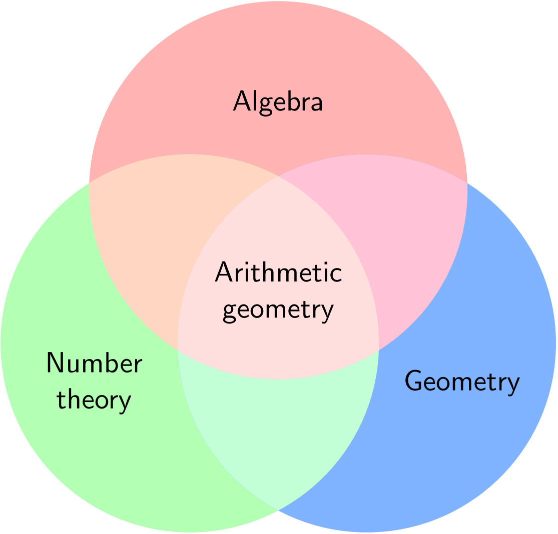
Number of rational points on singular curves over finite fields

Annamaria Iezzi

PhD thesis defense

Marseilles, 6 July 2016

Arithmetic geometry



An example

$\sqrt{2}$ is an irrational number,
that is $\sqrt{2}$ cannot be written as $\frac{x}{y}$, with $x, y \in \mathbb{Z}$ and $y \neq 0$.

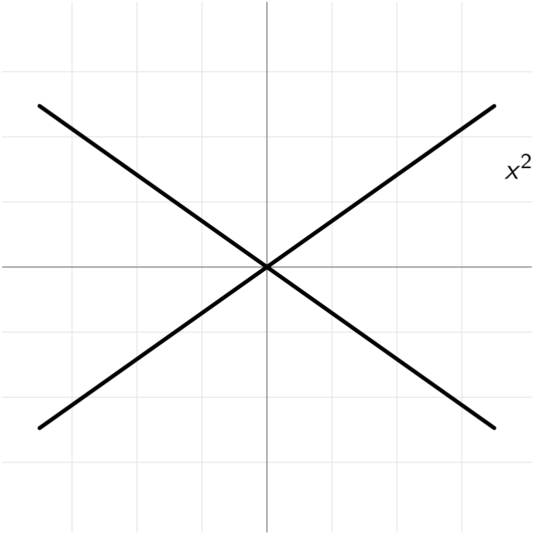
$$\Updownarrow$$

The polynomial equation

$$x^2 - 2y^2 = 0$$

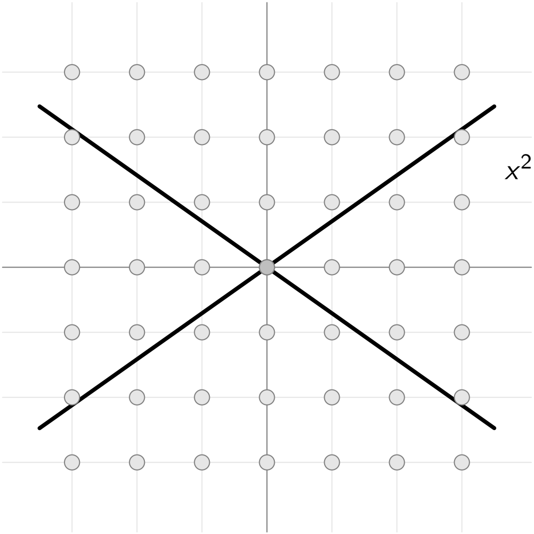
has no integer solutions (x, y), apart from $(0, 0)$.

An example



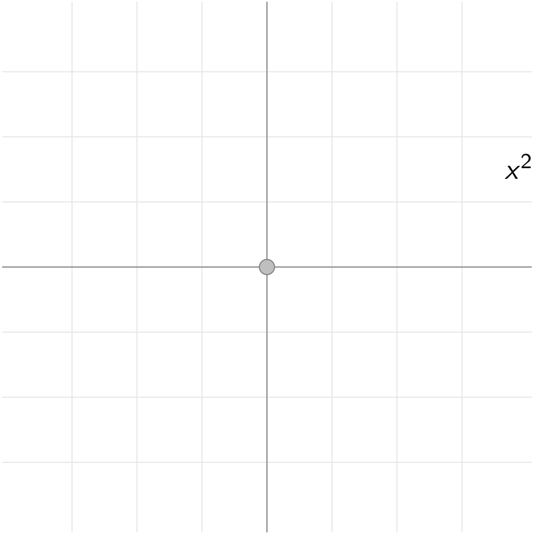
$x^2 - 2y^2 = 0$

An example



$x^2 - 2y^2 = 0$

An example



$$x^2 - 2y^2 = 0$$

An example

The polynomial equation

$$x^2 - 2y^2 = 0$$

has no integer solutions (x, y), apart from $(0, 0)$.

