On the difference of permutation polynomials

Nurdagül Anbar
(joint work with Almasa Odžak, Vandita Patel, Luciane Quoos, Anna Somoza, Alev Topuzoğlu)

RICAM, Linz, Austria

4-10 June 2017, Fq13

WIN-E2: Women in Numbers Europe 2, September 2016 (Organized by Irene Bouw, Rachel Newton, Ekin Özman)

Outline

Chowla–Zassenhaus Conjecture

$\mathbb{F}_q$: the finite field of order q

Any map $f : \mathbb{F}_q \to \mathbb{F}_q$ can be expressed uniquely as a polynomial of degree $< q$.

Definition:

f is called a permutation polynomial (PP) if f is a bijection.

Definition:

A PP f is called a complete mapping polynomial (CMP) if $f(x) + x$ is also a PP.

Chowla–Zassenhaus Conjecture (1968): Let p be *prime* with $p > (d^2 - 3d + 4)^2$ and $d \geq 2$. Then there is no CMP of degree d over $\mathbb{F}_p$.

Chowla–Zassenhaus Conjecture

$\mathbb{F}_q$: the finite field of order q

Any map $f : \mathbb{F}_q \to \mathbb{F}_q$ can be expressed uniquely as a polynomial of degree $< q$.

Definition:

f is called a permutation polynomial (PP) if f is a bijection.

Definition:

A PP f is called a complete mapping polynomial (CMP) if $f(x) + x$ is also a PP.

Chowla–Zassenhaus Conjecture (1968): Let p be *prime* with $p > (d^2 - 3d + 4)^2$ and $d \geq 2$. Then there is no CMP of degree d over $\mathbb{F}_p$.

Chowla–Zassenhaus Conjecture

$\mathbb{F}_q$: the finite field of order q

Any map $f : \mathbb{F}_q \to \mathbb{F}_q$ can be expressed uniquely as a polynomial of degree $< q$.

Definition:

f is called a permutation polynomial (PP) if f is a bijection.

Definition:

A PP f is called a complete mapping polynomial (CMP) if $f(x) + x$ is also a PP.

Chowla–Zassenhaus Conjecture (1968): Let p be *prime* with $p > (d^2 - 3d + 4)^2$ and $d \geq 2$. Then there is no CMP of degree d over $\mathbb{F}_p$.

Chowla–Zassenhaus Conjecture

$\mathbb{F}_q$: the finite field of order q

Any map $f : \mathbb{F}_q \to \mathbb{F}_q$ can be expressed uniquely as a polynomial of degree $< q$.

Definition:

f is called a permutation polynomial (PP) if f is a bijection.

Definition:

A PP f is called a complete mapping polynomial (CMP) if $f(x) + x$ is also a PP.

Chowla–Zassenhaus Conjecture (1968): Let p be *prime* with $p > (d^2 - 3d + 4)^2$ and $d \geq 2$. Then there is no CMP of degree d over $\mathbb{F}_p$.

The Chowla–Zassenhaus conjecture was proven by Stephen D. Cohen in 1990.

Theorem(Cohen, Mullen and Shiue, 1995):

Let $p > (d^2 - 3d + 4)^2$ and $d \geq 2$. If f and h are PPs of degree d, then $\deg(f - h) \geq \frac{3d}{5}$.

A *non-existence* result similar to the Chowla–Zassenhaus conjecture is given by L. Işık, A. Topuzoğlu and A. ~~Guenther~~ Winterhof in 2016.

The Chowla–Zassenhaus conjecture was proven by Stephen D. Cohen in 1990.

Theorem(Cohen, Mullen and Shiue, 1995):

Let $p > (d^2 - 3d + 4)^2$ and $d \geq 2$. If f and h are PPs of degree d, then $\deg(f - h) \geq \frac{3d}{5}$.

A *non-existence* result similar to the Chowla–Zassenhaus conjecture is given by L. Işık, A. Topuzoğlu and A. ~~Guenther~~ Winterhof in 2016.

The Chowla–Zassenhaus conjecture was proven by Stephen D. Cohen in 1990.

Theorem(Cohen, Mullen and Shiue, 1995):

Let $p > (d^2 - 3d + 4)^2$ and $d \geq 2$. If f and h are PPs of degree d, then $\deg(f - h) \geq \frac{3d}{5}$.

