Small complete caps and saturating sets in Galois spaces, II

Daniele Bartoli

University of Perugia (Italy)

Workshop in Finite Geometry -Szeged
10-14 June 2013

Complete arcs from singular cubics and small complete caps in affine spaces

Let $\mathcal{X}$ be a singular plane cubic defined over $\mathbb{F}_q$ with a node and at least one $\mathbb{F}_q$-rational inflection. The equation is

$$XY = (X-1)^3 \tag{1}$$

There exists an isomorphism between the points of the cubic and the multiplicative group of $\mathbb{F}_q$:

$$\begin{array}{ccc} (\mathbb{F}_q^*, \cdot) & \longrightarrow & (G, \oplus) \\ v & \mapsto & \left(v, \frac{(v-1)^3}{v}\right) \end{array} \tag{2}$$

the neutral element in $(G, \oplus)$ is $(1, 0)$.

Consider now two points of the cubic

$$P_1 = \left(v_1, \frac{(v_1-1)^3}{v_1}\right) \qquad P_2 = \left(v_2, \frac{(v_2-1)^3}{v_2}\right)$$

They are collinear with an affine point $P = (a, b)$ not belonging to $\mathcal{X}$ if and only if

$$\begin{vmatrix} v_1 & \frac{(v_1-1)^3}{v_1} & 1 \\ v_2 & \frac{(v_2-1)^3}{v_2} & 1 \\ a & b & 1 \end{vmatrix} = 0 \tag{3}$$

This condition is equivalent to

$$a(v_1^2 v_2 + v_1 v_2^2 - 3v_1 v_2 + 1) - b v_1 v_2 - v_1 v_2 (v_1 v_2 - 3) - (v_1 + v_2) = 0 \tag{4}$$

Take now a subgroup K of $(G, \oplus)$ of index m with $(m, 6) = 1$. Let $P_t = (t, (t-1)^3/t)$ be a point in $G \setminus K$.

Theorem

The coset $K_t = K \oplus P_t$ is an arc.

Note that we can write K_t in an algebraically parametrized form:

$$K_t = \left\{ \left(tw^m, \frac{(tw^m - 1)^3}{tw^m} \right) \mid w \in \mathbb{F}_q^* \right\} \tag{5}$$

Problem

Let K_t be a coset.

Does K_t bicover all the points of $AG(2,q) \setminus \mathcal{X}$?

Let $P_1 = \left(tX_1^m, \frac{(tX_1^m-1)^3}{tX_1^m}\right), P_2 = \left(tY_1^m, \frac{(tY_1^m-1)^3}{tY_1^m}\right) \in K_t$ and $P = (a,b) \in AG(2,q) \setminus \mathcal{X}$ then if we proceed as above we get a new curve to study:

$$\mathcal{C}_P : f_{a,b,t,m}(X,Y) = 0, \tag{6}$$

where

$$\begin{aligned} f_{a,b,t,m}(X,Y) \quad = \quad & a(t^3X^{2m}Y^m + t^3X^mY^{2m} - 3t^2X^mY^m + 1) \\ & -bt^2X^mY^m - t^4X^{2m}Y^{2m} + 3t^2X^mY^m \\ & -tX^m - tY^m. \end{aligned} \tag{7}$$

In particular we want to know if it possesses an absolute irreducible component defined over $\mathbb{F}_q$ and also to know its genus.

In particular we want to know if it possesses an absolute irreducible component defined over $\mathbb{F}_q$ and also to know its genus.
Note that this curve in general is not irreducible: for instance when $a^3 = -1$ and $b = 1 - (a-1)^3$ we have the following

Proposition

Assume that $a^3 = -1$ and $b = 1 - (a-1)^3$. Then the curve $\mathcal{C}_P$ has an irreducible $\mathbb{F}_q$-rational component of genus less than m^2, with equation $a^2 + t^2 X^m Y^m - atX^m = 0$.

We have other cases to study, but for now on suppose now $a \neq 0$ and either $a^3 \neq -1$ or $b \neq 1-(a-1)^3$.
We study the following curve:

$$\begin{aligned} g_P(U,Z) &= a(t^3U^2Z + t^3UZ^2 - 3t^2UZ + 1) - bt^2UZ \\ &\quad -t^4U^2Z^2 + 3t^2UZ - tU - tZ. \end{aligned}$$

- U_∞ and Z_∞ are the only ideal points of $\mathcal{C}_P$, and they are both ordinary double points.
- The tangent lines of $\mathcal{C}_P$ at U_∞ are $Z = 0$ and $Z = a/t$; similarly, $U = 0$ and $U = a/t$ are the tangent lines at Z_∞.

Proposition

$$\begin{aligned} g_P(U,Z) &= a(t^3U^2Z + t^3UZ^2 - 3t^2UZ + 1) - bt^2UZ \\ &\quad -t^4U^2Z^2 + 3t^2UZ - tU - tZ \end{aligned}$$

is absolutely irreducible.

- It can have linear components: the only possibilities are lines through the ideal points of $g_P(U,Z)$. By easy calculation we get a contradiction.
- It can have components of degree two: the two conics must have the lines $Z = 0$, $Z = a/t$, $U = 0$ and $U = a/t$ as tangent lines at the ideal points. Then we can reconstruct the equations of the conics. In fact both conics are of type

$$T_1 T_2 + \alpha = 0,$$

where T_1 and T_2 are the tangent lines at U_∞ and Z_∞. In all the cases we get a contradiction.

Definition

An algebraic function field $\mathbb{F}$ over $\mathbb{K}$ is an extension $\mathbb{F}$ of $\mathbb{K}$ such that $\mathbb{F}$ is a finite algebraic extension of $\mathbb{K}(x)$, for some element $x \in \mathbb{F}$ transcendental over $\mathbb{K}$. If $\mathbb{F} = \mathbb{K}(x)$, then $\mathbb{F}$ is called the rational function field over $\mathbb{K}$.

Let $\mathcal{C} : f(x, y) = 0$ be an irreducible curve defined over $\mathbb{K}$: the field of the rational functions of $\mathcal{C}$ is $\mathbb{K}(\bar{x}, \bar{y})$, where $f(\bar{x}, \bar{y}) = 0$. Conversely, to a function field F over $\mathbb{K}$ one can associate a curve $\mathcal{C}$, defined over $\mathbb{K}$, such that $\mathbb{K}(\mathcal{C})$ is $\mathbb{K}$-isomorphic to F. The genus of F as a function field coincides with the genus of $\mathcal{C}$.

If a curve $\mathcal{C}$ is singular we can find a curve equivalent to $\mathcal{C}$ but non-singular: this curve is called the non-singular model of $\mathcal{C}$.
A place of $\mathcal{C}$ can be viewed as a point of its non-singular model.
The valuation v of a rational function ϕ at a place γ is an integer which indicates the 'multiplicity' of ϕ in γ.

- $v_\gamma(\phi) > 0 \Longrightarrow \gamma$ is a zero of ϕ
- $v_\gamma(\phi) < 0 \Longrightarrow \gamma$ is a pole of ϕ
- $v_\gamma(\phi) = 0 \Longrightarrow \gamma$ is not zero nor pole of ϕ

Consider a rational function $\phi = \frac{H+(F)}{G+(F)}$ in $\mathbb{K}(\mathcal{C})$, where $\mathcal{C}$ is defined by $F(x, y) = 0$. Then

$$v_\gamma(\phi) = \mathcal{I}(H, F, \gamma) - \mathcal{I}(G, F, \gamma),$$

where $\mathcal{I}(F, G, \alpha)$ is the multiplicity of intersection of the curves defined by $F = 0$ and $G = 0$ in the place α.

Example

For instance consider the curve $\mathcal{C}$ defined by $F(x,y) = y - x^3 = 0$. Consider the rational function $\phi = \frac{y+(F)}{T+(F)}$, where $T = 0$ is the line at infinity. Let $\gamma = (0,0)$, then $v_\gamma(\phi) = 3$ since the multiplicity of intersection between $y = 0$ and $F(x,y)$ is equal to three and $T = 0$ does not pass through γ.

A rational function has a finite number of poles and zeros.
To a rational function ϕ is associated its divisor

$$(\phi) = \sum_{P \in \mathcal{C}} v_P(\phi) P.$$

Note that only for a finite number of $P \in \mathcal{C}$ $v_P(\phi) \neq 0$.

In the following we will use the Kummer's Theorem.

Theorem

Let F be an algebraic function field over $\mathbb{K}$, and let $m > 1$ be an integer relatively prime to the characteristic of $\mathbb{K}$. Suppose that $u \in F$ is an element satisfying

$$u \neq \omega^e \text{ for all } \omega \in F \text{ and } e|m,\ e > 1.$$

Then we have a formula to calculate the genus of the function field $F' = F(y)$ with $y^m = u$.

An extension such as F' is said to be a Kummer extension of F.
In the following we will apply this theorem in order to calculate the genus of some curves.