$\Updownarrow$

The curve defined by the equation

$$x^2 - 2y^2 = 0$$

has only one rational point $P(0, 0)$.

$\overset{\text{homogenous equation}}{\Longleftarrow}$

The reduced equation mod 3

$$x^2 + y^2 = 0$$

has no solutions (x, y) with $x, y \in \mathbb{F}_3 = \{0, 1, 2\}$, apart from $(0, 0)$.

$\Updownarrow$

The reduced curve mod 3 defined by the equation

$$x^2 + y^2 = 0$$

has only one rational point over $\mathbb{F}_3$, given by $P(0, 0)$.

$\overset{\text{homogenous equation}}{\Longleftarrow}$

Example

$\longrightarrow$ Check that $(0,0)$ is the unique element of the finite set

$$\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$$

that verifies the equation of the curve:

$$x^2 + y^2 = 0$$

Curves over finite fields

A *curve* $\mathcal{C}$ *over a finite field* $\mathbb{F}_q$ (in its simplest form):

$$\mathcal{C} : f(x, y) = 0,$$

with $f(x, y) \in \mathbb{F}_q[x, y]$.

A *rational point* over $\mathbb{F}_q$ on $\mathcal{C}$: a point (x_0, y_0) with $x_0, y_0 \in \mathbb{F}_q$ such that $f(x_0, y_0) = 0$.

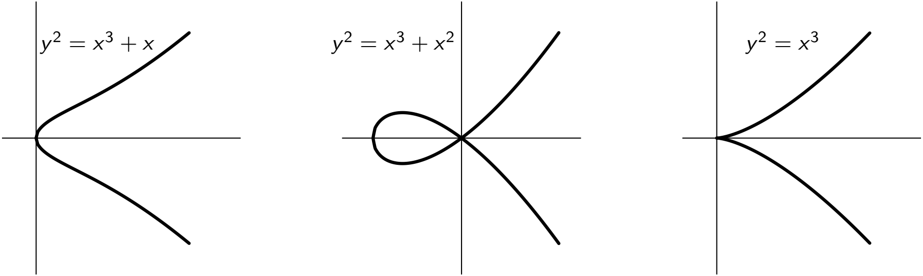
Interest: a curve defined over a finite field has always a finite number of rational points.

$\Downarrow$

Applications to information theory:

- cryptography;
- coding theory.

Most of the results on curves over finite fields are stated for *smooth* curves, that is, curves with no *singular points*.



Here we deal more generally with questions on the number of rational points on a **singular curve over a finite field**.

Outline

Background

Notation

- $\mathbb{F}_q$ the finite field with q elements.
- The word *curve* will always stand for an absolutely irreducible projective algebraic curve.
- The word *point* will stand for a closed point, unless otherwise specified.

Let X be a curve defined over $\mathbb{F}_q$. We denote by:

- $\mathbb{F}_q(X)$ the function field of X;
- $\tilde{X}$ the normalisation of X and $\nu : \tilde{X} \to X$ the normalisation map (regular, finite and birational): $\mathbb{F}_q(X) = \mathbb{F}_q(\tilde{X})$;
- $\sharp X(\mathbb{F}_{q^n})$ the number of rational points on X over $\mathbb{F}_{q^n}$;
- g the *geometric genus* of X, i.e. the genus of $\tilde{X}$;
- π the *arithmetic genus* of X.

The arithmetic genus

Let Q be a point on X and let $\mathcal{O}_Q$ be the local ring of X at Q.

Fact: $\mathcal{O}_Q$ is integrally closed if and only if Q is a nonsingular point.

Let $\overline{\mathcal{O}_Q}$ be the integral closure of $\mathcal{O}_Q$. We have that $\overline{\mathcal{O}_Q}/\mathcal{O}_Q$ is a finite dimensional $\mathbb{F}_q$-vector space. We define the **degree of singularity of** Q:

$$\delta_Q := \dim_{\mathbb{F}_q} \overline{\mathcal{O}_Q}/\mathcal{O}_Q.$$

The **arithmetic genus** π of a curve X is the integer:

$$\pi := g + \underbrace{\sum_{Q \in X} \delta_Q}_{\delta}.$$

- $\pi \geq g$;
- $\pi = g$ if and only if X is a smooth curve;
- If X is a plane curve of degree d, $\pi = \frac{(d-1)(d-2)}{2}$.

