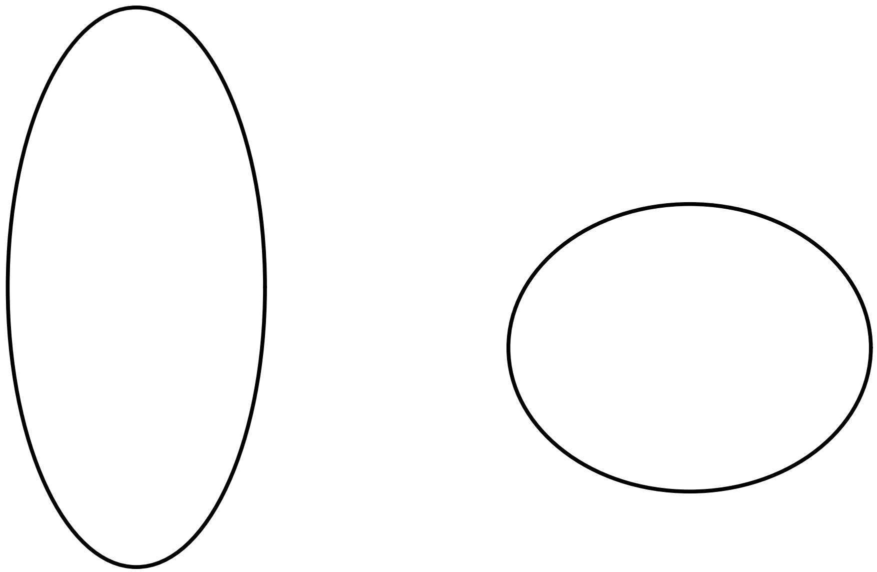
The Pellegrino cap

One celebrated result on caps is due to Pellegrino who showed that the maximal size of a cap in both $AG(4,3)$ and $PG(4,3)$ is 20.

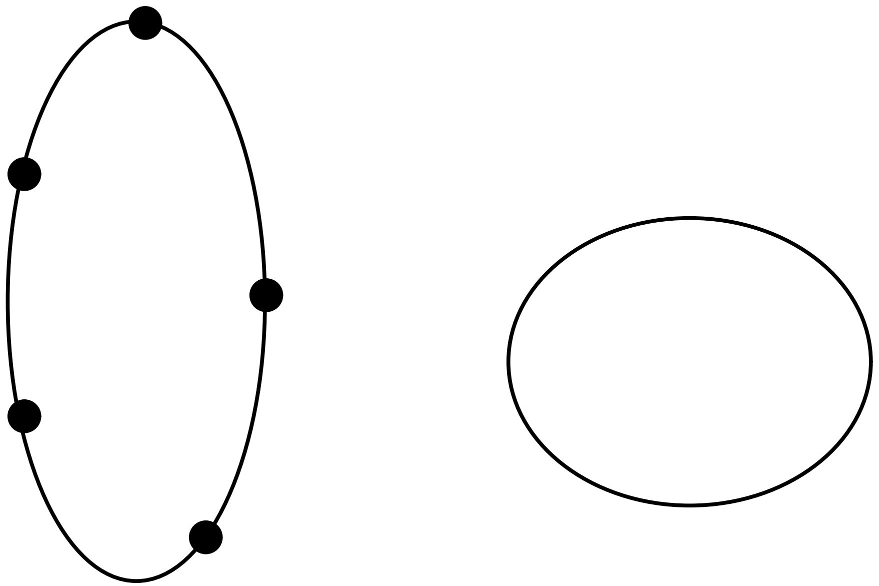
As part of an undergraduate research project, Tucker provides an interesting analysis of Pellegrino's cap in $AG(4,3)$. Viewing $GF(9)$ as a two-dimensional vector space over $GF(3)$ with basis $\{1,\epsilon\}$, there is a natural bijection between the points of $AG(4,3)$ and the points of $AG(2,9)$, via $(a,b,c,d) \leftrightarrow (a+b\epsilon, c+d\epsilon)$.