Recall our curve $\mathcal{C}_P : g_P(U, Z) = 0$ with

$$\begin{aligned} g_P(U,Z) &= a(t^3U^2Z + t^3UZ^2 - 3t^2UZ + 1) - bt^2UZ \\ &\quad -t^4U^2Z^2 + 3t^2UZ - tU - tZ \end{aligned}$$

Let $\bar{u}$ and $\bar{z}$ denote the rational functions of $\mathbb{K}(\mathcal{C}_P)$ associated to the affine coordinates U and Z, respectively. Then

$$a(t^3\bar{u}^2\bar{z}+t^3\bar{u}\bar{z}^2-3t^2\bar{u}\bar{z}+1)-bt^2\bar{u}\bar{z}-t^4\bar{u}^2\bar{z}^2+3t^2\bar{u}\bar{z}-t\bar{u}-t\bar{z}=0. \tag{8}$$

- Both U_∞ and Z_∞ are ordinary double points of $\mathcal{Q}_P$; hence, they both are the center of two linear places of $\mathbb{K}(\bar{u}, \bar{z})$.
- Let γ_1 be the linear place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at U_∞ with tangent $Z = a/t$, γ_2 the linear place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at U_∞ with tangent $Z = 0$. γ_3 be the linear place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at Z_∞ with tangent $U = a/t$, and γ_4 the linear place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at Z_∞ with tangent $U = 0$. Let $Q_1 = (0, a/t)$ and $Q_2 = (a/t, 0)$. It is easily seen that both Q_1 and Q_2 are simple points of $\mathcal{Q}_P$, and hence they both are the center of precisely one linear place of $\mathbb{K}(\bar{u}, \bar{z})$. Let γ_5 be the place of $\mathbb{K}(\bar{u}, \bar{z})$ centered at Q_1, and γ_6 the place centered at Q_2. Then

$$\operatorname{div}(\bar{u}) = \gamma_4 + \gamma_5 - \gamma_1 - \gamma_2,$$

and

$$\operatorname{div}(\bar{z}) = \gamma_2 + \gamma_6 - \gamma_3 - \gamma_4.$$

We now consider the extension

$$\mathbb{K}(\bar{u},\bar{z})(\bar{y}) \text{ of } \mathbb{K}(\bar{u},\bar{z})$$

defined by the equation $\bar{y}^m = \bar{z}$. Clearly, $\mathbb{K}(\bar{u},\bar{z},\bar{y}) = \mathbb{K}(\bar{u},\bar{y})$ holds.
By the previous calculations on the $\mathrm{div}(\bar{z})$ there exists no rational function $\omega \in \mathbb{K}(\bar{u},\bar{z})$ such that $\omega^e = \bar{z}$ for some $e|m$ and $e > 1$. Then we can apply Kummer's Theorem and calculate the genus of $\mathbb{K}(\bar{u},\bar{y})$: it is equal to $2m-1+m(g-1)$, where g denotes the genus of $\mathcal{Q}_P$. Since $\mathcal{Q}_P$ is a quartic with two double points, $g \leq 1$ holds and hence the genus of $\mathbb{K}(\bar{u},\bar{z},\bar{y})$ is less than or equal to

$$2m-1.$$

It is also possible to compute the divisor of $\bar{u}$ in $\mathbb{K}(\bar{u}, \bar{y})$.
We have

$$\mathrm{div}(\bar{u}) = m\bar{\gamma}_4 + \sum_{i=1}^{m} \bar{\gamma}_5^i - m\bar{\gamma}_2 - \sum_{i=1}^{m} \bar{\gamma}_1^i.$$

As before there exists no rational function $\omega \in \mathbb{K}(\bar{u}, \bar{y})$ such that $\omega^e = \bar{u}$ for some $e|m$ and $e > 1$. Then we can apply Kummer's Theorem also to $\mathbb{K}(\bar{u}, \bar{y})(\bar{x}) = \mathbb{K}(\bar{y}, \bar{x})$ of $\mathbb{K}(\bar{u}, \bar{y})$ defined by the equation $\bar{x}^m = \bar{u}$. Its genus is

$$1 + m\Big(g' - 1 + \frac{1}{2}(1 - \frac{1}{m})2m\Big),$$

where g' is the genus of $\mathbb{K}(\bar{u}, \bar{y})$. Taking into account that $g' \leq 2m - 1$ the genus of $\mathbb{K}(\bar{x}, \bar{y})$ is at most

$$3m^2 - 3m + 1.$$

Finally we can prove that the curve $\mathcal{C}_p$ is absolutely irreducible

Proposition

Assume that $a \neq 0$ and either $a^3 \neq -1$ or $b \neq 1-(a-1)^3$. Then the curve $\mathcal{C}_P$ is an absolutely irreducible curve defined over $\mathbb{F}_q$ with genus less than or equal to

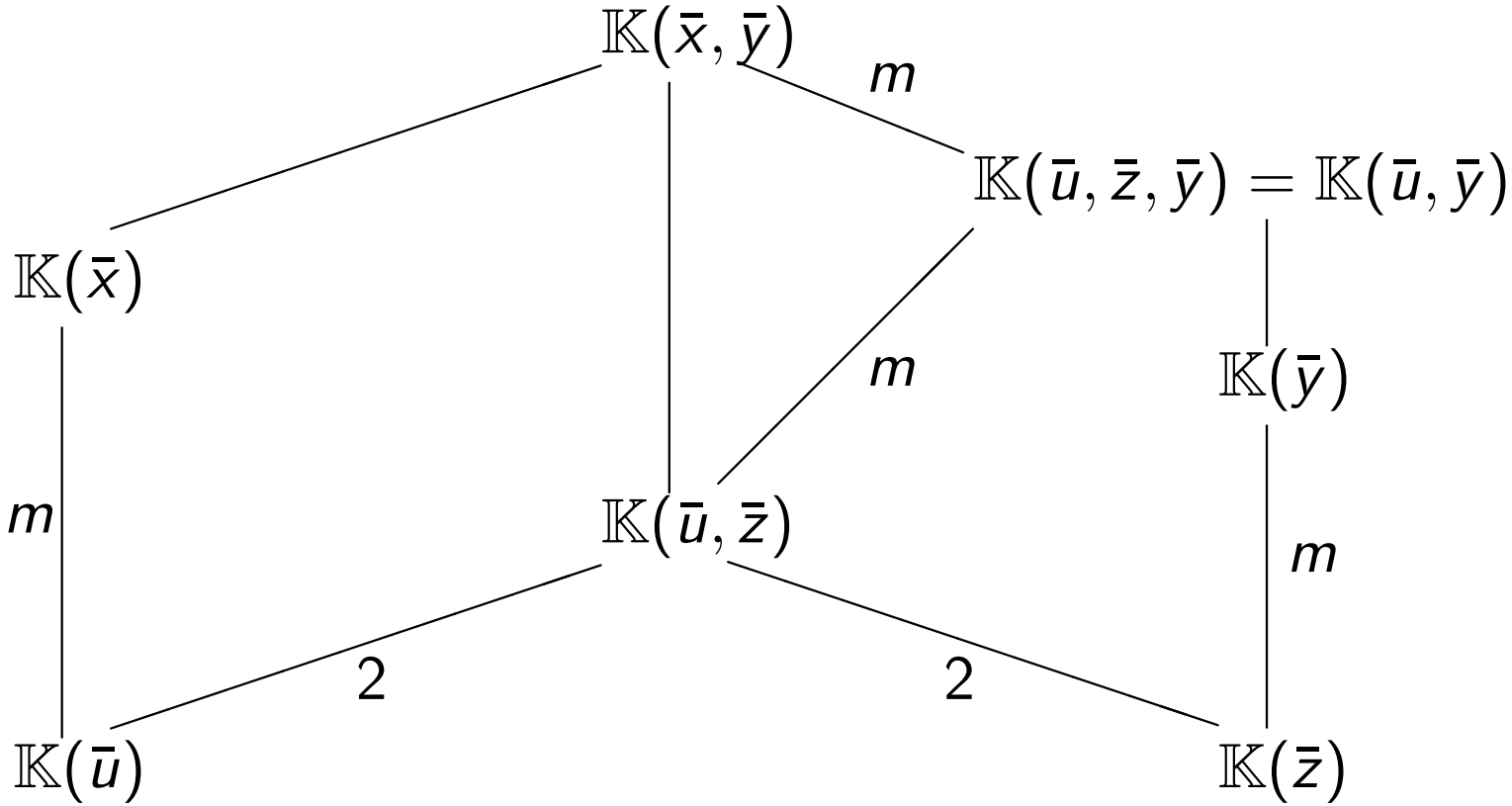
$$3m^2 - 3m + 1.$$

Suppose that $f_{a,b,t,m}(X, Y)$ admits a non-trivial factorization

$$f_{a,b,t,m}(X, Y) = g_1(X, Y)^{m_1} \cdots g_s(X, Y)^{m_s},$$

By construction, $f_{a,b,t,m}(\bar{x}, \bar{y}) = 0$ holds and hence there exists $i_0 \in \{1, \ldots, s\}$ such that $g_{i_0}(\bar{x}, \bar{y}) = 0$.
Clearly, either $\deg_X(g_{i_0}) < 2m$ or $\deg_Y(g_{i_0}) < 2m$ holds.
To get a contradiction, it is then enough to show that the extensions $\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{x})$ and $\mathbb{K}(\bar{x}, \bar{y}) : \mathbb{K}(\bar{y})$ have both degree $2m$: in fact this should mean that the minimal polynomial of $\bar{x}$ over $\mathbb{K}(\bar{y})$ and viceversa has degree $2m$, but we found g_{i_0} of degree less than $2m$.

From the diagram



it follows that $[\mathbb{K}(\bar{x},\bar{y}) : \mathbb{K}(\bar{u})] = [\mathbb{K}(\bar{x},\bar{y}) : \mathbb{K}(\bar{z})] = 2m^2$; hence both $[\mathbb{K}(\bar{x},\bar{y}) : \mathbb{K}(\bar{y})] = 2m$ and $[\mathbb{K}(\bar{x},\bar{y}) : \mathbb{K}(\bar{x})] = 2m$ hold.

The case $a = 0$ is a little more complicated, but also in this case we can prove that $f_{a,b,t,m}(X, Y)$ is absolutely irreducible and it has genus $\frac{3m^2-3m+2}{2}$.

Problem

How can we use the information on the curve $f_{a,b,t,m}(X, Y)$ to get information on the bicovering properties of the arc we construct?

Recall that a point $P = (a, b) \notin \mathcal{A}$ is bicovered by $\mathcal{A}$ if there exist four points $P_1, P_2, P_3, P_4 \in \mathcal{A}$ such that P is internal to the segment P_1P_2 and external to the segment P_3P_4. This means that

$$(a - x_1)(a - x_2) \notin \square \qquad (a - x_3)(a - x_4) \in (\square \setminus \{0\}).$$

Recall now that our points belong to a coset of the subgroup K of G and then $x_i = tX_i^m$.

In the three-dimensional space over $\mathbb{K}$, fix an affine coordinate system (X, Y, W) and for any $c \in \mathbb{K}$, $c \neq 0$ let $\mathcal{Y}_P$ be the curve defined by

$$\mathcal{Y}_P : \begin{cases} W^2 = c(a - tX^m)(a - tY^m) \\ f_{a,b,t,m}(X, Y) = 0 \end{cases} .$$

We can easily prove that if there exists an $\mathbb{F}_q$-rational point of $\mathcal{Y}_P$ then P is bicovered by the arc comprising the points of a coset of index m in the abelian group of the non-singular $\mathbb{F}_q$-rational points of a nodal cubic.

