

Complete $(k, 3)$ -arcs from quartic curves

Daniele Bartoli

(joint work with Massimo Giulietti and Giovanni Zini)

University of Gent (Belgium)

ALCOMA 2015

Kloster Banz, March 15 - 20, 2015

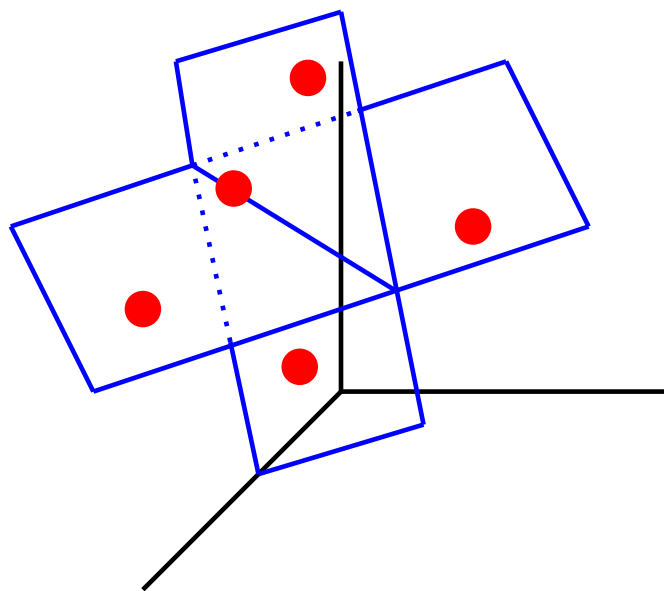
- (n, r) -arcs and Coding Theory
- Algebraic constructions of small **complete**
 $(n, 3)$ -arcs
- Possible developments

Complete arcs

Definition (Arc)

$\mathcal{A} \subset AG(r, q), PG(r, q)$
 n -arc \iff n points
 no $r + 1$ of which
 are in a hyperplane

\mathcal{A}
 complete \iff $\mathcal{A} \not\subset \mathcal{A}'$
 \mathcal{A}' $(n + 1)$ -arc

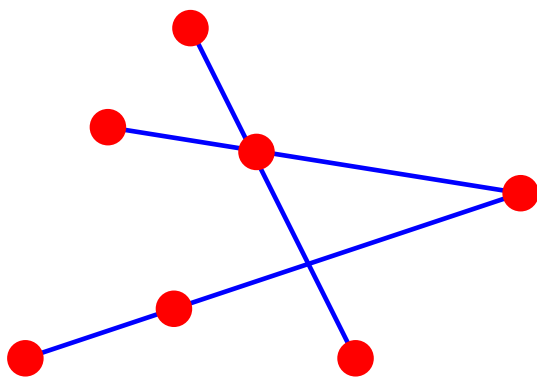


Complete (n, m) -arcs in projective planes

Definition $((n, m)$ -arc)

$\mathcal{A} \subset AG(2, q), PG(2, q)$
 (n, m) -arc \iff n points
no $m + 1$ of which
are collinear

\mathcal{A}
complete $\iff \mathcal{A}' \quad \mathcal{A} \not\subset \mathcal{A}'$
 $(n + 1, m)$ -arc



MDS codes

Linear code $\mathcal{C} < \mathbb{F}_q^N$

d Hamming distance

Singleton Bound

$$[n, k, d]_q \implies d \leq n - k + 1$$

Definition (MDS Codes)

$d = n - k + 1 \implies$ *Maximum Distance Separable (MDS)*

MDS $[n, k, d]_q$ -code \longleftrightarrow *n -arc in $PG(n - k - 1, q)$*

Columns of a parity-check matrix \longleftrightarrow *points in $PG(n - k - 1, q)$*

NMDS codes

Definition (Singleton defect)

$$\Delta(\mathcal{C}) = n - k + 1 - d$$

$$\Delta(\mathcal{C}) = 0 \quad \implies \quad \mathcal{C} \text{ MDS}$$

$$\Delta(\mathcal{C}) = 1 \quad \implies \quad \mathcal{C} \text{ A(lmost)MDS}$$

$$\begin{array}{l} \Delta(\mathcal{C}) = 1 \\ \Delta(\mathcal{C}^\perp) = 1 \end{array} \quad \implies \quad \mathcal{C} \text{ N(ear)MDS}$$

$\text{NMDS } [n, 3, d]_q\text{-code} \iff (n, 3)\text{-arc in } PG(2, q)$

$\text{Columns of a parity-check matrix} \iff \text{points in } PG(2, q)$

Algebraic constructions

Idea of Segre and Lombardo-Radice

*The points of the arc are chosen, with few exceptions, among the points of a **conic** or a **cubic curve***

- 1 Choose a $\mathcal{K} \subset \text{PG}(2, q)$ having a low degree parametrization
- 2 Prove that \mathcal{K} is an **arc**
- 3 $\forall P \in \text{PG}(2, q) \setminus \mathcal{K}$ **construct** \mathcal{H}_P algebraic curve which expresses the **collinearity condition** between P and $P_1, P_2 \in \mathcal{K}$
- 4 Show that \mathcal{H}_P is **absolutely irreducible** for almost all P
- 5 Use the **Hasse-Weil** theorem to show that, if q is large enough, then $(\bar{x}, \bar{y}) \in \mathcal{H}_P(\mathbb{F}_q)$: $P_1(\bar{x})$ and $P_2(\bar{y})$ collinear with P
- 6 Extend \mathcal{K} with some extra points

