Blocking Semiovals and their Applications in Cryptography

Keith E. Mellinger
University of Mary Washington

(joint work with Dr. Jeremy Dover)

June 2013

Introduction

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

Introduction

$PG(2, q)$ 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

$PG(2, q)$ 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

$PG(2, q)$ 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

what is this talk about?

Finite geometry has played a major role in many areas of discrete mathematics.

what is this talk about?

Finite geometry has played a major role in many areas of discrete mathematics.

In particular, the techniques of finite geometry can be used to construct robust examples of powerful linear codes, non-linear codes, and ciphers.

what is this talk about?

Finite geometry has played a major role in many areas of discrete mathematics.

In particular, the techniques of finite geometry can be used to construct robust examples of powerful linear codes, non-linear codes, and ciphers.

My goal is to:

what is this talk about?

Finite geometry has played a major role in many areas of discrete mathematics.

In particular, the techniques of finite geometry can be used to construct robust examples of powerful linear codes, non-linear codes, and ciphers.

My goal is to:

1. Introduce you to a not-so-well-known cryptographic protocol

what is this talk about?

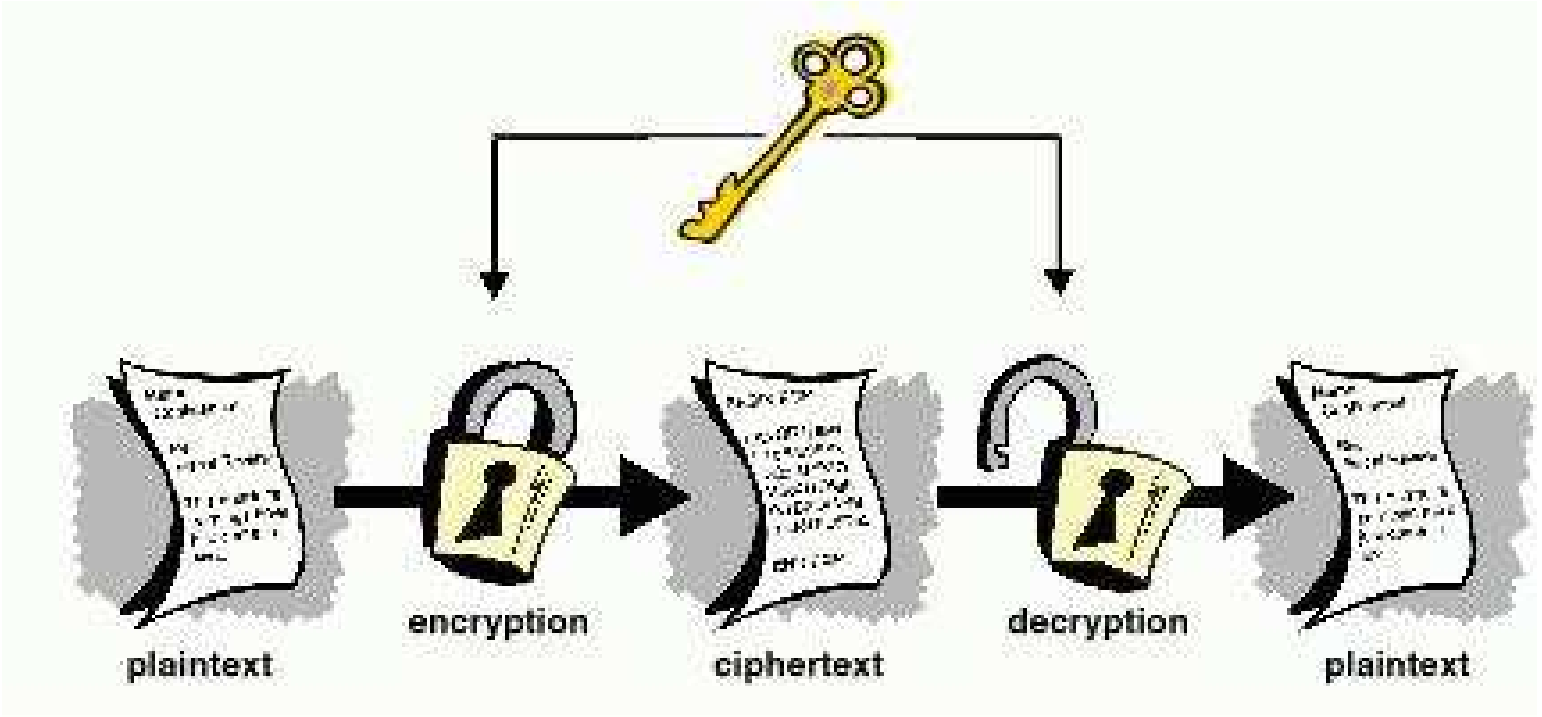
Finite geometry has played a major role in many areas of discrete mathematics.

In particular, the techniques of finite geometry can be used to construct robust examples of powerful linear codes, non-linear codes, and ciphers.

My goal is to:

1. Introduce you to a not-so-well-known cryptographic protocol
2. Describe my work in finite geometry that's related

Cryptography



from points/lines to matrices

$$\begin{array}{c} \\ l_1 \\ l_2 \\ l_3 \\ \vdots \\ l_n \end{array} \begin{array}{c} \begin{array}{ccccc} P_1 & P_2 & P_3 & \dots & P_n \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & \dots & 1 \\ 0 & 1 & 0 & \dots & 1 \\ 1 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & 1 & \dots & 0 \end{pmatrix} \end{array}$$

ciphertexts as vectors

A cryptographic protocol...

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

ciphertexts as vectors

A cryptographic protocol...

$$\left[\begin{array}{cccc|cccccc} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right]$$

ciphertexts as vectors

A cryptographic protocol...

$$\left[\begin{array}{cccc|cccccc}
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0
\end{array}\right]$$

ciphertexts as vectors

A cryptographic protocol...

$$\left[\begin{array}{cccc|cccccc} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right]$$

determining sets

We say a set $\mathcal{S}$ is a *determining set* if every line intersects $\mathcal{S}$ in a different pattern.

determining sets

We say a set $\mathcal{S}$ is a *determining set* if every line intersects $\mathcal{S}$ in a different pattern.

In finite projective planes, two points uniquely determine a line.

determining sets

We say a set $\mathcal{S}$ is a *determining set* if every line intersects $\mathcal{S}$ in a different pattern.

In finite projective planes, two points uniquely determine a line. So, if a line meets our set in two points, it is uniquely determined.

determining sets

We say a set $\mathcal{S}$ is a *determining set* if every line intersects $\mathcal{S}$ in a different pattern.

In finite projective planes, two points uniquely determine a line. So, if a line meets our set in two points, it is uniquely determined.

