Hasse-Weil type theorems and relevant classes of polynomial functions

Daniele Bartoli
University of Perugia, Italy

Seminario congiunto
UMI
Gruppo Crittografia e Codici e Iniziativa De Componendis Cifris
Gruppo MathCifris

Mercoledì 1 Dicembre 2021

Outline

1. Algebraic curves over finite fields

Outline

1. Algebraic curves over finite fields
2. How describe a problem via a curve?
3. Which machineries?

Outline

1. Algebraic curves over finite fields
2. How describe a problem via a curve?
3. Which machineries?
4. Applications:
   - Permutation polynomials
   - Fractional Permutation Polynomials
   - Planar polynomials
   - Scattered polynomials

Connections

Permutation polynomials	S-boxes, Public key cryptography, Coding Theory, orthogonal latin squares, bent-negabent functions
Planar polynomials, q odd	Construction of finite projective planes, Relative difference sets, Error-correcting codes S-boxes in block ciphers
Planar polynomials, q even	Relative difference sets, Error-correcting codes S-boxes in block ciphers
Scattered polynomials	blocking sets, small complete caps, two-intersection sets, MRD codes finite semifields, translation hyperovals

Toy example: a permutation problem

How to check if a polynomial $f(x)$ permutes $\mathbb{F}_q$?

Toy example: a permutation problem

How to check if a polynomial $f(x)$ permutes $\mathbb{F}_q$?

$f(x)$ permutes $\mathbb{F}_q$

Toy example: a permutation problem

How to check if a polynomial $f(x)$ permutes $\mathbb{F}_q$?

$$f(x) \text{ permutes } \mathbb{F}_q$$

$$\Updownarrow$$

$$\forall b \in \mathbb{F}_q \qquad f(x) = b \text{ has exactly one solution } \overline{x} \in \mathbb{F}_q$$

Toy example: a permutation problem

How to check if a polynomial $f(x)$ permutes $\mathbb{F}_q$?

$$f(x) \text{ permutes } \mathbb{F}_q$$

$$\Updownarrow$$

$$\forall b \in \mathbb{F}_q \qquad f(x) = b \text{ has exactly one solution } \overline{x} \in \mathbb{F}_q$$

$$\Updownarrow$$

$$f(x) = f(y) \text{ has only solutions } (\overline{x}, \overline{x}) \in \mathbb{F}_q^2$$

Toy example: a permutation problem

How to check if a polynomial $f(x)$ permutes $\mathbb{F}_q$?

$$f(x) \text{ permutes } \mathbb{F}_q$$

$$\Updownarrow$$

$$\forall b \in \mathbb{F}_q \qquad f(x) = b \text{ has exactly one solution } \overline{x} \in \mathbb{F}_q$$

$$\Updownarrow$$

$$f(x) = f(y) \text{ has only solutions } (\overline{x}, \overline{x}) \in \mathbb{F}_q^2$$

$$\Updownarrow$$

$$\frac{f(x)-f(y)}{x-y} = 0 \text{ has no solution } (\overline{x}, \overline{y}) \in \mathbb{F}_q^2 \text{ with } \overline{x} \neq \overline{y}$$

Toy example: a permutation problem

Example

Does $f(x) = x^3 + x$ permute $\mathbb{F}_7$?

Toy example: a permutation problem

Example

Does $f(x) = x^3 + x$ permute $\mathbb{F}_7$?

$\frac{f(x)-f(y)}{x-y} = 0$ reads $x^2 + xy + y^2 + 1 = 0$

Toy example: a permutation problem

Example

Does $f(x) = x^3 + x$ permute $\mathbb{F}_7$?

$\frac{f(x)-f(y)}{x-y} = 0$ reads $x^2 + xy + y^2 + 1 = 0$

solutions $\longrightarrow (1,3), (4,4), (6,4), (4,6), (3,3), (3,1)$

Toy example: a permutation problem

Example

Does $f(x) = x^3 + x$ permute $\mathbb{F}_7$?

$$\frac{f(x)-f(y)}{x-y} = 0 \text{ reads } x^2 + xy + y^2 + 1 = 0$$

solutions $\longrightarrow (1,3), \cancel{(4,4)}, (6,4), (4,6), \cancel{(3,3)}, (3,1)$

Toy example: a permutation problem

Example

Does $f(x) = x^3 + x$ permute $\mathbb{F}_7$?

$$\frac{f(x)-f(y)}{x-y} = 0 \text{ reads } x^2 + xy + y^2 + 1 = 0$$

$$\text{solutions} \longrightarrow (1,3), \cancel{(4,4)}, (6,4), (4,6), \cancel{(3,3)}, (3,1)$$

$f(x) = x^3 + x$ *does not permute* $\mathbb{F}_7$

Algebraic curves in Combinatorics

Construction of complete plane arcs

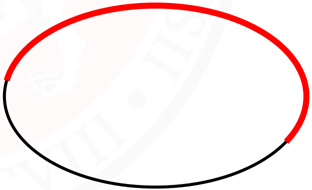
Definition

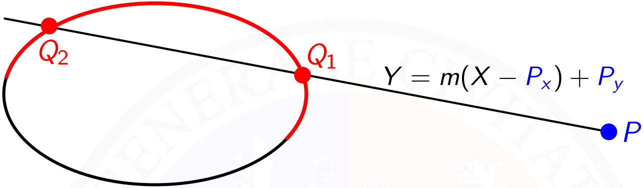
$\mathcal{A} \subset \mathrm{PG}(2,q)$ arc $\iff$ no three points collinear

$\mathcal{A} \subset \mathrm{PG}(2,q)$ complete arc $\iff$ $\forall P \in \mathrm{PG}(2,q) \setminus \mathcal{A}$ collinear with $Q_1 \neq Q_2 \in \mathcal{A}$

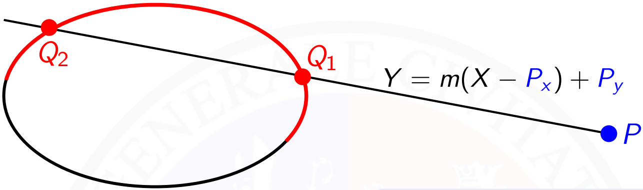
Idea of Segre and Lombardo-Radice

consider subsets of a conic or a cubic curve

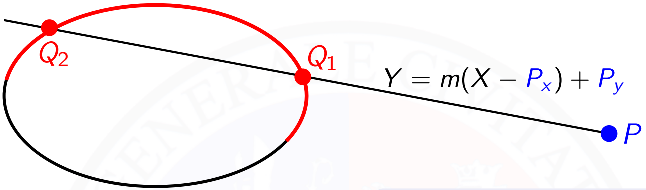




Q_2
Q_1
$Y = m(X - P_x) + P_y$
P



attach to P a curve $\mathcal{C}_P$ $\Longrightarrow$ *suitable points of $\mathcal{C}_P$ yield existence of bisecants through P*



attach to P a curve $\mathcal{C}_P$ $\Longrightarrow$ suitable points of $\mathcal{C}_P$ yield existence of bisecants through P

Complete planar arcs	*Segre, Hirschfeld, Abatangelo, Korchmàros, Szőnyi, Voloch, Giulietti, Platoni, Anbar, B., ...*
Complete planar k-arcs	*Hirschfeld, Voloch, Giulietti, Zini, Marcugini, Pambianco, B., ...*
Complete caps	*Giulietti, Anbar, Platoni, B., ...*
Complete arcs in projective spaces	*Giulietti, Platoni, B., ...*

What is a curve?

$\mathbb{F}_q$: *finite field with* $q = p^h$ *elements*

Definition (Affine plane)

$$\mathrm{AG}(2, q) := (\mathbb{F}_q)^2$$

What is a curve?