Example: Construction of arcs in projective planes

$$\mathcal{K} = \{(f(t), g(t)) \mid t \in \mathbb{F}_q\} \subset AG(2, q)$$

Example: Construction of arcs in projective planes

$$\mathcal{K} = \{(f(t), g(t)) \mid t \in \mathbb{F}_q\} \subset AG(2, q)$$

- \mathcal{K} is an arc if

$$\det \begin{pmatrix} f(x) & g(x) & 1 \\ f(y) & g(y) & 1 \\ f(z) & g(z) & 1 \end{pmatrix} \neq 0$$

Example: Construction of arcs in projective planes

$$\mathcal{K} = \{(f(t), g(t)) \mid t \in \mathbb{F}_q\} \subset AG(2, q)$$

- \mathcal{K} is an arc if

$$\det \begin{pmatrix} f(x) & g(x) & 1 \\ f(y) & g(y) & 1 \\ f(z) & g(z) & 1 \end{pmatrix} \neq 0$$

- $P = (a, b)$ covered by \mathcal{K} if there exist $x, y \in \mathbb{F}_q$ with

$$\det \begin{pmatrix} a & b & 1 \\ f(x) & g(x) & 1 \\ f(y) & g(y) & 1 \end{pmatrix} = 0$$

Example: Construction of arcs in projective planes

$$\mathcal{K} = \{(f(t), g(t)) \mid t \in \mathbb{F}_q\} \subset AG(2, q)$$

- \mathcal{K} is an arc if

$$\det \begin{pmatrix} f(x) & g(x) & 1 \\ f(y) & g(y) & 1 \\ f(z) & g(z) & 1 \end{pmatrix} \neq 0$$

- $P = (a, b)$ covered by \mathcal{K} if there exist $x, y \in \mathbb{F}_q$ with

$$\mathcal{H}_P : \det \begin{pmatrix} a & b & 1 \\ f(x) & g(x) & 1 \\ f(y) & g(y) & 1 \end{pmatrix} = 0$$

Example: Construction of arcs in projective planes

$$\mathcal{K} = \{(f(t), g(t)) \mid t \in \mathbb{F}_q\} \subset AG(2, q)$$

- \mathcal{K} is an arc if

$$\det \begin{pmatrix} f(x) & g(x) & 1 \\ f(y) & g(y) & 1 \\ f(z) & g(z) & 1 \end{pmatrix} \neq 0$$

- $P = (a, b)$ covered by \mathcal{K} if there exist $x, y \in \mathbb{F}_q$ with

$$\mathcal{H}_P : \det \begin{pmatrix} a & b & 1 \\ f(x) & g(x) & 1 \\ f(y) & g(y) & 1 \end{pmatrix} = 0$$

- the algebraic curve \mathcal{H}_P has an \mathbb{F}_q -rational point (\bar{x}, \bar{y})
- $(f(\bar{x}), g(\bar{x})) \neq (f(\bar{y}), g(\bar{y}))$, not a pole of x or y

Example: Construction of arcs in projective planes II

$$\mathcal{K} = \underbrace{\left\{ \overbrace{(L(t) + c)}^{f(t)}, \overbrace{(L(t) + c)^3}^{g(t)} \right\}}_{P_t} \mid t \in \mathbb{F}_q, \quad -3c \notin \text{Im}(L)$$

$$\mathcal{H}_P: \quad b + (L(x) + c)(L(y) + c)^2 + (L(x) + c)^2(L(y) + c) - a((L(x) + c)^2 + (L(x) + c)(L(y) + c) + (L(y) + c)^2) = 0$$

Example: Construction of arcs in projective planes II

$$\mathcal{K} = \left\{ \underbrace{\left(\overbrace{L(t) + c}^{f(t)}, \overbrace{(L(t) + c)^3}^{g(t)} \right)}_{P_t} \mid t \in \mathbb{F}_q \right\}, \quad -3c \notin \text{Im}(L)$$

$$\mathcal{H}_P: \quad b + (L(x) + c)(L(y) + c)^2 + (L(x) + c)^2(L(y) + c) - a((L(x) + c)^2 + (L(x) + c)(L(y) + c) + (L(y) + c)^2) = 0$$

(Szőnyi, 1985)

if $b \neq a^3$

- \mathcal{H}_P is absolutely irreducible
- \mathcal{H}_P has at least $q + 1 - 9 \deg(L)^2 \sqrt{q}$ points

