Relevant classes of polynomial functions with applications to Cryptography

Daniele Bartoli
University of Perugia, Italy

BFA 2023
The 8th International Workshop on Boolean Functions and their Applications

Voss, September 3-8, 2023

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
   - Planar polynomials in char 2
   - APN rational functions
   - APcN/PcN functions
   - Crooked functions

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 $\mathbb{F}_7$?

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

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

Toy example: a permutation problem

Example

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

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

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

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* $\mathbb{F}_7$

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

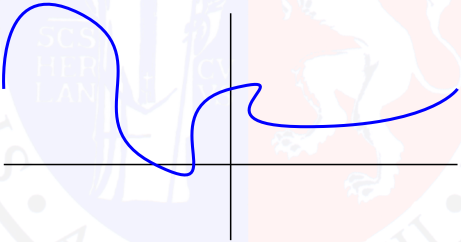
$$2X + 7Y^2 + 3 \iff 4X + 14Y^2 + 6$$

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, $s \notin \square_q$,
$\Longrightarrow (X-\eta Y)(X+\eta Y)$, $\eta^2=s$, $\eta \in \mathbb{F}_{q^2}$ 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

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

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

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

Example

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

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

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

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 $X - Y = 0$

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

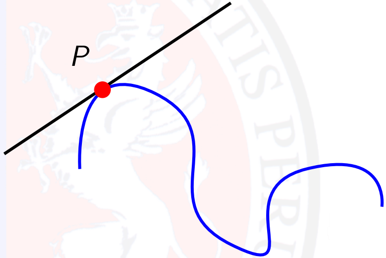
An easy criterion

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)

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

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

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

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

Definition (Frobenius automorphism)

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

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

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

$\varphi_q(\alpha) = \alpha \iff \alpha \in \mathbb{F}_q$
$\varphi_q(\alpha, \beta) = (\alpha, \beta) \iff (\alpha, \beta) \in \mathbb{A}^2(\mathbb{F}_q)$
$\varphi_q(\mathcal{C}) = \mathcal{C} \iff \lambda F \in \mathbb{F}_q[X, Y]$ *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

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

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

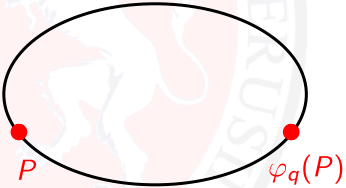
Frobenius automorphism and $\mathbb{F}_q$-rational components

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

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



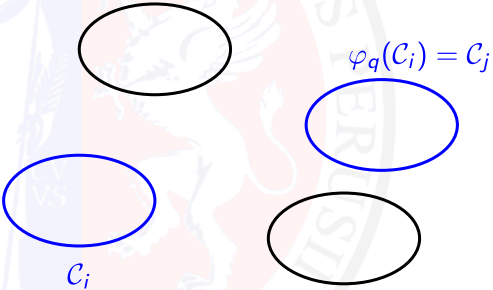
Frobenius automorphism and $\mathbb{F}_q$-rational components

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

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

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

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



Remark

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

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

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

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

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

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

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

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* $\mathbb{F}_q$

$P = \varphi_q(P)$

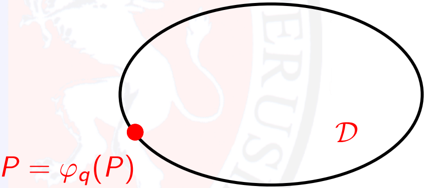
Existence of absolutely irreducible $\mathbb{F}_q$-rational components

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* $\mathbb{F}_q$



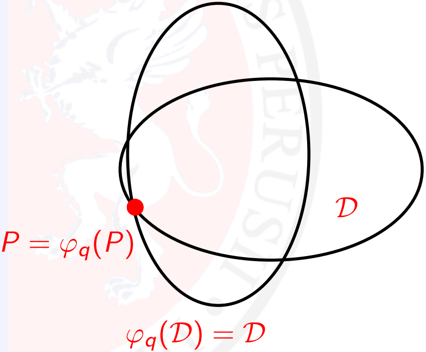
Existence of absolutely irreducible $\mathbb{F}_q$-rational components