Choose $c \notin \square$, then a point of this curve is $(\tilde{x}, \tilde{y}, \tilde{w})$ and there exist two points of the coset

$$P_1(c) = \left(t\tilde{x}^m, \frac{(t\tilde{x}^m - 1)^3}{t\tilde{x}^m} \right)$$

and

$$P_2(c) = \left(t\tilde{y}^m, \frac{(t\tilde{y}^m - 1)^3}{t\tilde{y}^m} \right)$$

collinear with $P = (a, b)$ and such that

$$(a - t\tilde{x}^m)(a - t\tilde{y}^m) \notin \square$$

This means that P is internal to the segment $P_1(c)P_2(c)$. Moreover if we choose $c \in (\square \setminus \{0\})$ we have the same conclusions, but in this case P is internal to the segment $P_1(c)P_2(c)$. Then P is bicovered by the coset.

To prove that the curve $\mathcal{Y}_P$ is absolutely irreducible it is enough to show that $c(a - tX^m)(a - tY^m)$ is not a square in $\mathbb{K}(\bar{x}, \bar{y})$.
This is true since we are able to find at least one place such that $v_\gamma(c(a - tX^m)(a - tY^m))$ is odd: this cannot be possible for a square.
We can calculate the genus of this curve and then we can apply Hasse-Weill bound: we have to impose some other conditions on the number of points of this curve, since not all the possible points of $\mathcal{Y}_P$ are good for our purpose.
Finally we get the following

Proposition

If

$$q + 1 - (12m^2 - 8m + 2)\sqrt{q} \geq 8m^2 + 8m + 1 \tag{9}$$

then every point P in $AG(2, q)$ off $\mathcal{X}$ is bicovered by K_t.

We know now that a single coset of K_t of the subgroup K in the group G bicovers all the affine points not in $\mathcal{X}$.

Problem

What about the points on $\mathcal{X}$?

We have to introduce the notion of a maximal-3-independent subset of a finite abelian group $\mathcal{G}$.

Definition

A subset M of $\mathcal{G}$ is said to be *maximal 3-independent* if

(a) $x_1 + x_2 + x_3 \neq 0$ for all $x_1, x_2, x_3 \in M$, and

(b) for each $y \in \mathcal{G} \setminus M$ there exist $x_1, x_2 \in M$ with $x_1 + x_2 + y = 0$.

If in (b) $x_1 \neq x_2$ can be assumed, then M is said to be *good*.

Maximal 3-independent subset can be constructed in an easy way:

Example

Let $G = A \times B$, $|A|, |B| \geq 4$ and let $a \in A$, $b \in B$ be fixed elements whose order is different from 3. The set

$$T = \{(a, x) : x \neq -2b\} \cup \{(y, b) : y \neq -2a\}$$

is a maximal 3-independent subset of G.

Now, let M be a maximal 3-independent subset of the factor group G/K containing K_t.
The union S of the cosets of K corresponding to M is a good maximal 3-independent subset of $(\mathcal{X}(\mathbb{F}_q), \oplus)$.
In geometrical terms, since three points in G are collinear if and only if their sum is equal to the neutral element, S is an arc whose secants cover all the points in G.

Consider two cosets and a point $P_0 \in \mathcal{X}$ which is covered by two points each of them in one coset.
Let $P_0 = (u_0, (u_0 - 1)^3/u_0)$ with $u_0 \neq 0$ and

$$P = \left(tx^m, \frac{(tx^m - 1)^3}{tx^m}\right),$$

then the point of $\mathcal{X}$ collinear with P_0 and P is

$$Q = \left(\frac{1}{u_0 tx^m}, \frac{(1 - u_0 tx^m)^3}{(u_0 tx^m)^2}\right).$$

If we want to know if P_0 is bicovered by P and Q then we have to investigate the following function

$$\eta(\bar{x}) = (u_0 - t\bar{x}^m)\left(u_0 - \frac{1}{u_0 tx^m}\right) = \frac{(u_0 - t\bar{x}^m)(u_0^2 t\bar{x}^m - 1)}{u_0 t\bar{x}^m}.$$

We can find as before a place with odd valuation, then η is not a square in $\mathbb{K}(\bar{x})$ and we can give an estimation on the genus.

Then we proved the following

Proposition

Let $K_{t'}$ be a coset of K such that $K_t \cup K_{t'}$ is an arc. Let P_0 be an $\mathbb{F}_q$-rational affine point of $\mathcal{X}$ not belonging to $K_t \cup K_{t'}$ but collinear with a point of K_t and a point of $K_{t'}$. If

$$q + 1 - (12m^2 - 8m + 2)\sqrt{q} \geq 8m^2 + 8m + 1$$

holds, then P_0 is bicovered by $K_t \cup K_{t'}$.

We can summarize the results on points on and off $\mathcal{X}$ in the following

Theorem

Let m be a proper divisor of $q-1$ such that $(m,6)=1$ and

$$q+1-(12m^2-8m+2)\sqrt{q} \geq 8m^2+8m+1$$

holds. Let M be a maximal 3-independent subset of the factor group G/K. Then

$$S = \bigcup_{K_{t_i} \in M} K_{t_i}$$

is a bicovering arc in $AG(2,q)$ of size $\#M \cdot \frac{q-1}{m}$.

Corollary

Let m be a proper divisor of $q-1$ such that $(m,6)=1$ and $m \leq \frac{\sqrt[4]{q}}{3.5}$. Assume that the cyclic group of order m admits a maximal 3-independent subset of size s. Then

(i) *there exists a bicovering arc in $AG(2,q)$ of size $\frac{s(q-1)}{m}$;*

(ii) *for $N \equiv 0 \pmod 4$, $N \geq 4$, there exists a complete cap in $AG(N,q)$ of size*

$$\frac{s(q-1)}{m} q^{\frac{N-2}{2}}.$$

In the case where a group $\mathcal{G}$ is the direct product of two groups $\mathcal{G}_1$, $\mathcal{G}_2$ of order at least 4, neither of which elementary 3-abelian, there exists a maximal 3-independent subset of $\mathcal{G}$ of size less than or equal to $(\#\mathcal{G}_1) + (\#\mathcal{G}_2)$.

Theorem

Let $q = p^h$ with $p > 3$, and let m be a proper divisor of $q - 1$ such that $(m, 6) = 1$ and $m \leq \frac{\sqrt[4]{q}}{3.5}$. Assume that $m = m_1 m_2$ with $(m_1, m_2) = 1$. Then

(i) *there exists a bicovering arc in $AG(2, q)$ of size less than or equal to*

$$\frac{(m_1 + m_2)(q-1)}{m_1 m_2};$$

(ii) *for $N \equiv 0 \pmod 4$, $N \geq 4$, there exists a complete cap in $AG(N, q)$ of size less than or equal to*

$$\frac{(m_1 + m_2)(q-1)}{m_1 m_2} q^{\frac{N-2}{2}}.$$

Complete caps in affine spaces of dimension 3

Let q odd, let $t = \lfloor \frac{q+1}{4} \rfloor$, and let $\square$ be the set of non-zero squares in $\mathbb{F}_q$. Fix an elliptic quadric $\mathcal{Q}$ in $PG(3, q)$ with affine equation

$$Z = X^2 + \epsilon Y^2$$

here $\epsilon \in \square$ if $q \equiv 3 \pmod 4$, whereas $\epsilon \notin \square$ for $q \equiv 1 \pmod 4$.

Let q odd, let $t = \lfloor \frac{q+1}{4} \rfloor$, and let $\square$ be the set of non-zero squares in $\mathbb{F}_q$. Fix an elliptic quadric $\mathcal{Q}$ in $PG(3, q)$ with affine equation

$$Z = X^2 + \epsilon Y^2$$

here $\epsilon \in \square$ if $q \equiv 3 \pmod 4$, whereas $\epsilon \notin \square$ for $q \equiv 1 \pmod 4$. For $\zeta \in \mathbb{F}_q^*$, let $\mathcal{C}_\zeta$ be the conic obtained as the intersection of $\mathcal{Q}$ and the plane with equation $Z = \zeta$:

$$\mathcal{C}_\zeta : \begin{cases} X^2 + \epsilon Y^2 = \zeta \\ Z = \zeta \end{cases};$$

for $\xi, r \in \mathbb{F}_q$ let $\mathcal{C}_\xi(r)$ be the (possibly degenerate) conic with equation

$$\mathcal{C}_\xi(r) : \begin{cases} X^2 + \epsilon Y^2 = r \\ Z = \xi \end{cases}. \tag{10}$$

Consider now two conics $\mathcal{C}_{\zeta_1}$, $\mathcal{C}_{\zeta_2}$, with $\zeta_1, \zeta_2 \in S$.

Problem

What are the points of $AG(3,q)$ lying on bisecants of $\mathcal{C}_{\zeta_1} \cup \mathcal{C}_{\zeta_2}$?

Note that if $\zeta \neq 0$ then all the conic lying on $Z = \zeta_1$ AND $Z = \zeta_2$ are covered by $\mathcal{C}_{\zeta_1} \cup \mathcal{C}_{\zeta_2}$.
Let $\mathcal{B}$ denote the set of points in the affine space $AG(3,q)$ lying on some bisecant of the set $\mathcal{C}_{\zeta_1} \cup \mathcal{C}_{\zeta_2}$, where ζ_1, ζ_2 are elements in S.
Choose two square roots $\sqrt{\zeta_1}$, $\sqrt{\zeta_2} \in \mathbb{F}_q$ and let

$$A(\xi, \zeta_1, \zeta_2) = \frac{\xi - \sqrt{\zeta_1}\sqrt{\zeta_2}}{\sqrt{\zeta_1} - \sqrt{\zeta_2}}, \qquad B(\xi, \zeta_1, \zeta_2) = \frac{\xi + \sqrt{\zeta_1}\sqrt{\zeta_2}}{\sqrt{\zeta_1} + \sqrt{\zeta_2}}.$$

Consider the conic $C_\xi(r)$, $\xi, r \in \mathbb{F}_q$ and $\xi \notin \{\zeta_1, \zeta_2\}$.