A *non-existence* result similar to the Chowla–Zassenhaus conjecture is given by L. Işık, A. Topuzoğlu and A. ~~Guenther~~ Winterhof in 2016.

Fact: The set of PPs over $\mathbb{F}_q$ forms a group G under composition and reduction modulo $x^q - x$.

Theorem (Carlitz, 1952): G is generated by x^{q-2} and $ax + b$ where $a, b \in \mathbb{F}_q$ and $a \neq 0$.

Corollary: If $f : \mathbb{F}_q \to \mathbb{F}_q$ is a PP, then $f(c) = P_n(c)$ for all $c \in \mathbb{F}_q$, where

$$P_n(x) = \left(\cdots \left((a_0 x + a_1)^{q-2} + a_2 \right)^{q-2} + \cdots + a_n \right)^{q-2} + a_{n+1}$$

for some $n \geq 0$, $a_0, a_2, \ldots, a_n \in \mathbb{F}_q^*$ and $a_1, a_{n+1} \in \mathbb{F}_q$.

Fact: The set of PPs over $\mathbb{F}_q$ forms a group G under composition and reduction modulo $x^q - x$.

Theorem (Carlitz, 1952): G is generated by x^{q-2} and $ax + b$ where $a, b \in \mathbb{F}_q$ and $a \neq 0$.

Corollary: If $f : \mathbb{F}_q \to \mathbb{F}_q$ is a PP, then $f(c) = P_n(c)$ for all $c \in \mathbb{F}_q$, where

$$P_n(x) = \left(\cdots \left((a_0 x + a_1)^{q-2} + a_2 \right)^{q-2} + \cdots + a_n \right)^{q-2} + a_{n+1}$$

for some $n \geq 0$, $a_0, a_2, \ldots, a_n \in \mathbb{F}_q^*$ and $a_1, a_{n+1} \in \mathbb{F}_q$.

Fact: The set of PPs over $\mathbb{F}_q$ forms a group G under composition and reduction modulo $x^q - x$.

Theorem (Carlitz, 1952): G is generated by x^{q-2} and $ax + b$ where $a, b \in \mathbb{F}_q$ and $a \neq 0$.

Corollary: If $f : \mathbb{F}_q \to \mathbb{F}_q$ is a PP, then $f(c) = P_n(c)$ for all $c \in \mathbb{F}_q$, where

$$P_n(x) = \left(\cdots \left((a_0 x + a_1)^{q-2} + a_2 \right)^{q-2} + \cdots + a_n \right)^{q-2} + a_{n+1}$$

for some $n \geq 0$, $a_0, a_2, \ldots, a_n \in \mathbb{F}_q^*$ and $a_1, a_{n+1} \in \mathbb{F}_q$.

Non-existence of CMP in terms of Carlitz rank and Linearity

Definition:

The Carlitz rank of a PP f over $\mathbb{F}_q$, denoted by $\mathrm{Crk}(f)$,

$$\mathrm{Crk}(f) = \min\{\, n \mid f(c) = P_n(c) \text{ for all } c \in \mathbb{F}_q \,\}.$$

Recall: The linearity of $f : \mathbb{F}_q \to \mathbb{F}_q$

$$\mathcal{L}(f) = \max_{a,b \in \mathbb{F}_q} \#\{\, c \in \mathbb{F}_q \mid f(c) = ac + b \,\}.$$

Theorem (Işik, Topuzoğlu, Winterhof, 2016):

Let f be a PP over $\mathbb{F}_q$ of $\mathrm{Crk}(f) = n$ with $\mathcal{L}(f) < (q+5)/2$. If $q > 2n + 1$, then f is not a CMP.

Non-existence of CMP in terms of Carlitz rank and Linearity

Definition:

The Carlitz rank of a PP f over $\mathbb{F}_q$, denoted by $\mathrm{Crk}(f)$,

$$\mathrm{Crk}(f) = \min\{\, n \mid f(c) = P_n(c) \text{ for all } c \in \mathbb{F}_q \,\}.$$

Recall: The linearity of $f : \mathbb{F}_q \to \mathbb{F}_q$

$$\mathcal{L}(f) = \max_{a,b \in \mathbb{F}_q} \#\{\, c \in \mathbb{F}_q \mid f(c) = ac + b \,\}.$$

Theorem (Işık, Topuzoğlu, Winterhof, 2016):

Let f be a PP over $\mathbb{F}_q$ of $\mathrm{Crk}(f) = n$ with $\mathcal{L}(f) < (q+5)/2$. If $q > 2n + 1$, then f is not a CMP.