Algebraic constructions

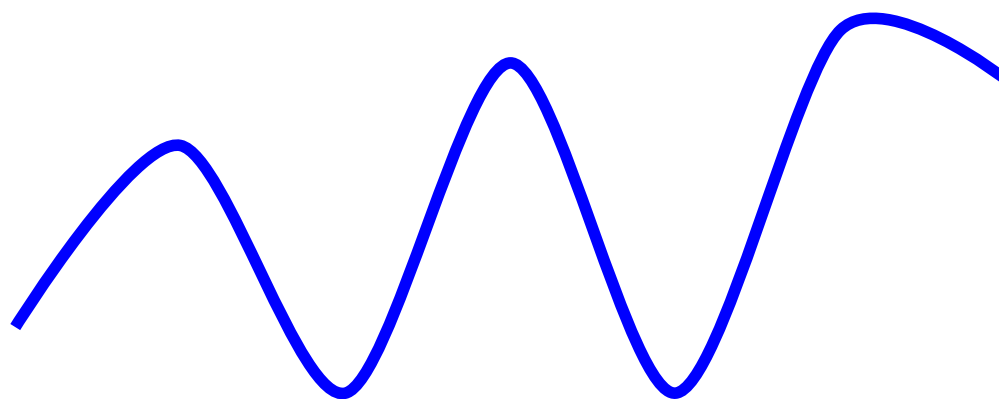
Idea of Segre and Lombardo-Radice

The points of the arc are chosen, with few exceptions, among the points of a conic or a cubic curve

- ① $q/2$: Segre, Hirschfeld
- ② $q/3$: Abatangelo, Korchmáros, Szőnyi, Voloch
- ③ $q/4$: Korchmáros
- ④ $2q^{9/10}$: Szőnyi
- ⑤ $cq^{3/4}$: Szőnyi-Voloch-Anbar-B.-Giulietti-Platoni

Infinite families of complete (n, r) -arcs, $r > 2$

- \mathbb{F}_q -rational points of irreducible curve of degree r



- 2-character sets in $\text{PG}(2, q)$

$$r = 3$$

No other examples than irreducible cubics!

Complete $(n, 3)$ -arcs from cubic curves

Proposition (Hirschfeld-Voloch)

- \mathcal{E} : plane elliptic curve
- $j(\mathcal{E}) \neq 0$
- $q \geq 121$

\mathcal{E} is a complete $(n, 3)$ -arc in $\text{PG}(2, q)$

Proposition (Giulietti)

- \mathcal{E} : plane elliptic curve
- $|\mathcal{E}|$ even
- $j(\mathcal{E}) = 0$
- $q = p^r$, $p > 3$, $q > 9887$
- r even or $p \equiv 1 \pmod{3}$

\mathcal{E} is a complete $(n, 3)$ -arc in $\text{PG}(2, q)$

$$\mathcal{E} \text{ complete } (n, 3)\text{-arc} \implies q - 2\sqrt{q} + 1 \leq |\mathcal{E}| \leq q + 2\sqrt{q} + 1$$

Complete $(n, 3)$ -arcs

UPPER and LOWER BOUNDS

\mathcal{A} : complete $(n, 3)$ -arc

$$\sqrt{6(q+1)} \leq |\mathcal{A}| \leq 2q+1$$

Random construction

$$q \leq 30000$$

$$|\mathcal{A}| \simeq \sqrt{6q} \log q$$

Algebraic constructions of small complete $(n, 3)$ -arcs

Idea of Segre and Lombardo-Radice

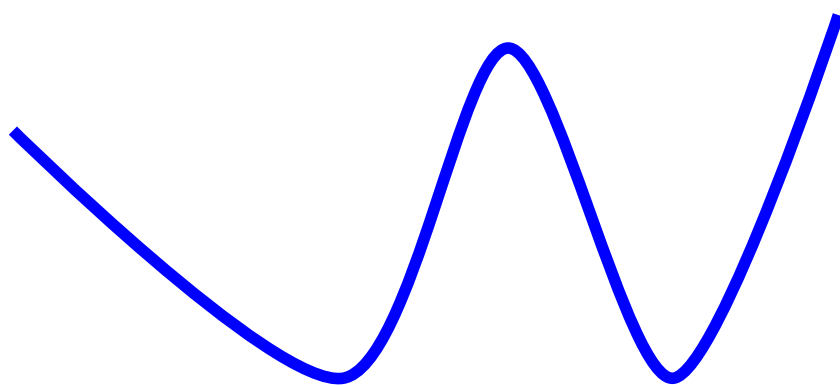
The points of the arc are chosen, with few exceptions, among the points of a conic or a cubic curve

Our Idea

*The points of the $(n, 3)$ -arc are chosen, with few exceptions, among the points of **an irreducible quartic curve***

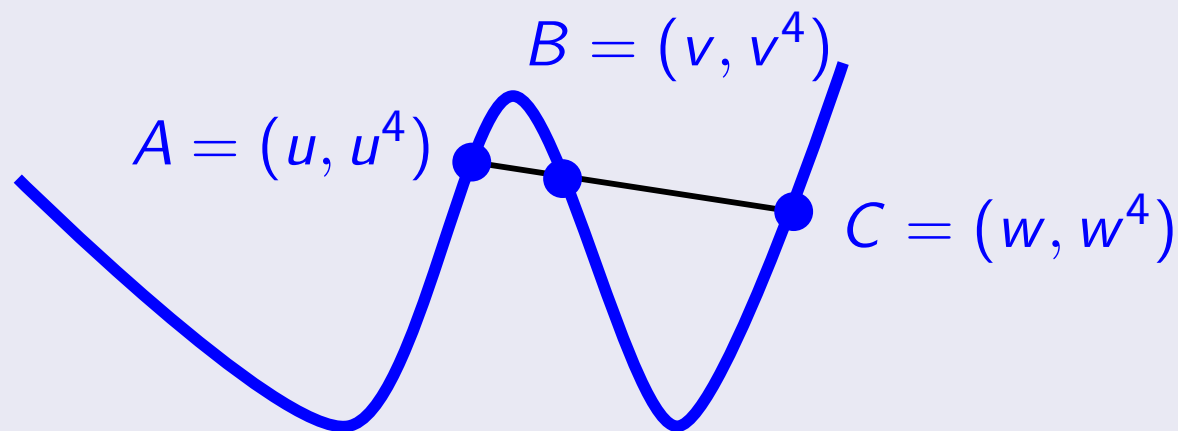
Small complete $(n, 3)$ -arcs from quartic curves

