Good covering codes from algebraic curves

Massimo Giulietti

University of Perugia (Italy)

Special Semester on Applications of Algebra and Number Theory
Workshop 2: Algebraic curves over finite fields
Linz, 14 November 2013
coverings codes

\((\mathbb{F}_q^n, d)\) \quad d \text{ Hamming distance} \quad C \subset \mathbb{F}_q^n
covering codes

\((\mathbb{F}_q^n, d)\)  \quad \text{d Hamming distance}  \quad C \subset \mathbb{F}_q^n

- covering radius of \(C\)

\[ R(C) := \max_{v \in \mathbb{F}_q^n} d(v, C) \]
covering codes

$((\mathbb{F}_q^n, d))$ $d$ Hamming distance $C \subset \mathbb{F}_q^n$

covering radius of $C$

$R(C) := \max_{v \in \mathbb{F}_q^n} d(v, C)$
covering codes

$(\mathbb{F}_q^n, d)$  \hspace{1cm} $d$ Hamming distance  \hspace{1cm} $C \subset \mathbb{F}_q^n$

- covering radius of $C$

\[
R(C) := \max_{v \in \mathbb{F}_q^n} d(v, C)
\]

- covering density of $C$

\[
\mu(C) := \# C \cdot \frac{\text{size of a sphere of radius } R(C)}{q^n}
\]
covering codes

\((\mathbb{F}_q^n, d)\) \hspace{1cm} \text{d Hamming distance} \quad \text{C} \subset \mathbb{F}_q^n

- covering radius of \text{C}

\[ R(C) := \max_{v \in \mathbb{F}_q^n} d(v, C) \]

\( \mathbb{F}_q^n \)

- covering density of \text{C}

\[ \mu(C) := \#C \cdot \frac{\text{size of a sphere of radius } R(C)}{q^n} \geq 1 \]
linear codes

\[ k = \text{dim } C \quad r = n - k \]

\[ \mu(C) = \frac{1 + n(q - 1) + \binom{n}{2}(q - 1)^2 + \ldots + \binom{n}{R(C)}(q - 1)^{R(C)}}{q^r} \]
linear codes

\[ k = \dim C \quad r = n - k \]

\[
\mu(C) = \frac{1 + n(q - 1) + \binom{n}{2}(q - 1)^2 + \ldots + \binom{n}{R(C)}(q - 1)^{R(C)}}{q^r}
\]

\[
\ell(r, q)_R := \min n \text{ for which there exists } C \subset \mathbb{F}_q^n \text{ with } R(C) = R, \quad n - \dim(C) = r
\]
linear codes

\[ k = \dim C \quad r = n - k \]

\[ \mu(C) = \frac{1 + n(q - 1) + \binom{n}{2}(q - 1)^2 + \ldots + \binom{n}{R(C)}(q - 1)^{R(C)}}{q^r} \]

\[ \ell(r, q)_R, d := \min n \text{ for which there exists } C \subset \mathbb{F}_q^n \text{ with } \]
\[ R(C) = R, \quad n - \dim(C) = r, \quad d(C) = d \]
linear codes

\[ k = \dim C \quad r = n - k \]

\[
\mu(C) = \frac{1 + n(q - 1) + \binom{n}{2}(q - 1)^2 + \ldots + \binom{n}{R(C)}(q - 1)^{R(C)}}{q^r}
\]

\[
\ell(r, q)_{R,d} := \min n \text{ for which there exists } C \subset \mathbb{F}_q^n \text{ with}\]
\[
R(C) = R, \quad n - \dim(C) = r, \quad d(C) = d
\]

\[ R = 2, \quad d = 4 \quad \text{(quasi-perfect codes)} \]

\[ R = r - 1, \quad d = r + 1 \quad \text{(MDS codes)} \]

\[ q \text{ odd} \]
\( l(3, q)_{2,4} \)
in geometrical terms...

$$\Sigma = \Sigma(2, q)$$

Galois plane over the finite field $\mathbb{F}_q$
in geometrical terms...

\[\Sigma = \Sigma(2, q)\]

Galois plane over the finite field \(\mathbb{F}_q\)

\(S \subset \Sigma\) is a **saturating** set if every point in \(\Sigma \setminus S\) is collinear with two points in \(S\)

![Diagram](image)
in geometrical terms...

\[ \Sigma = \Sigma(2, q) \]

Galois plane over the finite field \( \mathbb{F}_q \)

- \( S \subset \Sigma \) is a **saturating** set if every point in \( \Sigma \setminus S \) is collinear with two points in \( S \)
in geometrical terms...

$$\Sigma = \Sigma(2, q)$$

Galois plane over the finite field $\mathbb{F}_q$

$S \subset \Sigma$ is a **saturating** set if every point in $\Sigma \setminus S$ is collinear with two points in $S$
\[ \Sigma = \Sigma(2, q) \]

Galois plane over the finite field \( \mathbb{F}_q \)

\( S \subset \Sigma \) is a **saturating** set if every point in \( \Sigma \setminus S \) is collinear with two points in \( S \)
in geometrical terms...

\[ \Sigma = \Sigma(2, q) \]

Galois plane over the finite field \( \mathbb{F}_q \)

- \( S \subset \Sigma \) is a **saturating** set if every point in \( \Sigma \setminus S \) is collinear with two points in \( S \)
- a **complete cap** is a saturating set which does not contain 3 collinear points
in geometrical terms...

\[ \Sigma = \Sigma(2, q) \]

Galois plane over the finite field \( \mathbb{F}_q \)

- \( S \subset \Sigma \) is a **saturating** set if every point in \( \Sigma \setminus S \) is collinear with two points in \( S \)

- a **complete cap** is a saturating set which does not contain 3 collinear points

\[ \ell(3, q)_{2,4} = \text{minimum size of a complete cap in } \mathbb{P}^2(\mathbb{F}_q) \]
plane complete caps

- TLB:
  \[ #S > \sqrt{2q} + 1 \]
plane complete caps

- TLB:
  \[ \#S > \sqrt{2q} + 1 \]

- in \( \mathbb{P}^2(\mathbb{F}_q) \) there exists a complete cap \( S \) of size
  \[ \#S \leq D\sqrt{q} \log^{C} q \]

(Kim-Vu, 2003)
plane complete caps

- TLB:
  \[ \#S > \sqrt{2q} + 1 \]

- in \( \mathbb{P}^2(\mathbb{F}_q) \) there exists a complete cap \( S \) of size
  \[ \#S \leq D\sqrt{q} \log^C q \]
  (Kim-Vu, 2003)

- for every \( q \) prime \( q < 67000 \) there exists a complete cap \( S \) of size
  \[ \#S \leq \sqrt{q} \log q \]
  (Bartoli-Davydov-Faina-Marcugini-Pambianco, 2012)
plane complete caps

- TLB:
  \[ \#S > \sqrt{2q} + 1 \]

- In \( \mathbb{P}^2(\mathbb{F}_q) \) there exists a complete cap \( S \) of size
  \[ \#S \leq D \sqrt{q} \log^C q \]
  (Kim-Vu, 2003)

- For every prime \( q < 67000 \) there exists a complete cap \( S \) of size
  \[ \#S \leq \sqrt{q} \log q \]
  (Bartoli-Davydov-Faina-Marcugini-Pambianco, 2012)
• *naive* construction method:
naive construction method:

\[ S = \{ P_1, P_2, \} \]
naive construction method:

\[ S = \{ P_1, P_2, P_3, \} \]
*naive* construction method:

$$S = \{P_1, P_2, P_3, P_4, \}$$
naive construction method:

\[ S = \{ P_1, P_2, P_3, P_4, \ldots, \} \]
naive construction method:

\[ S = \{P_1, P_2, P_3, P_4, \ldots, P_n\} \]

- naive vs. theoretical
Naive algorithm
\( \sqrt{q} \cdot (\log q)^{0.75} \) →

\( \sqrt{3q + 1/2} \)

← Naive algorithm

TLB
$\mathcal{X}$ plane irreducible cubic curve
$\mathcal{X}$ plane irreducible cubic curve

$G = \mathcal{X}(\mathbb{F}_q) \setminus \text{Sing}(\mathcal{X})$

- If $O$ is an inflection point of $\mathcal{X}$, then $P, Q, T \in G$ are collinear if and only if

  $P \oplus Q \oplus T = O$
If $O$ is an inflection point of $\mathcal{X}$, then $P, Q, T \in G$ are collinear if and only if $P \oplus Q \oplus T = O$.

For a subgroup $K$ of index $m$ with $(3, m) = 1$, no 3 points in a coset $S = K \oplus Q$, $Q \notin K$ are collinear.
classification \((p > 3)\)
classification \((p > 3)\)
classification ($p > 3$)
classification \((p > 3)\)
Y = X^3

XY = (X - 1)^3

Y(X^2 - \beta) = 1

Y^2 = X^3 + AX + B
how to prove completeness?