Looking at the image of a Pellegrino cap in $AG(4,3)$ under this bijection, Tucker noticed that the resulting set in $AG(2,9)$ is the union of two conics, each conic consisting exclusively of interior points of the other conic.

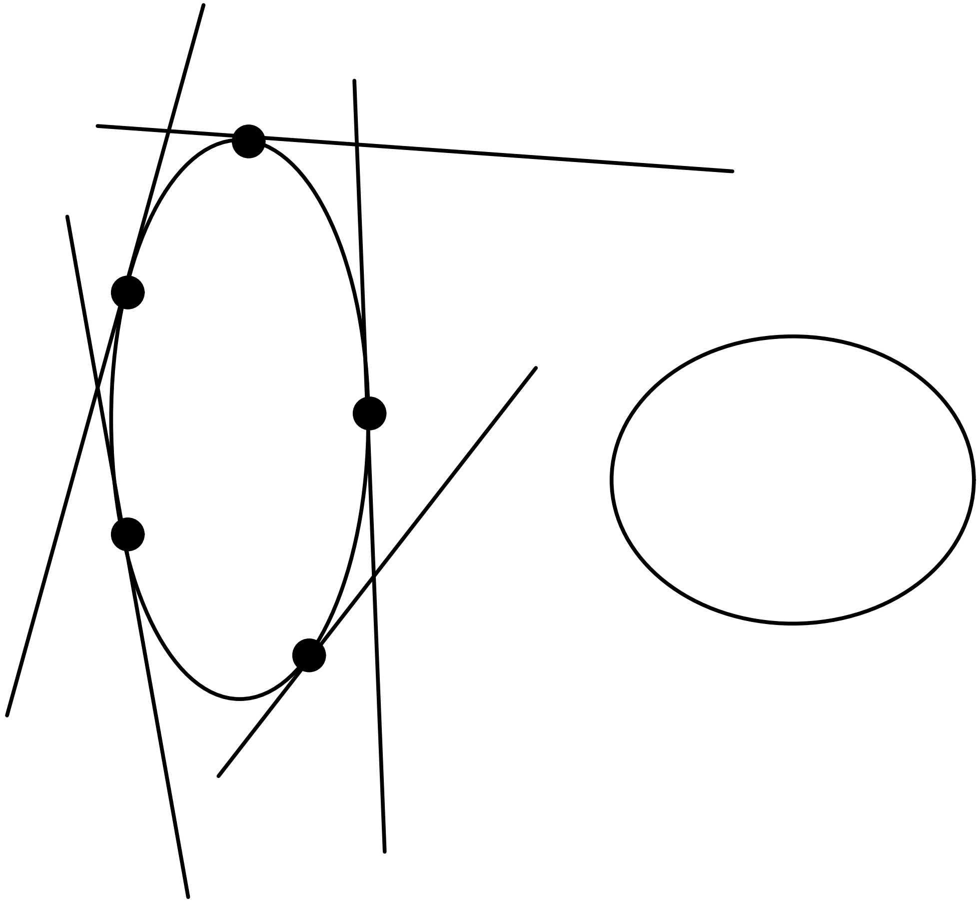
mutually interior conics