A tool for counting rational points

To study $\sharp X(\mathbb{F}_{q^n})$, we consider the zeta function of X is:

$$Z_X(T) := \exp\left(\sum_{n=1}^{\infty} \sharp X(\mathbb{F}_{q^n}) \frac{T^n}{n}\right),$$

the natural generalisation of the Riemann zeta function to curves over finite fields.

Fact: $Z_X(T)$ is a rational function in $\mathbb{Q}(T)$

The smooth case

In 1948 Weil showed that, if X is smooth of genus g,

$$Z_X(T) = \frac{P(T)}{(1-T)(1-qT)},$$

where

$$P(T) = \prod_{i=1}^{2g} (1 - \omega_i T) \in \mathbb{Z}[T]$$

and $\omega_i \in \mathbb{C}$ are algebraic integers of absolute value $\sqrt{q}$.

The polynomial $P(T)$ contains lots of information on the curve. In particular we have

$$\sharp X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{n=1}^{2g} \omega_i^n.$$

The smooth case

If X is a smooth curve defined over $\mathbb{F}_q$ of genus g, the integers $q, \sharp X(\mathbb{F}_q)$ and g satisfy the Serre-Weil bound:

Theorem (Serre-Weil bound)

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leq g[2\sqrt{q}].$$

Let us denote by

$$N_q(g)$$

the maximum number of rational points on a smooth curve defined over $\mathbb{F}_q$ of genus g. Clearly we have:

$$N_q(g) \leq q + 1 + g[2\sqrt{q}].$$

Furthermore $N_q(g)$ is explicit for $g = 0, 1, 2$.

The singular case

In 1996, Aubry and Perret found relations between a curve and its normalisation.

Let X be a curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π, they proved that:

- $Z_X(T) = Z_{\tilde{X}}(T) \prod_{P \in \operatorname{Sing} X} \left(\frac{\prod_{Q \in \nu^{-1}(P)} (1 - T^{\deg Q})}{1 - T^{\deg P}} \right)$;
- $|\sharp \tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)| \leq \pi - g$.

Theorem (Aubry-Perret bound)

$$|\sharp X(\mathbb{F}_q) - (q+1)| \leq g[2\sqrt{q}] + \pi - g.$$

The quantity $N_q(g, \pi)$

The quantity $N_q(g, \pi)$

We introduce an analogous quantity of $N_q(g)$ for singular curves:

Definition

For q a power of a prime, g and π non negative integers such that $\pi \geq g$, let us define the quantity

$$N_q(g, \pi)$$

as the maximum number of rational points over $\mathbb{F}_q$ on a curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π.

Obviously we have:

- $N_q(g, g) = N_q(g)$,
- $N_q(g, \pi) \leq N_q(g) + \pi - g$.
- $N_q(g, \pi) \leq q + 1 + g[2\sqrt{q}] + \pi - g$,

How to determine $N_q(g, \pi)$?

$\longrightarrow$ problem of constructing singular curves with prescribed ground field $\mathbb{F}_q$, geometric genus g and arithmetic genus π and with "many" rational points.

Idea : Starting from a smooth curve X of genus g defined over $\mathbb{F}_q$ we will construct a curve with singularities X' such that X is the normalisation of X', and the added singularities are rational on the base field and with the prescribed singularity degree.

How to determine $N_q(g, \pi)$?

Starting point for the construction:

Theorem (Rosenlicht - 1952)

In any birational class of curves, there exists one with prescribed singularities. More precisely, if we are given a finite number of local rings in a function field K, no two of which have a place in common, then there exists a projective model of K which contains points having the prescribed local rings and elsewhere is non-singular.

prescribed singularity $\longleftrightarrow$ prescribed local ring

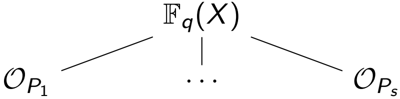
Curves with prescribed singularities

Construction of a prescribed singularity

Let start from a smooth curve X over $\mathbb{F}_q$ and let $S = \{P_1, \ldots, P_s\}$ be a non-empty finite set of closed points on X.