- p : odd prime, $p \equiv 2 \pmod{3}$
- $\sigma = p^{h'}$, h' odd
- $q = p^h$, $h > h'$, $h' \mid h$



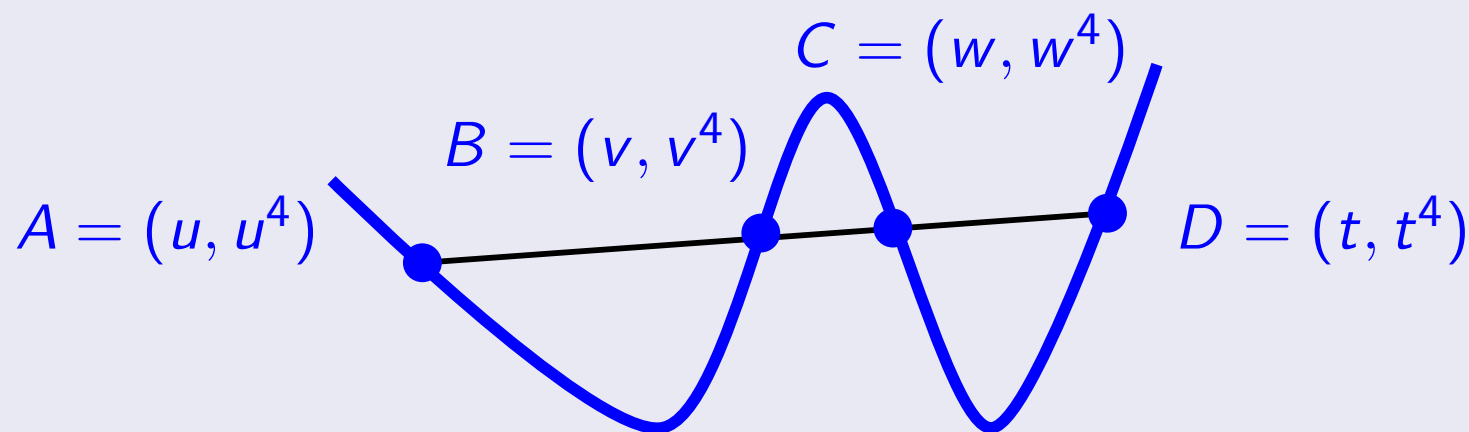
$$\mathcal{Q} = \{(x, x^4) \mid x \in \mathbb{F}_q\}$$

Proposition



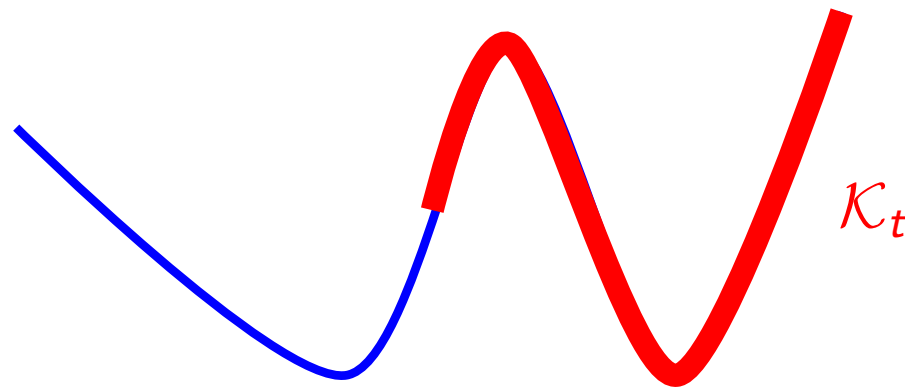
$$\text{COLLINEAR} \iff u^2 + v^2 + w^2 + uv + uw + vw = 0$$

Proposition

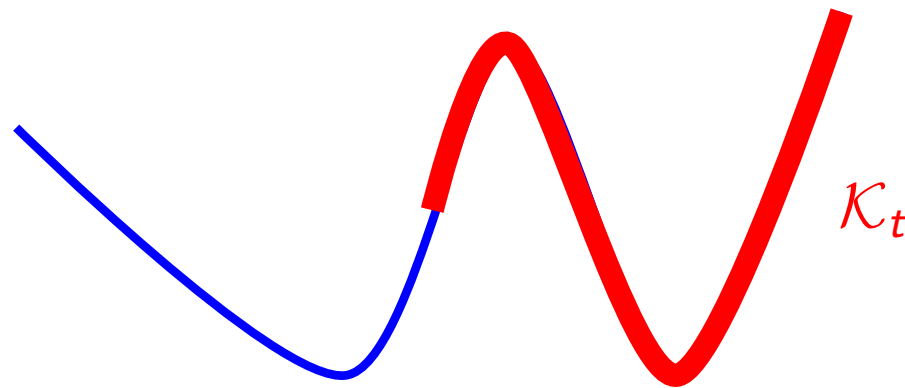


$$\text{COLLINEAR} \iff \begin{cases} u^2 + v^2 + w^2 + uv + uw + vw = 0 \\ u + v + w + t = 0 \end{cases}$$

