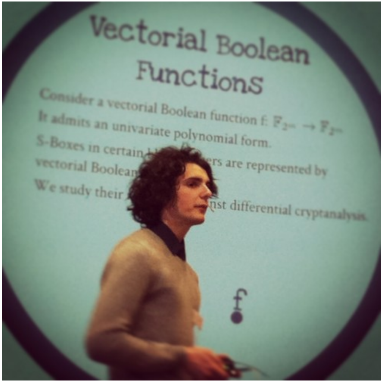
Hyperovals in $\mathbb{P}^2(\mathbb{F}_q)$

Kai-Uwe Schmidt

Department of Mathematics
Paderborn University
Germany



Florian Caullery

Federal University of Santa Catarina

Florianapolis, Brazil

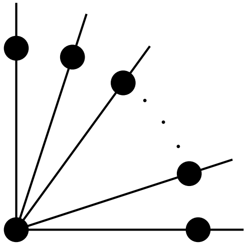
Arcs and hyperovals

An arc in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of points no three of which are collinear.

Arcs and hyperovals

An arc in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of points no three of which are collinear.

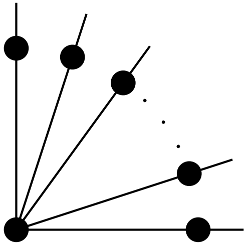
An arc contains at most $q+2$ points:



Arcs and hyperovals

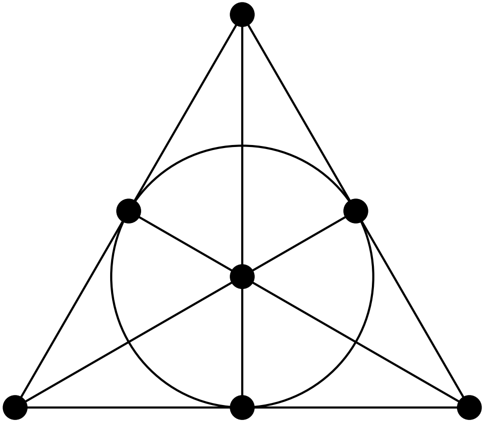
An arc in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of points no three of which are collinear.

An arc contains at most $q+2$ points:

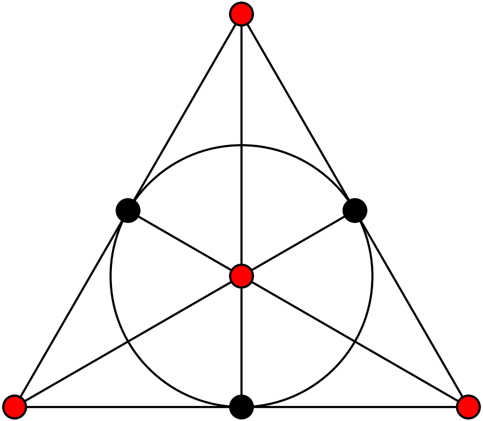


In case of equality, the arc is a called a hyperoval.

A hyperoval in the Fano plane



A hyperoval in the Fano plane



Which planes contain hyperovals?

Let H be a hyperoval in $\mathbb{P}^2(\mathbb{F}_q)$.

Which planes contain hyperovals?

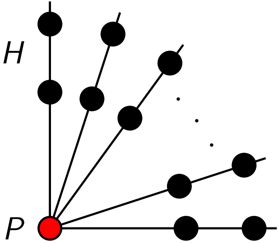
Let H be a hyperoval in $\mathbb{P}^2(\mathbb{F}_q)$.

- Each line meets H in 0 or 2 points.

Which planes contain hyperovals?

Let H be a hyperoval in $\mathbb{P}^2(\mathbb{F}_q)$.

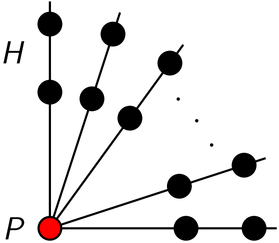
- Each line meets H in 0 or 2 points.
- A point P not in H meets H in $(q+2)/2$ lines.



Which planes contain hyperovals?

Let H be a hyperoval in $\mathbb{P}^2(\mathbb{F}_q)$.

- Each line meets H in 0 or 2 points.
- A point P not in H meets H in $(q+2)/2$ lines.

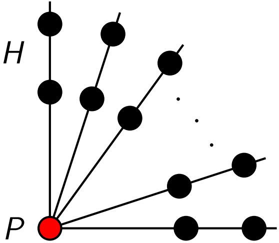


Hence q must be even.

Which planes contain hyperovals?

Let H be a hyperoval in $\mathbb{P}^2(\mathbb{F}_q)$.

- Each line meets H in 0 or 2 points.
- A point P not in H meets H in $(q+2)/2$ lines.



Hence q must be even.

An arc of size $q+1$ is called an oval.

Existence of ovals and hyperovals

All conics are ovals:

For every nongenerate quadratic form Q in $\mathbb{F}_q[x, y, z]$, the projective curve defined by Q gives an oval in $\mathbb{P}^2(\mathbb{F}_q)$.

Existence of ovals and hyperovals

All conics are ovals:

For every nongenerate quadratic form Q in $\mathbb{F}_q[x, y, z]$, the projective curve defined by Q gives an oval in $\mathbb{P}^2(\mathbb{F}_q)$.