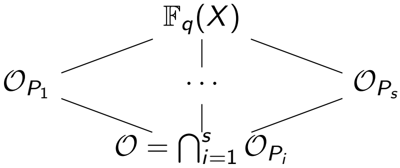
Construction of a prescribed singularity

Let start from a smooth curve X over $\mathbb{F}_q$ and let $S = \{P_1, \ldots, P_s\}$ be a non-empty finite set of closed points on X.



Construction of a prescribed singularity

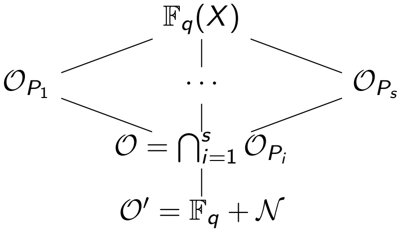
Let start from a smooth curve X over $\mathbb{F}_q$ and let $S = \{P_1, \ldots, P_s\}$ be a non-empty finite set of closed points on X.



$\mathcal{O}$ is a semi-local ring with maximal ideals $\mathcal{N}_{P_i} := \mathcal{M}_{P_i} \cap \mathcal{O}$ for $i = 1, \ldots, s$.

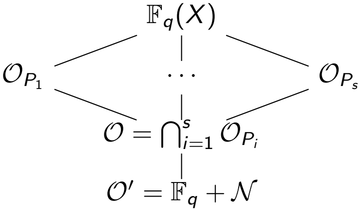
Construction of a prescribed singularity

Let start from a smooth curve X over $\mathbb{F}_q$ and let $S = \{P_1, \ldots, P_s\}$ be a non-empty finite set of closed points on X.



$\mathcal{O}$ is a semi-local ring with maximal ideals $\mathcal{N}_{P_i} := \mathcal{M}_{P_i} \cap \mathcal{O}$ for $i = 1, \ldots, s$.
Let $n_1, \ldots, n_s$ be s positive integers, let us set $\mathcal{N} := \mathcal{N}_{P_1}^{n_1} \cdots \mathcal{N}_{P_s}^{n_s}$ and let us consider:

$$\mathcal{O}' := \mathbb{F}_q + \mathcal{N}.$$

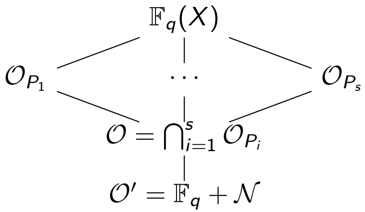


Proposition

$\mathcal{O}' = \mathbb{F}_q + \mathcal{N}$ *verifies the following properties:*

1. $\mathrm{Frac}(\mathcal{O}') = \mathbb{F}_q(X)$ *and* $\mathcal{O}$ *is the integral closure of* $\mathcal{O}'$ *in* $\mathbb{F}_q(X)$.
2. $\mathcal{O}'$ *is a local ring with maximal ideal* $\mathcal{N}$ *and residue field* $\mathcal{O}'/\mathcal{N} \cong \mathbb{F}_q$.
3. $\mathcal{O}/\mathcal{O}'$ *is a* $\mathbb{F}_q$*-vector space such that*

$$\dim_{\mathbb{F}_q}(\mathcal{O}/\mathcal{O}') = \sum_{i=1}^{s} n_i \deg P_i - 1.$$

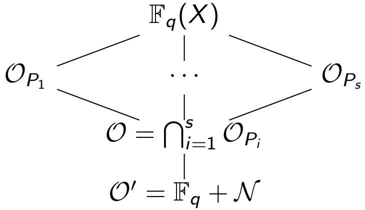


Theorem

There exists a curve X' defined over $\mathbb{F}_q$

1. $\mathrm{Frac}(\mathcal{O}') = \mathbb{F}_q(X)$ *and $\mathcal{O}$ is the integral closure of $\mathcal{O}'$ in $\mathbb{F}_q(X)$.*
2. *$\mathcal{O}'$ is a local ring with maximal ideal $\mathcal{N}$ and residual field $\mathcal{O}'/\mathcal{N} \cong \mathbb{F}_q$.*
3. *$\mathcal{O}/\mathcal{O}'$ is a $\mathbb{F}_q$-vector space such that*

$$\dim_{\mathbb{F}_q}(\mathcal{O}/\mathcal{O}') = \sum_{i=1}^{s} n_i \deg P_i - 1.$$