- $M := \{(a^\sigma - a) \mid a \in \mathbb{F}_q\} \quad M \simeq \mathbb{F}_{\frac{q}{\sigma}} \leq (\mathbb{F}_q, +)$
- $\mathcal{K}_t := \{(v, v^4) \mid v \in M + t\}$, with $t \notin M$



- $M := \{(a^\sigma - a) \mid a \in \mathbb{F}_q\} \quad M \simeq \mathbb{F}_{\frac{q}{\sigma}} \leq (\mathbb{F}_q, +)$
- $\mathcal{K}_t := \{(v, v^4) \mid v \in M + t\}$, with $t \notin M$



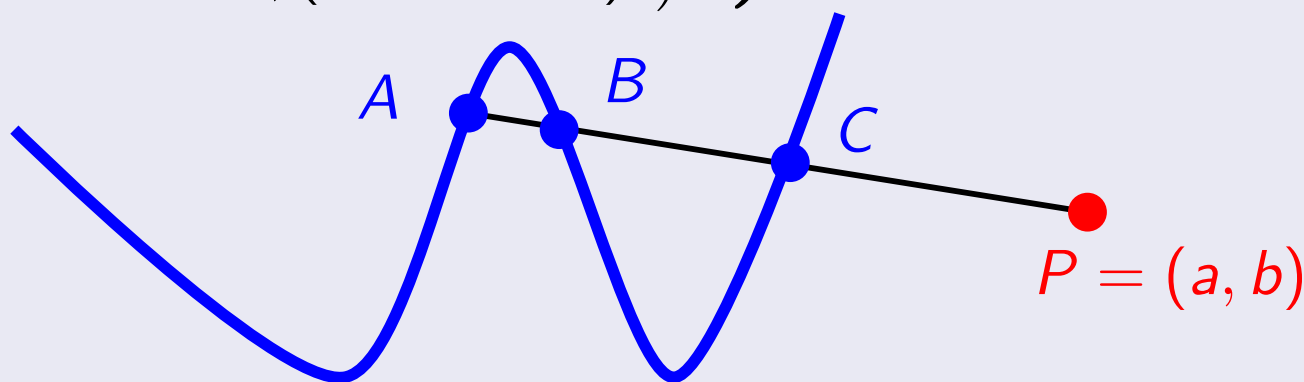
Proposition

\mathcal{K}_t is a $(k, 3)$ -arc.

Points off \mathcal{Q}

Proposition

$$\left. \begin{aligned} A &= (x^\sigma - x + t, (x^\sigma - x + t)^4) \\ B &= (y^\sigma - y + t, (y^\sigma - y + t)^4) \\ C &= (z^\sigma - z + t, (z^\sigma - z + t)^4) \end{aligned} \right\} \in \mathcal{K}_t \text{ and } P = (a, b) \in \text{AG}(2, q) \setminus \mathcal{Q}$$



COLLINEAR



$$\left\{ \begin{aligned} &(z^\sigma - z)^2 + (z^\sigma - z)((x^\sigma - x) + (y^\sigma - y) + 4t) + 4t(x^\sigma - x + y^\sigma - y) + \\ &+ 6t^2 + (x^\sigma - x)(y^\sigma - y) + (x^\sigma - x)^2 + (y^\sigma - y)^2 = 0 \\ &a((x^\sigma - x)^2 + (y^\sigma - y)^2 + 2t^2 + 2t(x^\sigma - x) + \\ &+ 2t(y^\sigma - y))(x^\sigma - x + y^\sigma - y + 2t) - (x^\sigma - x + t)(y^\sigma - y + t) \cdot \\ &\cdot ((x^\sigma - x)^2 + (y^\sigma - y)^2 + (x^\sigma - x)(y^\sigma - y) + 3t^2 \\ &+ 3t(x^\sigma - x + y^\sigma - y)) - b = 0 \end{aligned} \right.$$

\mathcal{H}_P

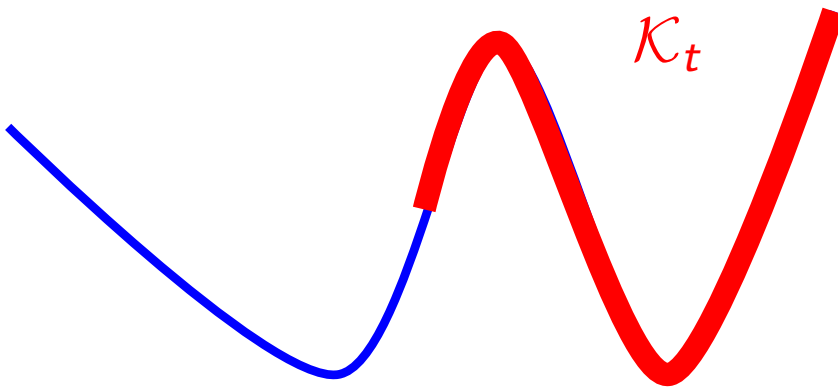
$$\left\{ \begin{array}{l} (z^\sigma - z)^2 + (z^\sigma - z)((x^\sigma - x) + (y^\sigma - y) + 4t) + 4t(x^\sigma - x + y^\sigma - y) + \\ + 6t^2 + (x^\sigma - x)(y^\sigma - y) + (x^\sigma - x)^2 + (y^\sigma - y)^2 = 0 \\ \\ a((x^\sigma - x)^2 + (y^\sigma - y)^2 + 2t^2 + 2t(x^\sigma - x) + \\ + 2t(y^\sigma - y))(x^\sigma - x + y^\sigma - y + 2t) - (x^\sigma - x + t)(y^\sigma - y + t) \cdot \\ \cdot ((x^\sigma - x)^2 + (y^\sigma - y)^2 + (x^\sigma - x)(y^\sigma - y) + 3t^2 + 3t(x^\sigma - x + y^\sigma - y)) - b = 0 \end{array} \right.$$