Ovals give (unique) hyperovals:

In even characteristic, all tangents of an oval meet in a single point, which can be included to give a hyperoval.

Existence of ovals and hyperovals

All conics are ovals:

For every nongenerate quadratic form Q in $\mathbb{F}_q[x, y, z]$, the projective curve defined by Q gives an oval in $\mathbb{P}^2(\mathbb{F}_q)$.

Ovals give (unique) hyperovals:

In even characteristic, all tangents of an oval meet in a single point, which can be included to give a hyperoval.

Do all ovals come from conics?

Existence of ovals and hyperovals

All conics are ovals:

For every nongenerate quadratic form Q in $\mathbb{F}_q[x, y, z]$, the projective curve defined by Q gives an oval in $\mathbb{P}^2(\mathbb{F}_q)$.

Ovals give (unique) hyperovals:

In even characteristic, all tangents of an oval meet in a single point, which can be included to give a hyperoval.

Do all ovals come from conics?

Yes in odd characteristic. (Segre 1955)

Existence of ovals and hyperovals

All conics are ovals:

For every nongenerate quadratic form Q in $\mathbb{F}_q[x, y, z]$, the projective curve defined by Q gives an oval in $\mathbb{P}^2(\mathbb{F}_q)$.

Ovals give (unique) hyperovals:

In even characteristic, all tangents of an oval meet in a single point, which can be included to give a hyperoval.

Do all ovals come from conics?

Yes in odd characteristic. (Segre 1955)
Not in even characteristic.

Classification of hyperovals

One of the most confounding and fundamental open problems in finite geometry is the question of classifying the hyperovals of the Desarguesian projective planes.

— John Bamberg, on http://symomega.wordpress.com, 2011

Classification of hyperovals

One of the most confounding and fundamental open problems in finite geometry is the question of classifying the hyperovals of the Desarguesian projective planes.

— John Bamberg, on http://symomega.wordpress.com, 2011

[the classification of hyperovals] remains the chief problem in the area. Open since 1955, it is considered to be a very difficult problem. We believe that this might possibly be accomplished within the next ten years.

— Bill Cherowitzo's hyperoval page, last updated 2004

Classification of hyperovals

One of the most confounding and fundamental open problems in finite geometry is the question of classifying the hyperovals of the Desarguesian projective planes.

— John Bamberg, on http://symomega.wordpress.com, 2011

[the classification of hyperovals] remains the chief problem in the area. Open since 1955, it is considered to be a very difficult problem. We believe that this might possibly be accomplished within the next ten years.

— Bill Cherowitzo's hyperoval page, last updated 2004

I know no-one of significance who shared his confidence in classifying hyperovals in the near future.

— Tim Penttila on http://symomega.wordpress.com, 2012

Coordinisation

- Wlog: every hyperoval contains the quadrangle

$$(1:0:0),\ (0:1:0),\ (0:0:1),\ (1:1:1).$$

Coordinisation

- Wlog: every hyperoval contains the quadrangle

$$(1:0:0),\ (0:1:0),\ (0:0:1),\ (1:1:1).$$

- Thus a hyperoval in $\mathbb{P}^2(\mathbb{F}_q)$ consists of $(1:0:0)$ and $(0:1:0)$ and q affine points $(a:b:1)$ that differ in two coordinates.

Coordinisation

- Wlog: every hyperoval contains the quadrangle

$$(1:0:0),\ (0:1:0),\ (0:0:1),\ (1:1:1).$$

- Thus a hyperoval in $\mathbb{P}^2(\mathbb{F}_q)$ consists of $(1:0:0)$ and $(0:1:0)$ and q affine points $(a:b:1)$ that differ in two coordinates.

- The unique hyperoval in $\mathbb{P}^2(\mathbb{F}_4)$:

$$(1:0:0), (0:1:0),$$

$$(0:0:1), (1:1:1), (\alpha:\alpha^2:1), (\alpha^2:\alpha:1).$$

Hyperovals and o-polynomials

For $q > 2$, a set of $q+2$ points in $\mathbb{P}(\mathbb{F}_q)$ is a hyperoval if and only if it can be written as

$$\big\{(1:0:0),(0:1:0)\big\} \cup \big\{(f(c):c:1) : c \in \mathbb{F}_q\big\},$$

where f is an o-polynomial of $\mathbb{F}_q$.

Hyperovals and o-polynomials

For $q > 2$, a set of $q + 2$ points in $\mathbb{P}(\mathbb{F}_q)$ is a hyperoval if and only if it can be written as

$$\{(1:0:0),(0:1:0)\} \cup \{(f(c):c:1) : c \in \mathbb{F}_q\},$$

where f is an o-polynomial of $\mathbb{F}_q$.

A polynomial $f \in \mathbb{F}_q[x]$ of degree at most $q-1$ satisfying:

Hyperovals and o-polynomials

For $q > 2$, a set of $q+2$ points in $\mathbb{P}(\mathbb{F}_q)$ is a hyperoval if and only if it can be written as

$$\big\{(1:0:0),(0:1:0)\big\} \cup \big\{(f(c):c:1) : c \in \mathbb{F}_q\big\},$$

where f is an o-polynomial of $\mathbb{F}_q$.