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* $\mathbb{F}_q$



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

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

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

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

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)

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

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

Exceptional Planar Functions

Theorem (B.-SCHMIDT, 2018)

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

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

Proposition (Connection with algebraic surfaces)

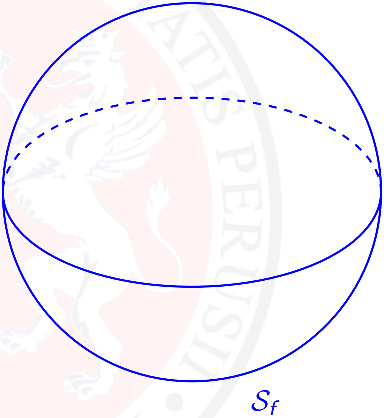
$f(X) \in \mathbb{F}_q[X]$ *planar* $\iff \mathcal{S}_f \; : \; \psi(X, Y, Z) = 0$

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

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

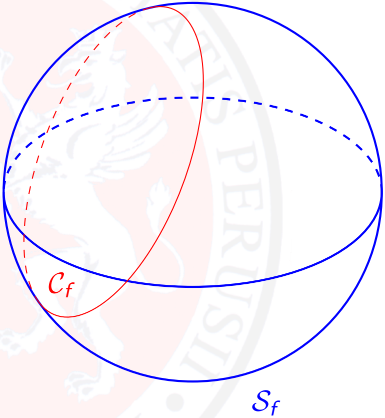
Proof Strategy

- Consider $\mathcal{S}_f$



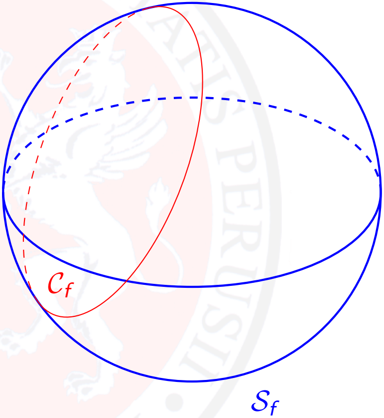
Proof Strategy

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



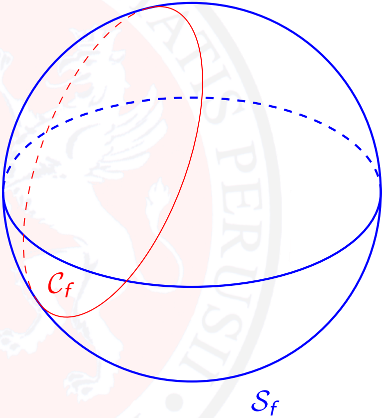
Proof Strategy

- 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 $\implies$ $\mathcal{S}_f$ 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