Non-existence of CMP in terms of Carlitz rank and Linearity

Definition:

The Carlitz rank of a PP f over $\mathbb{F}_q$, denoted by $\mathrm{Crk}(f)$,

$$\mathrm{Crk}(f) = \min\{\, n \mid f(c) = P_n(c) \text{ for all } c \in \mathbb{F}_q \,\}.$$

Recall: The linearity of $f : \mathbb{F}_q \to \mathbb{F}_q$

$$\mathcal{L}(f) = \max_{a,b\in\mathbb{F}_q} \#\{\, c \in \mathbb{F}_q \mid f(c) = ac + b \,\}.$$

Theorem (Işik, Topuzoğlu, Winterhof, 2016):

Let f be a PP over $\mathbb{F}_q$ of $\mathrm{Crk}(f) = n$ with $\mathcal{L}(f) < (q+5)/2$. If $q > 2n+1$, then f is not a CMP.

Idea of the proof: For $a, b, x \in \mathbb{F}_q$,

$$(ax+b)^{q-2} = \begin{cases} 1/(ax+b) & \text{if } ax+b \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

$\Longrightarrow f(x) = P_n(x) = \frac{ax+b}{cx+d} = R(x)$ for all $x \in \mathbb{F}_q \backslash \mathcal{O}$, where $\mathcal{O}$ is the set of poles.

$\Longrightarrow f(x) + x = R(x) + x$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If there exist $x_1, x_2 \in \mathbb{F}_q$ with $x_1 \neq x_2$ and

$$R(x_1) + x_1 = R(x_2) + x_2 = e \ , \qquad (*)$$

then x_1 or $x_2 \in \mathcal{O}$.

$(*)$ holds $\Longleftrightarrow p_e(x) := cx^2 + (a+d+ce)x + de$ has roots in $\mathbb{F}_q$.

□

Idea of the proof: For $a, b, x \in \mathbb{F}_q$,

$$(ax+b)^{q-2} = \begin{cases} 1/(ax+b) & \text{if } ax+b \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

$\Longrightarrow f(x) = P_n(x) = \frac{ax+b}{cx+d} = R(x)$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$, where $\mathcal{O}$ is the set of poles.

$\Longrightarrow f(x) + x = R(x) + x$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If there exist $x_1, x_2 \in \mathbb{F}_q$ with $x_1 \neq x_2$ and

$$R(x_1) + x_1 = R(x_2) + x_2 = e \;, \qquad (*)$$

then x_1 or $x_2 \in \mathcal{O}$.

$(*)$ holds $\Longleftrightarrow p_e(x) := cx^2 + (a+d+ce)x + de$ has roots in $\mathbb{F}_q$.

□

Idea of the proof: For $a, b, x \in \mathbb{F}_q$,

$$(ax+b)^{q-2} = \begin{cases} 1/(ax+b) & \text{if } ax+b \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

$\Longrightarrow f(x) = P_n(x) = \frac{ax+b}{cx+d} = R(x)$ for all $x \in \mathbb{F}_q \backslash \mathcal{O}$, where $\mathcal{O}$ is the set of poles.

$\Longrightarrow f(x) + x = R(x) + x$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If there exist $x_1, x_2 \in \mathbb{F}_q$ with $x_1 \neq x_2$ and

$$R(x_1) + x_1 = R(x_2) + x_2 = e \ , \qquad (*)$$

then x_1 or $x_2 \in \mathcal{O}$.

$(*)$ holds $\Longleftrightarrow p_e(x) := cx^2 + (a+d+ce)x + de$ has roots in $\mathbb{F}_q$.

□

Idea of the proof: For $a, b, x \in \mathbb{F}_q$,

$$(ax+b)^{q-2} = \begin{cases} 1/(ax+b) & \text{if } ax+b \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

$\Longrightarrow f(x) = P_n(x) = \frac{ax+b}{cx+d} = R(x)$ for all $x \in \mathbb{F}_q \backslash \mathcal{O}$, where $\mathcal{O}$ is the set of poles.

$\Longrightarrow f(x) + x = R(x) + x$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If there exist $x_1, x_2 \in \mathbb{F}_q$ with $x_1 \neq x_2$ and

$$R(x_1) + x_1 = R(x_2) + x_2 = e \ , \qquad (*)$$

then x_1 or $x_2 \in \mathcal{O}$.