for almost all $P \in \text{AG}(2, q) \setminus \mathcal{Q}$
the space curve \mathcal{H}_P is absolutely irreducible
and it has genus $g \leq 30\sigma^3 - 12\sigma^2 - 4\sigma + 1$

\mathcal{H}_P

$$\left\{ \begin{array}{l} (z^\sigma - z)^2 + (z^\sigma - z)((x^\sigma - x) + (y^\sigma - y) + 4t) + 4t(x^\sigma - x + y^\sigma - y) + \\ + 6t^2 + (x^\sigma - x)(y^\sigma - y) + (x^\sigma - x)^2 + (y^\sigma - y)^2 = 0 \\ \\ a((x^\sigma - x)^2 + (y^\sigma - y)^2 + 2t^2 + 2t(x^\sigma - x) + \\ + 2t(y^\sigma - y))(x^\sigma - x + y^\sigma - y + 2t) - (x^\sigma - x + t)(y^\sigma - y + t) \cdot \\ \cdot ((x^\sigma - x)^2 + (y^\sigma - y)^2 + (x^\sigma - x)(y^\sigma - y) + 3t^2 + 3t(x^\sigma - x + y^\sigma - y)) - b = 0 \end{array} \right.$$

for almost all $P \in \text{AG}(2, q) \setminus \mathcal{Q}$
the space curve \mathcal{H}_P is absolutely irreducible
and it has genus $g \leq 30\sigma^3 - 12\sigma^2 - 4\sigma + 1$

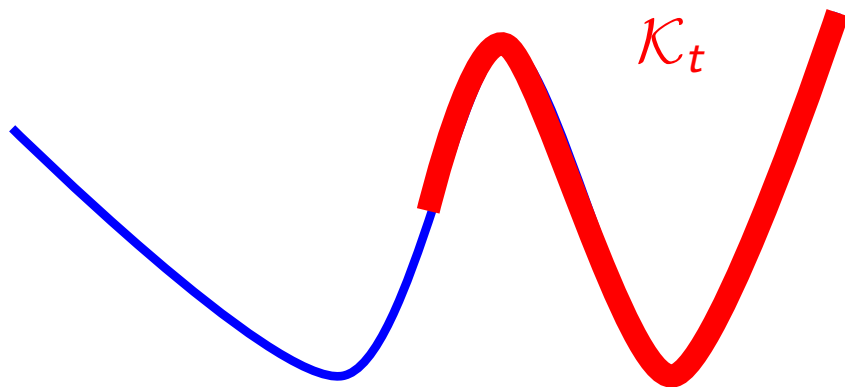


Theorem

$$q \geq 3600 \sigma^6$$

\mathcal{K}_t is a 3-arc
covering $\text{AG}(2, q) \setminus \mathcal{Q}$
(except possibly $Y = 0$)

Points of \mathcal{Q}

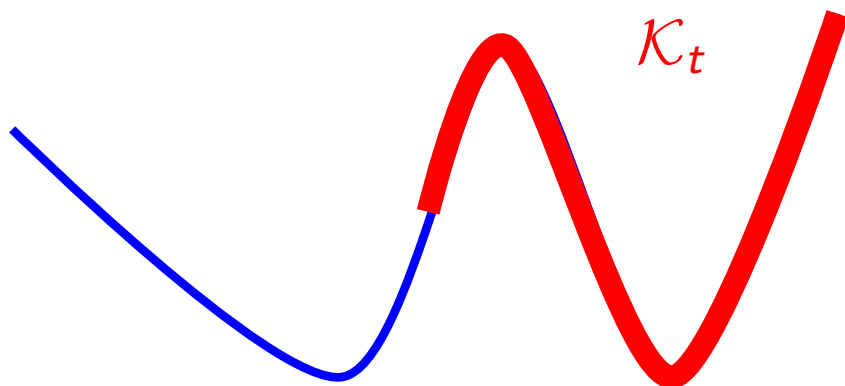


Problem

To find $T \subset \mathcal{Q}$

- T is a 3-arc
- T contains at least one coset \mathcal{K}_t
- T covers all the points of $\mathcal{Q} \setminus T$