- $S$ parametrized by polynomials defined over $\mathbb{F}_q$

$$S = \{(f(t), g(t)) | t \in \mathbb{F}_q\} \subset \mathbb{A}^2(\mathbb{F}_q)$$
how to prove completeness?

- $S$ parametrized by polynomials defined over $\mathbb{F}_q$

\[ S = \{(f(t), g(t)) \mid t \in \mathbb{F}_q \} \subset \mathbb{A}^2(\mathbb{F}_q) \]

- $P = (a, b)$ collinear with two points in $S$ if there exist $x, y \in \mathbb{F}_q$ with

\[
\det \begin{pmatrix} a & b & 1 \\ f(x) & g(x) & 1 \\ f(y) & g(y) & 1 \end{pmatrix} = 0
\]
How to prove completeness?

- \( S \) parametrized by polynomials defined over \( \mathbb{F}_q \)

\[
S = \{(f(t), g(t)) \mid t \in \mathbb{F}_q\} \subset \mathbb{A}^2(\mathbb{F}_q)
\]

- \( P = (a, b) \) collinear with two points in \( S \) if there exist \( x, y \in \mathbb{F}_q \) with \( F_{a,b}(x, y) = 0 \), where

\[
F_{a,b}(x, y) := \det \begin{pmatrix}
a & b & 1 \\
f(x) & g(x) & 1 \\
f(y) & g(y) & 1
\end{pmatrix}
\]
how to prove completeness?

- $S$ parametrized by polynomials defined over $\mathbb{F}_q$
  \[ S = \{(f(t), g(t)) \mid t \in \mathbb{F}_q\} \subset \mathbb{A}^2(\mathbb{F}_q) \]

- $P = (a, b)$ collinear with two points in $S$ if there exist $x, y \in \mathbb{F}_q$ with $F_{a,b}(x, y) = 0$, where
  \[ F_{a,b}(x, y) := \det \begin{pmatrix} a & b & 1 \\ f(x) & g(x) & 1 \\ f(y) & g(y) & 1 \end{pmatrix} \]

- $P = (a, b)$ collinear with two points in $S$ if the algebraic curve
  \[ C_P : F_{a,b}(X, Y) = 0 \]
  has a suitable $\mathbb{F}_q$-rational point $(x, y)$
how to prove completeness?

- $S$ parametrized by polynomials defined over $\mathbb{F}_q$

$$S = \{(f(t), g(t)) \mid t \in \mathbb{F}_q\} \subset \mathbb{A}^2(\mathbb{F}_q)$$

- $P = (a, b)$ collinear with two points in $S$ if there exist $x, y \in \mathbb{F}_q$ with $F_{a,b}(x, y) = 0$, where

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

- $P = (a, b)$ collinear with two points in $S$ if the algebraic curve

$$C_P : F_{a,b}(X, Y) = 0$$

has a suitable $\mathbb{F}_q$-rational point $(x, y)$
cuspidal case: $Y = X^3$

- $G$ is an elementary abelian $p$-group
  - $q = p^h$
cuspidal case: $Y = X^3$

- $G$ is an elementary abelian $p$-group $q = p^h$

$$K = \left\{ (t^p - t, (t^p - t)^3) \mid t \in \mathbb{F}_q \right\}$$
kuspidal case: \( Y = X^3 \)

- \( G \) is an elementary abelian \( p \)-group \( \quad q = p^h \)

\[
K = \{ (t^p - t, (t^p - t)^3) \mid t \in \mathbb{F}_q \}
\]

\[
S = \{ \underbrace{(t^p - t + \bar{t}, (t^p - t + \bar{t})^3)}_{P_t} \mid t \in \mathbb{F}_q \}
\]
cuspidal case: \( Y = X^3 \)

- \( G \) is an elementary abelian \( p \)-group \( q = p^h \)

\[
K = \{ (t^p - t, (t^p - t)^3) \mid t \in \mathbb{F}_q \}
\]

\[
S = \{ \underbrace{(t^p - t + \bar{t}, (t^p - t + \bar{t})^3)}_{P_t} \mid t \in \mathbb{F}_q \}
\]

- \( P = (a, b) \) is collinear with \( P_x \) and \( P_y \) if and only if

\[
F_{a,b}(x, y) := a + (x^p - x + \bar{t})(y^p - y + \bar{t})^2 +
(x^p - x + \bar{t})^2(y^p - y + \bar{t}) - b((x^p - x + \bar{t})^2
+(x^p - x + \bar{t})(y^p - y + \bar{t}) + (y^p - y + \bar{t})^2) = 0
\]
cuspidal case: \( Y = X^3 \)

- \( G \) is an elementary abelian \( p \)-group \quad \( q = p^h \)

\[
K = \{ (t^p - t, (t^p - t)^3) \mid t \in \mathbb{F}_q \}
\]

\[
S = \{ \{(t^p - t + \bar{t}, (t^p - t + \bar{t})^3) \mid t \in \mathbb{F}_q \}
\]

- \( P = (a, b) \) is collinear with \( P_x \) and \( P_y \) if and only if

\[
F_{a,b}(x, y) := a + (x^p - x + \bar{t})(y^p - y + \bar{t})^2 + (x^p - x + \bar{t})^2(y^p - y + \bar{t}) - b((x^p - x + \bar{t})^2 + (x^p - x + \bar{t})(y^p - y + \bar{t}) + (y^p - y + \bar{t})^2) = 0
\]

- the curve \( C_P \) then is \( F_{a,b}(X, Y) = 0 \)
applying Segre's criterion

(Segre, 1962)

if there exists a point $P \in C$ and a tangent $\ell$ of $C$ at $P$ such that
- $\ell$ counts once among the tangents of $C$ at $P$,
- the intersection multiplicity of $C$ and $\ell$ at $P$ equals $\deg(C)$,
- $C$ has no linear components through $P$,
then $C$ is irreducible.
applying Segre's criterion

(Segre, 1962)

if there exists a point $P \in C$ and a tangent $\ell$ of $C$ at $P$ such that
- $\ell$ counts once among the tangents of $C$ at $P$,  
- the intersection multiplicity of $C$ and $\ell$ at $P$ equals $\deg(C)$,
- $C$ has no linear components through $P$,

then $C$ is irreducible.

$$F_{a,b}(X, Y) := a + (X^p - X + \bar{t})(Y^p - Y + \bar{t})^2 + (X^p - X + \bar{t})^2(Y^p - Y + \bar{t}) - b((X^p - X + \bar{t})^2 + (X^p - X + \bar{t})(Y^p - Y + \bar{t}) + (Y^p - Y + \bar{t})^2) = 0$$
applying Segre’s criterion

(Segre, 1962)

if there exists a point $P \in C$ and a tangent $\ell$ of $C$ at $P$ such that

- $\ell$ counts once among the tangents of $C$ at $P$,
- the intersection multiplicity of $C$ and $\ell$ at $P$ equals $\deg(C)$,
- $C$ has no linear components through $P$,

then $C$ is irreducible.

$$F_{a,b}(X, Y) := a + (X^p - X + \bar{t})(Y^p - Y + \bar{t})^2 + (X^p - X + \bar{t})^2(Y^p - Y + \bar{t}) - b((X^p - X + \bar{t})^2 + (X^p - X + \bar{t})(Y^p - Y + \bar{t}) + (Y^p - Y + \bar{t})^2) = 0$$

at $P = X_\infty$ the tangents are $\ell : Y = \beta$ with $\beta^p - \beta + \bar{t} = b$
applying Segre’s criterion

(Segre, 1962)

if there exists a point \( P \in C \) and a tangent \( \ell \) of \( C \) at \( P \) such that
- \( \ell \) counts once among the tangents of \( C \) at \( P \),
- the intersection multiplicity of \( C \) and \( \ell \) at \( P \) equals \( \text{deg}(C) \),
- \( C \) has no linear components through \( P \),

then \( C \) is irreducible.

\[
F_{a,b}(X, Y) := a + (X^p - X + \bar{t})(Y^p - Y + \bar{t})^2 + (X^p - X + \bar{t})^2(Y^p - Y + \bar{t}) - b((X^p - X + \bar{t})^2 + (X^p - X + \bar{t})(Y^p - Y + \bar{t}) + (Y^p - Y + \bar{t})^2) = 0
\]

at \( P = X_\infty \) the tangents are \( \ell : Y = \beta \) with \( \beta^p - \beta + \bar{t} = b \)

\[
F_{a,b}(X, \beta) = a - b^3
\]
applying Segre's criterion

(Segre, 1962)

if there exists a point $P \in C$ and a tangent $\ell$ of $C$ at $P$ such that
- $\ell$ counts once among the tangents of $C$ at $P$,
- the intersection multiplicity of $C$ and $\ell$ at $P$ equals $\deg(C)$,
- $C$ has no linear components through $P$,

then $C$ is irreducible.