$\mathbb{F}_q$: *finite field with* $q = p^h$ *elements*

Definition (Affine plane)

$$\mathrm{AG}(2, q) := (\mathbb{F}_q)^2$$

Definition (Curve)

$\mathcal{C}$ in $\mathrm{AG}(2, q)$ Curve
class of proportional polynomials $F(X, Y) \in \mathbb{F}_q[X, Y]$
degree of $\mathcal{C}$ $= \deg(F(X, Y))$

What is a curve?

$\mathbb{F}_q$: *finite field with* $q = p^h$ *elements*

Definition (Affine plane)

$$\mathrm{AG}(2,q) := (\mathbb{F}_q)^2$$

Definition (Curve)

$\mathcal{C}$ in $\mathrm{AG}(2,q)$ Curve
class of proportional polynomials $F(X,Y) \in \mathbb{F}_q[X,Y]$
degree of $\mathcal{C}$ $= \deg(F(X,Y))$

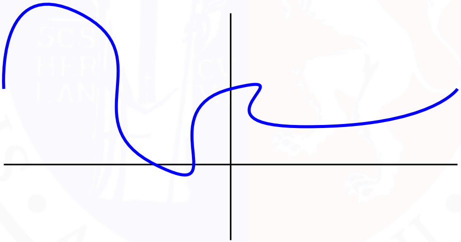
$$2X + 7Y^2 + 3 \iff 4X + 14Y^2 + 6$$

What is a curve?

$\mathcal{C}$ defined by $F(X, Y)$

Definition

$$\begin{array}{l}(a, b) \in \mathrm{AG}(2, q) \\ \text{(affine) } \mathbb{F}_q\text{-rational point of } \mathcal{C}\end{array} \iff F(a, b) = 0$$



$\mathcal{C} \ : \ F(X, Y) = 0$

Curves: absolute irreducibility

Definition

$\mathcal{C}$: $F(X, Y) = 0$ affine equation

Definition

$\mathcal{C}$ absolutely irreducible $\iff$

$$\nexists G(X, Y), H(X, Y) \in \overline{\mathbb{F}}_q[X, Y] \ :$$

$$F(X, Y) = G(X, Y)H(X, Y)$$

$\deg(G(X, Y)), \deg(H(X, Y)) > 0$

Example

$X^2 + Y^2 + 1$ absolutely irreducible
$X^2 - sY^2$, $s \notin \square_q$,
$\implies (X - \eta Y)(X + \eta Y)$, $\eta^2 = s$, $\eta \in \mathbb{F}_{q^2}$ not absolutely irreducible

A fundamental tool: Hasse-Weil Theorem

Question

How many $\mathbb{F}_q$-rational points can $\mathcal{C}$ have?

A fundamental tool: Hasse-Weil Theorem

Question

How many $\mathbb{F}_q$-rational points can $\mathcal{C}$ have?

Theorem (Hasse-Weil Theorem)

$\mathcal{C}$ *absolutely irreducible curve of degree d defined over $\mathbb{F}_q$*
The number N_q of $\mathbb{F}_q$-rational points is

$$|N_q - (q+1)| \leq (d-1)(d-2)\sqrt{q}.$$

A fundamental tool: Hasse-Weil Theorem

Question

How many $\mathbb{F}_q$-rational points can $\mathcal{C}$ have?

Theorem (Hasse-Weil Theorem)

$\mathcal{C}$ absolutely irreducible curve of degree d defined over $\mathbb{F}_q$
The number N_q of $\mathbb{F}_q$-rational points is

$$|N_q - (q+1)| \leq (d-1)(d-2)\sqrt{q}.$$

Example

$\mathcal{C} \;:\; X^2 - Y^2 = 0$ has $2q+1$ $\mathbb{F}_q$-rational points!
$\mathcal{C} \;:\; X^2 - sY^2 = 0, \quad s \notin \square_q$ has 1 $\mathbb{F}_q$-rational point!

Algebraic curves and Permutation Polynomials

Theorem

$$f(x) \in \mathbb{F}_q[x] \text{ is PP } \iff \begin{array}{l} \mathcal{C}_f \;:\; \frac{f(X)-f(Y)}{X-Y} = 0 \\ \text{has no affine } \mathbb{F}_q\text{-rational} \\ \text{points off } X - Y = 0 \end{array}$$

Algebraic curves and Permutation Polynomials

Theorem

$f(x) \in \mathbb{F}_q[x]$ *is PP* $\iff$ $\mathcal{C}_f \ : \ \frac{f(X)-f(Y)}{X-Y} = 0$ *has no affine* $\mathbb{F}_q$*-rational points off* $X - Y = 0$

Example

$f(x) = x^3 + x \in \mathbb{F}_q[x]$

$$\mathcal{C}_f : \frac{f(X) - f(Y)}{X - Y} = X^2 + XY + Y^2 + 1 = 0$$

Algebraic curves and Permutation Polynomials

Theorem

$f(x) \in \mathbb{F}_q[x]$ *is PP* $\iff$ $\mathcal{C}_f \; : \; \frac{f(X)-f(Y)}{X-Y} = 0$ *has no affine* $\mathbb{F}_q$*-rational points off* $X - Y = 0$

Example

$f(x) = x^3 + x \in \mathbb{F}_q[x]$

$$\mathcal{C}_f : \frac{f(X) - f(Y)}{X - Y} = X^2 + XY + Y^2 + 1 = 0$$

$\mathcal{C}_f$ CONIC $\Longrightarrow$ with at least $q - 3$ affine $\mathbb{F}_q$-rational points not on $X - Y = 0$

Algebraic curves and Permutation Polynomials

Theorem

$$f(x) \in \mathbb{F}_q[x] \text{ is PP } \iff \begin{array}{l} \mathcal{C}_f \ : \ \frac{f(X)-f(Y)}{X-Y} = 0 \\ \text{has no affine } \mathbb{F}_q\text{-rational} \\ \text{points off } X-Y=0 \end{array}$$

Example

$f(x) = x^3 + x \in \mathbb{F}_q[x]$

$$\mathcal{C}_f : \frac{f(X)-f(Y)}{X-Y} = X^2 + XY + Y^2 + 1 = 0$$

$$\mathcal{C}_f \text{ CONIC} \Longrightarrow \begin{array}{c} \text{with at least } q-3 \\ \text{affine } \mathbb{F}_q\text{-rational points} \\ \text{not on } X-Y=0 \end{array}$$

if $q > 3 \Longrightarrow f(x) = x^3 + x$ is NOT a PP

Toy example revisited: a permutation problem 2

Example

Does $f(x) = x^7 + x^5 + x$ permute $\mathbb{F}_{2^k}$?

Toy example revisited: a permutation problem 2

Example

Does $f(x) = x^7 + x^5 + x$ permute $\mathbb{F}_{2^k}$?

$\frac{f(X)-f(Y)}{X-Y} = 0$ reads $\begin{array}{c} X^6 + X^5Y + X^4Y^2 + X^4 + X^3Y^3 + X^3Y + \\ X^2Y^4 + X^2Y^2 + XY^5 + XY^3 + Y^6 + Y^4 + 1 \end{array} = 0$

Toy example revisited: a permutation problem 2

Example

Does $f(x) = x^7 + x^5 + x$ permute $\mathbb{F}_{2^k}$?

$$\frac{f(X)-f(Y)}{X-Y} = 0 \text{ reads } \begin{array}{l} X^6 + X^5Y + X^4Y^2 + X^4 + X^3Y^3 + X^3Y + \\ X^2Y^4 + X^2Y^2 + XY^5 + XY^3 + Y^6 + Y^4 + 1 \end{array} = 0$$

$$\mathcal{C}_f = C_1 \cup C_2 \cup C_3$$

$$\begin{aligned} C_1 &:= X^2 + \omega^3 XY + Y^2 + \omega^6 = 0 \\ C_2 &:= X^2 + \omega^6 XY + Y^2 + \omega^5 = 0 \\ C_3 &:= X^2 + \omega^5 XY + Y^2 + \omega^3 = 0 \end{aligned}$$

$\omega \in \mathbb{F}_8$ such that $\omega^3 + \omega + 1 = 0$

Toy example revisited: a permutation problem 2

Example

Does $f(x) = x^7 + x^5 + x$ permute $\mathbb{F}_{2^k}$?