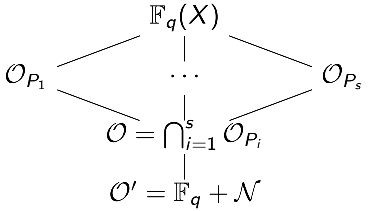


Theorem

There exists a curve X' defined over $\mathbb{F}_q$

1. *having X as normalisation,*
2. *$\mathcal{O}'$ is a local ring with maximal ideal $\mathcal{N}$ and residual field $\mathcal{O}'/\mathcal{N} \cong \mathbb{F}_q$.*
3. *$\mathcal{O}/\mathcal{O}'$ is a $\mathbb{F}_q$-vector space such that*

$$\dim_{\mathbb{F}_q}(\mathcal{O}/\mathcal{O}') = \sum_{i=1}^{s} n_i \deg P_i - 1.$$

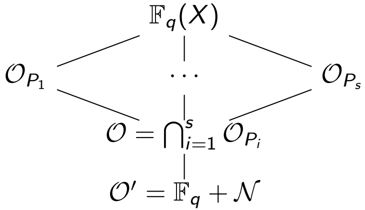


Theorem

There exists a curve X' defined over $\mathbb{F}_q$

1. *having X as normalisation,*
2. *with only one singular point Q such that $\mathcal{O}_Q = \mathcal{O}'$ and Q is rational.*
3. *$\mathcal{O}/\mathcal{O}'$ is a $\mathbb{F}_q$-vector space such that*

$$\dim_{\mathbb{F}_q}(\mathcal{O}/\mathcal{O}') = \sum_{i=1}^{s} n_i \deg P_i - 1.$$

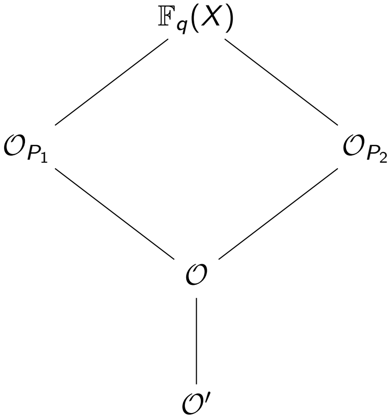


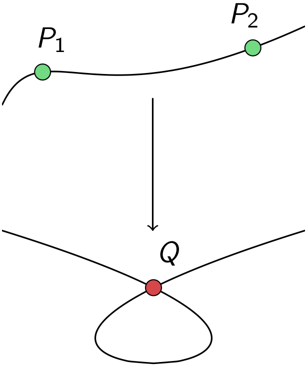
Theorem

There exists a curve X' defined over $\mathbb{F}_q$

1. *having X as normalisation,*
2. *with only one singular point Q such that $\mathcal{O}_Q = \mathcal{O}'$ and Q is rational.*
3. *Q has a degree of singularity equal to $\sum_{i=1}^{s} n_i \deg P_i - 1$ and*

$$\pi(X') = g + \sum_{i=1}^{s} n_i \deg P_i - 1.$$


$\mathbb{F}_q(X)$
$\mathcal{O}_{P_1}$
$\mathcal{O}_{P_2}$
$\mathcal{O}$
$\mathcal{O}'$


P_1
P_2
Q

$$\mathbb{F}_q(X)$$

$$|$$

$$\mathcal{O} = \mathcal{O}_P$$

$$|$$

$$\mathcal{O}' = \mathbb{F}_q + \mathcal{M}_P$$

Proposition

$\mathcal{O}' = \mathbb{F}_q + \mathcal{M}_P$ verifies the following properties:

1. $\mathrm{Frac}(\mathcal{O}') = \mathbb{F}_q(X)$ *and $\mathcal{O}$ is the integral closure of $\mathcal{O}'$ in $\mathbb{F}_q(X)$.*
2. *$\mathcal{O}'$ is a local ring with maximal ideal $\mathcal{N}$ and residual field $\mathcal{O}'/\mathcal{N} \cong \mathbb{F}_q$.*
3. *$\mathcal{O}/\mathcal{O}'$ is a $\mathbb{F}_q$-vector space such that*

$$\dim_{\mathbb{F}_q}(\mathcal{O}/\mathcal{O}') = \deg P - 1.$$

$$\begin{array}{c} \mathbb{F}_q(X) \\ | \\ \mathcal{O} = \mathcal{O}_P \\ | \\ \mathcal{O}' = \mathbb{F}_q + \mathcal{M}_P \end{array}$$