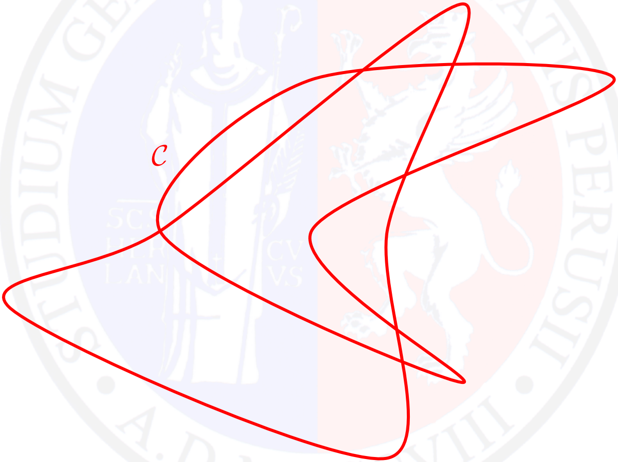


Another method based on singular points

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

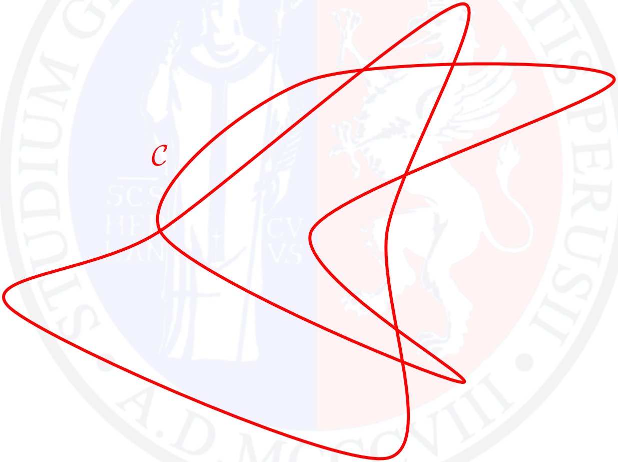
Another method based on singular points

- 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 $\mathbb{F}_q$

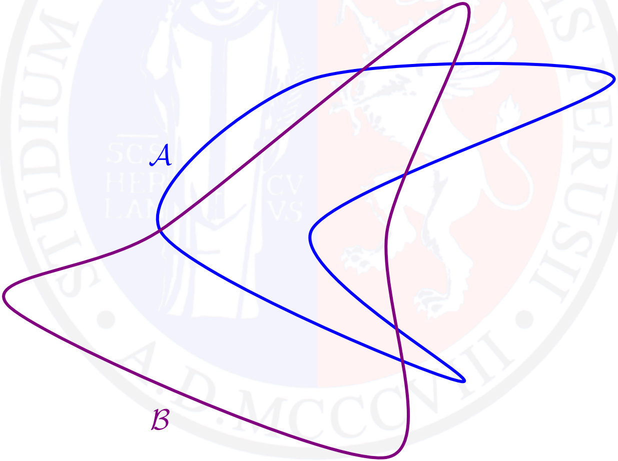


Another method based on singular points

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

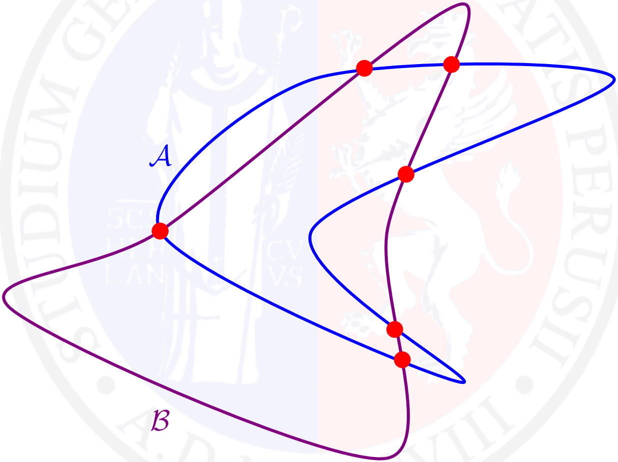
$$\mathcal{A} \ : \ A(X,Y) = 0, \quad \mathcal{B} \ : \ B(X,Y) = 0, \text{ with}$$

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



Another method based on singular points

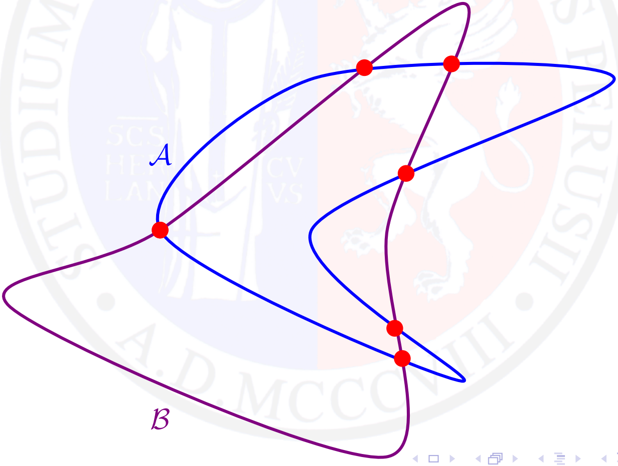
- $\mathcal{A} \cap \mathcal{B} \subset SING(\mathcal{C})$