$\frac{f(X)-f(Y)}{X-Y} = 0$ reads $\begin{array}{c} X^6 + X^5Y + X^4Y^2 + X^4 + X^3Y^3 + X^3Y + \\ X^2Y^4 + X^2Y^2 + XY^5 + XY^3 + Y^6 + Y^4 + 1 \end{array} = 0$

$$\mathcal{C}_f = C_1 \cup C_2 \cup C_3$$

$$\begin{aligned} C_1 &:= X^2 + \omega^3 XY + Y^2 + \omega^6 = 0 \\ C_2 &:= X^2 + \omega^6 XY + Y^2 + \omega^5 = 0 \\ C_3 &:= X^2 + \omega^5 XY + Y^2 + \omega^3 = 0 \end{aligned}$$

$\omega \in \mathbb{F}_8$ such that $\omega^3 + \omega + 1 = 0$

$3 \nmid k \implies$ *C_i not defined over $\mathbb{F}_{2^k}$* $\implies$ *no $\mathbb{F}_{2^k}$-rational points off $X = Y$* $\implies$ *$x^7 + x^5 + x$ is PP*

An easy criterion

Criterion (SEGRE)

$P \in \mathcal{C}$ has tangent t

- *non-repeated*
- $t \cap \mathcal{C} = \{P\}$

$\Longrightarrow$ *$\mathcal{C}$ is absolutely irreducible*

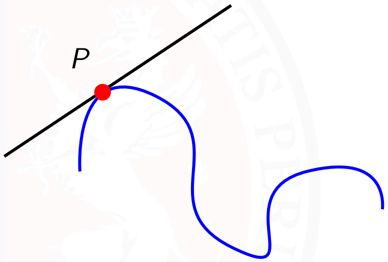
An easy criterion

Criterion (SEGRE)

$P \in \mathcal{C}$ *has tangent* t

- *non-repeated*
- $t \cap \mathcal{C} = \{P\}$

$\Longrightarrow \mathcal{C}$ *is absolutely irreducible*



BARTOCCI-SEGRE. Acta Arith XVIII, 1971

Frobenius automorphism and $\mathbb{F}_q$-rational components

Definition (Frobenius automorphism)

$$\begin{aligned} \varphi_q \quad : \quad & \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q} \\ & \alpha \mapsto \alpha^q \end{aligned}$$

Frobenius automorphism and $\mathbb{F}_q$-rational components

Definition (Frobenius automorphism)

$$\begin{aligned}\varphi_q \quad : \quad & \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q} \\ & \alpha \mapsto \alpha^q\end{aligned}$$

$$\varphi_q : \begin{array}{ccc} \mathbb{A}^2(\overline{\mathbb{F}_q}) & \to & \mathbb{A}^2(\overline{\mathbb{F}_q}) \\ (\alpha, \beta) & \mapsto & (\alpha^q, \beta^q) \end{array}$$

$$\varphi_q : \begin{array}{ccc} \overline{\mathbb{F}_q}[X, Y] & \to & \overline{\mathbb{F}_q}[X, Y] \\ \sum \alpha_{i,j} X^i Y^j & \mapsto & \sum \alpha_{i,j}^q X^i Y^j \end{array}$$

Frobenius automorphism and $\mathbb{F}_q$-rational components

Definition (Frobenius automorphism)

$$\begin{aligned} \varphi_q \quad : \quad & \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q} \\ & \alpha \mapsto \alpha^q \end{aligned}$$

$$\begin{array}{rccc} \varphi_q : & \mathbb{A}^2(\overline{\mathbb{F}_q}) & \to & \mathbb{A}^2(\overline{\mathbb{F}_q}) \\ & (\alpha, \beta) & \mapsto & (\alpha^q, \beta^q) \end{array}$$

$$\begin{array}{rccc} \varphi_q : & \overline{\mathbb{F}_q}[X, Y] & \to & \overline{\mathbb{F}_q}[X, Y] \\ & \sum \alpha_{i,j} X^i Y^j & \mapsto & \sum \alpha_{i,j}^q X^i Y^j \end{array}$$

$\varphi_q(\alpha) = \alpha \iff \alpha \in \mathbb{F}_q$

$\varphi_q(\alpha, \beta) = (\alpha, \beta) \iff (\alpha, \beta) \in \mathbb{A}^2(\mathbb{F}_q)$

$\varphi_q(\mathcal{C}) = \mathcal{C} \iff \lambda F \in \mathbb{F}_q[X, Y]$ *for some* $\lambda \in \overline{\mathbb{F}_q}^*$

Frobenius automorphism and $\mathbb{F}_q$-rational components

$F(X,Y) \in \mathbb{F}_q[X,Y]$, $\qquad \mathcal{C} : F(X,Y) = 0$ curve

Frobenius automorphism and $\mathbb{F}_q$-rational components

$F(X,Y) \in \mathbb{F}_q[X,Y]$, $\qquad \mathcal{C} : F(X,Y) = 0$ curve

$$F(X,Y) = F_1(X,Y) \cdot F_2(X,Y) \cdot \dots \cdot F_k(X,Y), \quad F_i \in \overline{\mathbb{F}_q}[X,Y]$$

$\mathcal{C}_i : F_i(X,Y) = 0$ components of $\mathcal{C}$

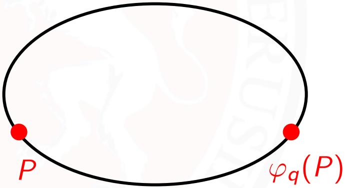
Frobenius automorphism and $\mathbb{F}_q$-rational components

$F(X,Y) \in \mathbb{F}_q[X,Y]$, $\qquad \mathcal{C} : F(X,Y) = 0$ curve

$$F(X,Y) = F_1(X,Y) \cdot F_2(X,Y) \cdot \cdots \cdot F_k(X,Y), \quad F_i \in \overline{\mathbb{F}_q}[X,Y]$$

$\mathcal{C}_i : F_i(X,Y) = 0$ components of $\mathcal{C}$

$$P \in \mathcal{C} \Longrightarrow \varphi_q(P) \in \mathcal{C}$$



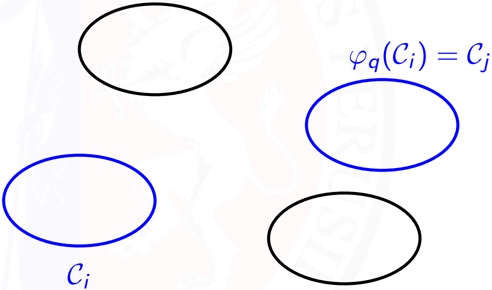
Frobenius automorphism and $\mathbb{F}_q$-rational components

$F(X,Y) \in \mathbb{F}_q[X,Y]$, $\quad \mathcal{C} : F(X,Y) = 0$ curve

$$F(X,Y) = F_1(X,Y) \cdot F_2(X,Y) \cdot \cdots \cdot F_k(X,Y), \qquad F_i \in \overline{\mathbb{F}_q}[X,Y]$$

$\mathcal{C}_i : F_i(X,Y) = 0$ components of $\mathcal{C}$

$$\varphi_q(\mathcal{C}_i) = \mathcal{C}_j$$



Remark

$$\varphi_q(\mathcal{C}_i) = \mathcal{C}_i \Longrightarrow \begin{array}{c} \mathcal{C}_i \textit{ is defined over } \mathbb{F}_q \\ \mathcal{C}_i \ \mathbb{F}_q\textit{-rational A.I. component of } \mathcal{C} \end{array}$$

Another toy example: a permutation problem

Example

Does $f(x) = x^6$ permute $\mathbb{F}_{23}$?