However, we must avoid passant lines (lines not meeting our set at all), and..

determining sets

We say a set $\mathcal{S}$ is a *determining set* if every line intersects $\mathcal{S}$ in a different pattern.

In finite projective planes, two points uniquely determine a line. So, if a line meets our set in two points, it is uniquely determined.

However, we must avoid passant lines (lines not meeting our set at all), and.. multiple tangent lines.

determining sets

We say a set $\mathcal{S}$ is a *determining set* if every line intersects $\mathcal{S}$ in a different pattern.

In finite projective planes, two points uniquely determine a line. So, if a line meets our set in two points, it is uniquely determined.

However, we must avoid passant lines (lines not meeting our set at all), and.. multiple tangent lines.

That is, any particular point of a determining set $\mathcal{S}$ can have at most one tangent line through it.

tools and keys

The cryptographic protocol... start with the following:

tools and keys

The cryptographic protocol... start with the following:

1. a finite projective plane π along with its incidence matrix M

tools and keys

The cryptographic protocol... start with the following:

1. a finite projective plane π along with its incidence matrix M
2. a determining set B in π

tools and keys

The cryptographic protocol... start with the following:

1. a finite projective plane π along with its incidence matrix M
2. a determining set B in π
3. a cipher ρ that acts on the columns of M_B (the columns corresponding to points of B)

tools and keys

The cryptographic protocol... start with the following:

1. a finite projective plane π along with its incidence matrix M
2. a determining set B in π
3. a cipher ρ that acts on the columns of M_B (the columns corresponding to points of B)
4. a cipher σ that acts on the columns of $M_{\pi \setminus B}$ (the columns *not* corresponding to points of B)

the keys

As with many cryptosystems, part of our key is public and part is private. Suppose Alice is sending a message to Bob.

the keys

As with many cryptosystems, part of our key is public and part is private. Suppose Alice is sending a message to Bob.

The incidence matrix is public – anybody can know it.

the keys

As with many cryptosystems, part of our key is public and part is private. Suppose Alice is sending a message to Bob.

The incidence matrix is public – anybody can know it.

The determining set B and the cipher on it, ρ, are known to both Alice and Bob

the keys

As with many cryptosystems, part of our key is public and part is private. Suppose Alice is sending a message to Bob.

The incidence matrix is public – anybody can know it.

The determining set B and the cipher on it, ρ, are known to both Alice and Bob

The cipher σ is private (known only to Alice)

encryption

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

encryption

$$\left[\begin{array}{cccc|cccccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right]$$

encryption

$$\left[\begin{array}{cccc|cccccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right]$$

encryption

$$\left[\begin{array}{cccc|cccccc} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

decryption

$$\left[\begin{array}{cccc|cccccc} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

decryption

$$\left[\begin{array}{cccc|cccccc} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

Suppose Bob receives this.

decryption

$$\left[\begin{array}{cccc|cccc} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

Suppose Bob receives this.

Bob knows which entries correspond to the points of the determining set (the green ones above), and he knows the private cipher on those entries. So, he can decrypt them.

decryption

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

Suppose Bob receives this.

Bob knows which entries correspond to the points of the determining set (the green ones above), and he knows the private cipher on those entries. So, he can decrypt them.

decryption

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

Suppose Bob receives this.

Bob knows which entries correspond to the points of the determining set (the green ones above), and he knows the private cipher on those entries. So, he can decrypt them.

But now these entries *uniquely* determine a row of the incidence matrix.

decryption

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right]$$

Suppose Bob receives this.

Bob knows which entries correspond to the points of the determining set (the green ones above), and he knows the private cipher on those entries. So, he can decrypt them.

But now these entries *uniquely* determine a row of the incidence matrix.

semiovals

We wish to construct examples of determining sets. Let's use $\mathcal{S}$ for our set.

semiovals

We wish to construct examples of determining sets. Let's use $\mathcal{S}$ for our set.

If a line meets $\mathcal{S}$ in the single point P, then there can't be any other line meeting $\mathcal{S}$ precisely in the point P.

semiovals

We wish to construct examples of determining sets. Let's use $\mathcal{S}$ for our set.

If a line meets $\mathcal{S}$ in the single point P, then there can't be any other line meeting $\mathcal{S}$ precisely in the point P.

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

We wish to construct examples of determining sets. Let's use $\mathcal{S}$ for our set.

If a line meets $\mathcal{S}$ in the single point P, then there can't be any other line meeting $\mathcal{S}$ precisely in the point P.

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

blocking sets

Recall, also, that every line of π needs to intersect $\mathcal{S}$ (so that it can be "determined").

blocking sets

Recall, also, that every line of π needs to intersect $\mathcal{S}$ (so that it can be "determined").

We say the set $\mathcal{S}$ is a *blocking set* if every line of π meets $\mathcal{S}$ non-trivially. Typically, we also require no line of π to be completely contained in $\mathcal{S}$.

blocking sets

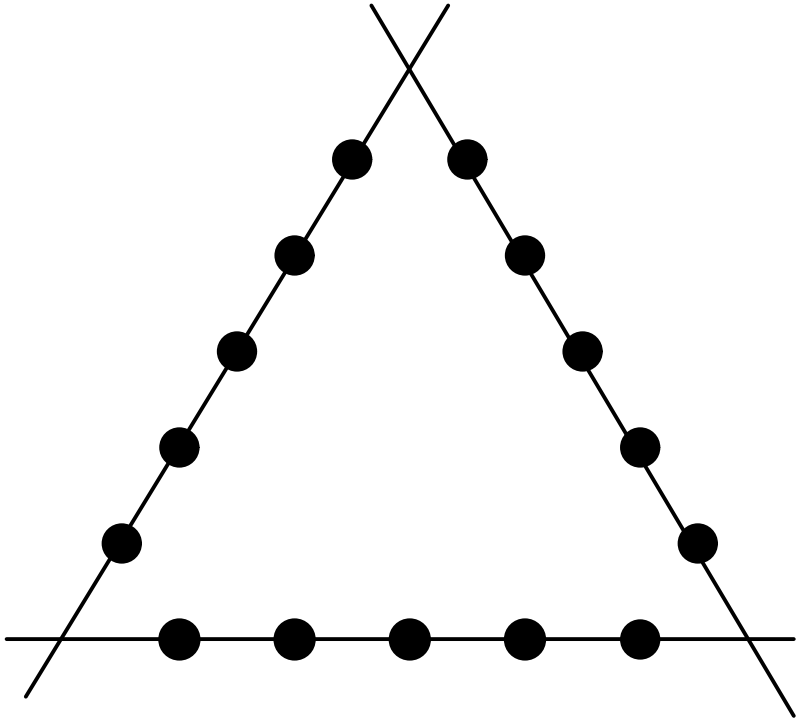
Recall, also, that every line of π needs to intersect $\mathcal{S}$ (so that it can be "determined").