Points of \mathcal{Q}



Problem

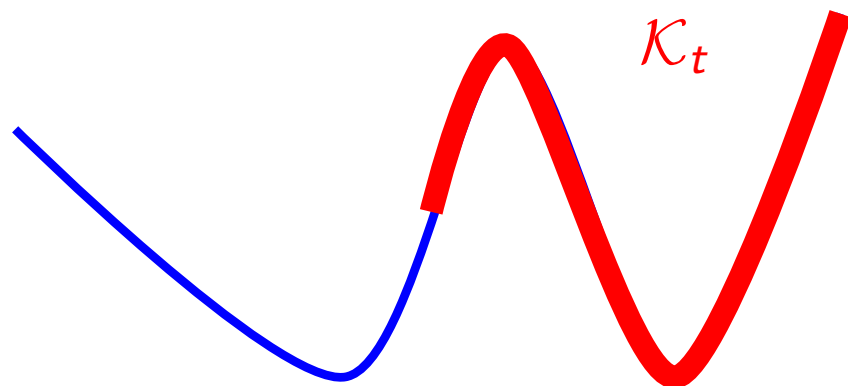
To find $T \subset \mathcal{Q}$

- T is a 3-arc
- T contains at least one coset \mathcal{K}_t
- T covers all the points of $\mathcal{Q} \setminus T$

In particular

- 4 points of T are not collinear
- every point in $\mathcal{Q} \setminus T$ is collinear with 3 points of T

Points of \mathcal{Q}



Problem

To find $T \subset \mathcal{Q}$

- T is a 3-arc
- T contains at least one coset \mathcal{K}_t
- T covers all the points of $\mathcal{Q} \setminus T$

In particular

- 4 points of T are not collinear
- every point in $\mathcal{Q} \setminus T$ is collinear with 3 points of T

Solution

Use 4-independent subsets!

k -independent subsets

Definition

\mathcal{G} : abelian group, $A \subset \mathcal{G}$

- $A \subset \mathcal{G}$
 k -independent subset $\iff x_1 + x_2 + \cdots + x_k \neq 0$
 $\forall x_i \in A$
- $g \in \mathcal{G} \setminus A$
 $covered$ by A $\iff x_1 + x_2 + \cdots + x_{k-1} + g = 0$
for some $x_i \in A$
- A maximal
 k -independent subset $\iff \forall g \in \mathcal{G} \setminus A$
 g is covered by A

3-independent subsets

Proposition

G abelian, *not* elementary 3-abelian

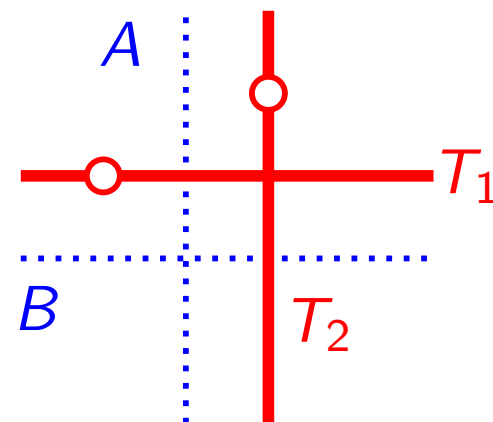
$T \subset G$ *maximal 3-independent subset*

$$c_1 \sqrt{|G|} \leq |T| \leq \frac{|G|}{2}$$

- (Voloch) $p \equiv 2 \pmod{3} \implies T = \{\pm 1, \pm 3, \dots, \pm \frac{p-2}{3}\} \subset \mathbb{Z}_p$
- (Voloch) $p \equiv 1 \pmod{3} \implies T = \{-1, 1, 3, 4, \dots, \frac{p-1}{3}\} \subset \mathbb{Z}_p$
- (Szőnyi) $G = A \times B$, A, B not elementary 3-abelian

$$T_1 = \{(a, x) \mid x \in B, x \neq -2a\}$$

$$T_2 = \{(y, b) \mid y \in A, y \neq -2b\}$$



4-independent subsets

- $M := \{(a^\sigma - a) \mid a \in \mathbb{F}_q\}$
- $\mathcal{K}_t := \{(v, v^4) \mid v \in M + t\}$, with $t \notin M$

4-independent subset in $\mathbb{F}_q/M \equiv \mathbb{F}_\sigma$

4-independent subsets

- $M := \{(a^\sigma - a) \mid a \in \mathbb{F}_q\}$
- $\mathcal{K}_t := \{(v, v^4) \mid v \in M + t\}$, with $t \notin M$

4-independent subset in $\mathbb{F}_q/M \equiv \mathbb{F}_\sigma$

Proposition

\mathcal{T} : 4-independent subset of \mathbb{F}_q/M

$$\mathcal{K}_{\mathcal{T}} = \bigcup_{M+t \in \mathcal{T}} \mathcal{K}_t$$

$\mathcal{K}_{\mathcal{T}}$ is a $(k, 3)$ -arc

4-independent subsets

- $M := \{(a^\sigma - a) \mid a \in \mathbb{F}_q\}$
- $\mathcal{K}_t := \{(v, v^4) \mid v \in M + t\}$, with $t \notin M$