$$F_{a,b}(X, Y) := a + (X^p - X + \bar{t})(Y^p - Y + \bar{t})^2 + (X^p - X + \bar{t})^2(Y^p - Y + \bar{t}) - b((X^p - X + \bar{t})^2 + (X^p - X + \bar{t})(Y^p - Y + \bar{t}) + (Y^p - Y + \bar{t})^2) = 0$$

at $P = X_\infty$ the tangents are $\ell : Y = \beta$ with $\beta^p - \beta + \bar{t} = b$

if $P \notin \mathcal{X}$

$$F_{a,b}(X, \beta) = a - b^3$$

$C_P$ is irreducible of genus $g \leq 3p^2 - 3p + 1$
applying Segre’s criterion

(Segre, 1962)

if there exists a point $P \in C$ and a tangent $\ell$ of $C$ at $P$ such that

- $\ell$ counts once among the tangents of $C$ at $P$,
- the intersection multiplicity of $C$ and $\ell$ at $P$ equals $\deg(C)$,
- $C$ has no linear components through $P$,

then $C$ is irreducible.

$$F_{a, b}(X, Y) := a + (X^p - X + \bar{t})(Y^p - Y + \bar{t})^2 +
(X^p - X + \bar{t})^2(Y^p - Y + \bar{t}) - b((X^p - X + \bar{t})^2
+ (X^p - X + \bar{t})(Y^p - Y + \bar{t}) + (Y^p - Y + \bar{t})^2) = 0$$

at $P = X_\infty$ the tangents are $\ell : Y = \beta$ with $\beta^p - \beta + \bar{t} = b$

if $P \notin X$

- $C_P$ is irreducible of genus $g \leq 3p^2 - 3p + 1$
- $C_P$ has at least $q + 1 - (6p^2 - 6p + 2)\sqrt{q}$ points
cuspidal case: $Y = X^3$

- $G$ is elementary abelian, isomorphic to $(\mathbb{F}_q, +)$
cuspidal case: $Y = X^3$

- $G$ is elementary abelian, isomorphic to $(\mathbb{F}_q, +)$

$$S = \{(L(t) + \bar{t}, (L(t) + \bar{t})^3) \mid t \in \mathbb{F}_q\}$$

$$L(T) = \prod_{\alpha \in M} (T - \alpha), \quad M < (\mathbb{F}_q, +), \quad \#M = m$$
cuspidal case: \( Y = X^3 \)

- \( G \) is elementary abelian, isomorphic to \((\mathbb{F}_q, +)\)

\[
S = \{(L(t) + \bar{t}, (L(t) + \bar{t})^3) \mid t \in \mathbb{F}_q\}
\]

\[
L(T) = \prod_{\alpha \in M} (T - \alpha), \quad M < (\mathbb{F}_q, +), \quad \#M = m
\]

- \( P = (a, b) \) is collinear with \( P_x \) and \( P_y \) if and only if

\[
F_{a,b}(x, y) := a + (L(x) + \bar{t})(L(y) + \bar{t})^2 + \\
(L(x) + \bar{t})^2(L(y) + \bar{t}) - b((L(x) + \bar{t})^2 \\
+ (L(x) + \bar{t})(L(y) + \bar{t}) + (L(y) + \bar{t})^2) = 0
\]
cuspidal case: \( Y = X^3 \)

- \( G \) is elementary abelian, isomorphic to \((\mathbb{F}_q,+)\)

\[
S = \left\{ \left( (L(t) + \bar{t}, (L(t) + \bar{t})^3) \right) \middle| t \in \mathbb{F}_q \right\}
\]

\[
L(T) = \prod_{\alpha \in M} (T - \alpha), \quad M < (\mathbb{F}_q,+), \quad \#M = m
\]

- \( P = (a, b) \) is collinear with \( P_x \) and \( P_y \) if and only if

\[
F_{a,b}(x, y) := a + (L(x) + \bar{t})(L(y) + \bar{t})^2 + (L(x) + \bar{t})^2(L(y) + \bar{t}) - b((L(x) + \bar{t})^2 + (L(x) + \bar{t})(L(y) + \bar{t}) + (L(y) + \bar{t})^2) = 0
\]

if \( P \notin \mathcal{X} \)

- \( C_P \) is irreducible of genus \( g \leq 3m^2 - 3m + 1 \)
cuspidal case: $Y = X^3$

- $G$ is elementary abelian, isomorphic to $(\mathbb{F}_q, +)$

$$S = \left\{ (L(t) + \bar{t}, (L(t) + \bar{t})^3) \mid t \in \mathbb{F}_q \right\}$$

$$L(T) = \prod_{\alpha \in M} (T - \alpha), \quad M < (\mathbb{F}_q, +), \quad \#M = m$$

- $P = (a, b)$ is collinear with $P_x$ and $P_y$ if and only if

$$F_{a, b}(x, y) := a + (L(x) + \bar{t})(L(y) + \bar{t})^2 + (L(x) + \bar{t})^2(L(y) + \bar{t}) - b((L(x) + \bar{t})^2 + (L(x) + \bar{t})(L(y) + \bar{t}) + (L(y) + \bar{t})^2) = 0$$

if $P \notin \mathcal{X}$

- $C_P$ is irreducible of genus $g \leq 3m^2 - 3m + 1$

- $C_P$ has at least $q + 1 - (6m^2 - 6m + 2)\sqrt{q}$ points
let $P = (a, b)$ be a point in $\mathbb{A}^2(\mathbb{F}_q) \setminus \mathcal{X}$; if

$$m < \sqrt[q/36]{q}$$

then there is a secant of $S$ passing through $P$.  

(Szőnyi, 1985 - Anbar, Bartoli, G., Platoni, 2013)
(Szőnyi, 1985 - Anbar, Bartoli, G., Platoni, 2013)

let $P = (a, b)$ be a point in $\mathbb{A}^2(F_q) \setminus \mathcal{X}$; if

$$m < \frac{4\sqrt{q}}{36}$$

then there is a secant of $S$ passing through $P$.

- $m$ is a power of $p$
let $P = (a, b)$ be a point in $\mathbb{A}^2(\mathbb{F}_q) \setminus \mathcal{X}$; if

$$m < \sqrt[4]{q/36}$$

then there is a secant of $S$ passing through $P$.

- $m$ is a power of $p$
- the points in $\mathcal{X} \setminus S$ need to be dealt with
(Szőnyi, 1985 - Anbar, Bartoli, G., Platoni, 2013)

let $P = (a, b)$ be a point in $\mathbb{A}^2(\mathbb{F}_q) \setminus \mathcal{X}$; if

$$m < \frac{4\sqrt{q}}{36}$$

then there is a secant of $S$ passing through $P$.

- $m$ is a power of $p$
- the points in $\mathcal{X} \setminus S$ need to be dealt with

**Theorem**

if $m < \frac{4\sqrt{q}}{36}$, then there exists a complete cap in $\mathbb{A}^2(\mathbb{F}_q)$ with size

$$m + \frac{q}{m} - 3$$
(Szőnyi, 1985 - Anbar, Bartoli, G., Platoni, 2013)

let $P = (a, b)$ be a point in $\mathbb{A}^2(\mathbb{F}_q) \setminus \mathcal{X}$; if

$$m < \sqrt[4]{q/36}$$

then there is a secant of $S$ passing through $P$.