A polynomial $f \in \mathbb{F}_q[x]$ of degree at most $q-1$ satisfying:

- $f(0) = 0$ and $f(1) = 1$,

Hyperovals and o-polynomials

For $q > 2$, a set of $q+2$ points in $\mathbb{P}(\mathbb{F}_q)$ is a hyperoval if and only if it can be written as

$$\big\{(1:0:0),(0:1:0)\big\} \cup \big\{(f(c):c:1) : c \in \mathbb{F}_q\big\},$$

where f is an o-polynomial of $\mathbb{F}_q$.

A polynomial $f \in \mathbb{F}_q[x]$ of degree at most $q-1$ satisfying:

- $f(0) = 0$ and $f(1) = 1$,
- f induces a permutation of $\mathbb{F}_q$,

Hyperovals and o-polynomials

For $q > 2$, a set of $q+2$ points in $\mathbb{P}(\mathbb{F}_q)$ is a hyperoval if and only if it can be written as

$$\big\{(1:0:0),(0:1:0)\big\} \cup \big\{(f(c):c:1) : c \in \mathbb{F}_q\big\},$$

where f is an o-polynomial of $\mathbb{F}_q$.

A polynomial $f \in \mathbb{F}_q[x]$ of degree at most $q-1$ satisfying:

- $f(0) = 0$ and $f(1) = 1$,
- f induces a permutation of $\mathbb{F}_q$,
- $\det \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ f(a) & f(b) & f(c) \end{pmatrix} \neq 0 \quad$ for all distinct $a, b, c \in \mathbb{F}_q$.

Alternative definitions

The determinant condition can be replaced by one of the following conditions:

Alternative definitions

The determinant condition can be replaced by one of the following conditions:

- For each $a \in \mathbb{F}_q$, the mapping

$$x \mapsto \frac{f(x+a)+f(a)}{x}$$

  is a permutation on $\mathbb{F}_q$ fixing 0 (Segre 1962).

Alternative definitions

The determinant condition can be replaced by one of the following conditions:

- For each $a \in \mathbb{F}_q$, the mapping

  $$x \mapsto \frac{f(x+a)+f(a)}{x}$$

  is a permutation on $\mathbb{F}_q$ fixing 0 (Segre 1962).

- For each $a \in \mathbb{F}_q^*$, the mapping

  $$x \mapsto f(x) + ax$$

  is 2-to-1 on $\mathbb{F}_q$ (Carlet-Mesnager 2011).

Known o-polynomials of $\mathbb{F}_{2^h}$

- x^2 (these give conics)

Known o-polynomials of $\mathbb{F}_{2^h}$

- x^2 (these give conics)
- x^{2^k} (Segre 1962)

Known o-polynomials of $\mathbb{F}_{2^h}$

- x^2 (these give conics)
- x^{2^k} (Segre 1962)
- x^6 (Segre-Bartocci 1971)

Known o-polynomials of $\mathbb{F}_{2^h}$

- x^2 (these give conics)
- x^{2^k} (Segre 1962)
- x^6 (Segre-Bartocci 1971)
- $x^{\sigma+\gamma}$ and $x^{3\sigma+4}$ (Glynn 1983)

$$\sigma = 2^{(h+1)/2} \qquad \gamma = \begin{cases} 2^{(3h+1)/4} & \text{for } h \equiv 1 \pmod 4 \\ 2^{(h+1)/4} & \text{for } h \equiv 3 \pmod 4 \end{cases}$$

Known o-polynomials of $\mathbb{F}_{2^h}$

- x^2 (these give conics)
- x^{2^k} (Segre 1962)
- x^6 (Segre-Bartocci 1971)
- $x^{\sigma+\gamma}$ and $x^{3\sigma+4}$ (Glynn 1983)
- $x^{1/6} + x^{1/2} + x^{5/6}$ (Payne 1985)

$$\sigma = 2^{(h+1)/2} \qquad \gamma = \begin{cases} 2^{(3h+1)/4} & \text{for } h \equiv 1 \pmod 4 \\ 2^{(h+1)/4} & \text{for } h \equiv 3 \pmod 4 \end{cases}$$

Known o-polynomials of $\mathbb{F}_{2^h}$

- x^2 (these give conics)
- x^{2^k} (Segre 1962)
- x^6 (Segre-Bartocci 1971)
- $x^{\sigma+\gamma}$ and $x^{3\sigma+4}$ (Glynn 1983)
- $x^{1/6} + x^{1/2} + x^{5/6}$ (Payne 1985)
- $x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$ (Cherowitzo 1998)

$$\sigma = 2^{(h+1)/2} \qquad \gamma = \begin{cases} 2^{(3h+1)/4} & \text{for } h \equiv 1 \pmod 4 \\ 2^{(h+1)/4} & \text{for } h \equiv 3 \pmod 4 \end{cases}$$

Known o-polynomials of $\mathbb{F}_{2^h}$

- x^2 (these give conics)
- x^{2^k} (Segre 1962)
- x^6 (Segre-Bartocci 1971)
- $x^{\sigma+\gamma}$ and $x^{3\sigma+4}$ (Glynn 1983)
- $x^{1/6} + x^{1/2} + x^{5/6}$ (Payne 1985)
- $x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$ (Cherowitzo 1998)
- Subiaco hyperovals (Cherowitzo-Penttila-Pinneri-Royle 1996)

$$\sigma = 2^{(h+1)/2} \qquad \gamma = \begin{cases} 2^{(3h+1)/4} & \text{for } h \equiv 1 \pmod 4 \\ 2^{(h+1)/4} & \text{for } h \equiv 3 \pmod 4 \end{cases}$$