Theorem

There exists a curve X' defined over $\mathbb{F}_q$

1. *having X as normalisation,*
2. *with only one singular point Q such that $\mathcal{O}_Q = \mathcal{O}'$ and Q is rational.*
3. *Q has a degree of singularity equal to $\deg P - 1$ and*

$$\pi(X') = g + \deg P - 1.$$

Singular curves with many points and small π

Theorem

Let X be a smooth curve of genus g defined over $\mathbb{F}_q$. Let π be an integer of the form

$$\pi = g + a_2 + 2a_3 + 3a_4 + \cdots + (n-1)a_n$$

with $0 \leq a_i \leq B_i(X)$, where $B_i(X)$ is the number of closed points of degree i on the curve X. Then there exists a (singular) curve X' over $\mathbb{F}_q$ of arithmetic genus π such that X is the normalisation of X' and

$$\sharp X'(\mathbb{F}_q) = \sharp X(\mathbb{F}_q) + a_2 + a_3 + a_4 + \cdots + a_n.$$

Roughly speaking we can "transform" a point of degree d on a smooth curve in a singular rational one, provided that we increase the value of the arithmetic genus by $d - 1$.

Singular curves with many points and small π

Theorem

Let X be a smooth curve of genus g defined over $\mathbb{F}_q$. Let π be an integer of the form

$$\pi = g + a_2 + 2a_3 + 3a_4 + \cdots + (n-1)a_n$$

with $0 \leq a_i \leq B_i(X)$, where $B_i(X)$ is the number of closed points of degree i on the curve X. Then there exists a (singular) curve X' over $\mathbb{F}_q$ of arithmetic genus π such that X is the normalisation of X' and

$$\sharp X'(\mathbb{F}_q) = \sharp X(\mathbb{F}_q) + a_2 + a_3 + a_4 + \cdots + a_n.$$

Remark: Points of degree 2 play a fundamental role in this construction: they are the only ones that make it possible to increase the number of rational points as much as the degree of singularity of the curve.

Question

For which values of q, g and π are the bounds

- $N_q(g,\pi) \leq N_q(g) + \pi - g$
- $N_q(g,\pi) \leq q + 1 + g[2\sqrt{q}] + \pi - g$

reached?

Optimal and maximal curves

Terminology

Definition

Let X be a curve over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π. The curve X is said to be:

(i) an *optimal curve* if

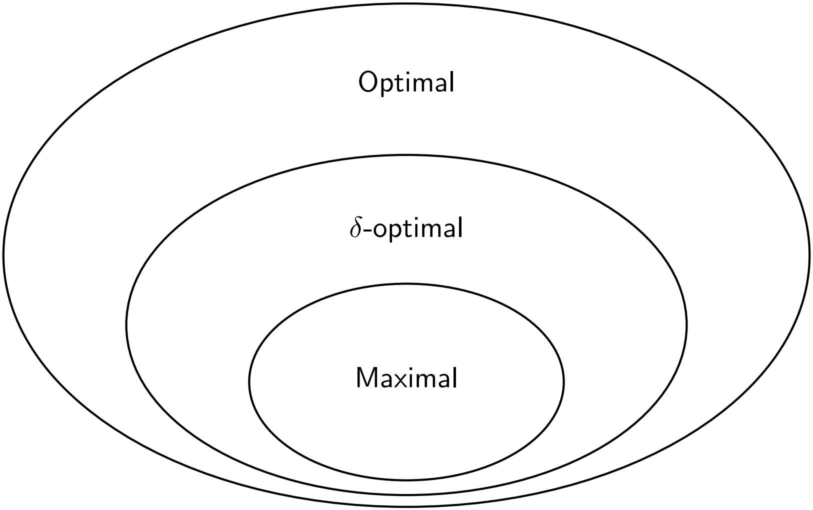
$$\sharp X(\mathbb{F}_q) = N_q(g, \pi);$$