- $m$ is a power of $p$
- the points in $\mathcal{X} \setminus S$ need to be dealt with

**theorem**

if $m < \sqrt[4]{q/36}$, then there exists a complete cap in $\mathbb{A}^2(\mathbb{F}_q)$ with size

$$m + \frac{q}{m} - 3 \sim p^{1/4} \cdot q^{3/4}$$
nodal case: $XY = (X - 1)^3$

- $G$ is isomorphic to $(\mathbb{F}_q^*, \cdot)$

$$G \rightarrow \mathbb{F}_q^* \quad \left( v, \frac{(v - 1)^3}{v} \right) \mapsto v$$
nodal case: $XY = (X - 1)^3$

- $G$ is isomorphic to \((\mathbb{F}_q^*, \cdot)\)
  $$G \to \mathbb{F}_q^* \quad \left( v, \frac{(v - 1)^3}{v} \right) \mapsto v$$

- the subgroup of index $m$ ($m$ a divisor of $q - 1$):
  $$K = \left\{ \left( t^m, \frac{(t^m - 1)^3}{t^m} \right) \mid t \in \mathbb{F}_q^* \right\}$$
nodal case: $XY = (X - 1)^3$

- $G$ is isomorphic to $(\mathbb{F}_q^*, \cdot)$
  
  $$G \rightarrow \mathbb{F}_q^* \quad \left( v, \frac{(v - 1)^3}{v} \right) \mapsto v$$

- the subgroup of index $m$ ($m$ a divisor of $q - 1$):
  
  $$K = \left\{ \left( t^m, \frac{1 - t^m}{t^m} \right) \mid t \in \mathbb{F}_q^* \right\}$$

- a coset:
  
  $$S = \left\{ \left( \overline{tt}^m, \frac{1 - \overline{tt}^m}{\overline{tt}^m} \right) \mid t \in \mathbb{F}_q^* \right\}$$
nodal case: \( XY = (X - 1)^3 \)

- \( G \) is isomorphic to \((\mathbb{F}_q^*, \cdot)\)

\[
G \rightarrow \mathbb{F}_q^* \quad \left( v, \frac{(v - 1)^3}{v} \right) \mapsto v
\]

- the subgroup of index \( m \) (\( m \) a divisor of \( q - 1 \)):

\[
K = \left\{ \left( t^m, \frac{(t^m - 1)^3}{t^m} \right) \mid t \in \mathbb{F}_q^* \right\}
\]

- a coset:

\[
S = \left\{ \left( \tt t^m, \frac{(tt^m - 1)^3}{tt^m} \right) \mid t \in \mathbb{F}_q^* \right\}
\]
nodal case: $XY = (X - 1)^3$

- $G$ is isomorphic to $\left( \mathbb{F}_q^*, \cdot \right)$
  $$G \rightarrow \mathbb{F}_q^* \quad \left( v, \frac{(v - 1)^3}{v} \right) \mapsto v$$
- the subgroup of index $m$ ($m$ a divisor of $q - 1$):
  $$K = \left\{ \left( t^m, \frac{(t^m - 1)^3}{t^m} \right) \mid t \in \mathbb{F}_q^* \right\}$$
- a coset:
  $$S = \left\{ \left( \tilde{t} t^m, \frac{(\tilde{t} t^m - 1)^3}{\tilde{t} t^m} \right) \mid t \in \mathbb{F}_q^* \right\}$$

- the curve $C_P$:
  $$F_{a, b}(X, Y) = a(\tilde{t}^3 X^{2m} Y^m + \tilde{t}^3 X^m Y^{2m} - 3 \tilde{t}^2 X^m Y^m + 1)$$
  $$- b \tilde{t}^2 X^m Y^m - \tilde{t}^4 X^{2m} Y^{2m} + 3 \tilde{t}^2 X^m Y^m$$
  $$- \tilde{t} X^m - \tilde{t} Y^m = 0$$
let $P$ be a point in $\mathbb{A}^2(\mathbb{F}_q) \setminus \mathcal{X}$; if

$$m < \sqrt[4]{q}/36$$

then there is a secant of $S$ passing through $P$
let $P$ be a point in $\mathbb{A}^2(\mathbb{F}_q) \setminus \mathcal{X}$; if

$$m < \frac{4 \sqrt{q}}{36}$$

then there is a secant of $S$ passing through $P$

- $m$ is a divisor of $q - 1$
(Anbar-Bartoli-G.-Platoni, 2013)

let $P$ be a point in $\mathbb{A}^2(\mathbb{F}_q) \setminus \mathcal{X}$; if

$$m < \frac{4\sqrt{q}}{36}$$

then there is a secant of $S$ passing through $P$

- $m$ is a divisor of $q - 1$
- some points from $\mathcal{X} \setminus S$ need to be added to $S$
let $P$ be a point in $\mathbb{A}^2(F_q) \setminus \mathcal{X}$; if

$$m < \sqrt[4]{q/36}$$

then there is a secant of $S$ passing through $P$

- $m$ is a divisor of $q - 1$
- some points from $\mathcal{X} \setminus S$ need to be added to $S$

**Theorem**

if $m$ is a divisor of $q - 1$ with $m < \sqrt[4]{q/36}$, and in addition $(m, \frac{q-1}{m}) = 1$, then there exists a complete cap in $\mathbb{A}^2(F_q)$ with size

$$m + \frac{q-1}{m} - 3$$
(Anbar-Bartoli-G.-Platoni, 2013)

let $P$ be a point in $\mathbb{A}^2(F_q) \setminus \mathcal{X}$; if

$$m < \frac{4\sqrt{q}}{36}$$

then there is a secant of $S$ passing through $P$

- $m$ is a divisor of $q - 1$
- some points from $\mathcal{X} \setminus S$ need to be added to $S$

**Theorem**

if $m$ is a divisor of $q - 1$ with $m < \frac{4\sqrt{q}}{36}$, and in addition $(m, \frac{q-1}{m}) = 1$, then there exists a complete cap in $\mathbb{A}^2(F_q)$ with size

$$m + \frac{q-1}{m} - 3 \sim q^{3/4}$$
isolated double point case: \( Y(X^2 - \beta) = 1 \)

- \( G \) cyclic of order \( q + 1 \)
isolated double point case: \( Y(X^2 - \beta) = 1 \)

- \( G \) cyclic of order \( q + 1 \)

(Anbar-Bartoli-G.-Platoni, 2013)

if \( m \) is a divisor of \( q + 1 \) with \( m < \frac{4}{36} \sqrt{q} \), and in addition \( (m, \frac{q+1}{m}) = 1 \), then there exists a complete cap in \( \mathbb{A}^2(\mathbb{F}_q) \) with size at most

\[
m + \frac{q+1}{m}
\]
isolated double point case: \( Y(X^2 - \beta) = 1 \)

- \( G \) cyclic of order \( q + 1 \)

(Anbar-Bartoli-G.-Platoni, 2013)

if \( m \) is a divisor of \( q + 1 \) with \( m < \sqrt[4]{q/36} \), and in addition \((m, \frac{q+1}{m}) = 1\), then there exists a complete cap in \( \mathbb{A}^2(\mathbb{F}_q) \) with size at most

\[
m + \frac{q + 1}{m} \sim q^{3/4}
\]
elliptic case: \( Y^2 = X^3 + AX + B \)

if 
\[
n \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}] \quad n \not\equiv q + 1 \pmod{p}
\]

there exists an elliptic cubic curve \( \mathcal{C} \) over \( \mathbb{F}_q \) with \( \#G = n \)
elliptic case: $Y^2 = X^3 + AX + B$

if

$$n \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}] \quad n \not\equiv q + 1 \pmod{p}$$

there exists an elliptic cubic curve $\mathcal{X}$ over $\mathbb{F}_q$ with $\#G = n$

(Voloch, 1988)

if $p$ does not divide $\#G - 1$, then $G$ can be assumed to be cyclic
elliptic case: \( Y^2 = X^3 + AX + B \)

if 
\[
n \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}] \quad n \not\equiv q + 1 \pmod{p}
\]
then there exists an elliptic cubic curve \( \mathcal{X} \) over \( \mathbb{F}_q \) with \( \#G = n \)

(Voloch, 1988)

if \( p \) does not divide \( \#G - 1 \), then \( G \) can be assumed to be cyclic

- **Problem:** no polynomial or rational parametrization of the points of \( S \) is possible
elliptic case: \( Y^2 = X^3 + AX + B \)

if

\[
n \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}] \quad n \not\equiv q + 1 \pmod{p}
\]

there exists an elliptic cubic curve \( \mathcal{X} \) over \( \mathbb{F}_q \) with \( \#G = n \)

(Voloch, 1988)

if \( p \) does not divide \( \#G - 1 \), then \( G \) can be assumed to be cyclic

- **problem**: no polynomial or rational parametrization of the points of \( S \) is possible
- Voloch’s solution (1990): implicit description of \( C_p \)
elliptic case: $Y^2 = X^3 + AX + B$

if

$$n \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}] \quad n \not\equiv q + 1 \pmod{p}$$

there exists an elliptic cubic curve $\mathcal{X}$ over $\mathbb{F}_q$ with $\#G = n$

(Voloch, 1988)

if $p$ does not divide $\#G - 1$, then $G$ can be assumed to be cyclic

- **problem**: no polynomial or rational parametrization of the points of $S$ is possible
- Voloch's solution (1990): implicit description of $C_P$
- Voloch's result would provide complete caps of size $\sim q^{3/4}$ for every $q$ large enough
elliptic case: $Y^2 = X^3 + AX + B$

if

$$n \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}] \quad n \not\equiv q + 1 \pmod{p}$$

there exists an elliptic cubic curve $\mathcal{C}$ over $\mathbb{F}_q$ with $\#G = n$