Proposition

$$C_\xi(r) \subset \mathcal{B} \iff (r - A(\xi, \zeta_1, \zeta_2)^2)(r - B(\xi, \zeta_1, \zeta_2)^2) \notin S$$

Let s be the minimum integer such that $\binom{s}{2} > t$ holds, and fix s distinct elements in S, say $\zeta_1, \ldots, \zeta_s$. In the work of Pellegrino it is claimed that:

(i) every point $P = (\alpha, \beta, \gamma)$ in $AG(3, q) \setminus \mathcal{Q}$ with $(\alpha, \beta) \neq (0, 0)$ belongs to some bisecant of $\mathcal{C}_{\zeta_1} \cup \ldots \cup \mathcal{C}_{\zeta_s}$;

(ii) if the conic $\mathcal{C}_\xi(r)$, with $\xi \notin \{\zeta_1, \ldots, \zeta_{s-1}\}$ and $r \in S$, is disjoint from the bisecants of $\mathcal{C}_{\zeta_1} \cup \ldots \cup \mathcal{C}_{\zeta_{s-1}}$, then every point $P = (\alpha, \beta, \gamma)$ in $AG(3, q)$ with $(\alpha, \beta) \neq (0, 0)$ belongs to some bisecant of $\mathcal{C}_{\zeta_1} \cup \ldots \cup \mathcal{C}_{\zeta_{s-1}} \cup \mathcal{C}_\xi(r)$.

The previous theorems (in particular (ii)) would yield the possibility of constructing complete caps of size of the same order of magnitude as $q\sqrt{q/2}$: in fact it could be possible to add at most two extra points on the line $X = 0$ $Y = 0$ and points on the plane at infinity which in general could be not covered.

Problem

Unfortunately, both (i) and (ii) turn out to be false.

Counterexamples can be found for instance in $AG(3, 19)$.
In fact a gap in the proofs of (i) and (ii) can be easly found.

Idea

Use a similar approach of Pellegrino, constructing caps consisting of union of conics from parallel planes in $AG(3,q)$.

Difference: we do not require that all the conics but one lie in the same elliptic quadric.
Fix a primitive element ω in $\mathbb{F}_q$, and for $\xi, r \in \mathbb{F}_q$ with $\xi \neq 0$ let $\mathcal{C}_\xi(r)$ be as in above with $\epsilon = -\omega$ and consider three conics $\mathcal{C}_{\xi_1}(r_1)$, $\mathcal{C}_{\xi_2}(r_2)$, $\mathcal{C}_{\xi_3}(r_3)$ on different parallel planes.

Proposition

There exist three collinear points in $\mathcal{C} = \bigcup_{i=1}^{3} \mathcal{C}_{\xi_i}(r_i)$ if and only if

$$\frac{\left((\xi_2-\xi_1)^2 r_3 - r_1(\xi_2-\xi_3)^2 - r_2(\xi_3-\xi_1)^2\right)^2}{(\xi_2-\xi_3)^2(\xi_3-\xi_1)^2} - 4r_1r_2 \in \mathbb{F}_q \setminus S. \tag{11}$$

Three conics $\mathcal{C}_{\xi_i}(r_i)$, $i = 1, 2, 3$, with pairwise distinct ξ_i's, are said to be collinear if (11) holds.
We can now identify a conic $\mathcal{C}_{\xi_i}(r_i)$ with the pair (r_i, ξ_i) in $\mathbb{F}_q^2$.
Consider a set M of pairs (r_i, ξ_i) in $\mathbb{F}_q^2$ corresponding to non-degenerate conics lying on different parallel planes, that is

$$M = \{(r_i, \xi_i) \in \mathbb{F}_q^2 \mid i = 1, \ldots, n, r_i \neq 0, \xi_i \neq \xi_j\} \subset \mathbb{F}_q^2.$$

Definition

A pair $(r, \xi) \in \mathbb{F}_q^2$ with $r \neq 0$ is said to be covered by M if

- ξ equals ξ_i for some $i = 1, \ldots, n$: the conic is on the same plane of a conic in M
- (r, ξ) is collinear with two pairs in M.

A set M is said to be complete if no three pairs in M are collinear, and in addition any pair (r, ξ) with $r \neq 0$ is covered by M.

Remark

If M is complete, then the conics corresponding to the pairs in M, possibly together with one or two extra points on the line with equations $X = 0, Y = 0$, form a complete cap in $AG(3, q)$ of size at most $\#M(q + 1) + 2$.

Two single non-degenerate conics cover roughly half points of $AG(3, q)$:

Proposition

Let $M = \{(r_1, \xi_1), (r_2, \xi_2) \mid r_i \neq 0, \xi_1 \neq \xi_2\}$. Then the number of pairs covered by M is at least $\frac{q+1}{2}(q - 2) + 2(q - 1)$.

To extend this proposition to a number of pair greater than two is much more harder.

A computer search for small complete M's has been performed for q up to 30000.

Theorem

For q an odd prime power, $19 \leq q \leq 29989$, there exists a complete cap in the three-dimensional affine space $AG(3, q)$ with size at most $a_q(q+1)+2$, where

$$a_q = \begin{cases} 4 & \text{if } 19 \leq q \leq 31, \\ 5 & \text{if } 37 \leq q \leq 121, \\ 6 & \text{if } 127 \leq q \leq 509, \\ 7 & \text{if } 521 \leq q \leq 2347, \\ 8 & \text{if } 2351 \leq q \leq 5227, \\ 9 & \text{if } 5231 \leq q \leq 29989, \end{cases}$$

with the only exceptions of $q = 10531, 18493, 18973, 23677, 24077, 24121, 25163, 25639, 26227, 28643$, where $a_q = 10$.

Random arcs in the projective plane

Probabilistic bound for small complete arcs in $PG(2, q)$

$t(\mathcal{P}_q)$: size of the smallest complete arc in the projective plane $\mathcal{P}_q$ (not necessary Galois) of order q.

$$t(\mathcal{P}_q) \leq d\sqrt{q}\log^c q,\ c \leq 300$$
$$c, d \text{ absolute constants}$$

J.H. Kim, V. Vu, *Small complete arcs in projective planes*, Combinatorica 23 (2003) 311-363.

PROBABILISTIC METHODS

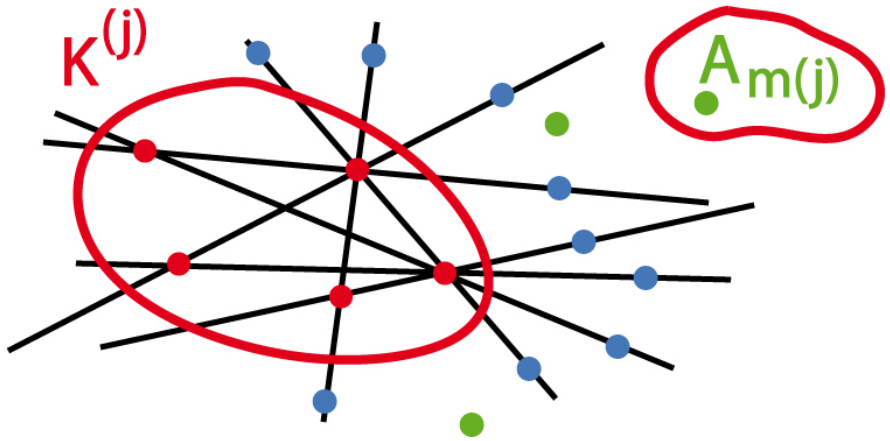
Fixed Order of Points

This is an easy algorithm in order to give an estimation on the minimum size of complete arcs in $PG(2, q)$ for q relatively big. It has been conjectured that a random complete arc has size significantly smaller than the size of the known constructions of complete arcs.

Algorithm

Fix an order on the points of $PG(2,q)$.

$$PG(2,q) := \{A_1, A_2, \ldots, A_{q^2+q+1}\}$$



$$K^{(0)} := \emptyset \quad K^{(1)} := \{P_1\} \quad K^{(2)} := \{P_1, P_2\}$$

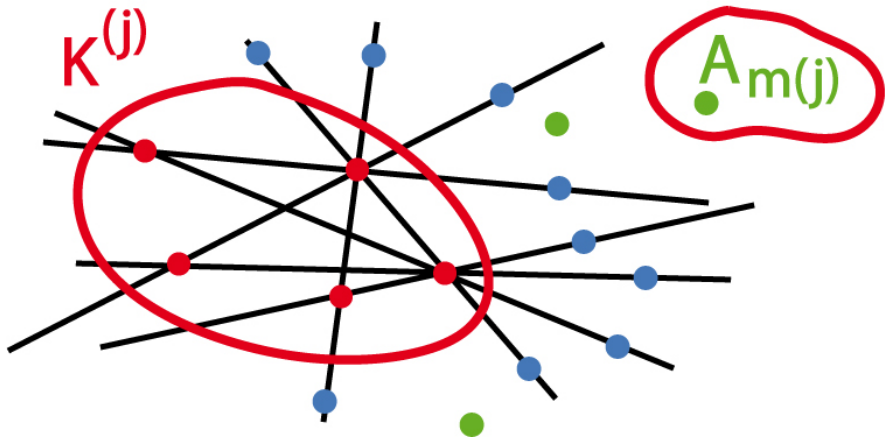
$$K^{(j+1)} = K^{(j)} \cup \{A_{m(j)}\}$$

$m(j)$: minimum index s.t. $A_{m(j)}$ is not saturated by $K^{(j)}$

Algorithm

Fix an order on the points of $PG(2,q)$.