$(*)$ holds $\Longleftrightarrow p_e(x) := cx^2 + (a+d+ce)x + de$ has roots in $\mathbb{F}_q$.

□

Idea of the proof: For $a, b, x \in \mathbb{F}_q$,

$$(ax+b)^{q-2} = \begin{cases} 1/(ax+b) & \text{if } ax+b \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

$\Longrightarrow f(x) = P_n(x) = \frac{ax+b}{cx+d} = R(x)$ for all $x \in \mathbb{F}_q \backslash \mathcal{O}$, where $\mathcal{O}$ is the set of poles.

$\Longrightarrow f(x) + x = R(x) + x$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If there exist $x_1, x_2 \in \mathbb{F}_q$ with $x_1 \neq x_2$ and

$$R(x_1) + x_1 = R(x_2) + x_2 = e\ , \qquad (*)$$

then x_1 or $x_2 \in \mathcal{O}$.

$(*)$ holds $\Longleftrightarrow p_e(x) := cx^2 + (a+d+ce)x + de$ has roots in $\mathbb{F}_q$.

□

Theorem (AOPQST, 2017):

Let f and $f+g$ be PPs over $\mathbb{F}_q$ such that $\mathrm{Crk}(f)=n$, $\deg(g)=k$ with $1 \le k < q-1$ and $\mathcal{L}(f) < (q+5)/2$. Then

$$nk + k(k-1)\sqrt{q} \ge q - n - \mu \ ,$$

where $\mu = \gcd(k, q-1)$.

Remark: This result is similar to the one given by Cohen, Mullen and Shiue in 1995.

Recall(Cohen, Mullen, Shiue, 1995): Let $p > (d^2 - 3d + 4)^2$ and $d \ge 2$. If f and h are PPs of degree d, then $\deg(f-h) \ge \frac{3d}{5}$.

Corollary:

$k = 1 \Longrightarrow$ the non-existence result given by Işık, Topuzoğlu, Winterhof in 2016

Theorem (AOPQST, 2017):

Let f and $f+g$ be PPs over $\mathbb{F}_q$ such that $\mathrm{Crk}(f)=n$, $\deg(g)=k$ with $1\le k<q-1$ and $\mathcal{L}(f)<(q+5)/2$. Then

$$nk+k(k-1)\sqrt{q}\ge q-n-\mu\ ,$$

where $\mu=\gcd(k,q-1)$.

Remark: This result is similar to the one given by Cohen, Mullen and Shiue in 1995.

Recall(Cohen, Mullen, Shiue, 1995): Let $p>(d^2-3d+4)^2$ and $d\ge 2$. If f and h are PPs of degree d, then $\deg(f-h)\ge\frac{3d}{5}$.

Corollary:

$k=1\Longrightarrow$ the non-existence result given by Işık, Topuzoğlu, Winterhof in 2016

Theorem (AOPQST, 2017):

Let f and $f+g$ be PPs over $\mathbb{F}_q$ such that $\mathrm{Crk}(f) = n$, $\deg(g) = k$ with $1 \le k < q-1$ and $\mathcal{L}(f) < (q+5)/2$. Then

$$nk + k(k-1)\sqrt{q} \ge q - n - \mu \ ,$$

where $\mu = \gcd(k, q-1)$.

Remark: This result is similar to the one given by Cohen, Mullen and Shiue in 1995.

Recall(Cohen, Mullen, Shiue, 1995): Let $p > (d^2 - 3d + 4)^2$ and $d \ge 2$. If f and h are PPs of degree d, then $\deg(f-h) \ge \frac{3d}{5}$.

Corollary:

$k = 1 \implies$ the non-existence result given by Işık, Topuzoğlu, Winterhof in 2016

Idea of the proof: To relate rational points of a curve over $\mathbb{F}_q$ to poles of f.

$f(x) = R(x) = \frac{ax+b}{cx+d}$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

$H(x) := R(x) + g(x) \Longrightarrow f(x) + g(x) = H(x)$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If $H(x) = H(y)$ for some $x, y \in \mathbb{F}_q$ with $x \neq y$, then x or $y \in \mathcal{O}$.