Another toy example: a permutation problem

Example

Does $f(x) = x^6$ permute $\mathbb{F}_{23}$?

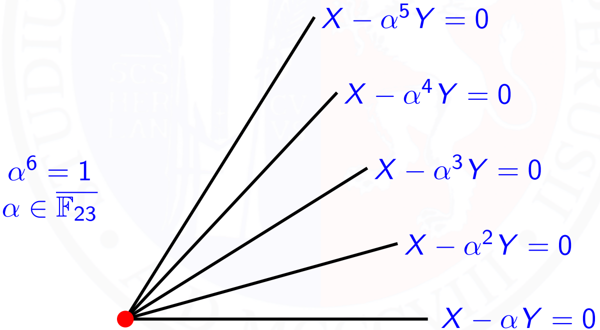
$\frac{f(X)-f(Y)}{X-Y} = 0$ reads $X^5 + X^4Y + X^3Y^2 + X^2Y^3 + XY^4 + Y^5 = 0$

Another toy example: a permutation problem

Example

Does $f(x) = x^6$ permute $\mathbb{F}_{23}$?

$\frac{f(X)-f(Y)}{X-Y} = 0$ reads $X^5 + X^4Y + X^3Y^2 + X^2Y^3 + XY^4 + Y^5 = 0$

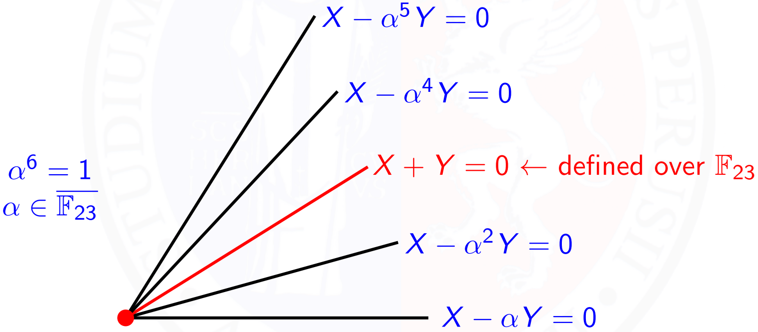


Another toy example: a permutation problem

Example

Does $f(x) = x^6$ permute $\mathbb{F}_{23}$?

$\frac{f(X)-f(Y)}{X-Y} = 0$ reads $X^5 + X^4Y + X^3Y^2 + X^2Y^3 + XY^4 + Y^5 = 0$



$X + Y = 0$ *defined over* $\mathbb{F}_{23}$ $\Longrightarrow$ *there are 22* $\mathbb{F}_{23}$*-rational points* (x, y) *with* $x \neq y$ $\Longrightarrow$ $f(x) = x^6$ *NO PP*

Hasse-Weil again

Theorem (Hasse-Weil Theorem)

$\mathcal{C}$ *absolutely irreducible curve of degree* d *defined over* $\mathbb{F}_q$

$$|N_q - (q+1)| \leq (d-1)(d-2)\sqrt{q}.$$

Hasse-Weil again

Theorem (Hasse-Weil Theorem)

$\mathcal{C}$ absolutely irreducible curve of degree d defined over $\mathbb{F}_q$

$$|N_q - (q+1)| \leq (d-1)(d-2)\sqrt{q}.$$

Corollary

$\deg f(x) < q^{1/4}$

$$f(x) \ PP \implies \mathcal{C}_f \ \textit{has no } \mathbb{F}_q - A.I.C. \textit{ distinct from } X - Y = 0$$

Hasse-Weil again

Theorem (Hasse-Weil Theorem)

$\mathcal{C}$ absolutely irreducible curve of degree d defined over $\mathbb{F}_q$

$$|N_q - (q+1)| \leq (d-1)(d-2)\sqrt{q}.$$

Corollary

$\deg f(x) < q^{1/4}$

$$f(x)\ \mathit{PP} \implies \mathcal{C}_f \textit{ has no } \mathbb{F}_q - A.I.C. \textit{ distinct from } X - Y = 0$$

Proof. $\mathcal{D}$ $\mathbb{F}_q$-A.I.C. By Hasse-Weil Theorem

$$\begin{aligned} N_q &\geq -(d-1)(d-2)\sqrt{q} + (q+1) \\ &\geq -(\sqrt[4]{q}-2)(\sqrt[4]{q}-3)\sqrt{q} + (q+1) \\ &= 5\sqrt[4]{q^3} - 6\sqrt{q} + 1 \end{aligned}$$

Number of points not at infinity nor on $X - Y = 0$

$$N_q - 2\deg(\mathcal{D}) \geq N_q - 2(\sqrt[4]{q}-1) \geq 5\sqrt[4]{q^3} - 6\sqrt{q} - 2\sqrt[4]{q} + 3 > 0$$

Existence of absolutely irreducible $\mathbb{F}_q$-rational components

Remark

$P \in \mathcal{C}$ *simple point* $\Longrightarrow$ P *belongs to a unique component of* $\mathcal{C}$

Existence of absolutely irreducible $\mathbb{F}_q$-rational components

Remark

$P \in \mathcal{C}$ *simple point* $\Longrightarrow$ P *belongs to a unique component of* $\mathcal{C}$

Criterion

$F(X, Y, T) \in \mathbb{F}_q[X, Y, T]$,
$P \in \mathcal{C}\ :\ F(X, Y, T) = 0$ *simple* $\mathbb{F}_q$*-point*
$\Longrightarrow \mathcal{C}$ *has* $\mathbb{F}_q$*-A.I.C. defined over* $\mathbb{F}_q$

$P = \varphi_q(P)$

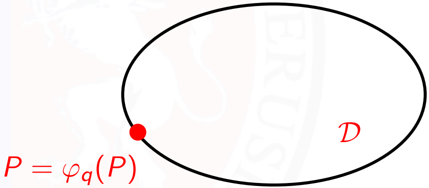
Existence of absolutely irreducible $\mathbb{F}_q$-rational components

Remark

$P \in \mathcal{C}$ *simple point* $\Longrightarrow$ P *belongs to a unique component of* $\mathcal{C}$

Criterion

$F(X, Y, T) \in \mathbb{F}_q[X, Y, T]$,
$P \in \mathcal{C} \; : \; F(X, Y, T) = 0$ *simple* $\mathbb{F}_q$*-point*
$\Longrightarrow$ $\mathcal{C}$ *has* $\mathbb{F}_q$*-A.I.C. defined over* $\mathbb{F}_q$



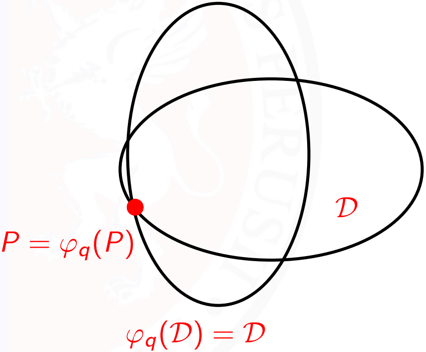
Existence of absolutely irreducible $\mathbb{F}_q$-rational components

Remark

$P \in \mathcal{C}$ *simple point* $\Longrightarrow$ *P belongs to a unique component of* $\mathcal{C}$