We say the set $\mathcal{S}$ is a *blocking set* if every line of π meets $\mathcal{S}$ non-trivially. Typically, we also require no line of π to be completely contained in $\mathcal{S}$.

Naturally, a *blocking semioval* is a set that is both a blocking set *and* a semioval.

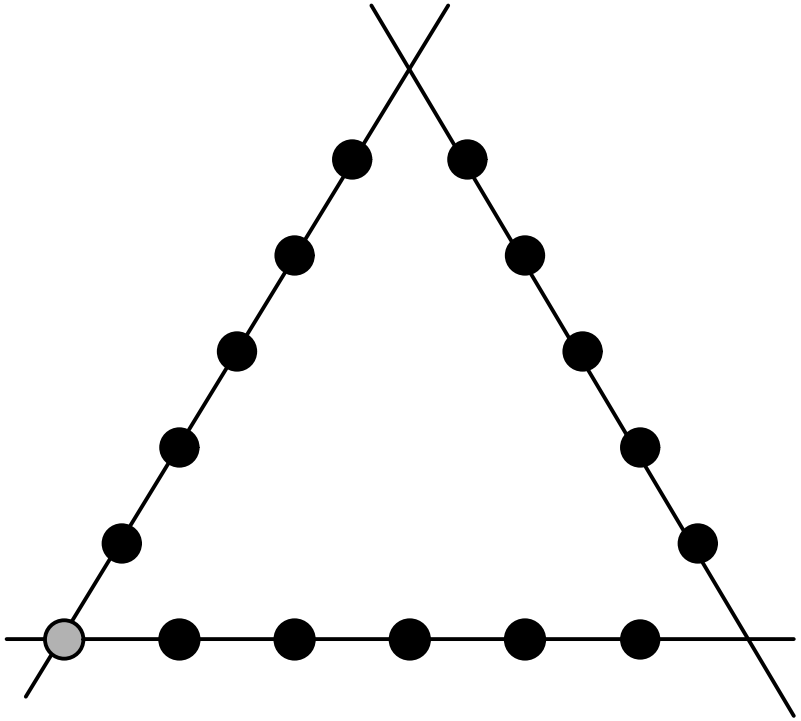
vertex-less triangle

Classic example: *the vertex-less triangle*



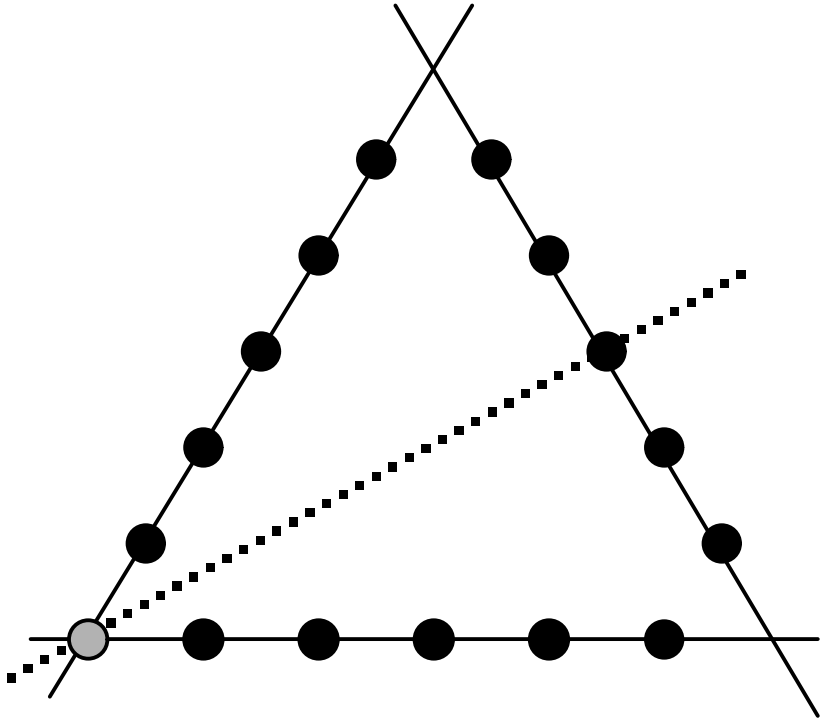
