Functions with low c-differential uniformity

Daniele Bartoli

University of Perugia, Italy

CRYPTO CONFERENCE 2021

Torino - 27/05/2021

Outline

1. Algebraic curves over finite fields

Outline

1. Algebraic curves over finite fields
2. How to prove absolutely irreducibility?
3. How to prove existence of absolutely irreducible $\mathbb{F}_q$-components?

Outline

1. Algebraic curves over finite fields
2. How to prove absolutely irreducibility?
3. How to prove existence of absolutely irreducible $\mathbb{F}_q$-components?
4. Applications to differential uniformity of polynomials

What is a curve?

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

Definition (Affine plane)

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

What is a curve?

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

Definition (Affine plane)

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

Definition (Curve)

$\mathcal{C}$ in $AG(2, q)$ 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)

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

Definition (Curve)

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

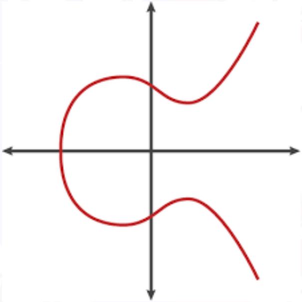
$$2X + 7Y^2 + 3 \iff 4X + 14Y^2 + 6$$

What is a curve?

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

Definition

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



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

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!

Definition

$f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, and $c \in \mathbb{F}_{p^n}$,

$$\underbrace{{}_cD_a f(x) = f(x+a) - cf(x)}_{\substack{\text{(multiplicative) c-derivative} \\ \text{of } f \text{ w.r.t. } a \in \mathbb{F}_{p^n}}} \quad , \qquad \forall x \in \mathbb{F}_{p^n}.$$

$${}_c\Delta_f(a,b) := |\{x \in \mathbb{F}_{p^n} \ : \ f(x+a) - cf(x) = b\}|,$$

and

$${}_c\Delta_f := \max\{{}_c\Delta_f(a,b) \ : \ a, b \in \mathbb{F}_{p^n}, (a,c) \neq (0,1)\},$$

${}_c\Delta_f \to c$-differential uniformity of f

- $c = 1 \to$ usual derivative of f and its differential uniformity
- ${}_c\Delta_f = 1 \to f$ is PcN
- ${}_c\Delta_f = 2 \to f$ is APcN

[Ellingsen, Felke, Riera, Stănică, Tkachenko, IEEE Trans. Inform. Theory 2020]

Planar Functions, q odd

Definition (Planar Function, q odd)

q odd prime power

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

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

Planar Functions, q odd

Definition (Planar Function, q odd)

q odd prime power
$f : \mathbb{F}_q \to \mathbb{F}_q$ planar or perfect nonlinear if

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

- 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.

Planar Functions, q even

Definition (Planar Function, q even)

q even

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

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

Planar Functions, q even

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

Planar Functions, q even

Theorem (B.-SCHMIDT, J. Algebra 2018)

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

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

Planar Functions, q even

Theorem (B.-SCHMIDT, J. Algebra 2018)

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

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

Proposition (Connection with algebraic surfaces)

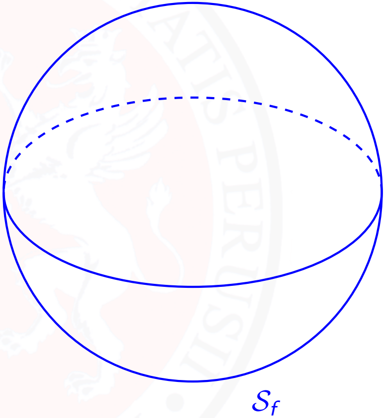
$f(X) \in \mathbb{F}_q[X]$ *planar* $\iff \mathcal{S}_f \; : \; \psi(X, Y, W) = 0$