Cohen (1970) $\Longrightarrow \frac{H(X)-H(Y)}{X-Y}$ has an absolutely irreducible factor $f(X,Y)$ over $\mathbb{F}_q$

$\mathcal{X}$: the projective curve over $\mathbb{F}_q$ defined by f

For a rational point $[x : y : 1] \in \mathcal{X}$, we have $H(x) = H(y)$.

$\Longrightarrow$ **# of rational points** $N(\mathcal{X})$ **of** $\mathcal{X}$ **gives a lower bound on** $\#\mathcal{O} \leq n$

Idea of the proof: To relate rational points of a curve over $\mathbb{F}_q$ to poles of f.

$f(x) = R(x) = \frac{ax+b}{cx+d}$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

$H(x) := R(x) + g(x) \Longrightarrow f(x) + g(x) = H(x)$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If $H(x) = H(y)$ for some $x, y \in \mathbb{F}_q$ with $x \neq y$, then x or $y \in \mathcal{O}$.

Cohen (1970) $\Longrightarrow \frac{H(X)-H(Y)}{X-Y}$ has an absolutely irreducible factor $f(X,Y)$ over $\mathbb{F}_q$

$\mathcal{X}$: the projective curve over $\mathbb{F}_q$ defined by f

For a rational point $[x : y : 1] \in \mathcal{X}$, we have $H(x) = H(y)$.

$\Longrightarrow$ **# of rational points $N(\mathcal{X})$ of $\mathcal{X}$ gives a lower bound on $\#\mathcal{O} \leq n$**

Idea of the proof: To relate rational points of a curve over $\mathbb{F}_q$ to poles of f.

$f(x) = R(x) = \frac{ax+b}{cx+d}$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

$H(x) := R(x) + g(x) \Longrightarrow f(x) + g(x) = H(x)$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If $H(x) = H(y)$ for some $x, y \in \mathbb{F}_q$ with $x \neq y$, then x or $y \in \mathcal{O}$.

Cohen (1970) $\Longrightarrow \frac{H(X)-H(Y)}{X-Y}$ has an absolutely irreducible factor $f(X,Y)$ over $\mathbb{F}_q$

$\mathcal{X}$: the projective curve over $\mathbb{F}_q$ defined by f

For a rational point $[x : y : 1] \in \mathcal{X}$, we have $H(x) = H(y)$.

$\Longrightarrow$ # of rational points $N(\mathcal{X})$ of $\mathcal{X}$ gives a lower bound on $\#\mathcal{O} \leq n$

Idea of the proof: To relate rational points of a curve over $\mathbb{F}_q$ to poles of f.

$f(x) = R(x) = \frac{ax+b}{cx+d}$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

$H(x) := R(x) + g(x) \Longrightarrow f(x) + g(x) = H(x)$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If $H(x) = H(y)$ for some $x, y \in \mathbb{F}_q$ with $x \neq y$, then x or $y \in \mathcal{O}$.

Cohen (1970) $\Longrightarrow \frac{H(X)-H(Y)}{X-Y}$ has an absolutely irreducible factor $f(X, Y)$ over $\mathbb{F}_q$

$\mathcal{X}$: the projective curve over $\mathbb{F}_q$ defined by f

For a rational point $[x : y : 1] \in \mathcal{X}$, we have $H(x) = H(y)$.

$\Longrightarrow$ **# of rational points** $N(\mathcal{X})$ **of** $\mathcal{X}$ **gives a lower bound on** $\#\mathcal{O} \leq n$

Idea of the proof: To relate rational points of a curve over $\mathbb{F}_q$ to poles of f.

$f(x) = R(x) = \frac{ax+b}{cx+d}$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

$H(x) := R(x) + g(x) \Longrightarrow f(x) + g(x) = H(x)$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If $H(x) = H(y)$ for some $x, y \in \mathbb{F}_q$ with $x \neq y$, then x or $y \in \mathcal{O}$.

Cohen (1970) $\Longrightarrow \frac{H(X)-H(Y)}{X-Y}$ has an absolutely irreducible factor $f(X, Y)$ over $\mathbb{F}_q$

$\mathcal{X}$: the projective curve over $\mathbb{F}_q$ defined by f

For a rational point $[x : y : 1] \in \mathcal{X}$, we have $H(x) = H(y)$.

$\Longrightarrow$ **# of rational points** $N(\mathcal{X})$ **of** $\mathcal{X}$ **gives a lower bound on** $\#\mathcal{O} \leq n$

Idea of the proof: To relate rational points of a curve over $\mathbb{F}_q$ to poles of f.