Criterion

$F(X,Y,T) \in \mathbb{F}_q[X,Y,T]$,
$P \in \mathcal{C} \ : \ F(X,Y,T) = 0$ *simple* $\mathbb{F}_q$*-point*
$\Longrightarrow \mathcal{C}$ *has* $\mathbb{F}_q$*-A.I.C. defined over* $\mathbb{F}_q$



What to do when the degree is too high: A Useful Criterion

Problem

The degree of $\mathcal{C}_f \ : \ \frac{f(x)-f(y)}{x-y} = 0$ *can be too high to use Hasse-Weil*

What to do when the degree is too high: A Useful Criterion

Problem

The degree of $\mathcal{C}_f \; : \; \frac{f(x)-f(y)}{x-y} = 0$ *can be too high to use Hasse-Weil*

$$f_{r,d,h}(x) = x^r h\left(x^{\frac{q-1}{d}}\right)$$

What to do when the degree is too high: A Useful Criterion

Problem

The degree of $\mathcal{C}_f \; : \; \frac{f(x)-f(y)}{x-y} = 0$ *can be too high to use Hasse-Weil*

$$f_{r,d,h}(x) = x^r h\left(x^{\frac{q-1}{d}}\right)$$

Criterion

$f_{r,d,h}(x) \in \mathbb{F}_q$ PP $\iff$

- $(r, (q-1)/d) = 1$
- $x^r h(x)^{\frac{q-1}{d}}$ *permutes* $\mu_d = \{a \in \mathbb{F}_q \; : \; a^d = 1\}$

PARK, LEE. Bull. Aust. Math. Soc., 2001
ZIEVE. Proc. Am. Math. Soc. 2009
AKBARY, GHIOCA, WANG. Finite Fields Appl., 2011

What to do when the degree is too high: A Useful Criterion

$$f_{\alpha,\beta}(x) = x + \alpha x^{q(q-1)+1} + \beta x^{2(q-1)+1}, q = 2^n$$

Problem

Find all $\alpha, \beta \in \mathbb{F}_{q^2}$, $q = 2^n$, *such that* $f_{\alpha,\beta}$ *is PP*

TU, ZENG, LI, HELLESETH. Finite Fields Appl., 2018

What to do when the degree is too high: A Useful Criterion

$$f_{\alpha,\beta}(x) = x + \alpha x^{q(q-1)+1} + \beta x^{2(q-1)+1},\, q = 2^n$$

Problem

Find all $\alpha, \beta \in \mathbb{F}_{q^2}$, $q = 2^n$, such that $f_{\alpha,\beta}$ is PP

TU, ZENG, LI, HELLESETH. Finite Fields Appl., 2018

$$f_{\alpha,\beta}(x) = x + \alpha x^{q(q-1)+1} + \beta x^{2(q-1)+1} = x\left(1 + \alpha\left(x^{q-1}\right)^{q} + \beta\left(x^{q-1}\right)^{2}\right)$$

$$f_{\alpha,\beta}(x) \in \mathbb{F}_{q^2} \text{ PP} \iff g_{\alpha,\beta}(x) = x\left(1 + \alpha x^{q} + \beta x^{2}\right)^{q-1} \text{ permutes } \mu_{q+1}$$

How to make life easier

$f_{\alpha,\beta}(x) \in \mathbb{F}_{q^2}$ PP $\iff$ $g_{\alpha,\beta}(x) = x\left(1 + \alpha x^q + \beta x^2\right)^{q-1}$ permutes μ_{q+1}

- $i \in \mathbb{F}_{q^2}$, $i^q + i = 1$
- $\alpha = A + iB$, $A, B \in \mathbb{F}_q$
- $\beta = C + iD$, $C, D \in \mathbb{F}_q$
- $x = \frac{x'+i}{x'+i+1}$, $x' \in \mathbb{F}_q$

How to make life easier

$f_{\alpha,\beta}(x) \in \mathbb{F}_{q^2}$ PP $\iff$ $g_{\alpha,\beta}(x) = x\left(1 + \alpha x^q + \beta x^2\right)^{q-1}$ permutes μ_{q+1}

- $i \in \mathbb{F}_{q^2},\ i^q + i = 1$
- $\alpha = A + iB,\ A, B \in \mathbb{F}_q$
- $\beta = C + iD,\ C, D \in \mathbb{F}_q$
- $x = \frac{x'+i}{x'+i+1},\ x' \in \mathbb{F}_q$

$$g_{\alpha,\beta}(x) \quad \mapsto \quad h(x) = \frac{h_1(x)}{h_2(x)}, \quad \begin{array}{l} h_1, h_2 \in \mathbb{F}_q[x] \\ \deg(h_1), \deg(h_2) \leq 3 \end{array}$$

How to make life easier

$f_{\alpha,\beta}(x) \in \mathbb{F}_{q^2}$ PP $\iff$ $g_{\alpha,\beta}(x) = x\left(1+\alpha x^q + \beta x^2\right)^{q-1}$ permutes μ_{q+1}

- $i \in \mathbb{F}_{q^2}$, $i^q + i = 1$
- $\alpha = A + iB$, $A, B \in \mathbb{F}_q$
- $\beta = C + iD$, $C, D \in \mathbb{F}_q$
- $x = \frac{x'+i}{x'+i+1}$, $x' \in \mathbb{F}_q$

$$g_{\alpha,\beta}(x) \quad \mapsto \quad h(x) = \frac{h_1(x)}{h_2(x)}, \quad \begin{array}{l} h_1, h_2 \in \mathbb{F}_q[x] \\ \deg(h_1), \deg(h_2) \leq 3 \end{array}$$

Proposition

$f_{\alpha,\beta}(x)$ *PP of* $\mathbb{F}_{q^2}$ $\iff$ $\mathcal{C}_{A,B} : \frac{h_1(X)h_2(Y) - h_1(Y)h_2(X)}{X-Y} = 0$, $\deg(\mathcal{C}_{A,B}) \leq 4$, *has no $\mathbb{F}_q$-rational points $(\overline{x}, \overline{y})$ with $\overline{x} \neq \overline{y}$*

B. Finite Fields Appl., 2018

Exceptional Planar Functions

Definition (Planar Function, q odd)

q odd prime power

$f : \mathbb{F}_q \to \mathbb{F}_q$ planar or perfect nonlinear if

$$\forall \epsilon \in \mathbb{F}_q^* \implies x \mapsto f(x+\epsilon) - f(x) \text{ is PP}$$

Exceptional Planar Functions

Definition (Planar Function, q odd)

q odd prime power

$f : \mathbb{F}_q \to \mathbb{F}_q$ planar or perfect nonlinear if

$$\forall \epsilon \in \mathbb{F}_q^* \Longrightarrow x \mapsto f(x+\epsilon) - f(x) \text{ is PP}$$

- Construction of finite projective planes

  DEMBOWSKI-OSTROM, Math. Z. 1968
- Relative difference sets

  GANLEY-SPENCE, J. Combin. Theory Ser. A 1975
- Error-correcting codes

  CARLET-DING-YUAN, IEEE Trans. Inform. Theory 2005
- S-boxes in block ciphers

  NYBERG-KNUDSEN, Advances in cryptology 1993.

Exceptional Planar Functions

Definition (Planar Function, q even)

q even

$f : \mathbb{F}_q \to \mathbb{F}_q$ planar if

$$\forall \epsilon \in \mathbb{F}_q^* \implies x \mapsto f(x+\epsilon) + f(x) + \epsilon x \text{ is PP}$$

Exceptional Planar Functions

Definition (Planar Function, q even)

q even

$f : \mathbb{F}_q \to \mathbb{F}_q$ planar if

$$\forall \epsilon \in \mathbb{F}_q^* \implies x \mapsto f(x+\epsilon) + f(x) + \epsilon x \text{ is PP}$$

ZHOU, J. Combin. Des. 2013.