$$PG(2,q) := \{A_1, A_2, \ldots, A_{q^2+q+1}\}$$



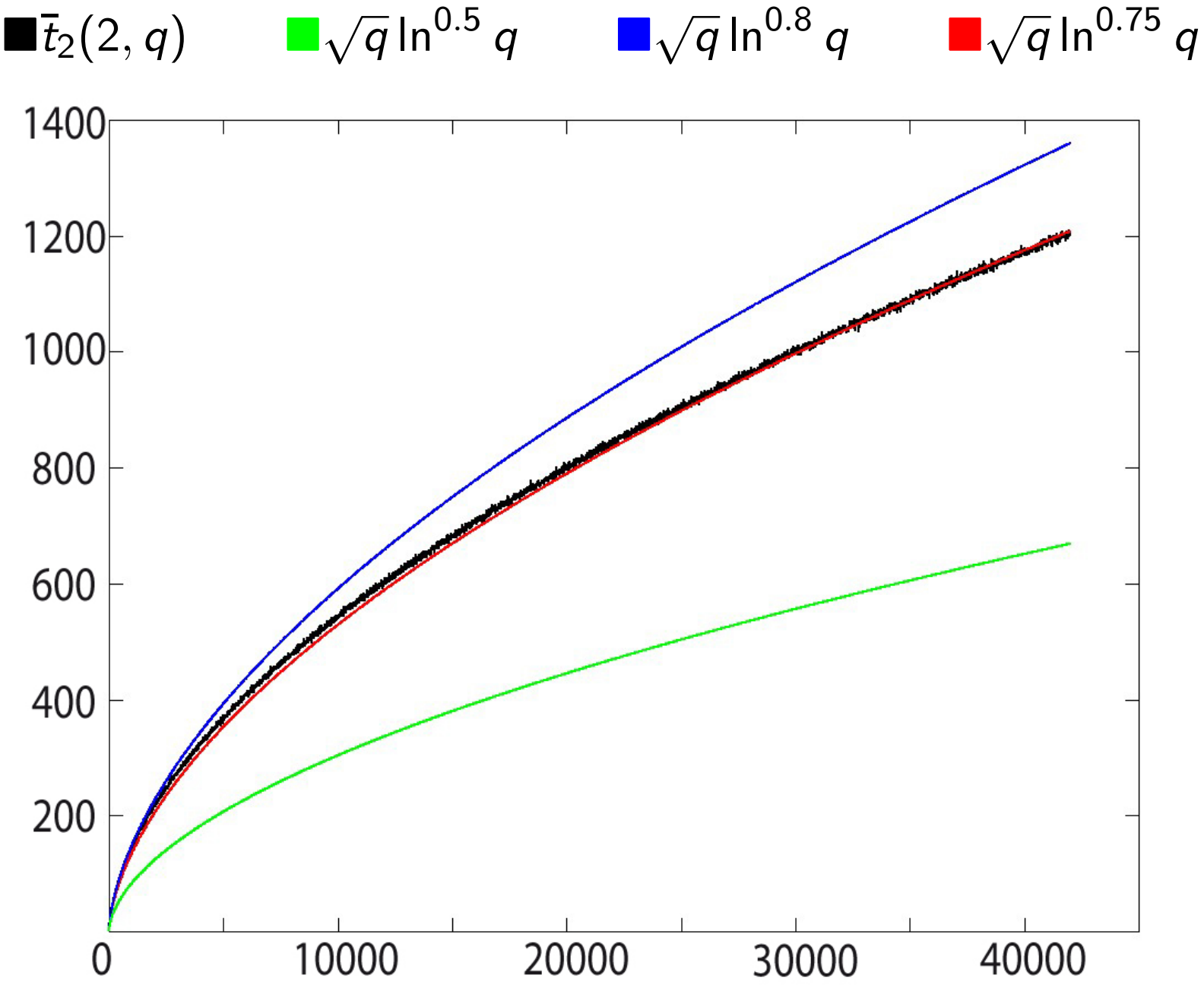
$$K^{(0)} := \emptyset \quad K^{(1)} := \{P_1\} \quad K^{(2)} := \{P_1, P_2\}$$

$$K^{(j+1)} = K^{(j)} \cup \{A_{m(j)}\}$$

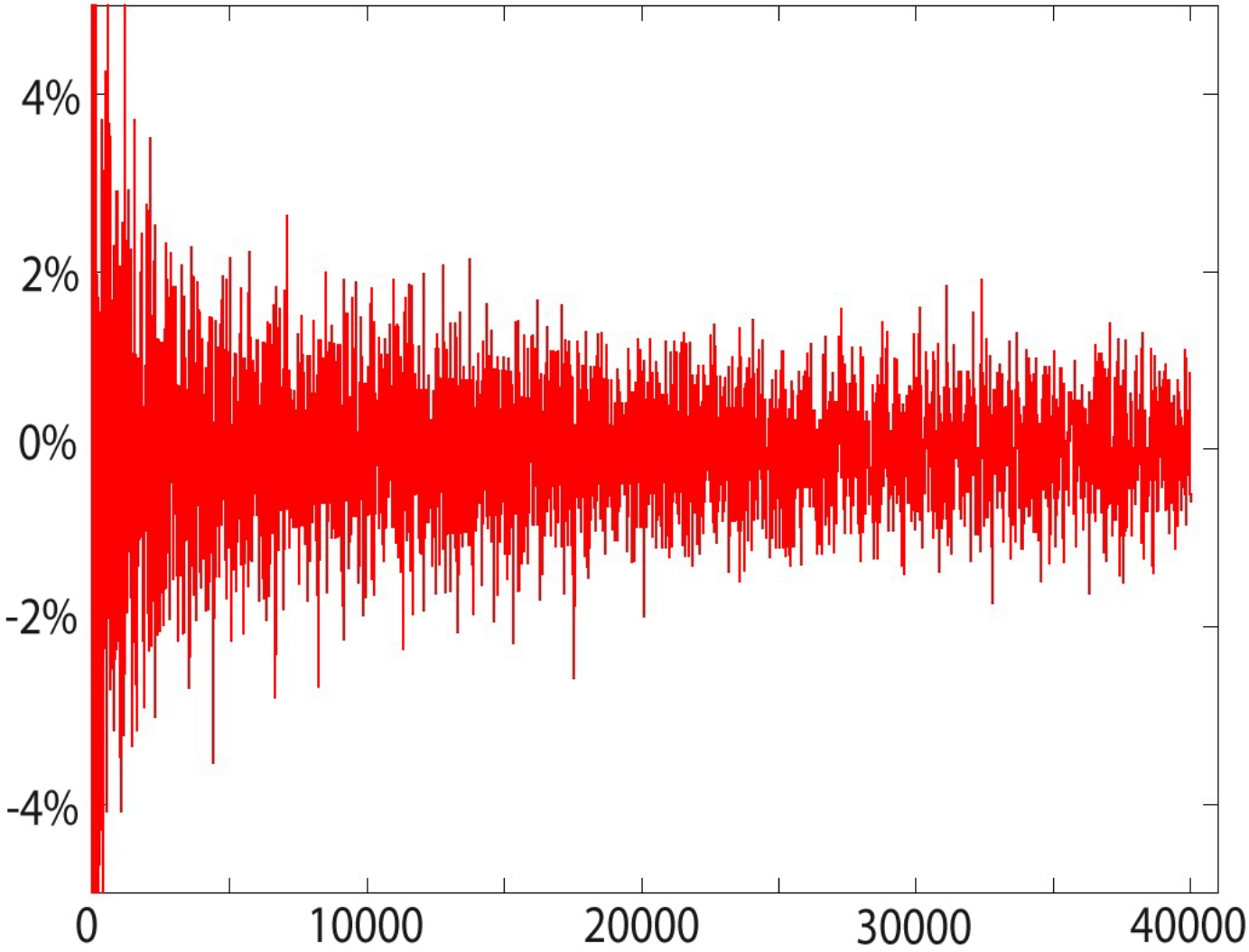
$m(j)$: minimum index s.t. $A_{m(j)}$ is not saturated by $K^{(j)}$

LEXICOGRAPHICAL SINGER

Results with Lexicographical order $q \leq 42009$



Comparison in percentage between Singer and Lexicographical



$R = \{69997, 70001, 79999, 80021, 81001, 82003, 83003, 84011, 85009, 86011, 87011, 88001, 89003, 90001, 91009, 92003, 93001, 94007, 95003, 96001, 97001, 98009, 99013, 99989, 99991, 109987, 110017\}$.

We denote

$$\theta_{up}(q) = \frac{2}{\ln(0.1q)} + 0.32.$$

Theorem

Let $d(q) < 1$ be a decreasing function of q. Then it holds that

$$t_2(2, q) = d(q)\sqrt{q}\ln q, \qquad d(q) < \theta_{up}(q),$$

where $q \leq 67993$, q prime, and $q \in R$. Complete arcs with sizes satisfying this bound can be obtained by Algorithm FOP with Lexicographical order of points represented in homogenous coordinates.

Conjecture

The upper bound holds for all q.

We also conjecture:

1. In $PG(2, q)$, there are 'many' complete k-arcs with size of order $k \approx \sqrt{q} \ln q$,
2. in $PG(2, q)$, a random complete k-arc has the size of order $k \approx \sqrt{q} \ln q$ with high probability;
3. the sizes of complete arcs obtained by Algorithm FOP vary insignificantly with the respect to the order of points.

Multiple coverings and multiple saturating sets

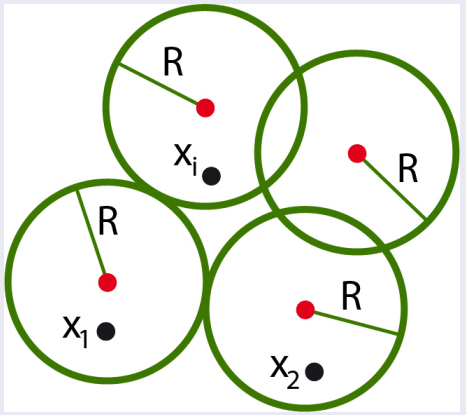
Definition (H. O. Hämäläinen et al., 1995; J. Quistorff, 2001)

(R, μ)-multiple covering of the farthest-off points ((R, μ)-MCF)

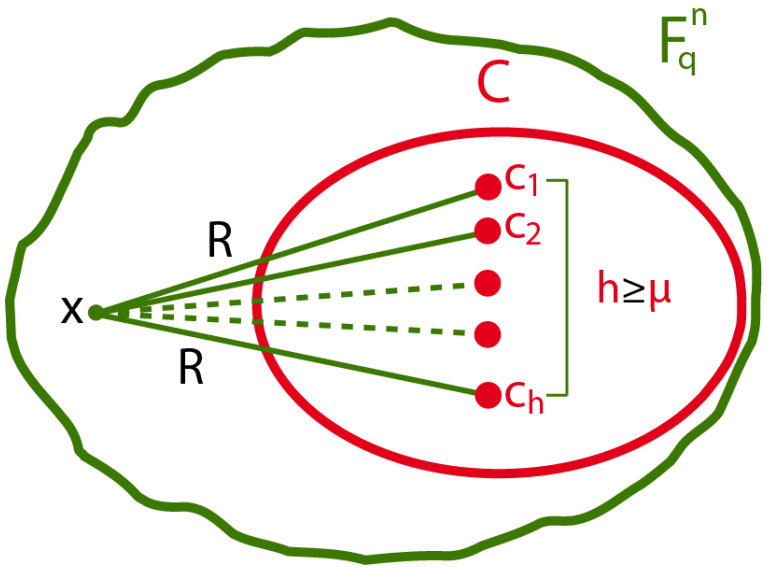
$(n, M, d)_q R$ code $\mathcal{C}$ such that