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 $\mathcal{C}$

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 $\mathcal{C}$

Another application: Exceptional APN rational functions

Definition

$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN (Almost Perfect Nonlinear) if

$$\forall \alpha, \beta \in \mathbb{F}_{2^n}, \quad \alpha \neq 0, \Longrightarrow f(x+\alpha) + f(x) = \beta$$

has at most two solutions.
If f is APN over $\mathbb{F}_{2^{mn}}$ for infinitely many extensions $\mathbb{F}_{2^{mn}}$ of $\mathbb{F}_{2^n}$, f is said to be exceptional APN

Another application: Exceptional APN rational functions

Definition

$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN (Almost Perfect Nonlinear) if

$$\forall \alpha, \beta \in \mathbb{F}_{2^n}, \quad \alpha \neq 0, \Longrightarrow f(x+\alpha) + f(x) = \beta$$

has at most two solutions.
If f is APN over $\mathbb{F}_{2^{mn}}$ for infinitely many extensions $\mathbb{F}_{2^{mn}}$ of $\mathbb{F}_{2^n}$, f is said to be exceptional APN

Theorem (Rodier, 2009)

$f \in \mathbb{F}_{2^n}[X]$ APN over $\mathbb{F}_{2^n}$ $\iff$ the surface

$$S_f : \varphi_f(X,Y,Z) := \frac{f(X)+f(Y)+f(Z)+f(X+Y+Z)}{(X+Y)(X+Z)(Y+Z)} = 0$$

has no affine $\mathbb{F}_{2^n}$-rational points off the planes $X = Y$, $X = Z$ e $Y = Z$.

Another application: Exceptional APN rational functions

Only polynomial functions have been considered so far (mostly)

Every function $h : \mathbb{F}_q \to \mathbb{F}_q$ can be described by a polynomial of degree at most $q-1$

Another application: Exceptional APN rational functions

Only polynomial functions have been considered so far (mostly)

Every function $h : \mathbb{F}_q \to \mathbb{F}_q$ can be described by a polynomial of degree at most $q-1$

non-existence results obtained via algebraic varieties require low degree

Another application: Exceptional APN rational functions

Only polynomial functions have been considered so far (mostly)

Every function $h : \mathbb{F}_q \to \mathbb{F}_q$ can be described by a polynomial of degree at most $q-1$

non-existence results obtained via algebraic varieties require low degree

It could be useful to investigate functions $h : \mathbb{F}_q \to \mathbb{F}_q$ described by rational functions $f(x)/g(x)$ of "low degree" to get new non-existence results

Another application: Exceptional APN rational functions

Let consider

- $q = 2^{19}$;
- $\psi : \mathbb{F}_q \to \mathbb{F}_q, \quad x \mapsto \dfrac{x}{x^3 + x + 1}$.
- $h \in \mathbb{F}_q[X]$, $\deg(h) \leq q - 1$, *such that* $\psi(x) = h(x)$ *for any* $x \in \mathbb{F}_q$.

Another application: Exceptional APN rational functions

Let consider

- $q = 2^{19}$;
- $\psi : \mathbb{F}_q \to \mathbb{F}_q, \quad x \mapsto \dfrac{x}{x^3 + x + 1}$.
- $h \in \mathbb{F}_q[X]$, $\deg(h) \leq q - 1$, *such that* $\psi(x) = h(x)$ *for any* $x \in \mathbb{F}_q$.

By the Lagrange Interpolation Formula

$$h(X) = \sum_{a \in \mathbb{F}_q} \psi(a)(1 - (X - a)^{q-1})$$

Another application: Exceptional APN rational functions

Let consider

- $q = 2^{19}$;
- $\psi : \mathbb{F}_q \to \mathbb{F}_q, \quad x \mapsto \dfrac{x}{x^3 + x + 1}$.
- $h \in \mathbb{F}_q[X]$, $\deg(h) \le q - 1$, *such that* $\psi(x) = h(x)$ *for any* $x \in \mathbb{F}_q$.