(Voloch, 1988)

if $p$ does not divide $\#G - 1$, then $G$ can be assumed to be cyclic

- **Problem**: no polynomial or rational parametrization of the points of $S$ is possible
- Voloch's solution (1990): implicit description of $C_P$
- Voloch's result would provide complete caps of size $\sim q^{3/4}$ for every $q$ large enough
elliptic case

$G$ cyclic $\quad m \mid q - 1 \quad m$ prime
elliptic case

$G$ cyclic  
$m \mid q - 1$  
$m$ prime

- Tate-Lichtenbaum Pairing

$\langle \cdot, \cdot \rangle: G[m] \times G/K \rightarrow \mathbb{F}_q^* / (\mathbb{F}_q^*)^m$
elliptic case

\[ G \text{ cyclic} \quad m \mid q - 1 \quad m \text{ prime} \]

- Tate-Lichtenbaum Pairing

\[ < \cdot, \cdot > : G[m] \times G/K \rightarrow \mathbb{F}_q^*/(\mathbb{F}_q^*)^m \]

- If \( m^2 \) does not divide \( \#G \), then for some \( T \) in \( G[m] \)

\[ < T, \cdot > : G/K \rightarrow \mathbb{F}_q^*/(\mathbb{F}_q^*)^m \]

is an isomorphism such that

\[ K \oplus Q \mapsto [\alpha_T(Q)] \]

where \( \alpha_T \) is a rational function on \( \mathcal{X} \)
elliptic case

\[ G \text{ cyclic} \quad m \mid q - 1 \quad m \text{ prime} \]

- Tate-Lichtenbaum Pairing

\[ < \cdot, \cdot > : G[m] \times G/K \rightarrow \mathbb{F}_q^*/(\mathbb{F}_q^*)^m \]

- if \( m^2 \) does not divide \#G, then for some \( T \) in \( G[m] \)

\[ < T, \cdot > : G/K \rightarrow \mathbb{F}_q^*/(\mathbb{F}_q^*)^m \]

is an isomorphism such that

\[ K \oplus Q \mapsto [\alpha_T(Q)] \]

where \( \alpha_T \) is a rational function on \( X \)

\[ S = \{ R \in G \mid \alpha_T(R) = dt^m \text{ for some } t \in \mathbb{F}_q \} \]
elliptic case

$$S = \{ R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ for some } t \in \mathbb{F}_q \}$$
elliptic case

\[ S = \{ R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ for some } t \in \mathbb{F}_q \} \]
elliptic case

\[ S = \{ R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ for some } t \in \mathbb{F}_q \} \]

\( P = (a, b) \) collinear with two points \((x, y), (u, v) \in S\) if there exist \(x, y, u, v, t, z \in \mathbb{F}_q\) with
elliptic case

\[ S = \{ R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ for some } t \in \mathbb{F}_q \} \]

\[ P = (a, b) \text{ collinear with two points } (x, y), (u, v) \in S \text{ if there exist } \]
\[ x, y, u, v, t, z \in \mathbb{F}_q \text{ with } \]
\[
\left\{
\begin{align*}
y^2 &= x^3 + Ax + B \\
v^2 &= u^3 + Au + B
\end{align*}
\right.
\]
elliptic case

\[ S = \{ R \in X \mid \alpha(R) = dt^m \text{ for some } t \in \mathbb{F}_q \} \]

\( P = (a, b) \) collinear with two points \((x, y), (u, v) \in S\) if there exist \(x, y, u, v, t, z \in \mathbb{F}_q\) with

\[
\begin{align*}
  y^2 &= x^3 + Ax + B \\
  v^2 &= u^3 + Au + B \\
  \alpha(x, y) &= dt^m \\
  \alpha(u, v) &= dz^m
\end{align*}
\]
elliptic case

\[ S = \{ R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ for some } t \in \mathbb{F}_q \} \]

\[ P = (a, b) \text{ collinear with two points } (x, y), (u, v) \in S \text{ if there exist } x, y, u, v, t, z \in \mathbb{F}_q \text{ with} \]

\[
\begin{align*}
  y^2 &= x^3 + Ax + B \\
  v^2 &= u^3 + Au + B \\
  \alpha(x, y) &= dt^m \\
  \alpha(u, v) &= dz^m \\
  \det \begin{pmatrix} a & b & 1 \\ x & y & 1 \\ u & v & 1 \end{pmatrix} &= 0
\end{align*}
\]
elliptic case

\[ S = \{ R \in \mathcal{X} \mid \alpha(R) = dt^m \text{ for some } t \in \mathbb{F}_q \} \]

\( P = (a, b) \) collinear with two points \((x, y), (u, v) \in S\) if there exist \(x, y, u, v, t, z \in \mathbb{F}_q\) with

\[
C_P : \begin{cases} 
  y^2 = x^3 + Ax + B \\
  v^2 = u^3 + Au + B \\
  \alpha(x, y) = dt^m \\
  \alpha(u, v) = dz^m \\
  \det \begin{pmatrix} a & b & 1 \\ x & y & 1 \\ u & v & 1 \end{pmatrix} = 0
\end{cases}
\]
(Anbar-G., 2012)

if $A \neq 0$, then $C_P$ is irreducible or admits an irreducible $\mathbb{F}_q$-rational component
(Anbar-G., 2012)

if $A \neq 0$, then $C_P$ is irreducible or admits an irreducible $\mathbb{F}_q$-rational component

if $m$ is a prime divisor of $q - 1$ with $m < \sqrt[4]{q/64}$, then there exists a complete cap in $\mathbb{A}^2(\mathbb{F}_q)$ with size at most

$$m + \left\lfloor \frac{q - 2\sqrt{q} + 1}{m} \right\rfloor + 31$$
(Anbar-G., 2012)

if $A \neq 0$, then $C_P$ is irreducible or admits an irreducible $\mathbb{F}_q$-rational component

if $m$ is a prime divisor of $q - 1$ with $m < \sqrt[4]{q/64}$, then there exists a complete cap in $\mathbb{A}^2(\mathbb{F}_q)$ with size at most

$$m + \left\lfloor \frac{q - 2\sqrt{q} + 1}{m} \right\rfloor + 31 \sim q^{3/4}$$
\ell (r, q)_{2,4}
in geometrical terms...

**Proposition**

\[ \ell(r, q)_{2,4} = \text{minimum size of a complete cap in } \mathbb{P}^{r-1}(\mathbb{F}_q) \]
in geometrical terms...

proposition

$$\ell(r, q)_{2,4} = \text{minimum size of a complete cap in } \mathbb{P}^{r-1}(\mathbb{F}_q)$$

trivial lower bound

$$\#S \geq \sqrt{2}q^{(N-1)/2} \text{ in } \mathbb{P}^N(\mathbb{F}_q)$$
proposition

\[ \ell(r, q)_{2,4} = \text{minimum size of a complete cap in } \mathbb{P}^{r-1}(\mathbb{F}_q) \]

trivial lower bound

\[ \# S \geq \sqrt{2q^{(N-1)/2}} \text{ in } \mathbb{P}^N(\mathbb{F}_q) \]
TLB:

\[ \sqrt{2} \cdot q \]
TLB:

\[
\sqrt{2} \cdot q
\]

\[
\frac{1}{2} q \sqrt{q} + 2
\]

(Pellegrino, 1999)
\( N = 3 \)

- **TLB:**

\[
\sqrt{2} \cdot q
\]

(Pellegrino, 1999)

\[
\frac{1}{2} q \sqrt{q} + 2
\]

(Faina, Faina-Pambianco, Hadnagy 1988-1999)

\[
\frac{q^2}{3}
\]
$N = 3$

- TLB:

$\sqrt{2} \cdot q$

(Pellegrino, 1999)
computational results
recursive constructions of complete caps

blow-up

\[ S \text{ cap in } \mathbb{A}^r(\mathbb{F}_{q^s}) \]
recursive constructions of complete caps

blow-up

- $S$ cap in $\mathbb{A}^r (\mathbb{F}_{q^s})$
- for each $P$ in $S$, substitute each coordinate in $\mathbb{F}_{q^s}$ with its expansion over $\mathbb{F}_q$

\[
(x_1, x_2, \ldots, x_r) \in \mathbb{A}^r (\mathbb{F}_{q^s})
\]

\[
(x_1^1, x_1^2, \ldots, x_1^s, \ldots, x_r^1, \ldots, x_r^s) \in \mathbb{A}^{rs} (\mathbb{F}_q)
\]
recursive constructions of complete caps

**blow-up**

- $S$ cap in $\mathbb{A}^r(F_{q^s})$
- for each $P$ in $S$, substitute each coordinate in $F_{q^s}$ with its expansion over $F_q$

\[
(x_1, x_2, \ldots, x_r) \in \mathbb{A}^r(F_{q^s})
\]

\[
(x_1^1, x_2^1, \ldots, x_1^s, \ldots, x_r^1, \ldots, x_r^s) \in \mathbb{A}^{rs}(F_q)
\]