Known o-polynomials of $\mathbb{F}_{2^h}$

- x^2 (these give conics)
- x^{2^k} (Segre 1962)
- x^6 (Segre-Bartocci 1971)
- $x^{\sigma+\gamma}$ and $x^{3\sigma+4}$ (Glynn 1983)
- $x^{1/6} + x^{1/2} + x^{5/6}$ (Payne 1985)
- $x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$ (Cherowitzo 1998)
- Subiaco hyperovals (Cherowitzo-Penttila-Pinneri-Royle 1996)
- Adelaide hyperovals (Cherowitzo-O'Keefe-Penttila 2003)

$$\sigma = 2^{(h+1)/2} \qquad \gamma = \begin{cases} 2^{(3h+1)/4} & \text{for } h \equiv 1 \pmod 4 \\ 2^{(h+1)/4} & \text{for } h \equiv 3 \pmod 4 \end{cases}$$

Known o-polynomials of $\mathbb{F}_{2^h}$

- x^2 (these give conics)
- x^{2^k} (Segre 1962)
- x^6 (Segre-Bartocci 1971)
- $x^{\sigma+\gamma}$ and $x^{3\sigma+4}$ (Glynn 1983)
- $x^{1/6} + x^{1/2} + x^{5/6}$ (Payne 1985)
- $x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$ (Cherowitzo 1998)
- Subiaco hyperovals (Cherowitzo-Penttila-Pinneri-Royle 1996)
- Adelaide hyperovals (Cherowitzo-O'Keefe-Penttila 2003)
- one sporadic example in $\mathbb{F}_{32}$ (O'Keefe-Penttila 1992)

$$\sigma = 2^{(h+1)/2} \qquad \gamma = \begin{cases} 2^{(3h+1)/4} & \text{for } h \equiv 1 \pmod 4 \\ 2^{(h+1)/4} & \text{for } h \equiv 3 \pmod 4 \end{cases}$$

Known classification results

Planes of small order:

- O-polynomials of $\mathbb{F}_{16}$ (Hall 1975)
- O-polynomials of $\mathbb{F}_{32}$ (Penttila-Royle 1994)
- O-monomials of $\mathbb{F}_{2^h}$ for $h \leq 30$ (Glynn 1989)

Known classification results

Planes of small order:

- O-polynomials of $\mathbb{F}_{16}$ (Hall 1975)
- O-polynomials of $\mathbb{F}_{32}$ (Penttila-Royle 1994)
- O-monomials of $\mathbb{F}_{2^h}$ for $h \leq 30$ (Glynn 1989)

Polynomials of small degree:

- O-polynomials of degree at most 6 (Hirschfeld 1971)

Known classification results

Planes of small order:

- O-polynomials of $\mathbb{F}_{16}$ (Hall 1975)
- O-polynomials of $\mathbb{F}_{32}$ (Penttila-Royle 1994)
- O-monomials of $\mathbb{F}_{2^h}$ for $h \leq 30$ (Glynn 1989)

Polynomials of small degree:

- O-polynomials of degree at most 6 (Hirschfeld 1971)

Polynomials of a certain form:

- Linearised o-polynomials (Payne 1971, Hirschfeld 1975)
- O-monomials of degree $2^i + 2^j$ (Cherowitzo-Storme 1998)
- O-monomials of degree $2^i + 2^j + 2^k$ (Vis 2010)

A new classification result

Call two polynomials $f, g \in \mathbb{F}_q[x]$ equivalent if there exists an $a \in \mathbb{F}_q$ such that

$$g(x) = \frac{f(x+a) + f(a)}{f(1+a) + f(a)}.$$

A new classification result

Call two polynomials $f, g \in \mathbb{F}_q[x]$ equivalent if there exists an $a \in \mathbb{F}_q$ such that

$$g(x) = \frac{f(x+a) + f(a)}{f(1+a) + f(a)}.$$

This preserves the o-polynomial property.

A new classification result

Call two polynomials $f, g \in \mathbb{F}_q[x]$ equivalent if there exists an $a \in \mathbb{F}_q$ such that

$$g(x) = \frac{f(x+a) + f(a)}{f(1+a) + f(a)}.$$

This preserves the o-polynomial property.

Theorem (Caullery-S. 2015)

If f is an o-polynomial of $\mathbb{F}_q$ of degree less than $\frac{1}{2}q^{1/4}$, then f is equivalent to either x^6 or x^{2^k} for a positive integer k.

A new classification result

Call two polynomials $f, g \in \mathbb{F}_q[x]$ equivalent if there exists an $a \in \mathbb{F}_q$ such that

$$g(x) = \frac{f(x+a) + f(a)}{f(1+a) + f(a)}.$$

This preserves the o-polynomial property.

Theorem (Caullery-S. 2015)

If f is an o-polynomial of $\mathbb{F}_q$ of degree less than $\frac{1}{2}q^{1/4}$, then f is equivalent to either x^6 or x^{2^k} for a positive integer k.