Other works

SCHMIDT-ZHOU, J. Algebraic Combin., 2014
SCHERR-ZIEVE, Ann. Comb., 2014
HU-LI-ZHANG-FENG-GE, Des. Codes Cryptogr., 2015
QU, IEEE Trans. Inform. Theory, 2016

Exceptional Planar Functions

Theorem (B.-SCHMIDT, 2018.)

$f(X) \in \mathbb{F}_q[X]$, $\deg(f) \leq q^{1/4}$

$$f(X) \ \textcolor{red}{\textit{planar}} \ \textit{on} \ \mathbb{F}_q \iff f(X) = \sum_i a_i X^{2^i}$$

Exceptional Planar Functions

Theorem (B.-SCHMIDT, 2018.)

$f(X) \in \mathbb{F}_q[X]$, $\deg(f) \leq q^{1/4}$

$$f(X) \ \textcolor{red}{\textit{planar}} \ \textit{on}\ \mathbb{F}_q \iff f(X) = \sum_i a_i X^{2^i}$$

Proposition (Connection with algebraic surfaces)

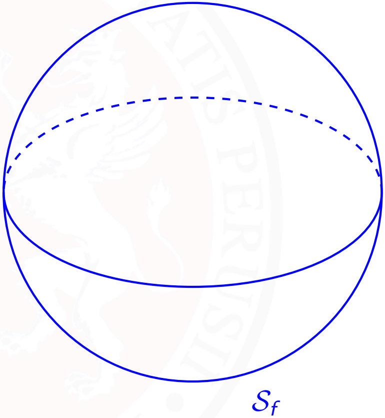
$f(X) \in \mathbb{F}_q[X]$ *planar* $\iff \mathcal{S}_f \ : \ \psi(X,Y,Z) = 0$

$$\psi(X,Y,Z) = 1 + \frac{f(X)+f(Y)+f(Z)+f(X+Y+Z)}{(X+Y)(X+Z)} \in \mathbb{F}_q[X,Y,Z]$$

has no affine $\mathbb{F}_q$-rational points off $X = Y$ and $Z = X$

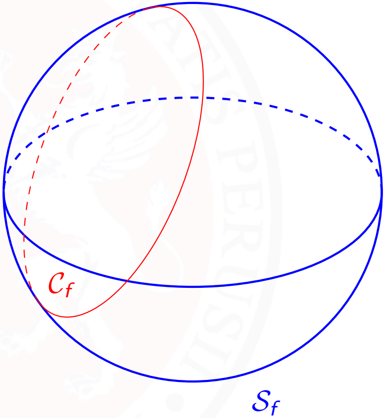
Proof Strategy

- Consider $\mathcal{S}_f$



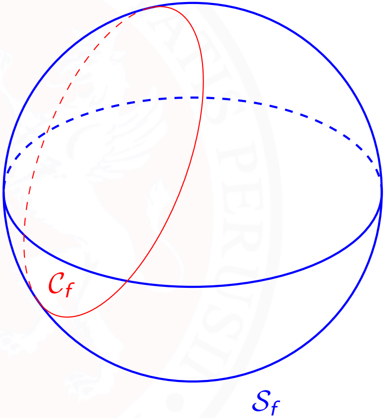
Proof Strategy

- Consider $\mathcal{S}_f$
- $\mathcal{C}_f = \mathcal{S}_f \cap \pi$



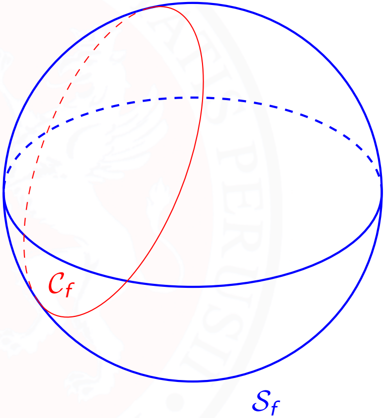
Proof Strategy

- Consider $\mathcal{S}_f$
- $\mathcal{C}_f = \mathcal{S}_f \cap \pi$
- $\mathcal{C}_f$ has $\mathbb{F}_q$-rational A.I. component



Proof Strategy

- Consider $\mathcal{S}_f$
- $\mathcal{C}_f = \mathcal{S}_f \cap \pi$
- $\mathcal{C}_f$ has $\mathbb{F}_q$-rational A.I. component
- Hasse-Weil $\Longrightarrow$ $\mathcal{S}_f$ has $\mathbb{F}_q$-rational points $(\overline{x}, \overline{y}, \overline{z})$, $\overline{x} \neq \overline{y}$, $\overline{x} \neq \overline{z}$, if q is large enough

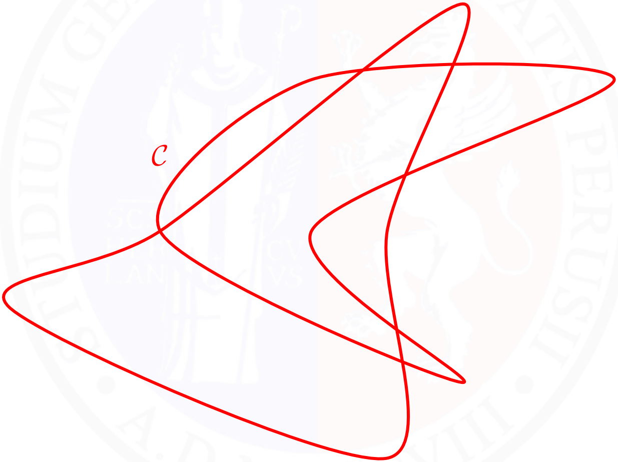


Another method based on singular points

JANWA-McGUIRE-WILSON, J. Algebra, 1995
JEDLICKA, Finite Fields Appl., 2007
HERNANDO-McGUIRE, J. Algebra, 2011
HERNANDO-McGUIRE, Des. Codes Cryptogr., 2012
HERNANDO-McGUIRE-MONSERRAT, Geometriae Dedicata, 2014
SCHMIDT-ZHOU, J. Algebraic Combin., 2014
LEDUCQ, Des. Codes Cryptogr., 2015
B.-ZHOU, J. Algebra, 2018

Another method based on singular points

- Consider a curve $\mathcal{C}$ defined by $F(X, Y) = 0$, $\deg(F) = d$



Another method based on singular points

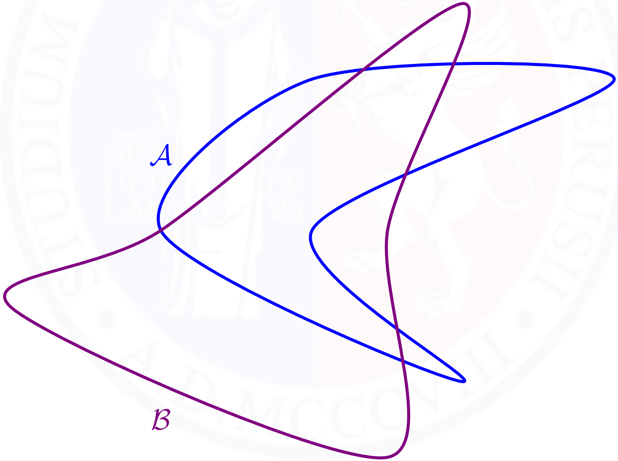
- Consider a curve $\mathcal{C}$ defined by $F(X, Y) = 0$, $\deg(F) = d$
- Suppose $\mathcal{C}$ has no A.I. components defined over $\mathbb{F}_q$