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

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

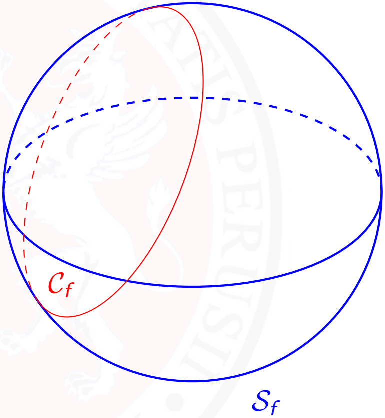
Proof Strategy

- Consider $\mathcal{S}_f$



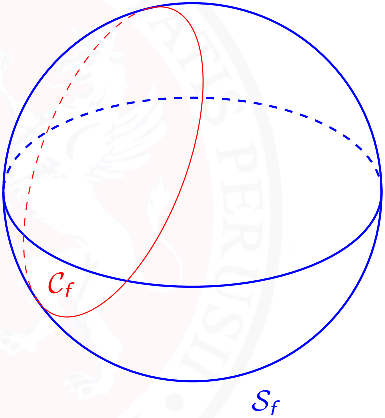
Proof Strategy

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



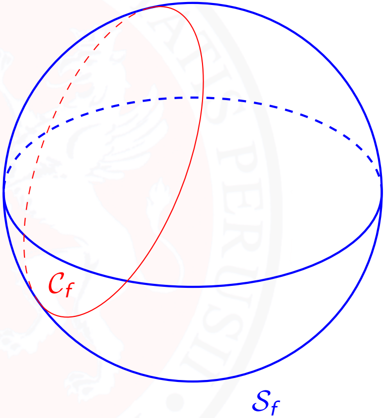
Proof Strategy

- 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 $\Longrightarrow$ $\mathcal{C}_f$ has "good" points if q is large enough



Theorem

Suppose $f(x)$ not linearized

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

Then $\mathcal{C}_f$ is $\mathbb{F}_q$-birationally equivalent to $\mathcal{C}'_f$ and $\mathcal{C}'_f$ contains an absolutely irreducible $\mathbb{F}_q$-rational component

Theorem

Suppose $f(x)$ not linearized

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

Then $\mathcal{C}_f$ is $\mathbb{F}_q$-birationally equivalent to $\mathcal{C}'_f$ and $\mathcal{C}'_f$ contains an absolutely irreducible $\mathbb{F}_q$-rational component

Also $\mathcal{C}_f$ contains an absolutely irreducible $\mathbb{F}_q$-rational component $\mathcal{D}$

Theorem

Suppose $f(x)$ not linearized

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

Then $\mathcal{C}_f$ is $\mathbb{F}_q$-birationally equivalent to $\mathcal{C}'_f$ and $\mathcal{C}'_f$ contains an absolutely irreducible $\mathbb{F}_q$-rational component

Also $\mathcal{C}_f$ contains an absolutely irreducible $\mathbb{F}_q$-rational component $\mathcal{D}$

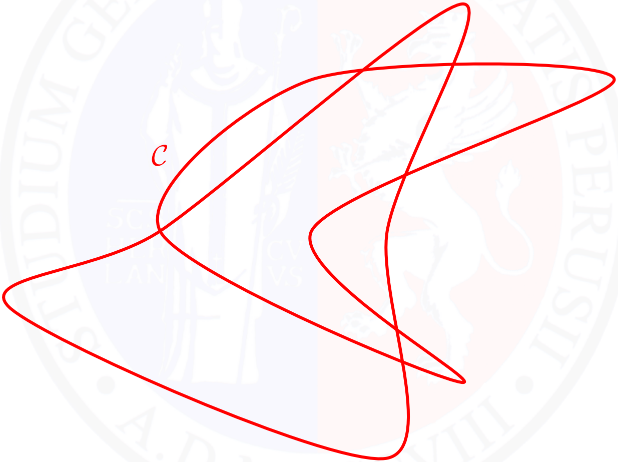
If $\deg f(x)$ small enough $\mathcal{D}$ has good points and $f(x)$ is not planar