vertex-less triangle

Classic example: *the vertex-less triangle*



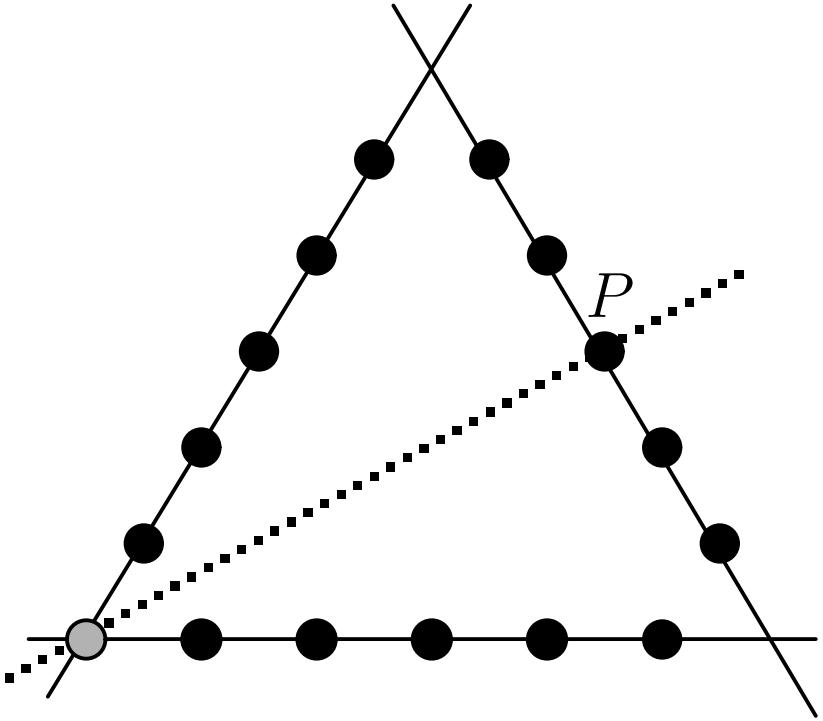
vertex-less triangle

Classic example: *the vertex-less triangle*



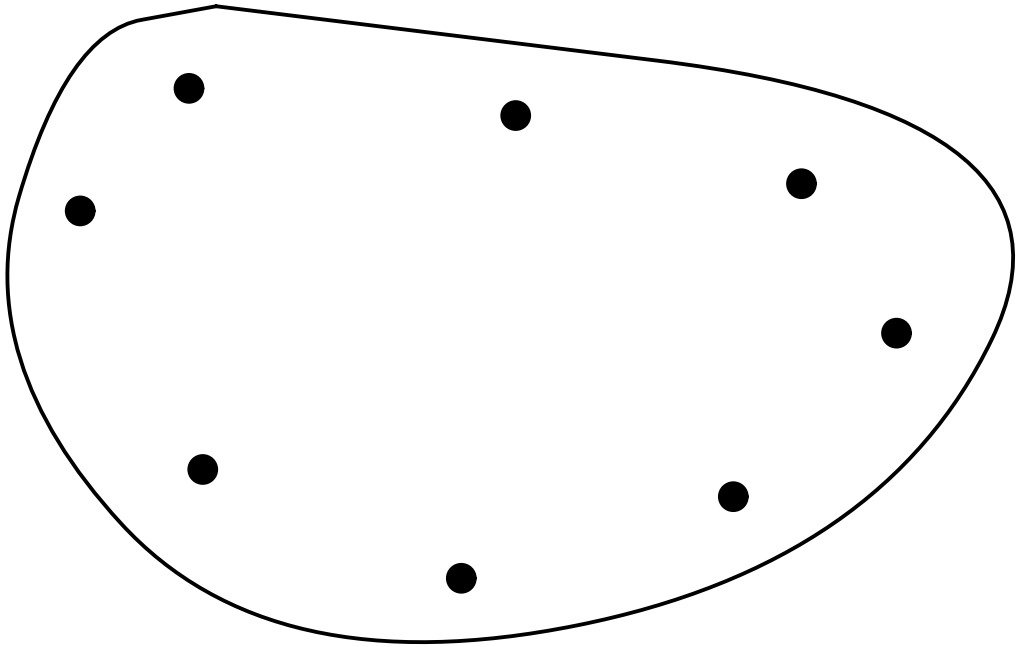
vertex-less triangle

Classic example: *the vertex-less triangle*



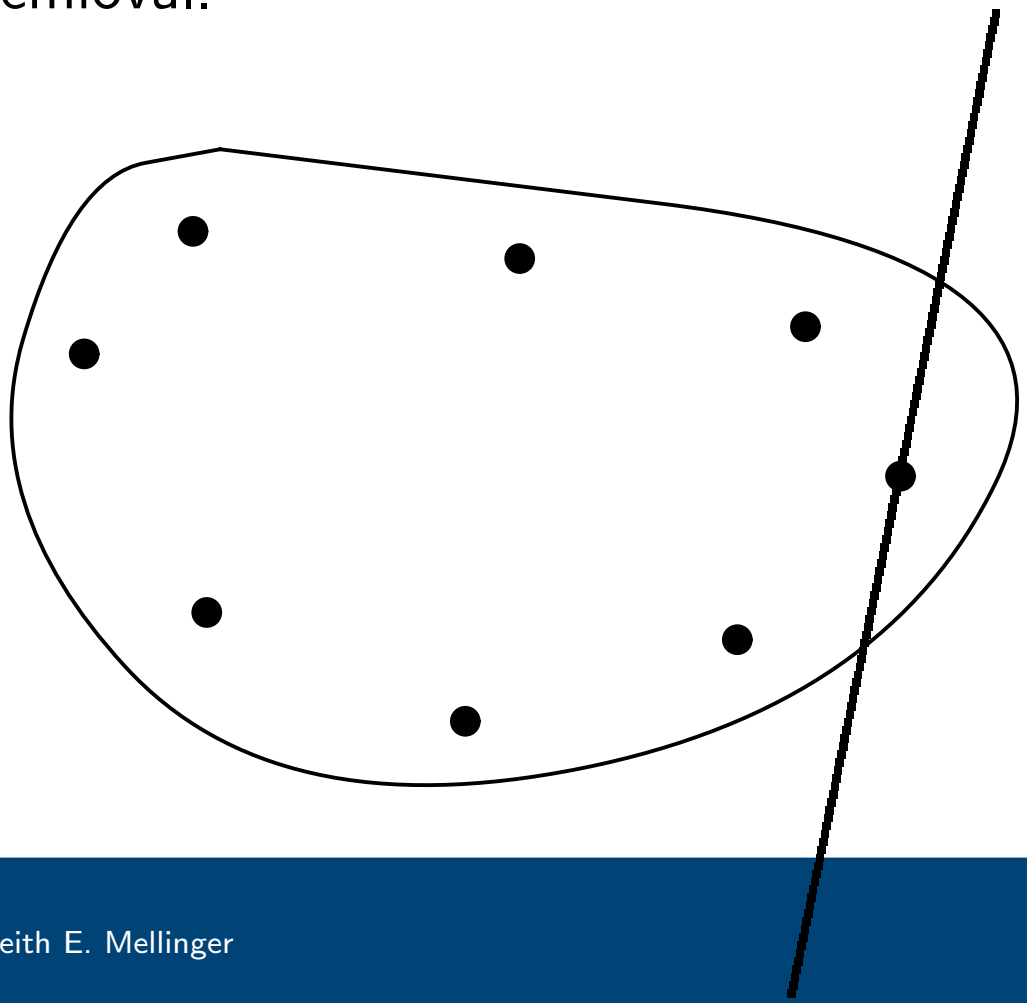
extremal in two ways

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.