- the resulting subset of $\mathbb{A}^{rs}(F_q)$ is a cap
recursive constructions of complete caps

blow-up

- $S$ cap in $\mathbb{A}^r(\mathbb{F}_{q^s})$
- for each $P$ in $S$, substitute each coordinate in $\mathbb{F}_{q^s}$ with its expansion over $\mathbb{F}_q$

\[
(x_1, x_2, \ldots, x_r) \in \mathbb{A}^r(\mathbb{F}_{q^s})
\]

\[
(x_1^1, x_1^2, \ldots, x_1^s, \ldots, x_r^1, \ldots, x_r^s) \in \mathbb{A}^{rs}(\mathbb{F}_q)
\]

- the resulting subset of $\mathbb{A}^{rs}(\mathbb{F}_q)$ is a cap

product

- $S_1$ cap in $\mathbb{A}^r(\mathbb{F}_q)$, $S_2$ cap in $\mathbb{A}^s(\mathbb{F}_q)$
recursive constructions of complete caps

blow-up

- $S$ cap in $\mathbb{A}^r(F_{q^s})$
- for each $P$ in $S$, substitute each coordinate in $F_{q^s}$ with its expansion over $\mathbb{F}_q$

\[
(x_1, x_2, \ldots, x_r) \in \mathbb{A}^r(F_{q^s})
\]

\[
(x_1^1, x_2^2, \ldots, x_1^s, \ldots, x_r^1, \ldots, x_r^s) \in \mathbb{A}^{rs}(\mathbb{F}_q)
\]

- the resulting subset of $\mathbb{A}^{rs}(\mathbb{F}_q)$ is a cap

product

- $S_1$ cap in $\mathbb{A}^r(\mathbb{F}_q)$, $S_2$ cap in $\mathbb{A}^s(\mathbb{F}_q)$
- $S_1 \times S_2$ is a cap in $\mathbb{A}^{r+s}(\mathbb{F}_q)$
recursive constructions of complete caps

**blow-up**

- $S$ cap in $\mathbb{A}^r(F_{q^s})$
- for each $P$ in $S$, substitute each coordinate in $F_{q^s}$ with its expansion over $F_q$

\[
(x_1, x_2, \ldots, x_r) \in \mathbb{A}^r(F_{q^s})
\]

\[
(x_1^1, x_1^2, \ldots, x_1^s, \ldots, x_r^1, \ldots, x_r^s) \in \mathbb{A}^{rs}(F_q)
\]

- the resulting subset of $\mathbb{A}^{rs}(F_q)$ is a cap

**product**

- $S_1$ cap in $\mathbb{A}^r(F_q)$, $S_2$ cap in $\mathbb{A}^s(F_q)$
- $S_1 \times S_2$ is a cap in $\mathbb{A}^{r+s}(F_q)$

- do such constructions preserve completeness?
recursive constructions of complete caps

$T_N$ blow-up of a parabola of $\mathbb{A}^2(\mathbb{F}_{q^{N/2}})$
recursive constructions of complete caps

$T_N$ blow-up of a parabola of $\mathbb{A}^2(F_{q^{N/2}})$

(Davydov-Östergård, 2001)

$T_N$ is complete in $\mathbb{A}^N(F_q) \iff N/2$ is odd.
recursive constructions of complete caps

\[ T_N \] blow-up of a parabola of \( \mathbb{A}^2(\mathbb{F}_{q^{N/2}}) \)

(Davydov-Östergård, 2001)

\( T_N \) is complete in \( \mathbb{A}^N(\mathbb{F}_q) \) \( \iff \) \( N/2 \) is odd.

**Problem:** When \( T_N \times S \) is complete?
external/internal points to a segment
external/internal points to a segment

(Segre, 1973)

$P, P_1, P_2$ distinct collinear points in $\mathbb{A}^2(\mathbb{F}_q)$
external/internal points to a segment

(Segre, 1973)

$P, P_1, P_2$ distinct collinear points in $\mathbb{A}^2(\mathbb{F}_q)$

the point $P$ is internal or external to the segment $P_1P_2$ if

$$(x - x_1)(x - x_2)$$

is a non-square in $\mathbb{F}_q$ or not,

$x, x_1, x_2$ coordinates of $P, P_1, P_2$ w.r.t. any affine frame of $\ell$. 

bicovering and almost bicovering caps
bicovering and almost bicovering caps

let $S$ be a complete cap in $\mathbb{A}^2(\mathbb{F}_q)$. 
Let $S$ be a complete cap in $\mathbb{A}^2(\mathbb{F}_q)$.

A point $P \notin S$ is **bicovery by $S$** if it is external to a segment $P_1P_2$, with $P_1, P_2 \in S$ and internal to another segment $P_3P_4$, with $P_3, P_4 \in S$. 
bicovering and almost bicovering caps

let $S$ be a complete cap in $\mathbb{A}^2(\mathbb{F}_q)$.

a point $P \notin S$ is **bicovery by $S$** if it is external to a segment $P_1P_2$, with $P_1, P_2 \in S$ and internal to another segment $P_3P_4$, with $P_3, P_4 \in S$
let \( S \) be a complete cap in \( \mathbb{A}^2(\mathbb{F}_q) \).

a point \( P \notin S \) is \textit{bicovered by} \( S \) if it is external to a segment \( P_1P_2 \), with \( P_1, P_2 \in S \) and internal to another segment \( P_3P_4 \), with \( P_3, P_4 \in S \).
bicovering and almost bicovering caps

Let \( S \) be a complete cap in \( \mathbb{A}^2(\mathbb{F}_q) \).

A point \( P \notin S \) is bicovered by \( S \) if it is external to a segment \( P_1P_2 \), with \( P_1, P_2 \in S \) and internal to another segment \( P_3P_4 \), with \( P_3, P_4 \in S \).

Definition

\( S \) is said to be

- bicovering if for every \( P \notin S \) is bicovered by \( S \)
bicovering and almost bicovering caps

let $S$ be a complete cap in $\mathbb{A}^2(\mathbb{F}_q)$.

a point $P \not\in S$ is **bicovered by $S$** if it is external to a segment $P_1P_2$, with $P_1, P_2 \in S$ and internal to another segment $P_3P_4$, with $P_3, P_4 \in S$

**definition**

$S$ is said to be

- **bicovering** if for every $P \not\in S$ is bicovered by $S$
- **almost bicovering** if there exists precisely one point not bicovered by $S$
recursive constructions of complete caps

- $T_N$ blow-up of a parabola in $\mathbb{A}^N(\mathbb{F}_q)$, $N \equiv 2 \pmod{4}$
- $S$ complete cap in $\mathbb{A}^2(\mathbb{F}_q)$
recursive constructions of complete caps

- $T_N$ blow-up of a parabola in $\mathbb{A}^N(\mathbb{F}_q)$, $N \equiv 2 \pmod{4}$
- $S$ complete cap in $\mathbb{A}^2(\mathbb{F}_q)$

(G., 2007)

(i) $K_S = T_N \times S$ is complete if and only if $S$ is bicovering
recursive constructions of complete caps

- \( T_N \) blow-up of a parabola in \( \mathbb{A}^N(\mathbb{F}_q) \), \( N \equiv 2 \pmod{4} \)
- \( S \) complete cap in \( \mathbb{A}^2(\mathbb{F}_q) \)

(G., 2007)

(i) \( K_S = T_N \times S \) is complete if and only if \( S \) is bicovering

(ii) if \( S \) is almost bicovering, then

\[
K_S \cup \{(a, a^2 - z_0, x_0, y_0) \mid a \in \mathbb{F}_{q^{N/2}}\}
\]

is complete for some \( x_0, y_0, z_0 \in \mathbb{F}_q \)
bicovering caps in $\mathbb{A}^2(F_q)$

**remarks:**

- no probabilistic result is known
bicovering caps in $\mathbb{A}^2(\mathbb{F}_q)$

**Remarks:**
- no probabilistic result is known
- no computational constructive method is known
bicovering caps in $\mathbb{A}^2(\mathbb{F}_q)$

**remarks:**
- no probabilistic result is known
- no computational constructive method is known
- in the Euclidean plane, no conic is bicovering or almost bicovering
bicovering caps in $\mathbb{A}^2(\mathbb{F}_q)$

remarks:
- no probabilistic result is known
- no computational constructive method is known
- in the Euclidean plane, no conic is bicovering or almost bicovering

(Segre, 1973)

if $q > 13$, ellipses and hyperbolas are almost bicovering caps
bicovering caps in $\mathbb{A}^2(F_q)$