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

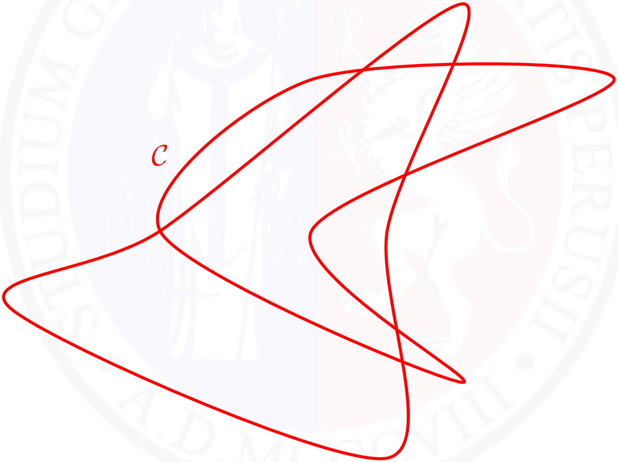
Another method based on singular points

- 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 $\mathbb{F}_q$

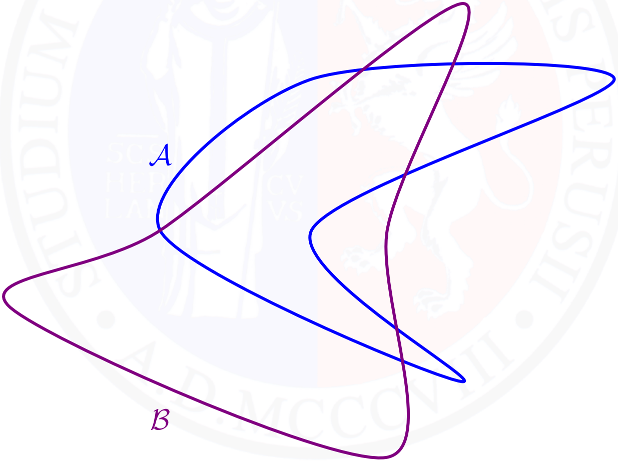


Another method based on singular points

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

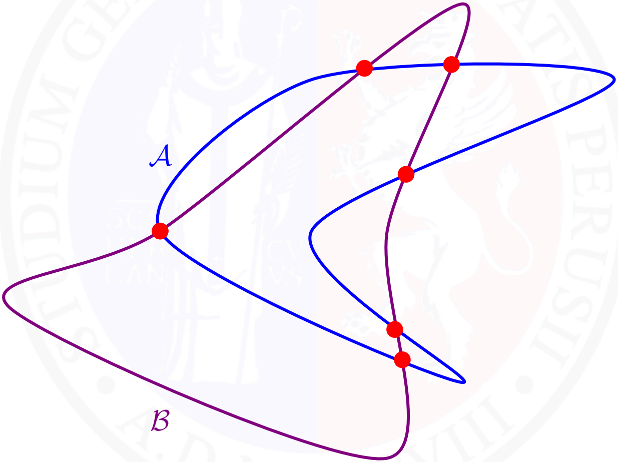
$$\mathcal{A} \ : \ A(X,Y) = 0, \quad \mathcal{B} \ : \ B(X,Y) = 0, \text{ with}$$

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



Another method based on singular points

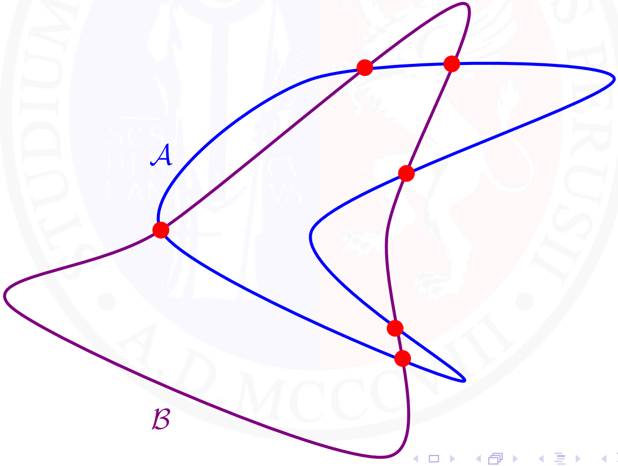
- $\mathcal{A} \cap \mathcal{B} \subset SING(\mathcal{C})$



Another method based on singular points

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

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



How to get a contradiction

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

How to get a contradiction

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

- 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 $\mathcal{C}$

Non-existence results for PcN-monomials

Theorem

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

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

[B.-TIMPANELLA, J. Alg. Combin. 2020]

Non-existence results for PcN monomials

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

Non-existence results for PcN monomials

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

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

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

Non-existence results for PcN monomials

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

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

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

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

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

Non-existence results for APcN monomials x^d

$p \nmid d(d-1)$, s the smallest positive integer such that $d-1 \mid (p^s-1)$

$$\forall a, b \in \mathbb{F}_q \Longrightarrow (x+a)^d - cx^d = b \text{ has at most two solutions.}$$

$$(d, q-1) \leq 2 \qquad \textit{and}$$

$$\forall b \in \mathbb{F}_q \Longrightarrow (x+1)^d - cx^d = b \textit{ has at most two solutions}$$

$$\mathcal{C}_{f,c} \; : \; \frac{(X+1)^d - (Y+1)^d - c(X^d - Y^d)}{X-Y} = 0$$

Remark

The existence of an $\mathbb{F}_q$-rational component in $\mathcal{C}_{f,c}$ is not enough to exclude the APcN case

[B.-CALDERINI, FFA 2021]

Non-existence results for APcN monomials x^d

Proposition

$\sqrt[d-1]{c} \notin \mathbb{F}_{p^s} \Longrightarrow \mathcal{C}_{f,c}$ *is nonsingular* $\Longrightarrow \mathcal{C}_{f,c}$ *is absolutely irreducible*

$$F_{c,d} := (x+1)^d - cx^d - t$$

$$\begin{aligned} G_{c,d}^{arith} &= \mathrm{Gal}(F_{c,d}(t,x) : \mathbb{F}_q(t)) \\ G_{c,d}^{geom} &= \mathrm{Gal}(F_{c,d}(t,x) : \overline{\mathbb{F}}_q(t)) \end{aligned}$$