4-independent subset in $\mathbb{F}_q/M \equiv \mathbb{F}_\sigma$

Proposition

\mathcal{T} : 4-independent subset of \mathbb{F}_q/M

$$\mathcal{K}_{\mathcal{T}} = \bigcup_{M+t \in \mathcal{T}} \mathcal{K}_t$$

$\mathcal{K}_{\mathcal{T}}$ is a $(k, 3)$ -arc

$$\begin{array}{l} \sigma = p^{h'} \\ h' \text{ odd} \end{array}$$

\implies

$$\sigma = p, \sigma = p^3, \dots$$

Theorem

- \mathcal{T} : 4-independent subset of \mathbb{F}_q/M
- $|\mathcal{T}| = n$
- $|\mathbb{F}_q/M \setminus \text{Cov}(\mathcal{T})| \leq m$
- $\mathcal{K}_{\mathcal{T}} = \bigcup_{M+t \in \mathcal{T}} \mathcal{K}_t$
- $q \geq 3600 \sigma^6$

\exists \mathcal{K} complete 3-arc

$$\mathcal{K}_{\mathcal{T}} \subset \mathcal{K} \subset \mathcal{Q}$$

$$|\mathcal{K}| \leq (n + m) \frac{q}{\sigma} + 6$$

$$|\mathcal{K}| \leq (n + m) \frac{q}{\sigma} + 6$$

- $$\begin{array}{l} \sigma = p \\ p \equiv 1 \pmod{4} \\ p \geq 29 \end{array} \Rightarrow \begin{array}{l} n = \frac{p-5}{4} \\ m = 1 \end{array} \Rightarrow |\mathcal{K}| \lesssim \frac{q}{4}$$
- $$\begin{array}{l} \sigma = p \\ p \equiv 3 \pmod{4} \\ p > 29 \end{array} \Rightarrow \begin{array}{l} n = \frac{p-7}{4} \\ m = 3 \end{array} \Rightarrow |\mathcal{K}| \lesssim \frac{q}{4}$$
- $$\sigma \geq p^3 \Rightarrow \begin{array}{l} n = 2\sqrt{\frac{\sigma}{p}} + p - 4 \\ m = 2(\sqrt{\sigma p} - \sqrt{\frac{\sigma}{p}}) \end{array} \Rightarrow |\mathcal{K}| \lesssim 2\sqrt{\frac{p}{\sigma}}q$$

$$|\mathcal{K}| \leq (n + m) \frac{q}{\sigma} + 6$$

- $$\begin{array}{l} \sigma = p \\ p \equiv 1 \pmod{4} \\ p \geq 29 \end{array} \Rightarrow \begin{array}{l} n = \frac{p-5}{4} \\ m = 1 \end{array} \Rightarrow |\mathcal{K}| \lesssim \frac{q}{4}$$
- $$\begin{array}{l} \sigma = p \\ p \equiv 3 \pmod{4} \\ p > 29 \end{array} \Rightarrow \begin{array}{l} n = \frac{p-7}{4} \\ m = 3 \end{array} \Rightarrow |\mathcal{K}| \lesssim \frac{q}{4}$$
- $$\sigma \geq p^3 \Rightarrow \begin{array}{l} n = 2\sqrt{\frac{\sigma}{p}} + p - 4 \\ m = 2(\sqrt{\sigma p} - \sqrt{\frac{\sigma}{p}}) \end{array} \Rightarrow |\mathcal{K}| \lesssim 2\sqrt{\frac{p}{\sigma}}q$$

$$\begin{array}{l} \sigma = p^3 \\ p > 13 \\ q = \sigma^7 \end{array} \Rightarrow |\mathcal{K}| \simeq q^{20/21}$$

Future developments

Idea of Segre and Lombardo-Radice

*The points of the arc are chosen, with few exceptions,
among the points of a conic or a cubic curve*

Our Idea

*The points of the $(n, 3)$ -arc are chosen, with few exceptions,
among the points of *an irreducible quartic curve**

Future developments

Idea of Segre and Lombardo-Radice

*The points of the arc are chosen, with few exceptions,
among the points of a conic or a cubic curve*

Our Idea

*The points of the $(n, 3)$ -arc are chosen, with few exceptions,
among the points of *an irreducible quartic curve**

(n, r) -arcs?

NATURAL IDEA:

*The points of the (n, r) -arc are chosen, with few exceptions,
among the points of **an irreducible curve**
of degree $r + 1$ ($Y = X^{r+1}$)*

Future developments

NATURAL IDEA:

*The points of the (n, r) -arc are chosen, with few exceptions,
among the points of **an irreducible curve**
of degree $r + 1$ ($Y = X^{r+1}$)*

PROBLEM:

The curve \mathcal{H}_P is more complicated

Future developments

NATURAL IDEA:

*The points of the (n, r) -arc are chosen, with few exceptions, among the points of **an irreducible curve** of degree $r + 1$ ($Y = X^{r+1}$)*

PROBLEM:

The curve \mathcal{H}_P is more complicated

$r = 4$: Collinearity condition between

$$P = (a, b), P_1 = (u, u^5), P_2 = (v, v^5), P_3 = (w, w^5), P_4 = (s, s^5)$$

$$\begin{cases} b + uv(u^3 + u^2v + uv^2 + v^3) - a(u^4 + u^3v + u^2v^2 + uv^3 + v^4) = 0 \\ w^3 + w^2(u + v) + w(u^2 + uv + v^2) + (u^3 + u^2v + uv^2 + v^3) = 0 \\ s^2 + s(u + v + w) + u^2 + v^2 + w^2 + uv + uw + vw = 0 \end{cases}$$

THANK YOU
FOR YOUR ATTENTION!