$f(x) = R(x) = \frac{ax+b}{cx+d}$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

$H(x) := R(x) + g(x) \Longrightarrow f(x) + g(x) = H(x)$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If $H(x) = H(y)$ for some $x, y \in \mathbb{F}_q$ with $x \neq y$, then x or $y \in \mathcal{O}$.

Cohen (1970) $\Longrightarrow \frac{H(X)-H(Y)}{X-Y}$ has an absolutely irreducible factor $f(X,Y)$ over $\mathbb{F}_q$

$\mathcal{X}$: the projective curve over $\mathbb{F}_q$ defined by f

For a rational point $[x : y : 1] \in \mathcal{X}$, we have $H(x) = H(y)$.

$\Longrightarrow$ **# of rational points** $N(\mathcal{X})$ **of** $\mathcal{X}$ **gives a lower bound on** $\#\mathcal{O} \leq n$

Idea of the proof: To relate rational points of a curve over $\mathbb{F}_q$ to poles of f.

$f(x) = R(x) = \frac{ax+b}{cx+d}$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

$H(x) := R(x) + g(x) \Longrightarrow f(x) + g(x) = H(x)$ for all $x \in \mathbb{F}_q \setminus \mathcal{O}$.

If $H(x) = H(y)$ for some $x, y \in \mathbb{F}_q$ with $x \neq y$, then x or $y \in \mathcal{O}$.

Cohen (1970) $\Longrightarrow \frac{H(X)-H(Y)}{X-Y}$ has an absolutely irreducible factor $f(X, Y)$ over $\mathbb{F}_q$

$\mathcal{X}$: the projective curve over $\mathbb{F}_q$ defined by f

For a rational point $[x : y : 1] \in \mathcal{X}$, we have $H(x) = H(y)$.

$\Longrightarrow$ **# of rational points $N(\mathcal{X})$ of $\mathcal{X}$ gives a lower bound on $\#\mathcal{O} \leq n$**

By the Hasse-Weil Bound,

$$N(\mathcal{X}) \geq q + 1 - k(k-1)\sqrt{q}$$

Bezout's Theorem $\implies nk + k(k-1)\sqrt{q} \geq q - n - \mu$, where $\mu = \gcd(k, q-1)$

□

Theorem (AOPQST, 2017):

Let f and $f + cx^k$ be PPs over $\mathbb{F}_q$ with $1 \leq k < q-1$ and $\mathrm{Crk}(f) = n$. If the last pole of f is zero, then

$$k(n+3) - (m-1)(k-1)\sqrt{q} \geq q - n \ ,$$

where $m = \gcd(k+1, q-1)$. In particular, if $m = 1$, then $k \geq (q-n)(n+3)$.

By the Hasse-Weil Bound,

$$N(\mathcal{X}) \geq q + 1 - k(k-1)\sqrt{q}$$

Bezout's Theorem $\Longrightarrow nk + k(k-1)\sqrt{q} \geq q - n - \mu$, where $\mu = \gcd(k, q-1)$

□

Theorem (AOPQST, 2017):

Let f and $f + cx^k$ be PPs over $\mathbb{F}_q$ with $1 \leq k < q-1$ and $\mathrm{Crk}(f) = n$. If the last pole of f is zero, then

$$k(n+3) - (m-1)(k-1)\sqrt{q} \geq q - n\ ,$$

where $m = \gcd(k+1, q-1)$. In particular, if $m = 1$, then $k \geq (q-n)(n+3)$.

By the Hasse-Weil Bound,

$$N(\mathcal{X}) \geq q + 1 - k(k-1)\sqrt{q}$$

Bezout's Theorem $\implies nk + k(k-1)\sqrt{q} \geq q - n - \mu$, where $\mu = \gcd(k, q-1)$

$\square$

Theorem (AOPQST, 2017):

Let f and $f + cx^k$ be PPs over $\mathbb{F}_q$ with $1 \leq k < q-1$ and $\mathrm{Crk}(f) = n$. If the last pole of f is zero, then

$$k(n+3) - (m-1)(k-1)\sqrt{q} \geq q - n \ ,$$

where $m = \gcd(k+1, q-1)$. In particular, if $m = 1$, then $k \geq (q-n)(n+3)$.

Grazie per l'attenzione!