Proposition

$$\mathcal{S}_d = G_{c,d}^{geom} \leq G_{c,d}^{arith} \leq \mathcal{S}_d$$

Non-existence results for APcN monomials x^d

[G. Micheli, SIAM J. Appl. Algebra Geometry 2019]
[G. Micheli, IEEE Trans. Inform. Theory 2020]

Theorem

$\sqrt[d-1]{c} \notin \mathbb{F}_{p^s}$ *and* q *is large enough*
$\exists t_0 \in \mathbb{F}_q$ *such that* $(x+1)^d - cx^d = t_0$ *has* d *solutions in* $\mathbb{F}_q$

Remark

$\sqrt[d-1]{c} \notin \mathbb{F}_{p^s}$ *and* q *is large enough*

$$ {}_c\Delta_{x^d} = d $$

Rational PN or APN functions

Only polynomial functions have been considered so far

Remark

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

Rational PN or APN functions

Only polynomial functions have been considered so far

Remark

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

Remark

non-existence results obtained via algebraic varieties require low degree

Rational PN or APN functions

Only polynomial functions have been considered so far

Remark

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

Remark

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

APN rational functions

[B.-FATABBI-GHIANDONI, in preparation 202?]

Proposition

q *even*, $\psi = \frac{f}{g} \in \mathbb{F}_q(X)$, $g(x) \neq 0$ *forall* $x \in \mathbb{F}_q$ $(f, g) = 1$

ψ *is APN over* $\mathbb{F}_q$ $\iff$ $S_\psi : \dfrac{\theta_\psi(X,Y,Z)}{(X+Y)(X+Z)(Y+Z)} = 0$ *has no* $\mathbb{F}_q$*-rational points off* $X = Y$, $X = Z$, $Y = Z$

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

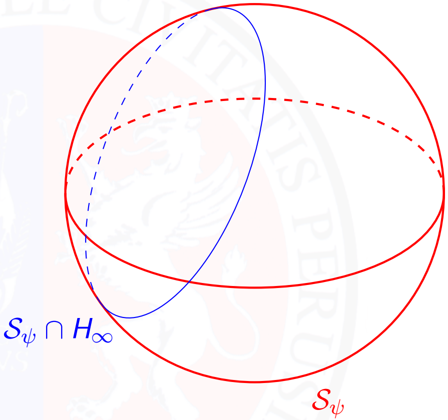
APN rational functions

$\deg(f) - \deg(g) = 2\ell$, $\ell > 0$ odd

- $g \notin \mathbb{F}_q[X^p]$; or
- $f' \neq \gamma g$ for all $\gamma \in \mathbb{F}_q$

$\deg(g) - \deg(f) = 2\ell$, $\ell > 0$ odd

- $\ell \equiv 1 \pmod 4$; or
- $\ell \equiv 3 \pmod 8$



Proposition

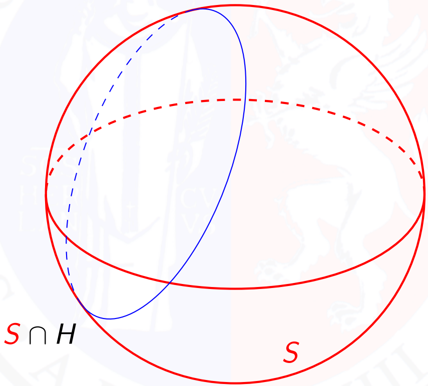
$\mathcal{S}_\psi \cap H_\infty$ contains a non-repeated absolutely irreducible component defined over $\mathbb{F}_q$

Proposition

$H \subset \mathrm{PG}(3, q)$ hyperplane

$S \cap H$ has non-repeated absolutely irreducible component over $\mathbb{F}_q$

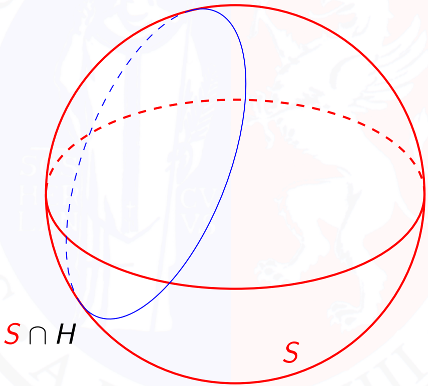
$\implies S$ has a non-repeated absolutely irreducible component over $\mathbb{F}_q$