**Remarks:**

- no probabilistic result is known
- no computational constructive method is known
- in the Euclidean plane, no conic is bicovering or almost bicovering

(Segre, 1973)

if $q > 13$, ellipses and hyperbolas are almost bicovering caps

let $N \equiv 0 \pmod{4}$; if $q > 13$, then there exists a complete cap of size

$\# T_{N-2} \cdot [(q - 1) + 1] = q^{\frac{N}{2}}$
how to prove that an algebraic cap is bicoverying

$$S = \{(f(t), g(t)) \mid t \in \mathbb{F}_q\}$$
how to prove that an algebraic cap is bicoverying

\[ S = \{(f(t), g(t)) \mid t \in \mathbb{F}_q\} \]

\[ P = (a, b) \in \mathbb{A}^2(\mathbb{F}_q) \]
how to prove that an algebraic cap is bicovering

\[ S = \left\{ (f(t), g(t)) \mid t \in \mathbb{F}_q \right\} \]

\[ P = (a, b) \in \mathbb{A}^2(\mathbb{F}_q) \]

(1) consider the space curve

\[ \mathcal{Y}_P : \begin{cases} F_P(X, Y) = 0 \\ (a - f(X))(a - f(Y)) = Z^2 \end{cases} \]
how to prove that an algebraic cap is bica
cov
ering

\[ S = \{ (f(t), g(t)) \mid t \in \mathbb{F}_q \} \]

\( P = (a, b) \in \mathbb{A}^2(\mathbb{F}_q) \)

(1) consider the space curve

\[ \mathcal{Y}_P : \left\{ \begin{aligned} F_P(X, Y) &= 0 \\ (a - f(X))(a - f(Y)) &= Z^2 \end{aligned} \right\} \]

(2) apply Hasse-Weil to \( \mathcal{Y}_P \) (if possible) and find a suitable point \((x, y, z) \in \mathcal{Y}_P(\mathbb{F}_q)\)
how to prove that an algebraic cap is bicovering

\[ S = \{ (f(t), g(t)) \mid t \in \mathbb{F}_q \} \]

\[ P = (a, b) \in \mathbb{A}^2(\mathbb{F}_q) \]

(1) consider the space curve

\[ \mathcal{Y}_P : \begin{cases} F_P(X, Y) = 0 \\ (a - f(X))(a - f(Y)) = Z^2 \end{cases} \]

(2) apply Hasse-Weil to \( \mathcal{Y}_P \) (if possible) and find a suitable point \((x, y, z) \in \mathcal{Y}_P(\mathbb{F}_q)\)

the point \( P \) is external to the segment joining \( P_x \) and \( P_y \)
how to prove that an algebraic cap is bicoverying

$$S = \left\{ (f(t), g(t)) \mid t \in \mathbb{F}_q \right\}_{P_t}$$

$$P = (a, b) \in \mathbb{A}^2(\mathbb{F}_q)$$

(1) consider the space curve

$$\mathcal{Y}_{P,c} : \begin{cases} F_P(X, Y) = 0 \\ (a - f(X))(a - f(Y)) = cZ^2 \end{cases}$$

(2) apply Hasse-Weil to $$\mathcal{Y}_P$$ (if possible) and find a suitable point $$(x, y, z) \in \mathcal{Y}_P(\mathbb{F}_q)$$

the point $$P$$ is external to the segment joining $$P_x$$ and $$P_y$$

(3) fix a non-square $$c$$ in $$\mathbb{F}_q^*$$ and repeat for $$\mathcal{Y}_{P,c}$$
bicovering caps from cubic curves

the method works well for $S$ a coset of a cubic $\mathcal{C}$, and $P$ a point off the cubic.
bicovering caps from cubic curves

- the method works well for $S$ a coset of a cubic $\mathcal{X}$, and $P$ a point off the cubic.
- in order to bicover the points on the cubics, more cosets of the same subgroup are needed: the cosets corresponding to a maximal 3-independent subset in the factor group $G/K$
bicovering caps from cubic curves

- the method works well for $S$ a coset of a cubic $\mathcal{C}$, and $P$ a point off the cubic.
- in order to bicover the points on the cubics, more cosets of the same subgroup are needed: the cosets corresponding to a maximal 3-independent subset in the factor group $G/K$
- in the best case bicovering caps of size approximately $q^{7/8}$ are obtained
bicovering caps from cubic curves

- the method works well for $S$ a coset of a cubic $x$, and $P$ a point off the cubic.
- in order to bicover the points on the cubics, more cosets of the same subgroup are needed: the cosets corresponding to a maximal 3-independent subset in the factor group $G/K$
- in the best case bicovering caps of size approximately $q^{7/8}$ are obtained.
- for $N \equiv 0 \pmod{4}$ complete caps of size approximately $q^{N/2 - 1/8}$ are obtained, provided that suitable divisors of $q, q - 1, q + 1$ exist.
bicovering caps from cubic curves

- the method works well for $S$ a coset of a cubic $\mathcal{X}$, and $P$ a point off the cubic.
- in order to bicover the points on the cubics, more cosets of the same subgroup are needed: the cosets corresponding to a maximal 3-independent subset in the factor group $G/K$
- in the best case bicovering caps of size approximately $q^{7/8}$ are obtained
- for $N \equiv 0 \pmod{4}$ complete caps of size approximately $q^{N/2 - 1/8}$ are obtained, provided that suitable divisors of $q, q - 1, q + 1$ exist
- if Voloch’s gap is filled, we will have bicovering caps with roughly $q^{7/8}$ points for any odd $q$
the cuspidal case

\[ \mathcal{X} : Y - X^3 = 0 \]

(Anbar-Bartoli-G.-Platoni, 2013)

Let

- \( q = p^h \), with \( p > 3 \) a prime
- \( m = p^{h'} \), with \( h' < h \) and \( m \leq \frac{\sqrt[4]{q}}{4} \)

then there exists an almost biconvexing cap contained in \( \mathcal{X} \), of size

\[
n = \left\{ \begin{array}{ll}
(2\sqrt{m} - 3) \frac{q}{m}, & \text{if } h' \text{ is even} \\
\left( \sqrt{\frac{m}{p}} + \sqrt{mp} - 3 \right) \frac{q}{m}, & \text{if } h' \text{ is odd}
\end{array} \right.
\]

\( \sim q^{7/8} \)
the nodal case

\[ \mathcal{X} : XY - (X - 1)^3 = 0 \]

(Anbar-Bartoli-G.-Platoni, 2013)

assume that

- \( q = p^h \), with \( p > 3 \) a prime
- \( m \) is an odd divisor of \( q - 1 \), with \( (3, m) = 1 \) and \( m \leq \frac{\sqrt[3]{q}}{3.5} \)
- \( m = m_1 m_2 \) s.t. \( (m_1, m_2) = 1 \) and \( m_1, m_2 \geq 4 \)

then there exists a bicovering cap contained in \( \mathcal{X} \) of size

\[ n \leq \frac{m_1 + m_2}{m}(q - 1) \sim q^{7/8} \]
the isolated double point case

\[ \mathcal{X} : Y(X^2 - \beta) = 1 \]

(Anbar-Bartoli-G.-Platoni, 2013)

assume that

- \( q = p^h \), with \( p > 3 \) a prime
- \( m \) is a proper divisor of \( q + 1 \) such that \( (m, 6) = 1 \) and \( m \leq \frac{\sqrt[4]{q}}{4} \)
- \( m = m_1m_2 \) with \( (m_1, m_2) = 1 \)

then there exists an almost bicovering cap contained in \( \mathcal{X} \) of size less than or equal to

\[ (m_1 + m_2 - 3) \cdot \frac{q + 1}{m} + 3 \sim q^{7/8} \]
the elliptic case

\[ \mathcal{X} : Y^2 - X^3 - AX - B = 0 \]

(Anbar-G., 2012)

assume that

- \( q = p^h \), with \( p > 3 \) a prime
- \( m \) is a prime divisor of \( q - 1 \), with \( 7 < m < \frac{1}{8} \sqrt[4]{q} \)

then there exists a bicovering cap contained in \( \mathcal{X} \) of size

\[ n \leq 2\sqrt{m} \left( \left\lfloor \frac{q - 2\sqrt{q} + 1}{m} \right\rfloor + 31 \right) \sim q^{7/8} \]
\ell(r, q)_{r-1, r+1}
Reed-Solomon codes: $\ell(r, q)_{r-1, r+1} \leq q + 1$
AG codes from elliptic curves

- $\mathcal{C}: Y^2 = X^3 + AX + B \quad 4A^3 + 27B^2 \neq 0$
- $O$ common pole of $x$ and $y$
- $P_1, \ldots, P_n$ rational points of $\mathcal{C}$ (distinct from $O$)
AG codes from elliptic curves