By the Lagrange Interpolation Formula

$$h(X) = \sum_{a \in \mathbb{F}_q} \psi(a)(1 - (X - a)^{q-1})$$

and by computations with MAGMA,

$$\deg(f) = q - 1 > \sqrt[4]{q}$$

so Rodier's result cannot be applied.

Another application: Exceptional APN functions

However, one can consider

- *the rational representation* $\psi = \frac{f}{g} = \frac{X}{X^3+X+1} \in \mathbb{F}_q(X)$
- *the corresponding surface*

$$S_\psi = \frac{\frac{f}{g}(X) + \frac{f}{g}(Y) + \frac{f}{g}(Z) + \frac{f}{g}(X+Y+Z)}{(X+Y)(X+Z)(Y+Z)}$$

S_ψ *has degree* 10*, so the investigation of its* $\mathbb{F}_q$*-rational points becomes feasible by means of Lang-Weil bound.*

Another application: Exceptional APN rational functions

- $q = 2^n$,
- $\mathbb{F}_q(X)$ rational field over $\mathbb{F}_q$.
- $\psi = \frac{f}{g} \in \mathbb{F}_q(X)$

$$
\begin{aligned}
f &= a_m X^m + a_{m-1} X^{m-1} + \cdots + a_{i+1} X^{i+1} + a_i X^i, \\
g &= b_d X^d + b_{d-1} X^{d-1} + \cdots + b_1 X + b_0,
\end{aligned}
$$

$g(x) \neq 0$ for all $x \in \mathbb{F}_q$, $a_m \neq 0 \neq b_d$, and $a_i \neq 0$.

Link with algebraic surfaces

Proposition

ψ APN over $\mathbb{F}_q$ $\iff$

$$S_\psi : \varphi_\psi(X,Y,Z) := \frac{\theta_\psi(X,Y,Z)}{(X+Y)(X+Z)(Y+Z)} = 0,$$

$$\begin{aligned}\theta_\psi(X,Y,Z) := {} & f(X)g(Y)g(Z)g(X+Y+Z) + f(Y)g(X)g(Z)g(X+Y+Z) + \\ & + f(Z)g(X)g(Y)g(X+Y+Z) + f(X+Y+Z)g(X)g(Y)g(Z),\end{aligned}$$

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

Another application: Exceptional APN rational functions

Theorem (B.-FATABBI-GHIANDONI, 2023)

- $\deg(f) - \deg(g) = 2\ell$, $\ell > 0$ *odd*
  - $g \notin \mathbb{F}_q[X^p]$, *or*
  - $f' \neq \gamma g$ *for all* $\gamma \in \mathbb{F}_q$ $\quad\Longrightarrow\quad$ $\psi = \frac{f}{g}$ *is not exceptional APN*
- $\deg(g) - \deg(f) = \ell$, $\ell > 1$ *odd*
- $\deg(f) = 1$

1. Intersection with specific hyperplanes
2. Lang-Weil bound for surfaces

Another application: c-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: c-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 (c-Planar functions, odd characteristic)

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

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

[P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C*-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity, 2020]

Another application: c-planar functions

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

$c \in \mathbb{F}_{p^r} \setminus \{0,-1\}$, *k such that* $(t-1) \mid (p^k-1)$
$p \nmid t \leq \sqrt[4]{p^r}$, X^t *is NOT c-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* $\ell = \min_i\{m \mid p^i - 1, c^{(p^i-1)/m} = 1\}$.