- x^6 is an o-polynomial of $\mathbb{F}_{2^h}$ if and only if h is odd.

A new classification result

Call two polynomials $f, g \in \mathbb{F}_q[x]$ equivalent if there exists an $a \in \mathbb{F}_q$ such that

$$g(x) = \frac{f(x+a) + f(a)}{f(1+a) + f(a)}.$$

This preserves the o-polynomial property.

Theorem (Caullery-S. 2015)

If f is an o-polynomial of $\mathbb{F}_q$ of degree less than $\frac{1}{2}q^{1/4}$, then f is equivalent to either x^6 or x^{2^k} for a positive integer k.

- x^6 is an o-polynomial of $\mathbb{F}_{2^h}$ if and only if h is odd.
- x^{2^k} is an o-polynomial of $\mathbb{F}_{2^h}$ if and only if $(k,h) = 1$.

Known o-polynomials of $\mathbb{F}_{2^h}$

- x^2
- x^{2^k}
- x^6
- $x^{\sigma+\gamma}$ and $x^{3\sigma+4}$
- $x^{1/6} + x^{1/2} + x^{5/6}$
- $x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$
- Subiaco hyperovals
- Adelaide hyperovals
- one sporadic example in $\mathbb{F}_{32}$

$$\sigma = 2^{(h+1)/2} \qquad \gamma = \begin{cases} 2^{(3h+1)/4} & \text{for } h \equiv 1 \pmod 4 \\ 2^{(h+1)/4} & \text{for } h \equiv 3 \pmod 4 \end{cases}$$

Exceptional o-polynomials

A polynomial $f \in \mathbb{F}_q[x]$ is an exceptional o-polynomial of $\mathbb{F}_q$ if it is an o-polynomial of $\mathbb{F}_{q^r}$ for infinitely many r.

Exceptional o-polynomials

A polynomial $f \in \mathbb{F}_q[x]$ is an exceptional o-polynomial of $\mathbb{F}_q$ if it is an o-polynomial of $\mathbb{F}_{q^r}$ for infinitely many r.

Conjecture (Segre-Bartocci 1971)

The only exceptional o-monomials are x^6 and x^{2^k}.

Exceptional o-polynomials

A polynomial $f \in \mathbb{F}_q[x]$ is an exceptional o-polynomial of $\mathbb{F}_q$ if it is an o-polynomial of $\mathbb{F}_{q^r}$ for infinitely many r.

Conjecture (Segre-Bartocci 1971)

The only exceptional o-monomials are x^6 and x^{2^k}.

Proved by (Hernando-McGuire 2012), (Zieve 2015).

Exceptional o-polynomials

A polynomial $f \in \mathbb{F}_q[x]$ is an exceptional o-polynomial of $\mathbb{F}_q$ if it is an o-polynomial of $\mathbb{F}_{q^r}$ for infinitely many r.

Conjecture (Segre-Bartocci 1971)

The only exceptional o-monomials are x^6 and x^{2^k}.

Proved by (Hernando-McGuire 2012), (Zieve 2015).

Corollary (Caullery-S. 2015)

Up to equivalence, the only exceptional o-polynomials are x^6 and x^{2^k}.

Exceptional o-polynomials

A polynomial $f \in \mathbb{F}_q[x]$ is an exceptional o-polynomial of $\mathbb{F}_q$ if it is an o-polynomial of $\mathbb{F}_{q^r}$ for infinitely many r.

Conjecture (Segre-Bartocci 1971)

The only exceptional o-monomials are x^6 and x^{2^k}.

Proved by (Hernando-McGuire 2012), (Zieve 2015).

Corollary (Caullery-S. 2015)

Up to equivalence, the only exceptional o-polynomials are x^6 and x^{2^k}.

Similar classification problems have been studied extensively for permutation polynomials, cyclic codes, and planar functions, but no complete solution is known in these cases.

The determinant condition

Every o-polynomial f of $\mathbb{F}_q$ satisfies

$$\det\begin{pmatrix} 1 & 1 & 1 \\ x & y & z \\ f(x) & f(y) & f(z) \end{pmatrix} \neq 0 \quad \text{for all distinct } x, y, z \in \mathbb{F}_q.$$

The determinant condition

Every o-polynomial f of $\mathbb{F}_q$ satisfies

$$\det\begin{pmatrix}1 & 1 & 1\\ x & y & z\\ f(x) & f(y) & f(z)\end{pmatrix} \neq 0 \quad \text{for all distinct } x, y, z \in \mathbb{F}_q.$$

Associate with $f \in \mathbb{F}_q[x]$ the determinant polynomial:

$$\Phi_f = \frac{x(f(y)+f(z)) + y(f(x)+f(z)) + z(f(x)+f(y))}{(x+y)(x+z)(y+z)}.$$

The determinant condition

Every o-polynomial f of $\mathbb{F}_q$ satisfies

$$\det \begin{pmatrix} 1 & 1 & 1 \\ x & y & z \\ f(x) & f(y) & f(z) \end{pmatrix} \neq 0 \quad \text{for all distinct } x, y, z \in \mathbb{F}_q.$$

Associate with $f \in \mathbb{F}_q[x]$ the determinant polynomial:

$$\Phi_f = \frac{x(f(y) + f(z)) + y(f(x) + f(z)) + z(f(x) + f(y))}{(x + y)(x + z)(y + z)}.$$

Goal

Show that, for most $f \in \mathbb{F}_q[x]$ of low degree, the determinant polynomial Φ_f has roots in $\mathbb{F}_q^3$ with x, y, z distinct.