- $\mathcal{C} : Y^2 = X^3 + AX + B \quad 4A^3 + 27B^2 \neq 0$
- $O$ common pole of $x$ and $y$
- $P_1, \ldots, P_n$ rational points of $\mathcal{C}$ (distinct from $O$)

\[ C_r = C(D, G)^\perp, \quad \text{where } G = rO, D = P_1 + \ldots + P_n, \quad n > r \]
AG codes from elliptic curves

- \( \mathcal{X} : Y^2 = X^3 + AX + B \quad 4A^3 + 27B^2 \neq 0 \)
- \( O \) common pole of \( x \) and \( y \)
- \( P_1, \ldots, P_n \) rational points of \( \mathcal{X} \) (distinct from \( O \))

\[
C_r = C(D, G)^\perp, \quad \text{where } G = rO, D = P_1 + \ldots + P_n, \quad n > r
\]

- \( C_r \) is an \([n, n - r, r + 1]_q\)-MDS-code if and only if for every \( P_{i_1}, \ldots, P_{i_r} \)
  \[
  P_{i_1} \oplus \ldots \oplus P_{i_r} \neq O
  \]
AG codes from elliptic curves

- $\mathcal{X} : Y^2 = X^3 + AX + B \quad 4A^3 + 27B^2 \neq 0$
- $O$ common pole of $x$ and $y$
- $P_1, \ldots, P_n$ rational points of $\mathcal{X}$ (distinct from $O$)

$$C_r = C(D, G)^\perp, \quad \text{where } G = rO, D = P_1 + \ldots + P_n, \quad n > r$$

- $C_r$ is an $[n, n - r, r + 1]_q$-MDS-code if and only if for every $P_{i_1}, \ldots, P_{i_r}$
  $$P_{i_1} \oplus \ldots \oplus P_{i_r} \neq O$$

(Munuera, 1993)

If $C_r$ is MDS then, for $n > r + 2$,

$$n \leq \frac{1}{2}(\#\mathcal{X}(\mathbb{F}_q) - 3 + 2r)$$
covering radius of elliptic MDS codes

A subset $T$ of an abelian group $H$ is $r$-independent if for each $a_1, \ldots, a_r \in T$,

$$a_1 + a_2 + \ldots + a_r \neq 0$$
covering radius of elliptic MDS codes

A subset $T$ of an abelian group $H$ is $r$-independent if for each $a_1, \ldots, a_r \in T$,

$$a_1 + a_2 + \ldots + a_r \neq 0$$

$\{P_1, \ldots, P_n\}$ maximal $r$-independent subset of $\mathcal{X}(\mathbb{F}_q)$
covering radius of elliptic MDS codes

a subset $T$ of an abelian group $H$ is $r$-independent if for each $a_1, \ldots, a_r \in T$,

$$a_1 + a_2 + \ldots + a_r \neq 0$$

$$\{P_1, \ldots, P_n\}$$ maximal $r$-independent subset of $\mathcal{X}(\mathbb{F}_q)$

- let

$$\phi_r : \mathcal{X} \rightarrow \mathbb{P}^{r-1} \quad \phi_r = (1 : f_1 : \ldots : f_{r-1})$$

with

$$1, f_1, \ldots, f_{r-1}$$ basis of $L(rO)$
covering radius of elliptic MDS codes

a subset $T$ of an abelian group $H$ is \textit{r-independent} if for each $a_1, \ldots, a_r \in T$,

$$a_1 + a_2 + \ldots + a_r \neq 0$$

$\{P_1, \ldots, P_n\}$ maximal $r$-independent subset of $X(\mathbb{F}_q)$

- let
  $$\phi_r : X \rightarrow \mathbb{P}^{r-1} \quad \phi_r = (1 : f_1 : \ldots : f_{r-1})$$
  with
  $$1, f_1, \ldots, f_{r-1} \quad \text{basis of } L(rO)$$

- $R(C_r) = r - 1$ if and only if each point in $\mathbb{P}^{r-1}(\mathbb{F}_q)$ belongs to the hyperplane generated by some
  $$\phi_r(P_{i_1}), \phi_r(P_{i_2}), \ldots, \phi_r(P_{i_{r-1}})$$
(Bartoli-G.-Platoni, 2013)

if

- \((\mathcal{X}(\mathbb{F}_q), \oplus) \cong \mathbb{Z}_m \times K\) cyclic for \(m > 3\) a prime
- \(S = K \oplus P\) covers all the points in \(\mathbb{A}^2(\mathbb{F}_q)\) off \(\mathcal{X}\)
- \(T \supset S\) is a maximal \(r\)-independent subset of \(\mathcal{X}(\mathbb{F}_q)\)
(Bartoli-G.-Platoni, 2013)

if

- $(\mathcal{X}(\mathbb{F}_q), \oplus) \cong \mathbb{Z}_m \times K$ cyclic for $m > 3$ a prime
- $S = K \oplus P$ covers all the points in $\mathbb{A}^2(\mathbb{F}_q)$ off $\mathcal{X}$
- $T \supset S$ is a maximal $r$-independent subset of $\mathcal{X}(\mathbb{F}_q)$

then almost every point in $\mathbb{P}^{r-1}(\mathbb{F}_q)$ belongs to some hyperplane generated by $r-1$ points of $\phi_r(T)$
if
- \((\mathcal{X}(\mathbb{F}_q), \oplus) \cong \mathbb{Z}_m \times K\) cyclic for \(m > 3\) a prime
- \(S = K \oplus P\) covers all the points in \(\mathbb{A}^2(\mathbb{F}_q)\) off \(\mathcal{X}\)
- \(T \supset S\) is a maximal \(r\)-independent subset of \(\mathcal{X}(\mathbb{F}_q)\)

then almost every point in \(\mathbb{P}^{r-1}(\mathbb{F}_q)\) belongs to some hyperplane generated by \(r - 1\) points of \(\phi_r(T)\)

• if \(m\) is a prime divisor of \(q - 1\) with \(m < \sqrt[4]{q/64}\), then

\[
\ell(r, q)_{r-1,r+1} \leq ([r/2] - 1)(|S| - 1) + 2 \frac{m + 1}{r - 2} + 2r
\]
if
- \((\mathcal{X}(\mathbb{F}_q), \oplus) \cong \mathbb{Z}_m \times K\) cyclic for \(m > 3\) a prime
- \(S = K \oplus P\) covers all the points in \(\mathbb{A}^2(\mathbb{F}_q)\) off \(\mathcal{X}\)
- \(T \supset S\) is a maximal \(r\)-independent subset of \(\mathcal{X}(\mathbb{F}_q)\)

then almost every point in \(\mathbb{P}^{r-1}(\mathbb{F}_q)\) belongs to some hyperplane generated by \(r - 1\) points of \(\phi_r(T)\)

if \(m\) is a prime divisor of \(q - 1\) with \(m < \sqrt[4]{q/64}\), then

\[\ell(r, q)_{r-1, r+1} \leq ([r/2] - 1)(|S| - 1) + 2 \frac{m + 1}{r - 2} + 2r \sim ([r/2] - 1)q^{3/4}\]
(Bartoli-G.-Platoni, 2013)

if

- $(\mathcal{X}(\mathbb{F}_q), \oplus) \cong \mathbb{Z}_m \times K$ cyclic for $m > 3$ a prime
- $S = K \oplus P$ covers all the points in $\mathbb{A}^2(\mathbb{F}_q)$ off $\mathcal{X}$
- $T \supset S$ is a maximal $r$-independent subset of $\mathcal{X}(\mathbb{F}_q)$

then almost every point in $\mathbb{P}^{r-1}(\mathbb{F}_q)$ belongs to some hyperplane generated by $r - 1$ points of $\phi_r(T)$

if $m$ is a prime divisor of $q - 1$ with $m < \sqrt[4]{q/64}$, then

$$\ell(r, q)_{r-1,r+1} \leq (\lceil r/2 \rceil - 1)(|S| - 1) + 2\frac{m + 1}{r - 2} + 2r \sim (\lceil r/2 \rceil - 1)q^{3/4}$$
problems

- explanation for experimental results
problems

- explanation for experimental results
- Voloch's proof for plane caps in elliptic cubics
problems

- explanation for experimental results
- Voloch's proof for plane caps in elliptic cubics
- bicovering caps in dimensions different from 2
problems

- explanation for experimental results
- Voloch's proof for plane caps in elliptic cubics
- bicovering caps in dimensions different from 2
- non-recursive constructions in higher dimensions
problems

- explanation for experimental results
- Voloch's proof for plane caps in elliptic cubics
- bicovering caps in dimensions different from 2
- non-recursive constructions in higher dimensions
- probabilistic results intrinsic to higher dimensions