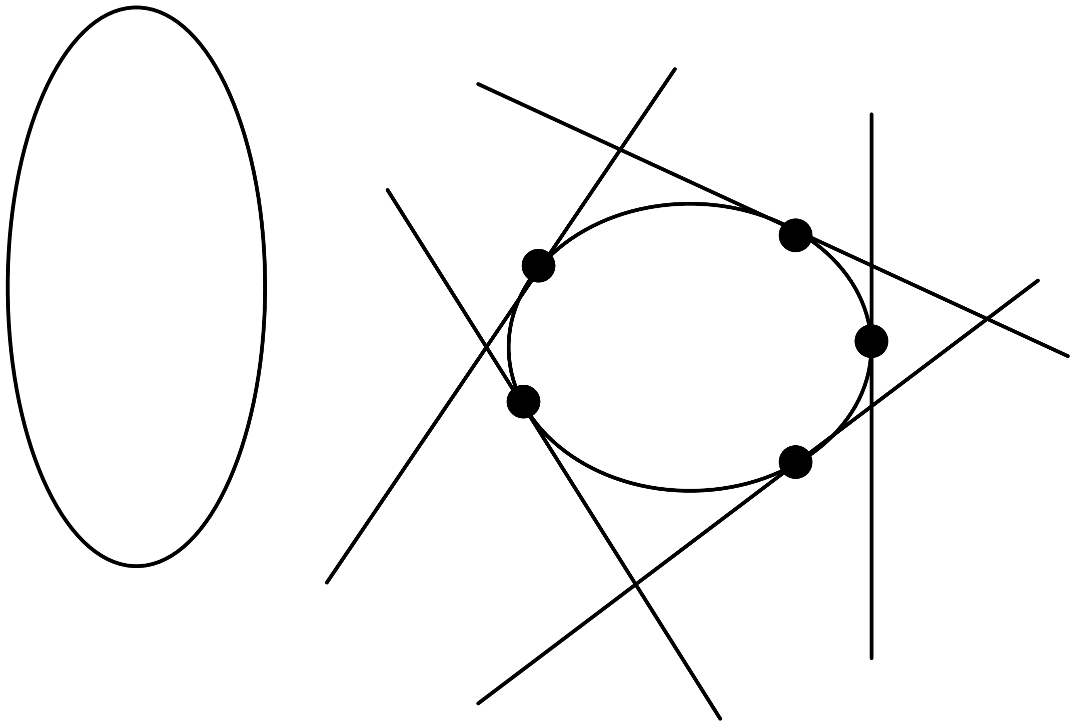
mutually interior conics



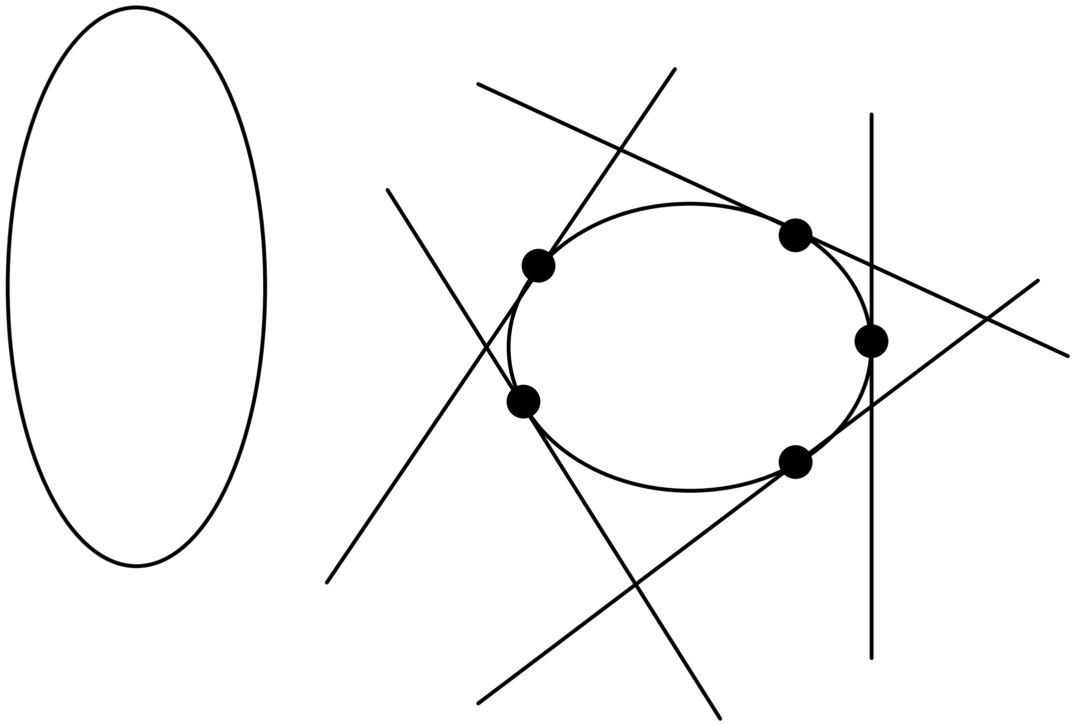
mutually interior conics



mutually interior conics