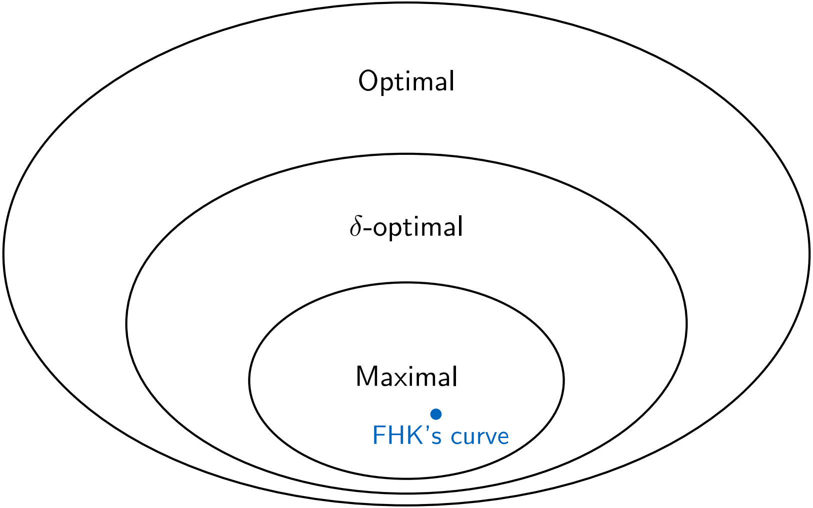
(ii) a δ-*optimal curve* if

$$\sharp X(\mathbb{F}_q) = N_q(g) + \pi - g = N_q(g) + \delta;$$

(iii) a *maximal curve* if

$$\sharp X(\mathbb{F}_q) = q + 1 + g[2\sqrt{q}] + \pi - g.$$


Optimal
δ-optimal
Maximal


Optimal
δ-optimal
Maximal
FHK's curve

Fukasawa, Homma and Kim's curve

In 2011, Fukasawa, Homma and Kim considered and studied the plane curve B over $\mathbb{F}_q$ defined as the image of

$$\begin{array}{cccc} \Phi: & \mathbb{P}^1 & \to & \mathbb{P}^2 \\ & (s,t) & \mapsto & (s^{q+1}, s^q t + s t^q, t^{q+1}) \end{array}$$

Properties of B:

1. B is a rational plane curve of degree $q+1 \Rightarrow g = 0, \pi = \frac{q^2-q}{2}$;
2. $\mathrm{Sing}(B) \subseteq B(\mathbb{F}_q)$;
3. For $P \in \mathbb{P}^1$, $\Phi(P) \in \mathrm{Sing}(B)$ if and only if $P \in \mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mathbb{P}^1(\mathbb{F}_q)$. In this case, $\Phi^{-1}(\Phi(P)) = \{P, P^q\}$.

$$\sharp B(\mathbb{F}_q) = q + 1 + \frac{\mathbf{q^2 - q}}{\mathbf{2}}$$

$\longrightarrow$ B is a maximal singular curve with $g = 0$ and $\pi = \frac{q^2-q}{2}$

δ-optimal and maximal curves

Proposition

Let X be a curve of geometric genus g and arithmetic genus π. If X is δ-optimal (maximal) then:

1. *the normalisation $\tilde{X}$ is an optimal (maximal) curve;*
2. $\mathrm{Sing}(X) \subset X(\mathbb{F}_q)$;
3. *if Q is a singular point on X, then $\nu^{-1}(Q) = \{P\}$, with P a point of degree 2 on $\tilde{X}$;*
4. $\pi - g \leq B_2(\tilde{X})$, *where $B_2(\tilde{X})$ denotes the number of points of degree 2 on $\tilde{X}$;*
5. $Z_X(T) = Z_{\tilde{X}}(T)(1+T)^{\pi-g}$.

A theorem for the existence of δ-optimal curves

The existence of δ-optimal curves is strictly connected to the existence of a large number of points of degree 2 on an optimal smooth curve.

Let us denote

$\mathcal{X}_q(g)$: the set of optimal smooth curves defined over $\mathbb{F}_q$ of genus g.

$B_2(\mathcal{X}_q(g))$: the maximum number of points of degree 2 on a curve of $\mathcal{X}_q(g)$.

Theorem

We have:

$$N_q(g,\pi) = N_q(g) + \pi - g \iff g \leq \pi \leq g + B_2(\mathcal{X}_q(g)).$$

The quantity $B_2(\mathcal{X}_q(g))$ is easy to calculate for g equal to 0 and 1.

The case of rational curves ($g = 0$)

$$B_2(\mathcal{X}_q(0)) = \frac{q^2 - q}{2}$$

Corollary

We have

$$N_q(0, \pi) = q + 1 + \pi$$

if and only if $0 \le \pi \le \frac{q^2-q}{2}$.