Another application: c-planar functions

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

Another application: c-planar functions

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

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

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

Another application: c-planar functions

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

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

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

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

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

Another application: Crooked functions

Definition

$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ crooked if

1. $f(0) = 0$
2. $f(x) + f(y) + f(z) + f(x + y + z) \neq 0$ for any x, y, z distinct
3. $f(x) + f(y) + f(z) + f(x + a) + f(y + a) + f(z + a) \neq 0$ for any x, y, z, and $a \neq 0$

$$\mathcal{W}_f : \frac{f(X)+f(Y)+f(Z)+f(X+U)+f(Y+U)+f(Z+U)}{U} = 0$$

Theorem

$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(0) = 0$

If there exists an affine $\mathbb{F}_{2^n}$-rational point $P \in \mathcal{W}_f$ not lying on $U = 0$, then $f(X)$ is not crooked over $\mathbb{F}_{2^n}$.

Theorem

Let $g(X) = (f(X))^{2^j}$, $j \geq 0$, $f(X) = \sum_{i=0}^{d} a_i X^i$, $a_d \neq 0$. $g(X)$ exceptional crooked function implies one of the following cases

- $f(X) = X^{2^k+1} + h(X)$, $\deg(h(X)) = 2^j + 1$, *and $f(X)$ is quadratic;*
- $f(X) = X^{2^k+1} + h(X)$, *where* $\deg(h(X)) \geq 2^{k-1} + 2$ *is even;*
- $d = 4e + \ldots$

[B.-CALDERINI-TIMPANELLA, Exceptional crooked functions, 2022]

$$\mathcal{W}_f : \frac{f(X)+f(Y)+f(Z)+f(X+U)+f(Y+U)+f(Z+U)}{U} = 0$$

Theorem

$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(0) = 0$

If there exists an affine $\mathbb{F}_{2^n}$-rational point $P \in \mathcal{W}_f$ not lying on $U = 0$, then $f(X)$ is not crooked over $\mathbb{F}_{2^n}$.

Theorem

Let $g(X) = (f(X))^{2^j}$, $j \geq 0$, $f(X) = \sum_{i=0}^{d} a_i X^i$, $a_d \neq 0$. $g(X)$ exceptional crooked function implies one of the following cases

- $f(X) = X^{2^k+1} + h(X)$, $\deg(h(X)) = 2^j + 1$, *and $f(X)$ is quadratic;*
- $f(X) = X^{2^k+1} + h(X)$, *where* $\deg(h(X)) \geq 2^{k-1} + 2$ *is even;*
- $d = 4e + \ldots$

1. Existence of simple $\mathbb{F}_q$-rational points
2. Direct proofs of irreducibility

Another application: c-differential uniformity

Definition (c-Planar functions)

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

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

Another application: c-differential uniformity

Definition (c-Planar functions)

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

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

What about the maximum number of solutions of

$$f(x+\epsilon) - cf(x) = \beta,$$

for $\beta \in \mathbb{F}_q$?

Another application: c-differential uniformity

Definition (c-Planar functions)

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

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

What about the maximum number of solutions of

$$f(x+\epsilon) - cf(x) = \beta,$$

for $\beta \in \mathbb{F}_q$?

$f(x) = x^d$

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

Another application: c-differential uniformity

Theorem

$p \nmid d(d-1)$

$$c \neq \left(\frac{1-\xi^i}{\xi^k-\xi^j}\right)^{d-1}, \qquad \xi^{d-1}=1, i,j,k \in \{0,\dots,d-2\}$$

Then the c-uniformity of x^d is d (asymptotically)

[B.-CALDERINI, On construction and (non)existence of c-(almost) perfect nonlinear functions. Finite Fields Their Appl. 2021]

Another application: c-differential uniformity

Theorem

$p \nmid d(d-1)$

$$c \neq \left(\frac{1-\xi^i}{\xi^k - \xi^j}\right)^{d-1}, \qquad \xi^{d-1} = 1, i, j, k \in \{0, \ldots, d-2\}$$

Then the c-uniformity of x^d is d (asymptotically)

[B.-CALDERINI, On construction and (non)existence of c-(almost) perfect nonlinear functions. Finite Fields Their Appl. 2021]

1. Algebraic curves
2. Monodromy groups of function field extensions

THANK YOU

FOR YOUR ATTENTION

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}

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

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

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