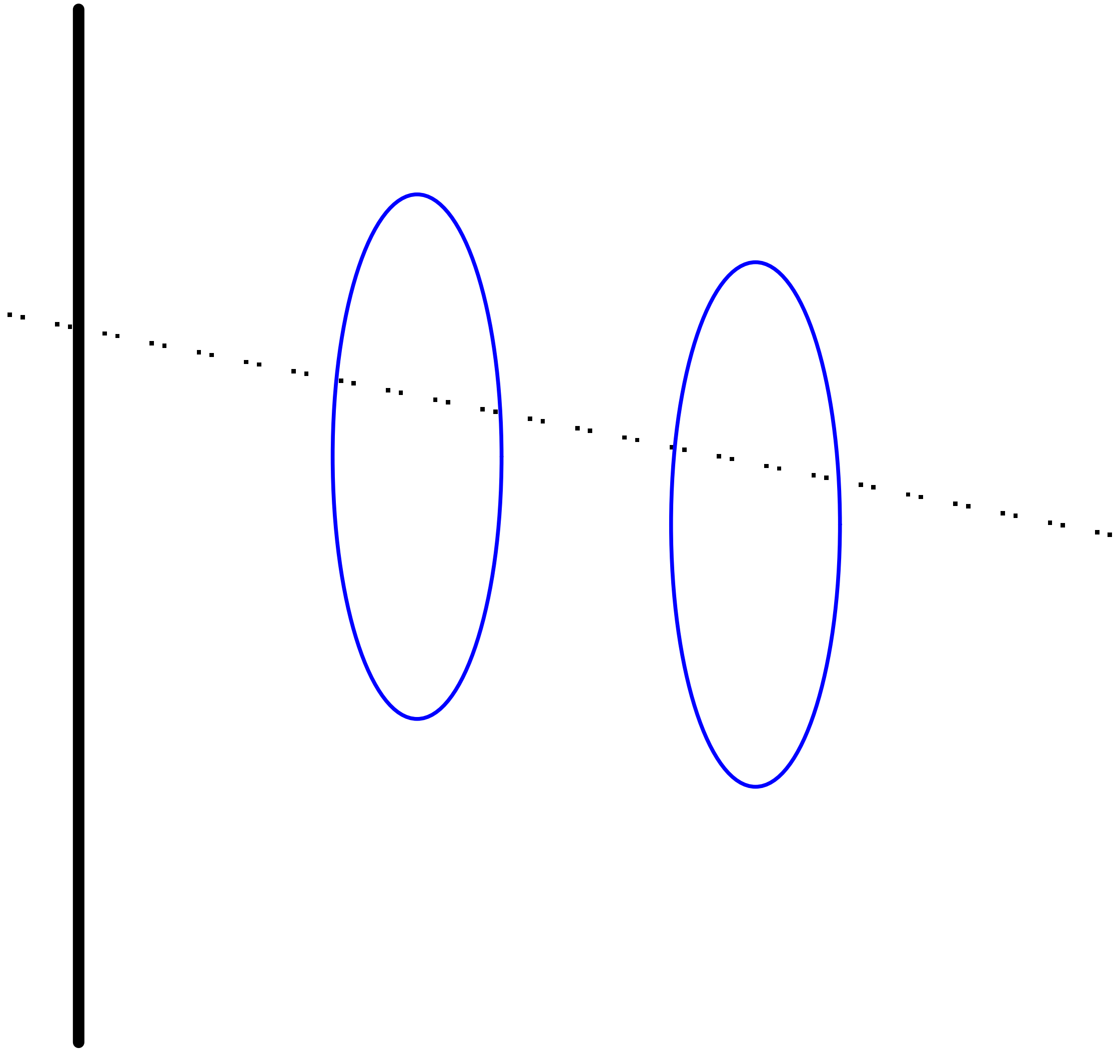


mutually interior conics

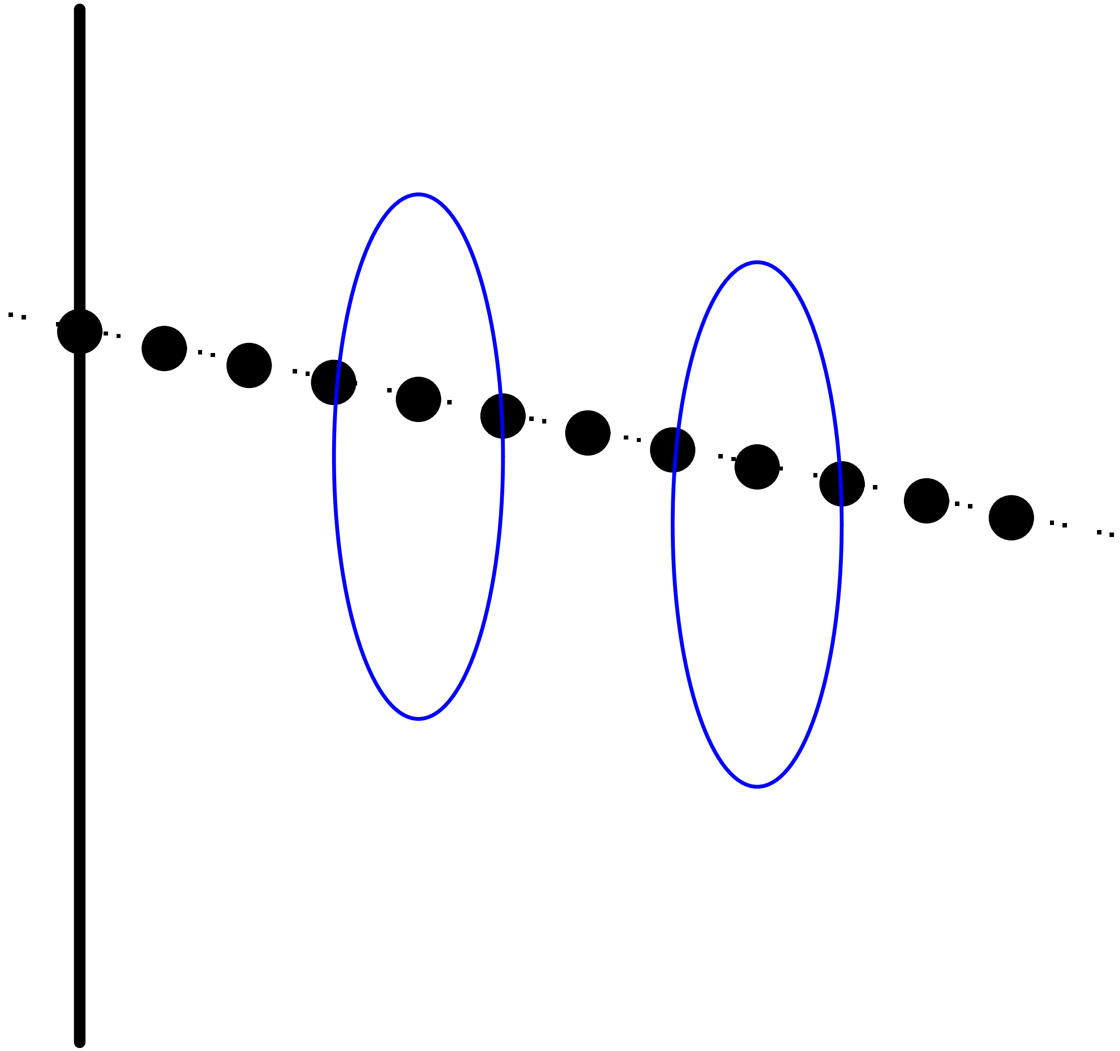


the conics are "mutually interior"