The Lang-Weil bound

A polynomial over a field $\mathbb{K}$ is absolutely irreducible if it is irreducible over the algebraic closure of $\mathbb{K}$.

The Lang-Weil bound

A polynomial over a field $\mathbb{K}$ is absolutely irreducible if it is irreducible over the algebraic closure of $\mathbb{K}$.

Examples:

- $x^2 + y^2$ is irreducible over $\mathbb{Q}$, but not over $\mathbb{C}$.

The Lang-Weil bound

A polynomial over a field $\mathbb{K}$ is absolutely irreducible if it is irreducible over the algebraic closure of $\mathbb{K}$.

Examples:

- $x^2 + y^2$ is irreducible over $\mathbb{Q}$, but not over $\mathbb{C}$.
- $x^2 + y^2 - 1$ is irreducible over $\mathbb{C}$, so is absolutely irreducible.

The Lang-Weil bound

A polynomial over a field $\mathbb{K}$ is absolutely irreducible if it is irreducible over the algebraic closure of $\mathbb{K}$.

Examples:

- $x^2 + y^2$ is irreducible over $\mathbb{Q}$, but not over $\mathbb{C}$.
- $x^2 + y^2 - 1$ is irreducible over $\mathbb{C}$, so is absolutely irreducible.

Lang-Weil Bound (Ghorpade-Lauchaud 2002)

Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be an absolutely irreducible polynomial of degree d and let N be its number of roots in $\mathbb{F}_q^n$. Then

$$|N - q^{n-1}| \leq (d-1)(d-2)q^{n-3/2} + 12(d+3)^{n+1}q^{n-2}.$$

Strategy

The determinant polynomial:

$$\Phi_f = \frac{x(f(y) + f(z)) + y(f(x) + f(z)) + z(f(x) + f(y))}{(x + y)(x + z)(y + z)}.$$

Strategy

The determinant polynomial:

$$\Phi_f = \frac{x(f(y)+f(z)) + y(f(x)+f(z)) + z(f(x)+f(y))}{(x+y)(x+z)(y+z)}.$$

New goal

Show that, for most $f \in \mathbb{F}_q[x]$ of low degree, the determinant polynomial Φ_f has an absolutely irreducible factor over $\mathbb{F}_q$.

Strategy

The determinant polynomial:

$$\Phi_f = \frac{x(f(y)+f(z))+y(f(x)+f(z))+z(f(x)+f(y))}{(x+y)(x+z)(y+z)}.$$

New goal

Show that, for most $f \in \mathbb{F}_q[x]$ of low degree, the determinant polynomial Φ_f has an absolutely irreducible factor over $\mathbb{F}_q$.

Very useful: For $q > 2$, every o-polynomial of $\mathbb{F}_q$ is even.

Strategy

The determinant polynomial:

$$\Phi_f = \frac{x(f(y)+f(z)) + y(f(x)+f(z)) + z(f(x)+f(y))}{(x+y)(x+z)(y+z)}.$$

New goal

Show that, for most $f \in \mathbb{F}_q[x]$ of low degree, the determinant polynomial Φ_f has an absolutely irreducible factor over $\mathbb{F}_q$.

Very useful: For $q > 2$, every o-polynomial of $\mathbb{F}_q$ is even.

Why? Write $f(x) = \sum_{i=1}^{q-1} c_i x^i$ and expand:

$$\left.\frac{f(x+a)+f(a)}{x}\right|_{x=0} = c_1 + c_3 a^3 + \cdots + c_{q-1} a^{q-2}.$$

The monomial case

For monomials $f(x) = x^d$ we have

$$\Phi_f = \frac{x(y^d + z^d) + y(x^d + z^d) + z(x^d + y^d)}{(x+y)(x+z)(y+z)}.$$

The monomial case

For monomials $f(x) = x^d$ we have

$$\Phi_f = \frac{x(y^d + z^d) + y(x^d + z^d) + z(x^d + y^d)}{(x+y)(x+z)(y+z)}.$$

Theorem (Hernando-McGuire 2012)

If d is an even positive integer, not equal to 6 or a power of two, then Φ_f has an absolutely irreducible factor over $\mathbb{F}_2$.

The monomial case

For monomials $f(x) = x^d$ we have

$$\Phi_f = \frac{x(y^d + z^d) + y(x^d + z^d) + z(x^d + y^d)}{(x+y)(x+z)(y+z)}.$$

Theorem (Hernando-McGuire 2012)

If d is an even positive integer, not equal to 6 or a power of two, then Φ_f has an absolutely irreducible factor over $\mathbb{F}_2$.

Their proof uses Bezout's Theorem: If g and h are projective curves over an algebraically closed field $\mathbb{K}$ with no common component, then

$$(\deg g)(\deg h) = \sum_{P \in \mathbb{P}^2(\mathbb{K})} I_P(g, h),$$

where $I_P(g, h)$ is the intersection number of g and h at P.