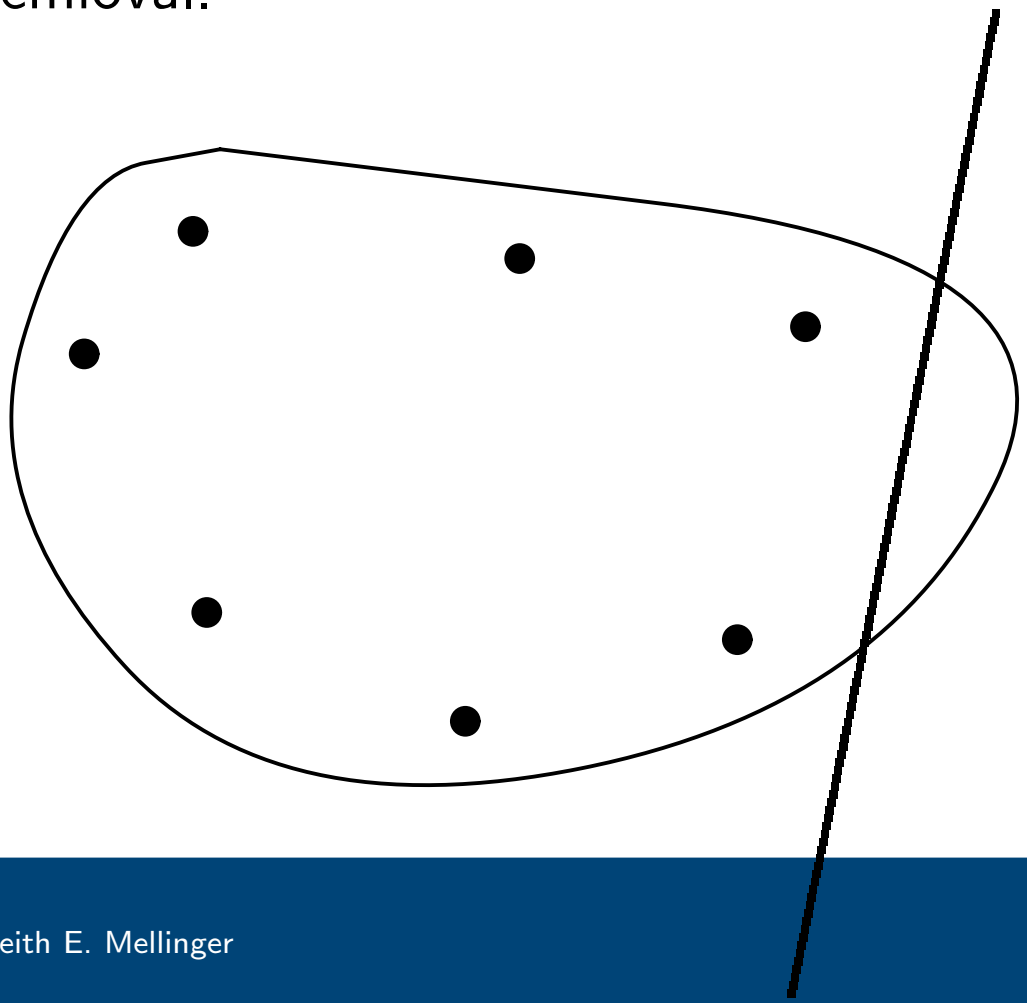
extremal in two ways

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.



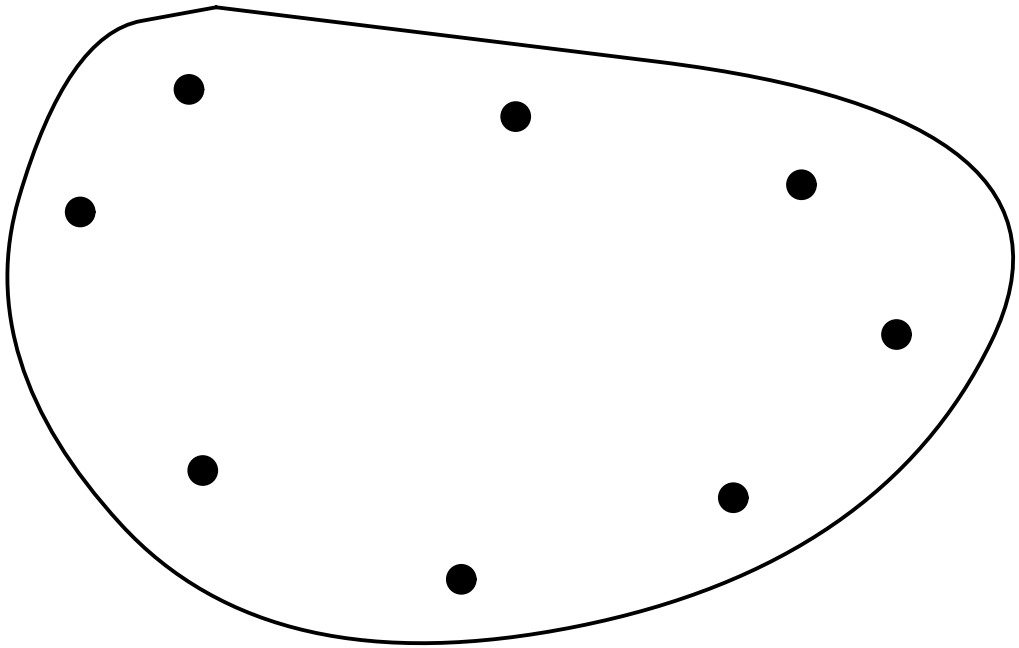
extremal in two ways

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.