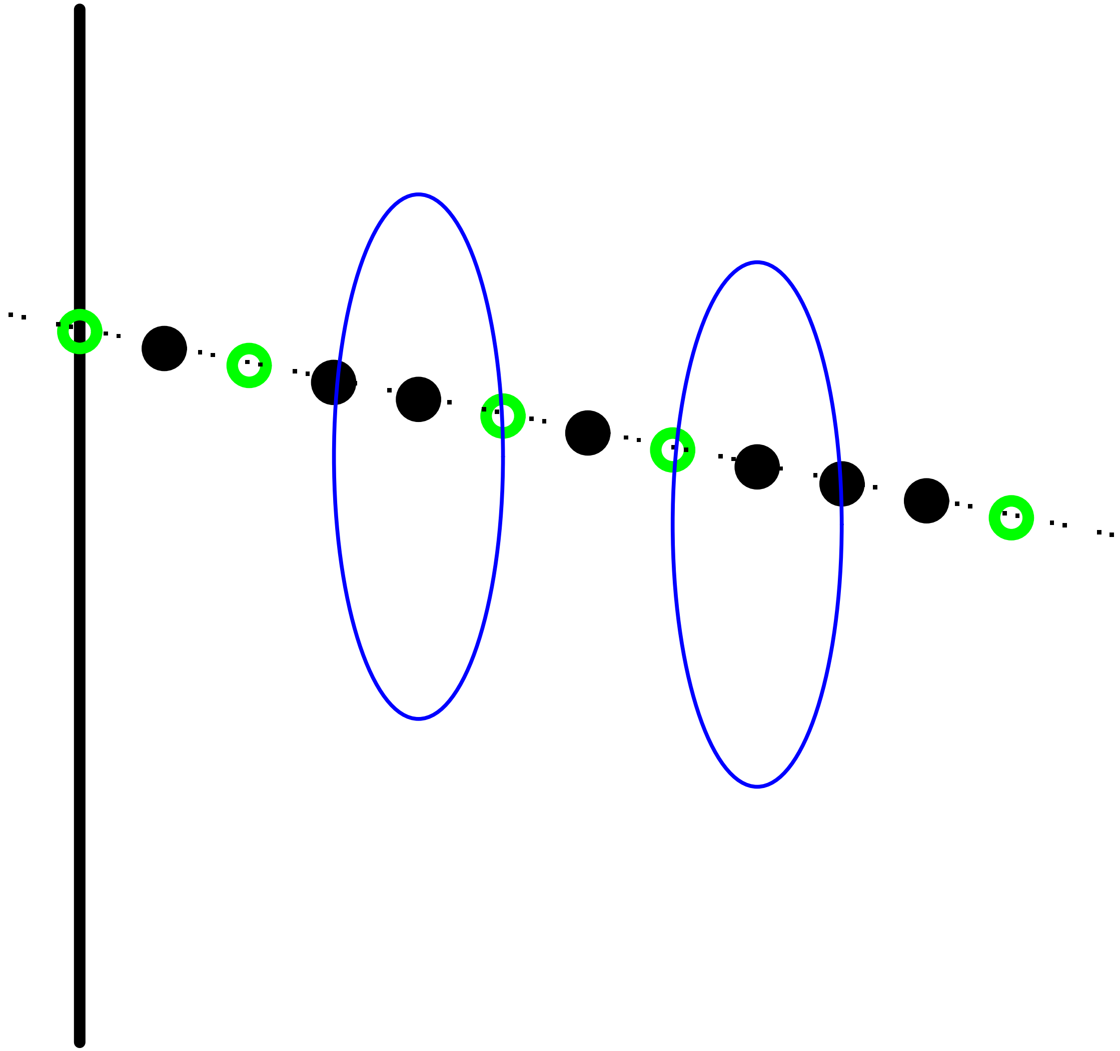
good pairs of conics



good pairs of conics



good pairs of conics



Mutually good ellipses

Let $\pi = AG(2, q^2)$, and let $\mathcal{P} = \{\mathcal{C}_\lambda : \lambda \in GF(q^2)\}$ be the linear pencil of conics with $\mathcal{C}_\lambda = \{(x, y) \in \pi : x^2 + xy + ey^2 = \lambda\}$, where $x^2 + x + e$ is irreducible.