Another method based on singular points

- There are two components of $\mathcal{C}$

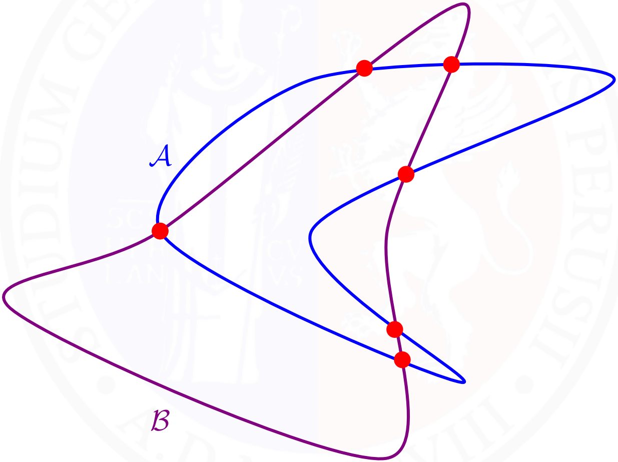
$$\mathcal{A} \; : \; A(X,Y) = 0, \quad \mathcal{B} \; : \; B(X,Y) = 0, \text{ with}$$

$$F(X,Y) = A(X,Y) \cdot B(X,Y), \quad \deg(A) \cdot \deg(B) \geq 2d^2/9$$



Another method based on singular points

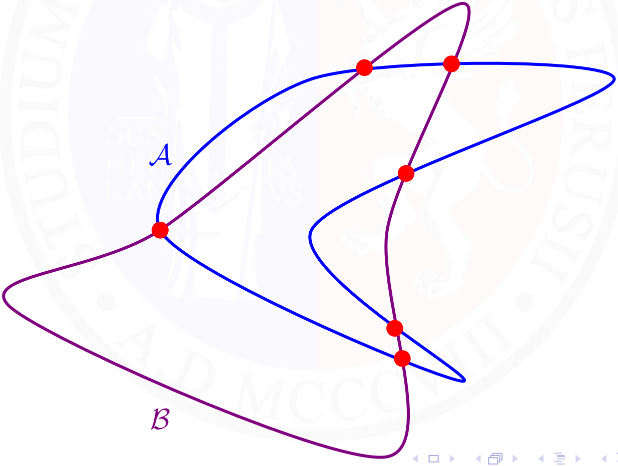
- $\mathcal{A} \cap \mathcal{B} \subset SING(\mathcal{C})$



Another method based on singular points

- $\mathcal{I}(P, \mathcal{A}, \mathcal{B}) \leq MAX_P$ for all $P \in SING(\mathcal{C})$

$$2d^2/9 \leq \overbrace{\deg(A) \cdot \deg(B) = \sum_{P \in \mathcal{A} \cap \mathcal{B}} \mathcal{I}(P, \mathcal{A}, \mathcal{B})}^{BEZOUT'S \quad THEOREM} \leq \sum_{P \in \mathcal{A} \cap \mathcal{B}} MAX_P$$



How to get a contradiction

$$2d^2/9 \leq \overbrace{\deg(A) \cdot \deg(B) = \sum_{P \in \mathcal{A} \cap \mathcal{B}} \mathcal{I}(P, \mathcal{A}, \mathcal{B})}^{BEZOUT'S\quad THEOREM} \leq \underbrace{\sum_{P \in \mathcal{A} \cap \mathcal{B}} MAX_P < 2d^2/9}_{CONTRADICTION}$$

How to get a contradiction

$$2d^2/9 \leq \overbrace{\deg(A) \cdot \deg(B) = \sum_{P \in \mathcal{A} \cap \mathcal{B}} \mathcal{I}(P, \mathcal{A}, \mathcal{B})}^{BEZOUT'S\quad THEOREM} \leq \underbrace{\sum_{P \in \mathcal{A} \cap \mathcal{B}} MAX_P < 2d^2/9}_{CONTRADICTION}$$

- Good estimates on $\mathcal{I}(P, \mathcal{A}, \mathcal{B})$, $P = (\xi, \eta)$
  - Analyzing the smallest homogeneous parts in

$$F(X + \xi, Y + \eta) = F_m(X, Y) + F_{m+1}(X, Y) + \cdots$$

  - Proving that there is a unique branch centered at P
  - Studying the structure of all the branches centered at P
- Good estimates on the number of singular points of $\mathcal{C}$

How to get a contradiction

$$2d^2/9 \le \overbrace{\deg(A)\cdot\deg(B) = \sum_{P\in\mathcal{A}\cap\mathcal{B}} \mathcal{I}(P,\mathcal{A},\mathcal{B})}^{BEZOUT'S\quad THEOREM} \le \underbrace{\sum_{P\in\mathcal{A}\cap\mathcal{B}} MAX_P < 2d^2/9}_{CONTRADICTION}$$

- Good estimates on $\mathcal{I}(P,\mathcal{A},\mathcal{B})$, $P=(\xi,\eta)$
  - Analyzing the smallest homogeneous parts in

$$F(X+\xi, Y+\eta) = F_m(X,Y) + F_{m+1}(X,Y) + \cdots$$

  - Proving that there is a unique branch centered at P
  - Studying the structure of all the branches centered at P
- Good estimates on the number of singular points of $\mathcal{C}$

Maximum Scattered linear sets in $\mathrm{PG}(1, q^n)$

$\mathrm{PG}(1, q^n) := \{(a : b) | a, b \in \mathbb{F}_{q^n}, (a, b) \neq (0, 0)\}$

Definition (Linear sets)

$\mathbb{U} \leq_q (\mathbb{F}_{q^n})^2$, $\dim(\mathbb{U}) = k$

$$L(\mathbb{U}) = \{(u : v) \ : \ (u, v) \in \mathbb{U} \setminus \{(0,0)\}\} \subset \mathrm{PG}(1, q^n)$$

$\mathbb{F}_q$-linear set of $\mathrm{PG}(1, q^n)$ of rank k

$f(X) = \sum_i a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$

$$\mathbb{U} = \{(x, f(x)) \ : \ x \in \mathbb{F}_{q^n}\} \leq (\mathbb{F}_{q^n})^2$$

Definition (Maximum scattered Linear sets in $\mathrm{PG}(1, q^n)$)

$$\begin{array}{l} \dim_q(\mathbb{U}) = n \\ |L(\mathbb{U})| = \frac{q^n - 1}{q - 1} \end{array} \Longrightarrow \begin{array}{l} L(\mathbb{U}) \text{ is Maximum scattered} \\ f(X) \text{ scattered polynomial [Sheekey, AMC 2016]} \end{array}$$

Scattered Polynomials of Low Degree

Definition

$$\mathbb{U} = \left\{(x^{q^t}, f(x)) \;:\; x \in \mathbb{F}_{q^n}\right\}$$

$L(\mathbb{U})$ maximum scattered linear set $\iff$ $f(x)$ scattered of index t

Scattered Polynomials of Low Degree

Definition

$$\mathbb{U} = \left\{ (x^{q^t}, f(x)) \ : \ x \in \mathbb{F}_{q^n} \right\} \iff f(x) \text{ scattered of index } t$$

$L(\mathbb{U})$ maximum scattered linear set

Lemma

$$\mathbb{U} = \left\{ (x^{q^t}, f(x)) \ : \ x \in \mathbb{F}_{q^n} \right\}$$

$L(\mathbb{U}) \subset \mathrm{PG}(1, q^n)$ *maximum scattered linear set* $\iff$

$$\mathcal{C}_f \ : \ \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0 \subset \mathrm{AG}(2, q^n)$$

contains only points (x, y) *with* $\frac{y}{x} \in \mathbb{F}_q$

$$\mathcal{C}_f \ : \ \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0$$

'small degree' $\iff$ $d \leq q^{n/4}$ in $\mathbb{F}_{q^n}$

Theorem (B.-ZHOU; J. Alg. 2018)