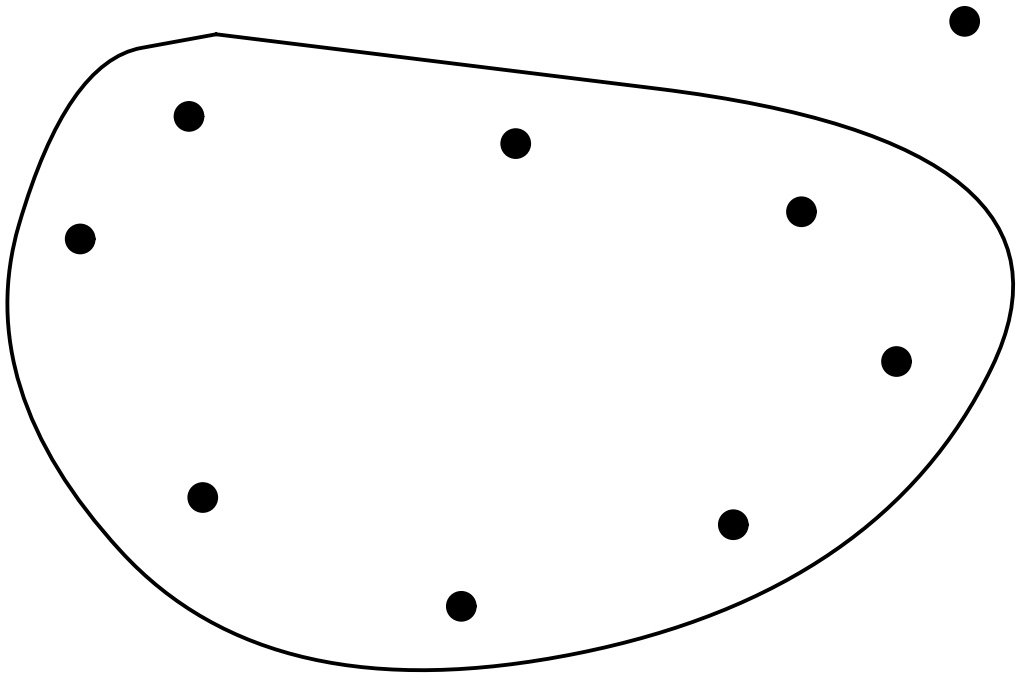
extremal in two ways

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



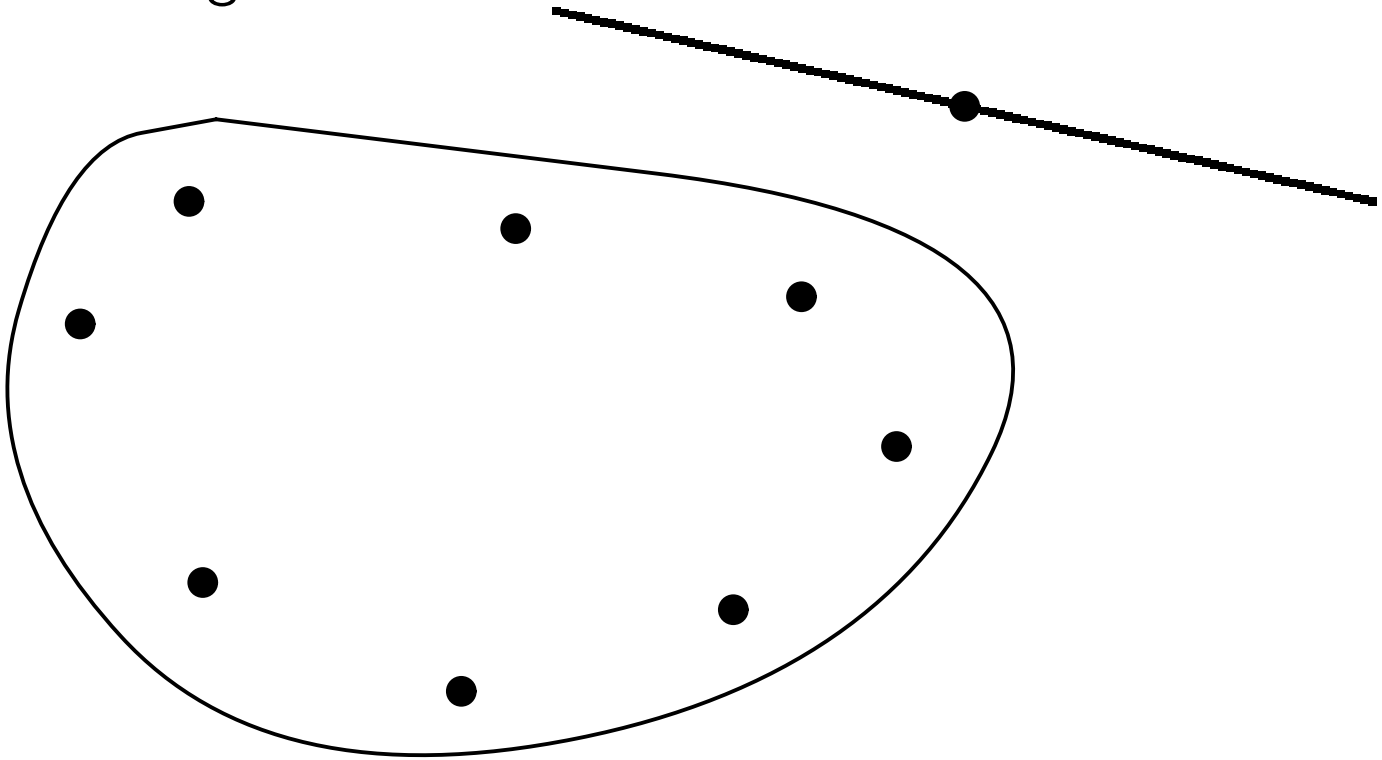
extremal in two ways

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



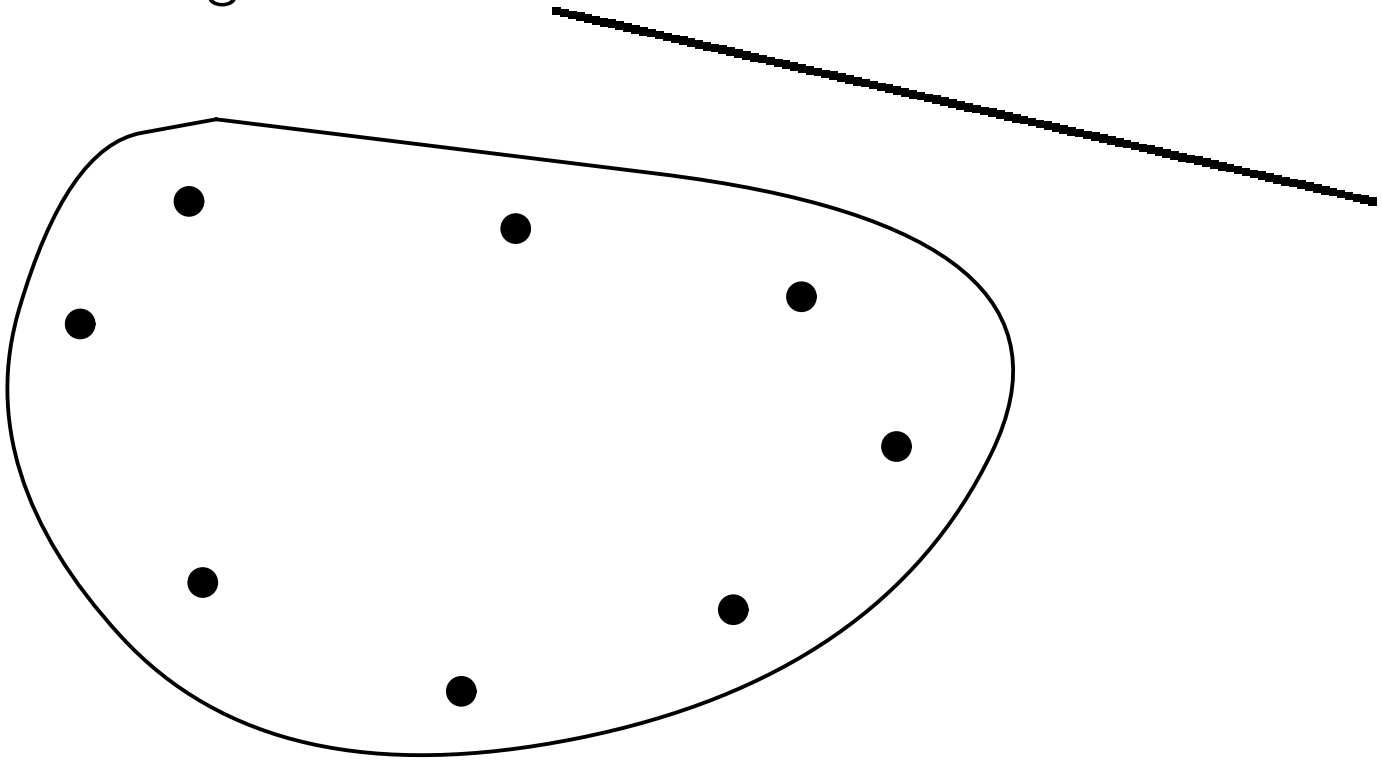