Exceptional polynomials

A polynomial $F \in \mathbb{F}_q[x]$ is exceptional if it induces a permutation on infinitely many extensions of $\mathbb{F}_q$.

Exceptional polynomials

A polynomial $F \in \mathbb{F}_q[x]$ is exceptional if it induces a permutation on infinitely many extensions of $\mathbb{F}_q$.

Fact: A polynomial $F \in \mathbb{F}_q[x]$ is exceptional if and only if

$$\frac{F(x) - F(y)}{x - y}$$

has no absolutely irreducible factor over $\mathbb{F}_q$.

Exceptional polynomials

A polynomial $F \in \mathbb{F}_q[x]$ is exceptional if it induces a permutation on infinitely many extensions of $\mathbb{F}_q$.

Fact: A polynomial $F \in \mathbb{F}_q[x]$ is exceptional if and only if

$$\frac{F(x) - F(y)}{x - y}$$

has no absolutely irreducible factor over $\mathbb{F}_q$.

Corollary: The determinant polynomial of $f(x) = x^d$ has no absolutely irreducible factor over $\mathbb{F}_2$ if and only if

$$F(x) = \frac{(x+1)^d + 1}{x}$$

is an exceptional polynomial.

Zieve's approach

A polynomial $F \in \mathbb{F}_q[x]$ is indecomposable if there do not exist $G, H \in \mathbb{F}_q[x]$ of degree at least two such that $F(x) = G(H(x))$.

Zieve's approach

A polynomial $F \in \mathbb{F}_q[x]$ is indecomposable if there do not exist $G, H \in \mathbb{F}_q[x]$ of degree at least two such that $F(x) = G(H(x))$.

Theorem

If $F \in \mathbb{F}_p[x]$ is an indecomposable exceptional polynomial of degree coprime to p, then there are polynomials $\mu, \nu \in \mathbb{F}_p[x]$ of degree one such that $\mu \circ F \circ \nu$ is either a monomial or a Dickson polynomial of degree coprime to $p^2 - 1$.

Zieve's approach

A polynomial $F \in \mathbb{F}_q[x]$ is indecomposable if there do not exist $G, H \in \mathbb{F}_q[x]$ of degree at least two such that $F(x) = G(H(x))$.

Theorem

If $F \in \mathbb{F}_p[x]$ is an indecomposable exceptional polynomial of degree coprime to p, then there are polynomials $\mu, \nu \in \mathbb{F}_p[x]$ of degree one such that $\mu \circ F \circ \nu$ is either a monomial or a Dickson polynomial of degree coprime to $p^2 - 1$.

Let d be even and suppose that

$$F(x) = \frac{(x+1)^d + 1}{x} = \sum_{i=1}^{d} \binom{d}{i} x^{i-1}$$

is an exceptional polynomial.

Zieve's approach

A polynomial $F \in \mathbb{F}_q[x]$ is indecomposable if there do not exist $G, H \in \mathbb{F}_q[x]$ of degree at least two such that $F(x) = G(H(x))$.

Theorem

If $F \in \mathbb{F}_p[x]$ is an indecomposable exceptional polynomial of degree coprime to p, then there are polynomials $\mu, \nu \in \mathbb{F}_p[x]$ of degree one such that $\mu \circ F \circ \nu$ is either a monomial or a Dickson polynomial of degree coprime to $p^2 - 1$.

Let d be even and suppose that

$$F(x) = \frac{(x+1)^d + 1}{x} = \sum_{i=1}^{d} \binom{d}{i} x^{i-1}$$

is an exceptional polynomial. Write $F = G \circ H$ for an indecomposable polynomial H and apply the theorem to H.

Finishing the proof

Therefore

$$\sum_{i=1}^{d} \binom{d}{i} x^{i-1} = G(H(x)),$$

where H is (up to compositions with linear polynomials) either

Finishing the proof

Therefore

$$\sum_{i=1}^{d} \binom{d}{i} x^{i-1} = G(H(x)),$$

where H is (up to compositions with linear polynomials) either

- a monomial, which forces d to be a power of 2; or

Finishing the proof

Therefore

$$\sum_{i=1}^{d} \binom{d}{i} x^{i-1} = G(H(x)),$$

where H is (up to compositions with linear polynomials) either

- a monomial, which forces d to be a power of 2; or
- a Dickson polynomial of degree s coprime to 6, thus

  $$H(x + x^{-1}) = x^s + x^{-s}$$

  and

  $$\sum_{i=1}^{d} \binom{d}{i} (x + x^{-1})^{i-1} = G(x^s + x^{-s}),$$

  which forces $d = 6$.

Recap: The monomial case

For monomials $f(x) = x^d$ we have

$$\Phi_f = \frac{x(y^d + z^d) + y(x^d + z^d) + z(x^d + y^d)}{(x+y)(x+z)(y+z)}.$$

Recap: The monomial case

For monomials $f(x) = x^d$ we have

$$\Phi_f = \frac{x(y^d + z^d) + y(x^d + z^d) + z(x^d + y^d)}{(x+y)(x+z)(y+z)}.$$

Theorem (Hernando-McGuire 2012, Zieve 2015)

If d is an even positive integer, not equal to 6 or a power of two, then Φ_f has an absolutely irreducible factor over $\mathbb{F}_2$.