- X^{q^k}, $q > 5$
  unique scattered monic polynomial of small degree index 0
- X
  $bX + X^{q^2}$, $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b) \neq 1$
  unique scattered monic polynomials of small degree of index 1
  (if $q = 2$ then $f(X) = X$)

$$\mathcal{C}_f \; : \; \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0$$

'small degree' $\iff$ $d \leq q^{n/4}$ in $\mathbb{F}_{q^n}$

Theorem (B.-ZHOU; J. Alg. 2018)

- X^{q^k}, $q > 5$
  unique scattered monic polynomial of small degree index 0
- X
  $bX + X^{q^2}$, $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b) \neq 1$
  unique scattered monic polynomials of small degree of index 1
  (if $q = 2$ *then* $f(X) = X$*)*

Branches centered at singular points $\Longrightarrow$ *better estimates for* $\mathcal{I}(P, \mathcal{A}, \mathcal{B})$

$$\mathcal{C}_f \ : \ \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0$$

'small degree' $\iff$ $d \leq q^{n/4}$ in $\mathbb{F}_{q^n}$

Theorem (B.-ZHOU; J. Alg. 2018)

- X^{q^k}, $q > 5$
  unique scattered monic polynomial of small degree index 0
- X
  $bX + X^{q^2}$, $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b) \neq 1$
  unique scattered monic polynomials of small degree of index 1
  (if $q = 2$ then $f(X) = X$)

Branches centered at singular points $\Longrightarrow$ *better estimates for* $\mathcal{I}(P, \mathcal{A}, \mathcal{B})$

(B.-MONTANUCCI, JCTA 2021)

$t = 2 \Longrightarrow$ *only monomials or binomials*

Further applications

- Arcs, caps in projective spaces: Anbar, Giulietti, Platoni, Zini, Marcugini, Pambianco, Speziali, Marino, Polverino
- Semiovals and Blocking semiovals: Kiss, Marcugini, Pambianco, Pavese
- Ovoids of $Q(4, q)$, $Q(5, q)$, $Q(6, q)$: Durante, Grimaldi
- Resolving sets: Kiss, Marcugini, Pambianco
- Permutation polynomials: Giulietti, Zini, Quoos, Timpanella, Bonini, Hou
- PN, APN, APcN functions: Schmidt, Calderini, Timpanella, Ghiandoni, Fatabbi, Bonini
- Kloosterman polynomials: Li, Zhou
- Moore exponent sets: Zhou
- Maximum scattered linear sets: Zanella, Zullo, Montanucci, Csajbók, Giulietti, Zini, Zullo
- r-fat linearized polynomials: Micheli, Zini, Zullo

THANK YOU

FOR YOUR ATTENTION

How to get a contradiction

$$2d^2/9 \le \overbrace{\deg(A)\cdot\deg(B) = \sum_{P\in\mathcal{A}\cap\mathcal{B}} \mathcal{I}(P,\mathcal{A},\mathcal{B})}^{BEZOUT'S\quad THEOREM} \le \underbrace{\sum_{P\in\mathcal{A}\cap\mathcal{B}} MAX_P < 2d^2/9}_{CONTRADICTION}$$

- Good estimates on $\mathcal{I}(P,\mathcal{A},\mathcal{B})$, $P=(\xi,\eta)$
  - Analyzing the smallest homogeneous parts in

$$F(X+\xi, Y+\eta) = F_m(X,Y) + F_{m+1}(X,Y) + \cdots$$

  - Proving that there is a unique branch centered at P
  - Studying the structure of all the branches centered at P
- Good estimates on the number of singular points of $\mathcal{C}$

Another application: β-planar functions

Definition (Planar functions, odd characteristic)

$f(X) \in \mathbb{F}_q[X]$ is planar polynomial if

$$\forall \epsilon \in \mathbb{F}_q^* \quad x \mapsto f(x+\epsilon) - f(x) \text{ BIJECTION}$$

Another application: β-planar functions

Definition (Planar functions, odd characteristic)

$f(X) \in \mathbb{F}_q[X]$ is planar polynomial if

$$\forall \epsilon \in \mathbb{F}_q^* \quad x \mapsto f(x+\epsilon) - f(x) \text{ BIJECTION}$$

Definition (β-Planar functions, odd characteristic)

$\beta \in \mathbb{F}_q \setminus \{0,1\}$, $f(X) \in \mathbb{F}_q[X]$ is β-planar polynomial if

$$\forall \epsilon \in \mathbb{F}_q \quad x \mapsto f(x+\epsilon) - \beta f(x) \text{ BIJECTION}$$

Another application: β-planar functions

Definition (Planar functions, odd characteristic)

$f(X) \in \mathbb{F}_q[X]$ is planar polynomial if

$$\forall \epsilon \in \mathbb{F}_q^* \quad x \mapsto f(x+\epsilon) - f(x) \text{ BIJECTION}$$

Definition (β-Planar functions, odd characteristic)

$\beta \in \mathbb{F}_q \setminus \{0,1\}$, $f(X) \in \mathbb{F}_q[X]$ is β-planar polynomial if

$$\forall \epsilon \in \mathbb{F}_q \quad x \mapsto f(x+\epsilon) - \beta f(x) \text{ BIJECTION}$$

Theorem (B.-TIMPANELLA, J. Alg. Combin. 2020)

$\beta \in \mathbb{F}_{p^r} \setminus \{0,-1\}$, *$k$ such that* $(t-1) \mid (p^k - 1)$
$p \nmid t \leq \sqrt[4]{p^r}$, *$X^t$ is NOT β-planar if*

1. $p \nmid t-1$, $\quad p \nmid \prod_{m=1}^{7} \prod_{\ell=-7}^{7-m} m\frac{p^k-1}{t-1} + \ell$, $\quad t \geq 470$;
2. $t = p^\alpha m + 1,\ (p,\alpha) \neq (3,1),\ \alpha \geq 1,\ p \nmid m,\ m \neq p^r - 1\ \forall\ r \mid \ell$, *where* $\ell = \min_i\{m \mid p^i - 1, \beta^{(p^i-1)/m} = 1\}$.

Another application: β-planar functions

$$\mathcal{C} \ : \ F(X,Y) = \frac{(X+1)^t - (Y+1)^t - \beta(X^t - Y^t)}{X - Y} \in \mathbb{F}_{p^r}[X,Y].$$

Another application: β-planar functions

$$\mathcal{C} \;:\; F(X,Y) = \frac{(X+1)^t - (Y+1)^t - \beta(X^t - Y^t)}{X-Y} \in \mathbb{F}_{p^r}[X,Y].$$

Singular points $SING(\mathcal{C})$ satisfy

$$\begin{cases} \left(\frac{X+1}{X}\right)^{t-1} = \beta \\ \left(\frac{X}{Y}\right)^{t-1} = 1 \\ \left(\frac{X+1}{Y+1}\right)^{t-1} = 1 \end{cases}$$

Another application: β-planar functions

$$\mathcal{C} \; : \; F(X,Y) = \frac{(X+1)^t - (Y+1)^t - \beta(X^t - Y^t)}{X-Y} \in \mathbb{F}_{p^r}[X,Y].$$

Singular points $SING(\mathcal{C})$ satisfy

$$\begin{cases} \left(\frac{X+1}{X}\right)^{t-1} = \beta \\ \left(\frac{X}{Y}\right)^{t-1} = 1 \\ \left(\frac{X+1}{Y+1}\right)^{t-1} = 1 \end{cases}$$

We use estimates on the number of points of particular Fermat curves

GARCIA-VOLOCH, Manuscripta Math., 1987
GARCIA-VOLOCH, J. Number Theory, 1988