Mutually good ellipses

Let $\pi = AG(2, q^2)$, and let $\mathcal{P} = \{\mathcal{C}_\lambda : \lambda \in GF(q^2)\}$ be the linear pencil of conics with $\mathcal{C}_\lambda = \{(x, y) \in \pi : x^2 + xy + ey^2 = \lambda\}$, where $x^2 + x + e$ is irreducible.

Theorem: The ellipse $\mathcal{C}_\lambda$, $\lambda \notin \{0, 1\}$, is $\mathcal{C}_1$-good if and only if for all $a, b \in GF(q^2)$ such that
$\frac{2a+b}{a^2+ab+eb^2} \in GF(q) \setminus \{-1, -2\}$,
$\lambda \neq (a + 1)^2 + (a + 1)b + eb^2$.

Mutually good ellipses

Let $\pi = AG(2, q^2)$, and let $\mathcal{P} = \{\mathcal{C}_\lambda : \lambda \in GF(q^2)\}$ be the linear pencil of conics with $\mathcal{C}_\lambda = \{(x, y) \in \pi : x^2 + xy + ey^2 = \lambda\}$, where $x^2 + x + e$ is irreducible.

Theorem: The ellipse $\mathcal{C}_\lambda$, $\lambda \notin \{0, 1\}$, is $\mathcal{C}_1$-good if and only if for all $a, b \in GF(q^2)$ such that $\frac{2a+b}{a^2+ab+eb^2} \in GF(q) \setminus \{-1, -2\}$, $\lambda \neq (a + 1)^2 + (a + 1)b + eb^2$.

At this point, more can be said if we look at the even and odd cases separately.

q odd vs. q even

Theorem: Let q be an odd prime power and let λ be an element of the subfield $GF(q)$ of $GF(q^2)$ such that $\sqrt{\lambda}$ lies in $GF(q^2) \setminus GF(q)$. Then, $\mathcal{C}_\lambda$ is $\mathcal{C}_1$-good. Letting λ be an element of the subfield $GF(q)$ of $GF(q^2)$ such that $\sqrt{\lambda}$ lies in $GF(q^2) \setminus GF(q)$, $\mathcal{C}_1 \cup \mathcal{C}_\lambda$ is a Baer-cap.

q odd vs. q even

Theorem: Let q be an odd prime power and let λ be an element of the subfield $GF(q)$ of $GF(q^2)$ such that $\sqrt{\lambda}$ lies in $GF(q^2) \setminus GF(q)$. Then, $\mathcal{C}_\lambda$ is $\mathcal{C}_1$-good. Letting λ be an element of the subfield $GF(q)$ of $GF(q^2)$ such that $\sqrt{\lambda}$ lies in $GF(q^2) \setminus GF(q)$, $\mathcal{C}_1 \cup \mathcal{C}_\lambda$ is a Baer-cap.

Theorem: Let q be an even prime power and suppose $\lambda^{q-1} = 1$ or $\lambda^{q+1} = 1$, with $\lambda \neq 1$. Then $\mathcal{C}_\lambda$ is $\mathcal{C}_1$-good. Letting $\lambda \neq 1$ satisfy either $\lambda^{q-1} = 1$ or $\lambda^{q+1} = 1$, $\mathcal{C}_1 \cup \mathcal{C}_\lambda$ is a Baer-cap. Moreover in the case where $\lambda^{q+1} = 1$, $\mathcal{C}_1 \cup \mathcal{C}_\lambda \cup \{(0,0)\}$ is a Baer-cap.

a special case

Let $q \equiv -1 \pmod 4$. Then, the set $\mathcal{C}_1 \cup \mathcal{C}_{-1}$ forms a pair of mutually good conics in $PG(2, q^2)$. Moreover, the group induced by matrices of the form

$$\phi_{a,b} = \begin{bmatrix} a+b & -b \\ eb & a \end{bmatrix}$$

with $a^2 + ab + eb^2 = \pm 1$ acts regularly on this set.

a special case

Let $q \equiv -1 \pmod 4$. Then, the set $\mathcal{C}_1 \cup \mathcal{C}_{-1}$ forms a pair of mutually good conics in $PG(2, q^2)$. Moreover, the group induced by matrices of the form

$$\phi_{a,b} = \begin{bmatrix} a+b & -b \\ eb & a \end{bmatrix}$$

with $a^2 + ab + eb^2 = \pm 1$ acts regularly on this set.