[Aubry, McGuire, Rodier, Contemp. Math. 2010]

Proposition

$H \subset \mathrm{PG}(3,q)$ hyperplane
$S \cap H$ has non-repeated absolutely irreducible component over $\mathbb{F}_q$
$\implies S$ has a non-repeated absolutely irreducible component over $\mathbb{F}_q$



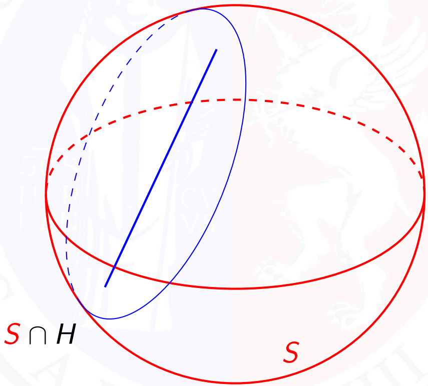
[Aubry, McGuire, Rodier, Contemp. Math. 2010]

Proposition

$H \subset \mathrm{PG}(3, q)$ hyperplane

$S \cap H$ has non-repeated absolutely irreducible component over $\mathbb{F}_q$

$\implies S$ has a non-repeated absolutely irreducible component over $\mathbb{F}_q$



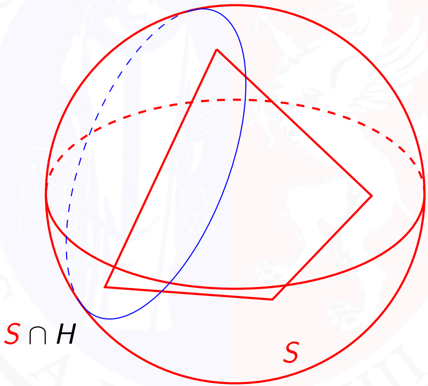
[Aubry, McGuire, Rodier, Contemp. Math. 2010]

Proposition

$H \subset \mathrm{PG}(3,q)$ hyperplane

$S \cap H$ has non-repeated absolutely irreducible component over $\mathbb{F}_q$

$\implies$ S has a non-repeated absolutely irreducible component over $\mathbb{F}_q$



[Aubry, McGuire, Rodier, Contemp. Math. 2010]

APN rational functions

Aubry-McGuire-Rodier

$\bigoplus$

Lang-Weil bound for surfaces

Theorem

$\deg(f) - \deg(g) = 2\ell$, $\ell > 0$ *odd*	$\deg(g) - \deg(f) = 2\ell$, $\ell > 0$ *odd*
• $g \notin \mathbb{F}_q[X^p]$; *or*	• $\ell \equiv 1 \pmod 4$; *or*
• $f' \neq \gamma g$ *for all* $\gamma \in \mathbb{F}_q$	• $\ell \equiv 1 \pmod 4$

$\Downarrow$

$\psi = \frac{f}{g}$ *is not exceptional APN*

PN rational functions

[B.-TIMPANELLA, in preparation 202?]

Proposition

q odd, $\psi = \frac{f}{g} \in \mathbb{F}_q(X)$, $g(x) \neq 0$ *forall* $x \in \mathbb{F}_q$ $(f, g) = 1$

ψ *is PN over* $\mathbb{F}_q$ $\iff$ $S_\psi : \dfrac{\theta_\psi(X, Y, Z)}{Z(X - Y)} = 0$ *has no* $\mathbb{F}_q$*-rational points off* $X = Y$, $Z = 0$

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

PN rational functions

Considering $S_\psi \cap H_\infty$

Proposition

$\deg(g) > \deg(f), \qquad q > (3\deg(g) + \deg(f))^{13/3}$

$$\psi(x) = f(x)/g(x) \text{ } PN \implies \psi(x) \text{ is permutation}$$

Proposition

$q > (\deg(g) - \deg(f))^4$ *and*

1. $\deg(g) > \deg(f)$, *and* $p \nmid (\deg(g) - \deg(f))$; *or*
2. $\deg(g) < \deg(f)$, $p \nmid (\deg(f) - \deg(g))$, *and* $x^{\deg(f)-\deg(g)}$ *is not PN*

$$\implies S_\psi \text{ has } \mathbb{F}_q\text{-rational a.i. component distinct from } X - Y = 0$$

$$\implies \psi(x) \text{ is not PN}$$

Open problems

- Try to extend nonexistence results for rational APN e PN in the remaining cases
- What for rational APcN and PcN?
- Is there any chance to obtain rational APcN permutation?

THANK YOU

FOR YOUR ATTENTION