↙ ↓ ↘

Length Cardinality Minimum Distance



$$\forall x \in \mathbb{F}_q^n : d(x, \mathcal{C}) = R \Longrightarrow |\{c \in \mathcal{C} : d(x, c) = R\}| \geq \mu$$

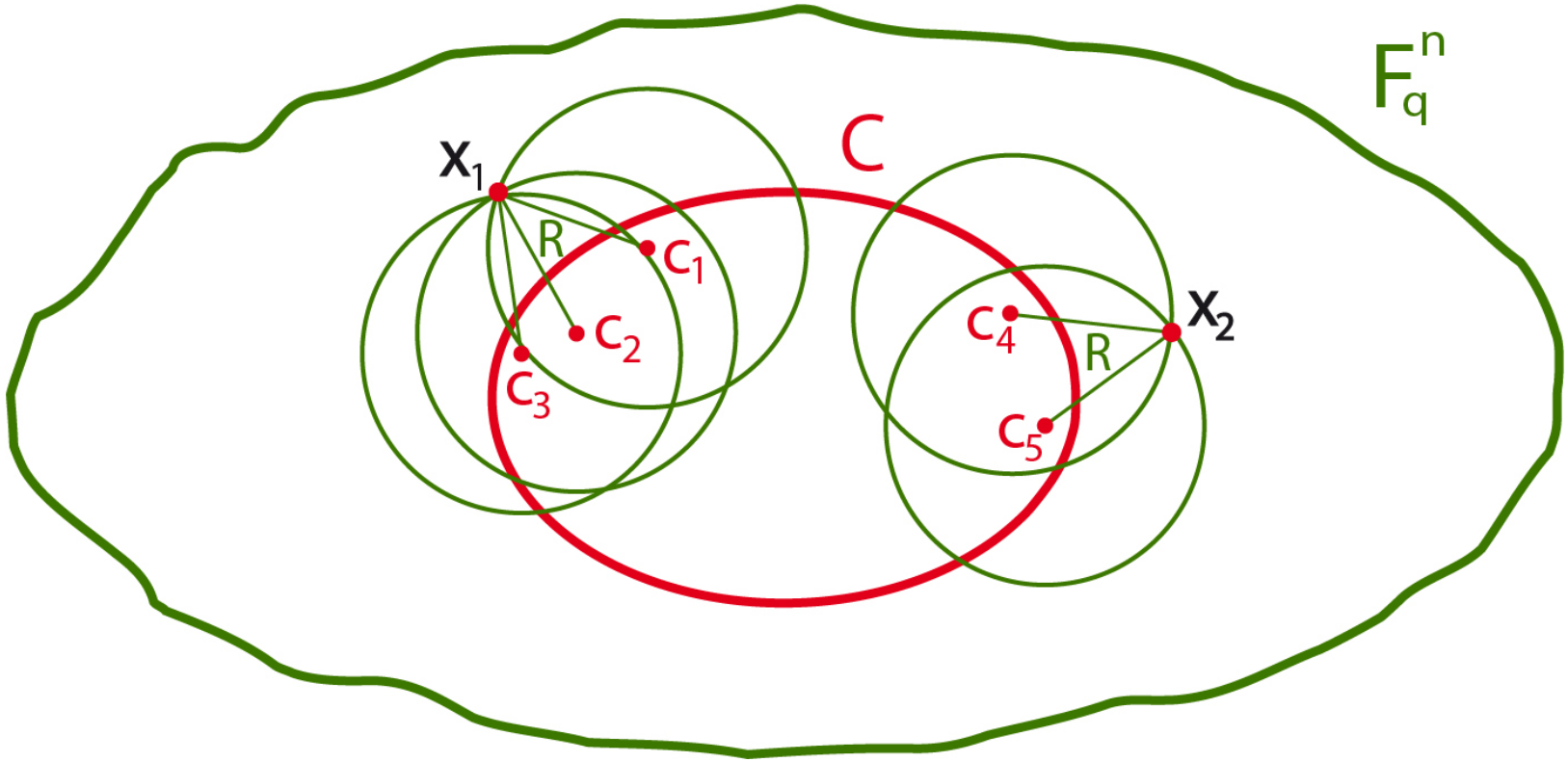


$h = \mu$

⇓

OPTIMAL (R, μ)-MCF

NOTATIONS $\mathcal{C}$: $(n, M, d(\mathcal{C}))_q R$ code



AVERAGE NUMBER OF SPHERES

$$\gamma(\mathcal{C}, r) \leq \frac{M\binom{n}{R}(q-1)^R}{N_R(\mathcal{C})}$$

$$= \text{if } d(\mathcal{C}) > 2R - 1$$

- of radius R
- center $c \in \mathcal{C}$
- containing $x \in \mathbb{F}_q^n$, $\quad d(x, c) = R$
- $N_R(\mathcal{C})$ number of elements of distance R from $\mathcal{C}$

μ-DENSITY

Definition

Let an $(n, M, d)_q R$ code $\mathcal{C}$ be (R, μ)-MCF

$$\mu\textbf{-density } \delta_\mu(\mathcal{C}, R) := \frac{\gamma(\mathcal{C},R)}{\mu} \leq \frac{M\binom{n}{R}(q-1)^R}{\mu N_R(\mathcal{C})}$$

$$\textbf{OPTIMAL } (R, \mu)\text{-MCF} : \delta_\mu(\mathcal{C}, R) = 1$$

Remark

If $\mathcal{C}$ *linear* $[n, k, d(\mathcal{C})]_q R$*-code,* $d(\mathcal{C}) > 2R - 1$,

$$\delta_\mu(\mathcal{C}, R) = \frac{\binom{n}{R}(q-1)^R}{\mu(q^{n-k} - V_q(n,R-1))}$$

SMALL μ-density $\Longrightarrow$ **BETTER (R, μ)-MCF codes**

(ρ, μ)- SATURATING SETS

Definition

$\mathcal{I} \subset PG(N,q)$ (ρ,μ)-**saturating set**, $1 \leq \rho \leq N$, $\mu \geq 1$, if

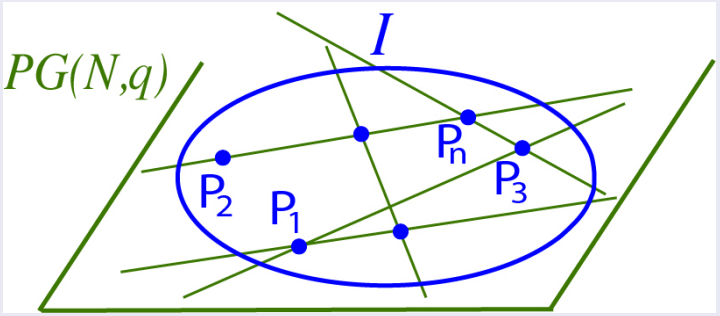
1. $\langle \mathcal{I} \rangle = PG(N,q)$
2. $\exists\, Q \in PG(N,q) : Q \notin \langle P_{i_1}, \ldots, P_{i_h} \rangle = \mathcal{U}$, $\dim \mathcal{U} = \rho - 1$
   $\{P_{i_1}, \ldots, P_{i_h}\} \subset \mathcal{I}$
3. $|\{T = \langle P_{i_1}, \ldots, P_{i_k} \rangle : P_{i_j} \in \mathcal{I}, \dim(T) = \rho \text{ and } Q \in T\}| \geq \mu$

(ρ, μ)- SATURATING SETS

Definition

$\mathcal{I} \subset PG(N,q)$ (ρ,μ)-**saturating set**, $1 \leq \rho \leq N$, $\mu \geq 1$, if

1. $\langle \mathcal{I} \rangle = PG(N,q)$



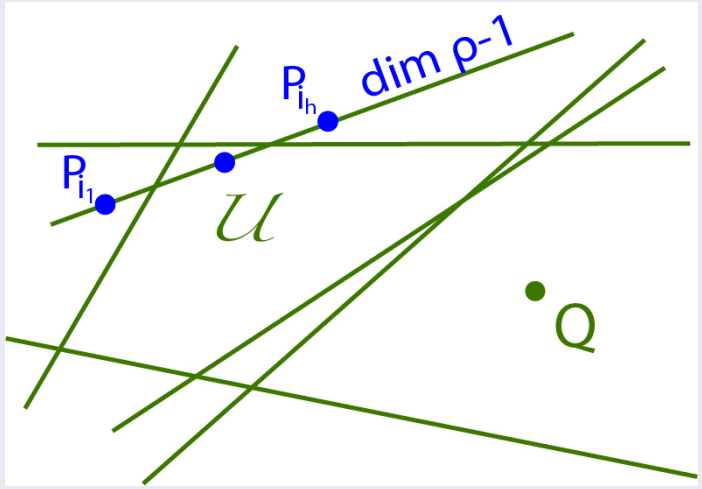
2. $\exists\, Q \in PG(N,q) : Q \notin \langle P_{i_1}, \ldots, P_{i_h} \rangle = \mathcal{U}, \quad \dim \mathcal{U} = \rho - 1$
   $\{P_{i_1}, \ldots, P_{i_h}\} \subset \mathcal{I}$
3. $|\{T = \langle P_{i_1}, \ldots, P_{i_k} \rangle : P_{i_j} \in \mathcal{I}, \dim(T) = \rho \text{ and } Q \in T\}| \geq \mu$

(ρ, μ)- SATURATING SETS

Definition

$\mathcal{I} \subset PG(N,q)$ (ρ,μ)-**saturating set**, $1 \le \rho \le N$, $\mu \ge 1$, if