Recap: The monomial case

For monomials $f(x) = x^d$ we have

$$\Phi_f = \frac{x(y^d + z^d) + y(x^d + z^d) + z(x^d + y^d)}{(x+y)(x+z)(y+z)}.$$

Theorem (Hernando-McGuire 2012, Zieve 2015)

If d is an even positive integer, not equal to 6 or a power of two, then Φ_f has an absolutely irreducible factor over $\mathbb{F}_2$.

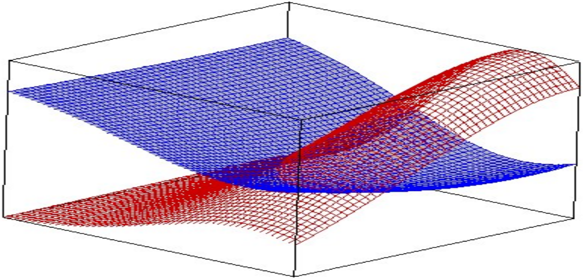
Corollary

If $f(x) = x^d$ is an o-polynomial of $\mathbb{F}_q$ with d less than $\frac{1}{2}q^{1/4}$, then d is either 6 or a power of 2.

Intersecting surfaces

Lemma (Aubry-McGuire-Rodier 2010)

Let S and P be projective surfaces in $\mathbb{P}^3(\overline{\mathbb{F}}_q)$, where P is defined over $\mathbb{F}_q$. If $S \cap P$ has a reduced absolutely irreducible component defined over $\mathbb{F}_q$, then S has an absolutely irreducible component defined over $\mathbb{F}_q$.



The reduction step

- Let $f(x) = \sum_i c_i x^i$ be of degree d. Then

$$\Phi_f(x, y, z) = \sum_{i=2}^{d} c_i \phi_i(x, y, z),$$

  where

$$\phi_i(x, y, z) = \frac{x(y^i + z^i) + y(x^i + z^i) + z(x^i + y^i)}{(x+y)(x+z)(y+z)}.$$

  is homogeneous of degree $i - 2$.

The reduction step

- Let $f(x) = \sum_i c_i x^i$ be of degree d. Then

  $$\Phi_f(x,y,z) = \sum_{i=2}^{d} c_i \phi_i(x,y,z),$$

  where

  $$\phi_i(x,y,z) = \frac{x(y^i+z^i)+y(x^i+z^i)+z(x^i+y^i)}{(x+y)(x+z)(y+z)}.$$

  is homogeneous of degree $i-2$.

- Homogenise by introducing the indeterminate w and intersect with the hyperplane $w=0$. This gives the projective curve defined by $\phi_d(x,y,z)$.

The reduction step

- Let $f(x) = \sum_i c_i x^i$ be of degree d. Then

$$\Phi_f(x, y, z) = \sum_{i=2}^{d} c_i \phi_i(x, y, z),$$

where

$$\phi_i(x, y, z) = \frac{x(y^i + z^i) + y(x^i + z^i) + z(x^i + y^i)}{(x + y)(x + z)(y + z)}.$$

is homogeneous of degree $i - 2$.

- Homogenise by introducing the indeterminate w and intersect with the hyperplane $w = 0$. This gives the projective curve defined by $\phi_d(x, y, z)$.

This is the curve defined by the monomial x^d!

The reduction step

- Let $f(x) = \sum_i c_i x^i$ be of degree d. Then

$$\Phi_f(x,y,z) = \sum_{i=2}^{d} c_i \phi_i(x,y,z),$$

  where

$$\phi_i(x,y,z) = \frac{x(y^i + z^i) + y(x^i + z^i) + z(x^i + y^i)}{(x+y)(x+z)(y+z)}.$$

  is homogeneous of degree $i-2$.

- Homogenise by introducing the indeterminate w and intersect with the hyperplane $w = 0$. This gives the projective curve defined by $\phi_d(x,y,z)$.

  This is the curve defined by the monomial x^d!

- We are left with o-polynomials of degree 6 or a power of 2.

The remaining degrees

Degree 6:

Lemma (Hirschfeld 1971)

If f is an o-polynomial of degree 6, then f is equivalent to x^6.

The remaining degrees

Degree 6:

Lemma (Hirschfeld 1971)

If f is an o-polynomial of degree 6, then f is equivalent to x^6.

Degree 2^k:

Proposition (Caullery-S. 2015)

If f is an even polynomial of degree 2^k, then Φ_f is absolutely irreducible or f is a linearised polynomial.

Proof: Use lots of divisibility and factoring arguments.

The remaining degrees

Degree 6:

Lemma (Hirschfeld 1971)

If f is an o-polynomial of degree 6, then f is equivalent to x^6.

Degree 2^k:

Proposition (Caullery-S. 2015)

If f is an even polynomial of degree 2^k, then Φ_f is absolutely irreducible or f is a linearised polynomial.

Proof: Use lots of divisibility and factoring arguments.

Lemma (Payne 1971, Hirschfeld 1975)

If f is a linearised o-polynomial, then it is of the form x^{2^k}.

Hyperovals in $\mathbb{P}^2(\mathbb{F}_q)$

Kai-Uwe Schmidt

Department of Mathematics
Paderborn University
Germany