A transitive group acting on the conics will induce a transitive action on the lifted set of points in $AG(4, q)$. Therefore, the cap admits a transitive automorphism group.

mutually good parabolas

Now let $\mathcal{D}_\mu = \{(x, y) \in \pi : x = y^2 + \mu\}$ for all $\mu \in GF(q^2)$, for q an odd prime power.

mutually good parabolas

Now let $\mathcal{D}_\mu = \{(x, y) \in \pi : x = y^2 + \mu\}$ for all $\mu \in GF(q^2)$, for q an odd prime power.

Proposition: Let q be an odd prime power. The parabola $\mathcal{D}_\mu$ is $\mathcal{D}_0$-good if and only if μ is a nonsquare in $GF(q^2)$.

mutually good parabolas

Now let $\mathcal{D}_\mu = \{(x,y) \in \pi : x = y^2 + \mu\}$ for all $\mu \in GF(q^2)$, for q an odd prime power.

Proposition: Let q be an odd prime power. The parabola $\mathcal{D}_\mu$ is $\mathcal{D}_0$-good if and only if μ is a nonsquare in $GF(q^2)$.

It follows that $AG(4,q)$, q odd, has a cap of size $2q^2$ lifted from two mutually good parabolas of $AG(2,q^2)$.

Larger Baer caps

It is natural to ask whether or not one could possible piece together more than 2 mutually good conics and lift them to a cap in 4-dimensional space.

Larger Baer caps

It is natural to ask whether or not one could possible piece together more than 2 mutually good conics and lift them to a cap in 4-dimensional space.

Theorem: Let q be an odd power of 2, so that $q \equiv 2 \pmod 3$. Let $\lambda \neq 1$ be a cube root of unity in $GF(q^2)$. Then $\mathcal{C}_1 \cup \mathcal{C}_\lambda \cup \mathcal{C}_{\lambda^2}$ is a Baer-cap.

Larger Baer caps

It is natural to ask whether or not one could possible piece together more than 2 mutually good conics and lift them to a cap in 4-dimensional space.

Theorem: Let q be an odd power of 2, so that $q \equiv 2 \pmod 3$. Let $\lambda \neq 1$ be a cube root of unity in $GF(q^2)$. Then $\mathcal{C}_1 \cup \mathcal{C}_\lambda \cup \mathcal{C}_{\lambda^2}$ is a Baer-cap.

It is not hard to show that the point $(0, 0)$ can also be added to this Baer-cap to obtain a larger Baer-cap.

Larger Baer caps

It is natural to ask whether or not one could possible piece together more than 2 mutually good conics and lift them to a cap in 4-dimensional space.

Theorem: Let q be an odd power of 2, so that $q \equiv 2 \pmod 3$. Let $\lambda \neq 1$ be a cube root of unity in $GF(q^2)$. Then $\mathcal{C}_1 \cup \mathcal{C}_\lambda \cup \mathcal{C}_{\lambda^2}$ is a Baer-cap.

It is not hard to show that the point $(0, 0)$ can also be added to this Baer-cap to obtain a larger Baer-cap.

The caps obtained here are almost certainly identical to the caps discovered by Edel and Bierbrauer, though their construction originated from a coding-theoretic perspective.

References

J. M. Dover and K. E. Mellinger. Semiovals from unions of conics. *Innov. Incidence Geom.*, to appear.

K. Scott. *Anti-blocking Sets.* UMW Honors Thesis, May 2012.

J. M. Dover, K. E. Mellinger, and K. L. Wantz, Generalized Pellegrino caps. *submitted.*

Conclusions

Questions?