1. $\langle \mathcal{I} \rangle = PG(N,q)$
2. $\exists\, Q \in PG(N,q) : Q \notin \langle P_{i_1}, \ldots, P_{i_h} \rangle = \mathcal{U}$, $\dim \mathcal{U} = \rho - 1$
   $\{P_{i_1}, \ldots, P_{i_h}\} \subset \mathcal{I}$



3. $|\{T = \langle P_{i_1}, \ldots, P_{i_k} \rangle : P_{i_j} \in \mathcal{I}, \dim(T) = \rho \text{ and } Q \in T\}| \ge \mu$

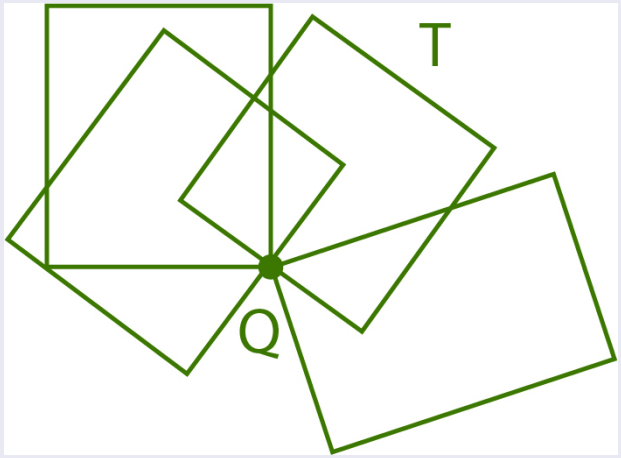
(ρ, μ)- SATURATING SETS

Definition

$\mathcal{I} \subset PG(N,q)$ (ρ,μ)-**saturating set**, $1 \le \rho \le N$, $\mu \ge 1$, if

1. $\langle \mathcal{I} \rangle = PG(N,q)$
2. $\exists\, Q \in PG(N,q) : Q \notin \langle P_{i_1}, \ldots, P_{i_h} \rangle = \mathcal{U}, \quad \dim \mathcal{U} = \rho - 1$
   $\{P_{i_1}, \ldots, P_{i_h}\} \subset \mathcal{I}$
3. $|\{T = \langle P_{i_1}, \ldots, P_{i_k} \rangle : P_{i_j} \in \mathcal{I}, \dim(T) = \rho \text{ and } Q \in T\}| \ge \mu$

Counted with multiplicity m_T



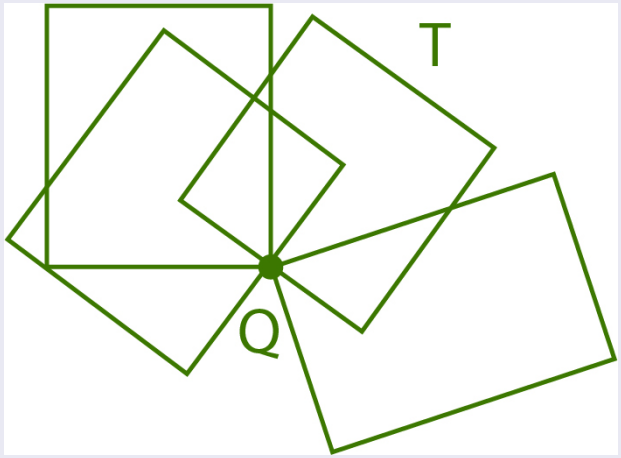
(ρ, μ)- SATURATING SETS

Definition

$\mathcal{I} \subset PG(N,q)$ (ρ,μ)-**saturating set**, $1 \le \rho \le N$, $\mu \ge 1$, if

1. $\langle \mathcal{I} \rangle = PG(N,q)$
2. $\exists\, Q \in PG(N,q) : Q \notin \langle P_{i_1}, \ldots, P_{i_h} \rangle = \mathcal{U}$, $\dim \mathcal{U} = \rho - 1$
   $\{P_{i_1}, \ldots, P_{i_h}\} \subset \mathcal{I}$
3. $|\{T = \langle P_{i_1}, \ldots, P_{i_k} \rangle : P_{i_j} \in \mathcal{I}, \dim(T) = \rho \text{ and } Q \in T\}| \ge \mu$

Counted with multiplicity m_T



Definition

$\mathcal{I}$ (ρ,μ)-saturating set is **minimal** if $\mathcal{I} \not\supset \mathcal{I}'$ (ρ,μ)-saturating set

(ρ, μ)-SATURATING SETS and CODING THEORY

$\{P_1, \quad P_2, \quad \ldots, \quad P_n\}$ (ρ, μ)-saturating set in $PG(n-k-1, q)$

$\downarrow \quad \downarrow \qquad \downarrow$

$(H^1, \quad H^2, \quad \ldots \quad , H^n)$ parity check matrix of a linear $[n, k]_q R$-code $\mathcal{C}$ $R = \rho + 1$

$\Updownarrow$ *Lemma*

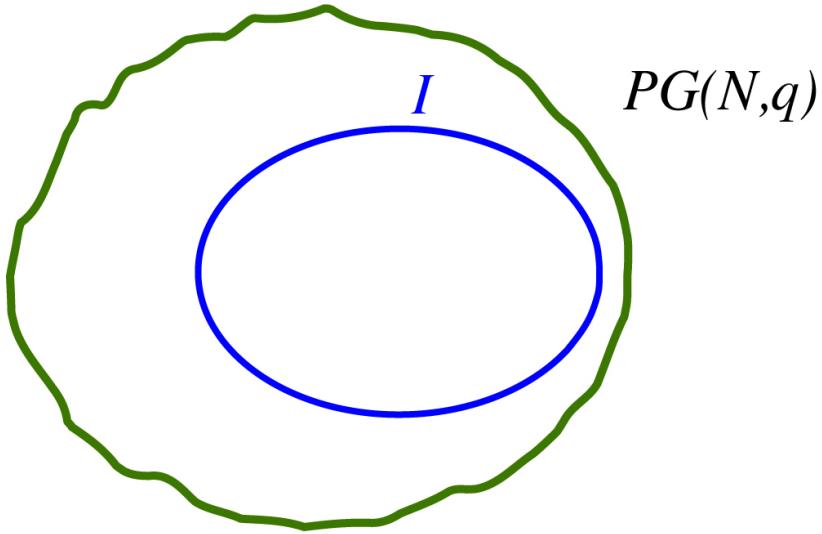
$\mathcal{C}$ is a linear $(\rho + 1, \mu)$-MCF code

(ρ, μ)-SATURATING SETS $\longleftrightarrow$ LINEAR $(\rho + 1, \mu)$-MCF CODES

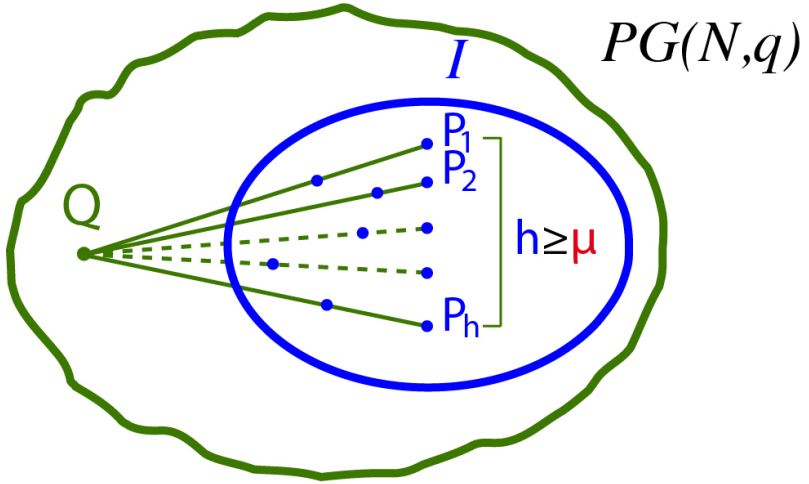
SPECIAL CASES

$\boxed{\rho = 1}$ $\quad \mathcal{I} \subset PG(N, q)$ $\quad$ $(1, \mu)$-saturating set

M2: $\mathcal{I} \neq PG(N, q)$



M3:

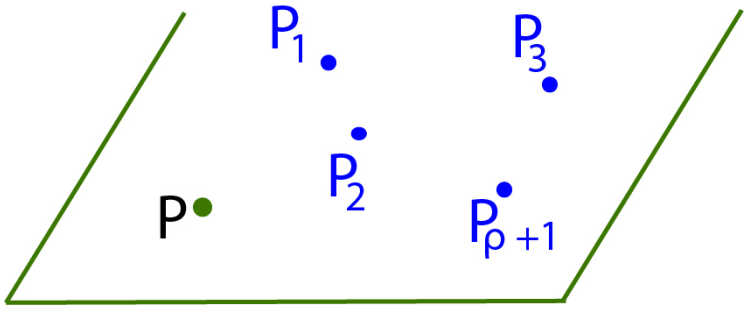


SPECIAL CASES

$\boxed{\mu = 1}$ $\mathcal{I}$ $(\rho, 1)$-saturating set in $PG(N, q) \rightarrow$ $\boxed{\rho\text{-saturating set}}$

ρ is the smallest integer :

$$\forall\, P \in PG(N,q)\ \exists \{P_1, P_2, \ldots, P_{\rho+1}\} \subset \mathcal{I} : P \in \langle P_1, P_2, \ldots, P_{\rho+1} \rangle$$



MINIMAL $(1,2)$-SATURATING SETS in $PG(2,q)$

SPECTRUM : $\forall\ q$ SEVERAL SIZES $< 2\ell(2,3,q)$ (or $2\bar{\ell}(2,3,q)$)

COMPLETE CLASSIFICATIONS $2 \leq q \leq 9$

q	$\ell(2,3,q)$	$\ell_2(2,3,q)$	Spectrum
2	4^2	5	$5^1 6^1$
3	4^1	6	6^4
4	5^1	6	$6^2 7^5$
5	6^6	6	$6^1 7^4 8^{18}$
7	6^3	8	$8^{13} 9^{564} 10^{424}$
8	6^1	8	$8^2 9^{154} 10^{3372} 11^{611}$
9	6^1	8	$8^1 9^{57} 10^{12145} 11^{76749} 12^{3049}$