extremal in two ways

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

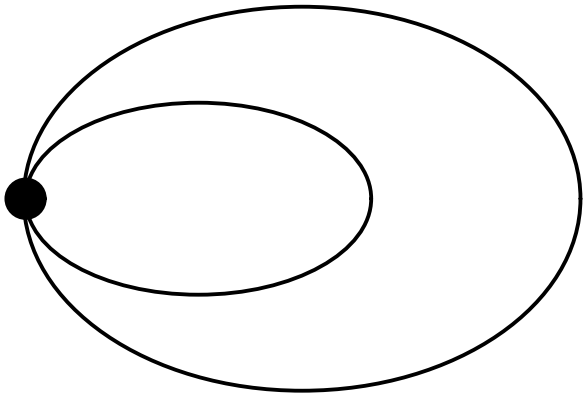


extremal in two ways

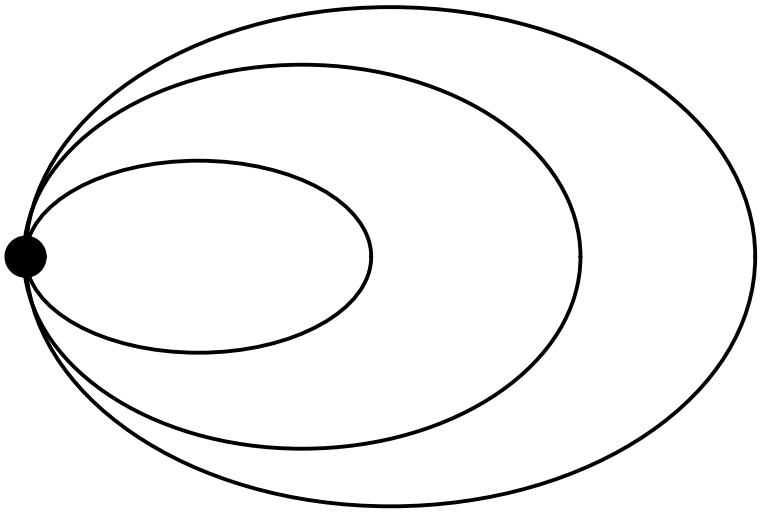
Second, you can't add another point to your set and still have a blocking semioval.



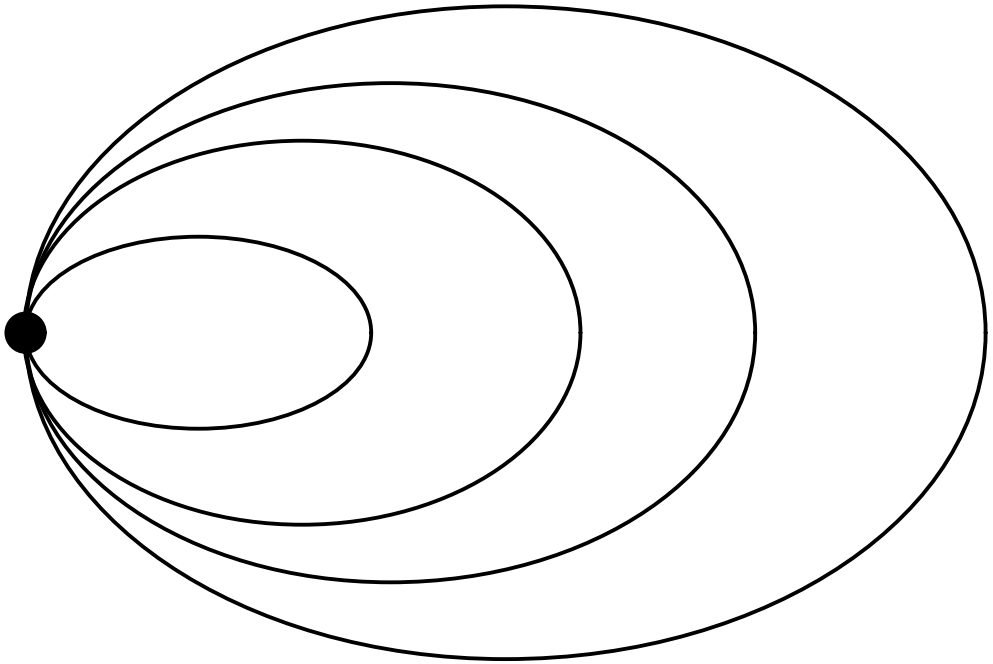
tangent pencil



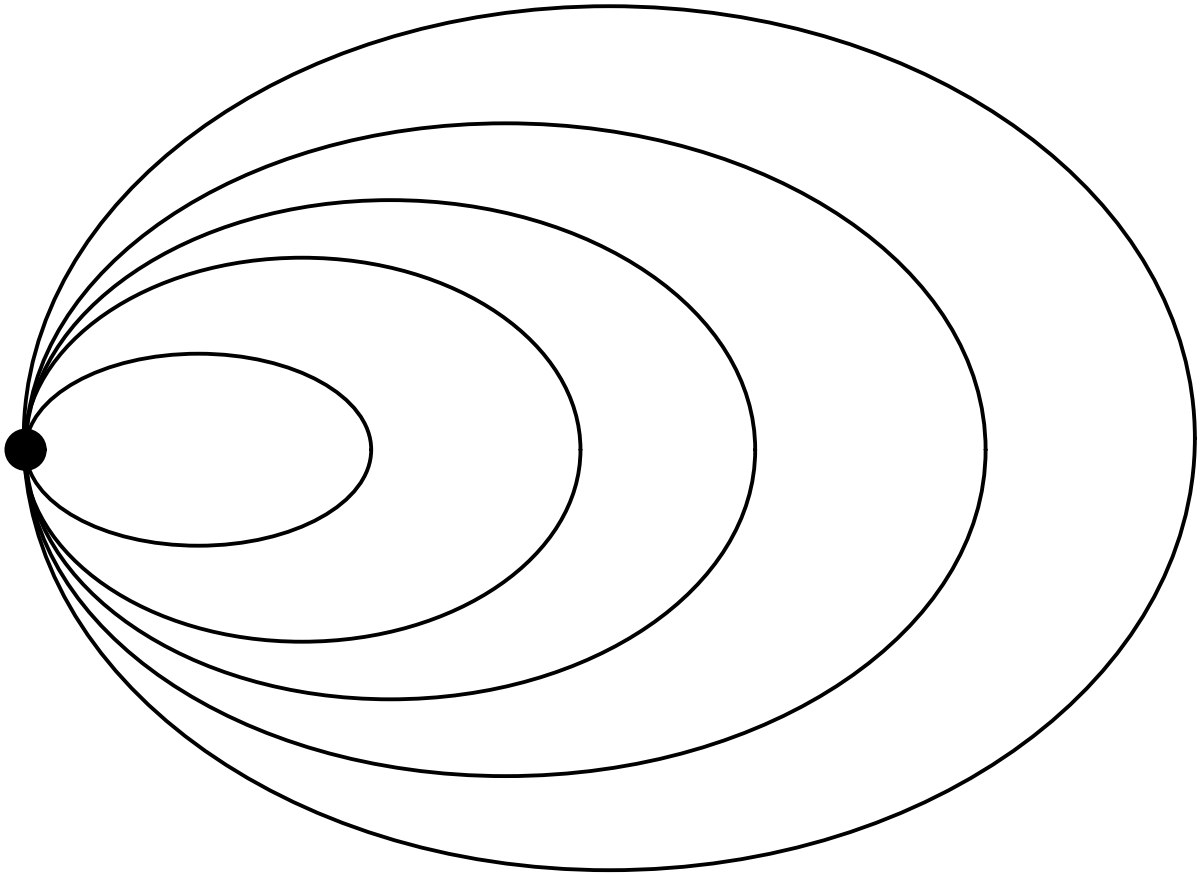
tangent pencil



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 $x^2 - yz + kz^2 = 0$.

Szőnyi shows that one can select certain conics from this algebraic pencil whose union is a blocking set (he was looking at constructing *blocking sets*).

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 unique 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 $z^2 = 0$

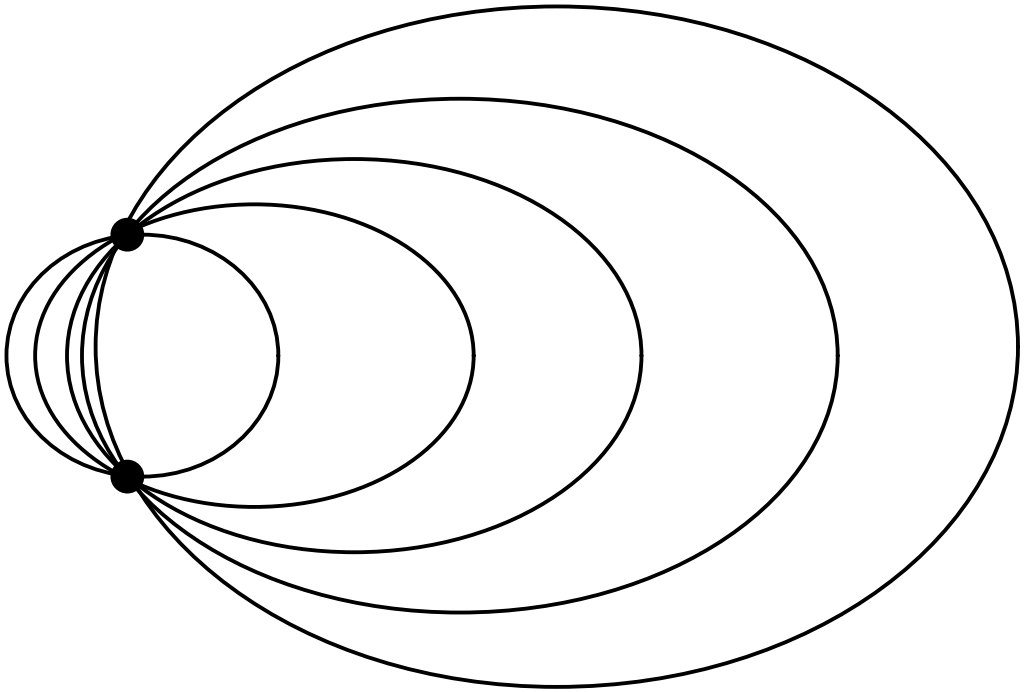
Then, the conics in the pencil are defined by the linear combinations of these: $\mathcal{C}_k$ is defined by $x^2 - yz + kz^2 = 0$.

Szőnyi shows that one can select certain conics from this algebraic pencil whose union is a blocking set (he was looking at constructing *blocking sets*).

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 unique tangent lines at each of the points.

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

other pencils



semiovals from unions of conics

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.

semiovals from unions of conics

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.

BSOs containing conics

The first construction we found relies on another object called a *unital*. Unitals can be described (and defined) synthetically. But in finite projective planes, a large class of them also has a nice algebraic description using cubic curves.

BSOs containing conics

The first construction we found relies on another object called a *unital*. Unitals can be described (and defined) synthetically. But in finite projective planes, a large class of them also has a nice algebraic description using cubic curves.

Theorem: In $\pi = PG(2, q^2)$, q odd, suppose $\mathcal{U}$ is a unital and $\mathcal{C}$ is a conic with commuting polarities μ and σ, respectively. $\mathcal{S} = \mathcal{C} \cup (\mathrm{Int}(\mathcal{C}) \cap \mathcal{U})$ is a blocking semioval in π.

BSOs containing conics

Our other construction relies on pencils again, but is considerable more complex. This was discovered through computer search, and then generalized. In the article, we give a specific example of field elements satisfying the condition.

BSOs containing conics

Our other construction relies on pencils again, but is considerable more complex. This was discovered through computer search, and then generalized. In the article, we give a specific example of field elements satisfying the condition.

Theorem: Suppose $q \equiv 1 \pmod 4$, and let $A \subset GF(q)^*$ be a maximal subset of nonzero squares whose pairwise differences are nonsquares. Moreover suppose there exists no $d \in \not\square$ such that $k - d \in \square$ for all $k \in A$. Then $\mathcal{S} = \bigcup_{k \in A} \mathcal{C}_k \cup \{(1, a, 0) : a \in \not\square\}$ is a blocking semioval.

Conclusions

- ✔ with Jeremy Dover and Kenneth Wantz, Blocking semiovals containing conics, *Adv. Geom.* **13**: 1 (January 2013) 29-40.
- ✔ with Jeremy Dover, Semiovals from unions of conics, *Innov. Incidence Geom.*, **12** (2011) 61-83.

Conclusions

- ✔ with Jeremy Dover and Kenneth Wantz, Blocking semiovals containing conics, *Adv. Geom.* **13**: 1 (January 2013) 29-40.
- ✔ with Jeremy Dover, Semiovals from unions of conics, *Innov. Incidence Geom.*, **12** (2011) 61-83.

Thanks!

Conclusions

- ✔ with Jeremy Dover and Kenneth Wantz, Blocking semiovals containing conics, *Adv. Geom.* **13**: 1 (January 2013) 29-40.
- ✔ with Jeremy Dover, Semiovals from unions of conics, *Innov. Incidence Geom.*, **12** (2011) 61-83.

Thanks!

Questions?