MINIMAL $(1,2)$-SATURATING SETS in $PG(2,q)$

COMPLETE SPECTRUM and PARTIAL CLASSIFICATION $11 \leq q \leq 17$

q	$\overline{\ell}(2,3,q)$	$\ell_2(2,3,q)$	Spectrum
11	7^1	10	$10^{1348}[11-13,14]$
13	8^2	10	$10^2 11^{50794}[12-15,16]$
16	9^4	11	$11^{52}[12-17,18,19]$
17	10^{3640}	12	$[12-19,20]$

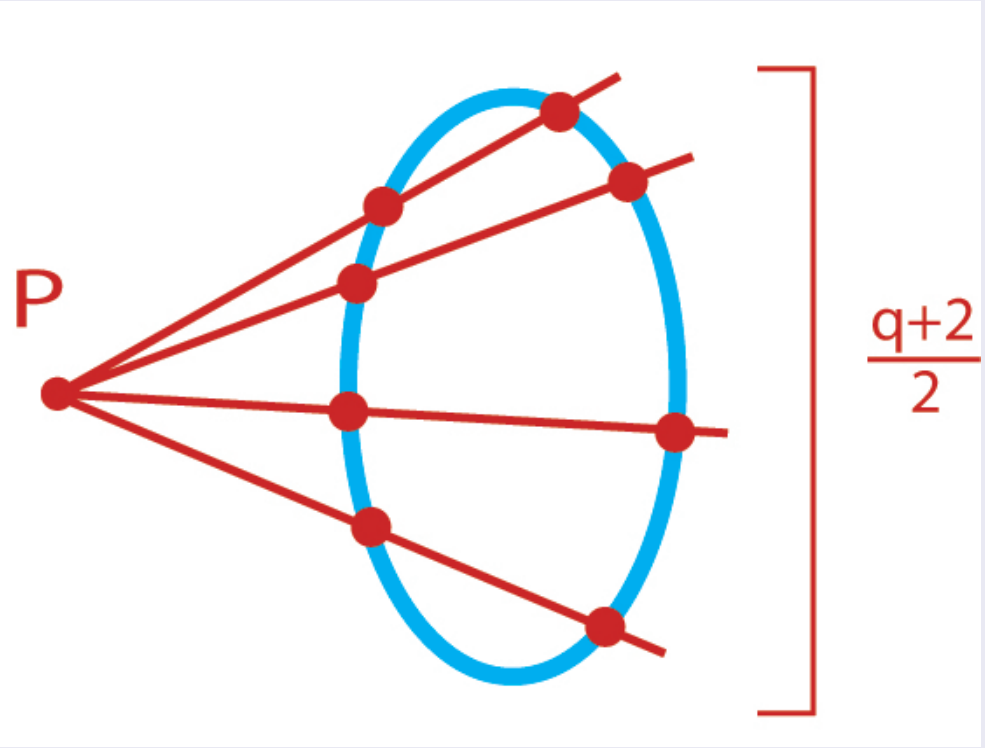
MINIMAL $(1,2)$-SATURATING SETS in $PG(2,q)$

SIZES OF SPECTRUM $19 \leq q \leq 49$

q	$\overline{\ell}(2,3,q)$	Trivial lower bound for $\ell_2(2,3,q) : 2\sqrt{q}$	Found sizes
19	10^{36}.	9	$[13-19, 20-22]$
23	10^{1}.	10	$[15-19, 20-26]$
25	12	10	$[17-23, 24-28]$
27	12	11	$[17-23, 24-30]$
29	13	11	$[19-25, 26-32]$
31	14	12	$[19, 21-27, 28-34]$
32	13	12	$[20-25, 26-35]$
37	15	13	$[23, 26-29, 30-40]$
41	16	13	$[25, 29-31, 32-44]$
43	16	14	$[25, 30, 31, 32-46]$
47	18	14	$[27, 34, 35, 36-50]$
49	18	14	$[29, 34, 35, 36-52]$

Corollary (HYPEROVAL)

q even



$\mathcal{C}$ $[q+2, q-1, 4]_q 2$ *linear code is* $\left(2, \frac{q+2}{2}\right)$*-MCF*

$\delta_\mu(\mathcal{C}, 2) = 1$ *OPTIMAL*

Proposition (OVAL)

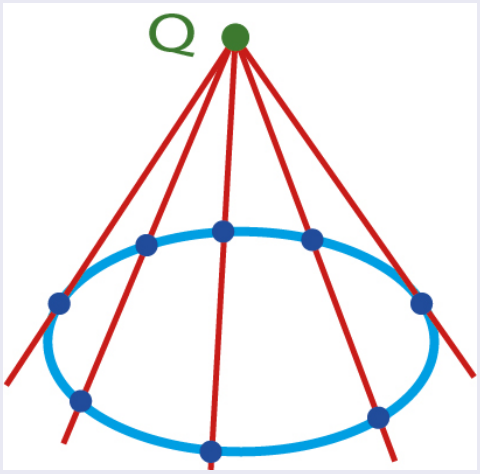
q odd: $\boxed{\textit{OVAL in } PG(2,q) \longleftrightarrow \mathcal{C} \quad [q+1, q-2, 4]_q 2}$

$$\Downarrow$$

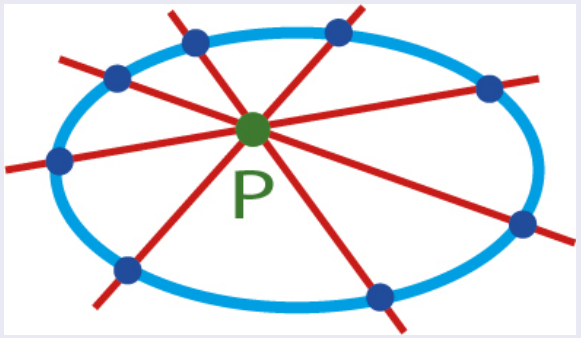
$$\boxed{\begin{array}{c}\mathcal{C} \textit{ is a } \left(2, \frac{q-1}{2}\right)\textit{-MCF} \\ \delta_\mu(\mathcal{C}, 2) \leq 1 + \frac{1}{q}\end{array}}$$

$$q \geq 5 \Longrightarrow q+1 < \mu\bar{\ell}(2,3,q)$$

Q external



P internal



$|\textit{Bisecants through } P| = \frac{q+1}{2}$ $\quad$ $|\textit{Bisecants through } Q| = \frac{q-1}{2} = \mu$

Proposition (HERMITIAN CURVE)

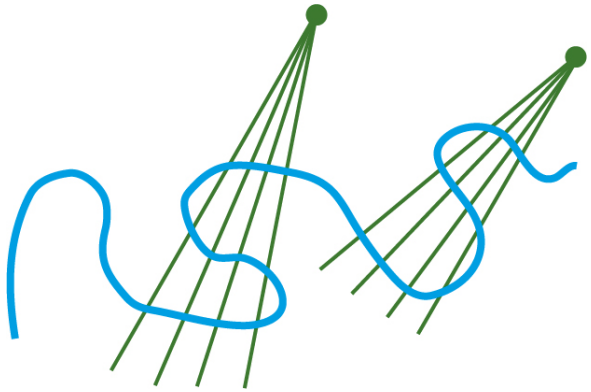
q square

Hermitian Curve in $PG(2,q) \leftrightarrow \mathcal{C} : [\underbrace{q\sqrt{q}+1}_{n}, q\sqrt{q}-2, 3]_q 2$

$\Downarrow$

$\mathcal{C}$ *is a* $\left(2, \underbrace{\frac{q^2-q}{2}}_{\mu}\right)$*-MCF*

$\delta_\mu(\mathcal{C}, 2) = 1$ *OPTIMAL*



$\leftarrow (q-\sqrt{q})$ lines

which are $(\sqrt{q}+1)$-secants

$\Rightarrow (q-\sqrt{q})\binom{\sqrt{q}+1}{2} = \underbrace{\frac{q^2-q}{2}}_{\mu}$ bisecants

AIM reached:

$\bar{\ell}(2,3,q) \geq 4 \Longrightarrow \boxed{n = q\sqrt{q}+1} < 2q^2 - q \leq \boxed{\mu\bar{\ell}(2,3,q)}$

Proposition (BAER SUBPLANE)

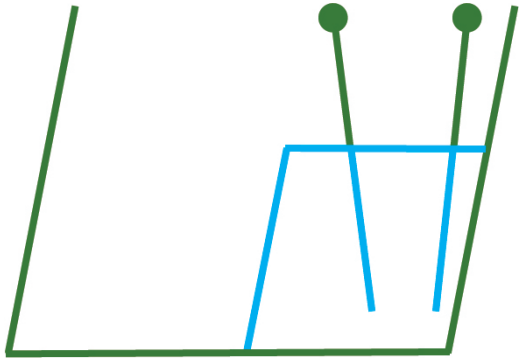
q square

Baer subplane in $PG(2,q) \leftrightarrow \mathcal{C} : [\underbrace{q+\sqrt{q}+1}_{n}, q+\sqrt{q}-2, 3]_q 2$

$\Downarrow$

$\mathcal{C}$ *is a* $\left(2, \underbrace{\frac{q+\sqrt{q}}{2}}_{\mu}\right)$*-MCF*

$\delta_\mu(\mathcal{C}, 2) = 1$ *OPTIMAL*



unique $(\sqrt{q}+1)$ secant

$\Longrightarrow \binom{\sqrt{q}+1}{2} = \underbrace{\frac{q^2+\sqrt{q}}{2}}_{\mu}$ bisecants

AIM reached:

$$\boxed{n = q+\sqrt{q}+1} < 2q+2\sqrt{q} \leq \boxed{\mu\bar{\ell}(2,3,q)}$$

Proposition (ELLIPTIC QUADRIC)

elliptic quadric in $PG(3,q) \longleftrightarrow \mathcal{C} \qquad [q^2+1, q^2-3, 4]_q 2$

$$\Downarrow$$

$\mathcal{C}$ *is a* $\Big(2, \underbrace{\frac{q^2-q}{2}}_{\mu}\Big)$*-MCF*

$\delta_\mu(\mathcal{C}, 2) = 1$ *OPTIMAL*