Fukasawa, Homma and Kim's curve is an explicit example of this corollary for $\pi = \frac{q^2-q}{2}$.

The case $g = 1$

Corollary

1. *If p does not divide m, or q is a square, or $q = p$ we have:*

$$N_q(1, \pi) = q + 1 + [2\sqrt{q}] + \pi - 1$$

if and only if $1 \leq \pi \leq 1 + \frac{q^2+q-[2\sqrt{q}]([2\sqrt{q}]+1)}{2}$.

2. *In the other cases we have*

$$N_q(1, \pi) = q + [2\sqrt{q}] + \pi - 1$$

if and only if $1 \leq \pi \leq 1 + \frac{q^2+q+[2\sqrt{q}](1-[2\sqrt{q}])}{2}$.

How to bound the quantity $B_2(\mathcal{X}_q(g))$?

$\longrightarrow$ problem of bounding the number of points of degree 2 on a smooth curve.

When $g \geq 2$ the information on the number of rational points on a smooth curve of genus g is not enough to determine the number of points of degree 2.

For X a smooth curve of genus g, we will bound the quantity $B_2(X)$ using an Euclidean approach developed by Hallouin and Perret.

Then, we will deduce bounds for $B_2(\mathcal{X}_q(g))$ by assuming X to be an optimal smooth curve.

The Hallouin-Perret's approach

Let X be a smooth curve defined over $\mathbb{F}_q$ of genus $g > 0$.
For every positive integer n, we associate to X a n-tuple $(x_1, \ldots, x_n)$ defined as follows:

$$x_i := \frac{(q^i + 1) - \sharp X(\mathbb{F}_{q^i})}{2g\sqrt{q^i}}, \quad i = 1, \ldots, n.$$

lower bound for $x_i \longleftrightarrow$ upper bound for $\sharp X(\mathbb{F}_{q^i})$

upper bound for $x_i \longleftrightarrow$ lower bound for $\sharp X(\mathbb{F}_{q^i})$.

The Hallouin-Perret's approach

$$x_i := \frac{(q^i + 1) - \sharp X(\mathbb{F}_{q^i})}{2g\sqrt{q^i}}, \quad i = 1, \ldots, n.$$

- A consequence of Riemann Hypothesis:

$$|x_i| \leq 1, \quad \text{for all } i = 1, \ldots, n$$

$$\Downarrow$$

$$(x_1, \ldots, x_n) \in \mathcal{C}_n = \{(x_1, \ldots, x_n) \in \mathbb{R}^n | -1 \leq x_i \leq 1, \ \forall\, i = 1, \ldots, n\}.$$

The Hallouin-Perret's approach

- Geometric point of view: a consequence of the Hodge Index Theorem.

$$G_n = \begin{pmatrix} 1 & x_1 & \cdots & x_{n-1} & x_n \\ x_1 & 1 & x_1 & \ddots & x_{n-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ x_{n-1} & \ddots & \ddots & 1 & x_1 \\ x_n & x_{n-1} & \cdots & x_1 & 1 \end{pmatrix}$$

is a Gram matrix and thus is positive semidefinite.

$$\Downarrow$$

$$(x_1, \ldots, x_n) \in \mathcal{W}_n = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid G_{n,I} \geq 0, \forall I \subset \{1, \ldots, n+1\}\}$$

The Hallouin-Perret's approach

- Arithmetic point of view: a consequence of the inequalities pointed out by Ihara:

$$\sharp X(\mathbb{F}_{q^i}) \geq \sharp X(\mathbb{F}_q), \quad \text{for all } i \geq 2.$$

$$x_i \leq \frac{x_1}{q^{\frac{i-1}{2}}} + \frac{q^{i-1}-1}{2gq^{\frac{i-2}{2}}}.$$

$$\Downarrow$$

$$(x_1, \ldots, x_n) \in \mathcal{H}_n^{q,g} = \{(x_1, \ldots, x_n) \in \mathbb{R}^n | h_i^{q,g}(x_1, x_i) \leq 0, \text{ for all } 2 \leq i \leq n\},$$

where

$$h_i^{q,g}(x_1, x_i) = x_i - \frac{x_1}{\sqrt{q}^{i-1}} - \frac{\sqrt{q}}{2g}\left(\sqrt{q}^{i-1} - \frac{1}{\sqrt{q}^{i-1}}\right)$$

The Hallouin-Perret's approach

To sum up, for every $n = 0, 1, 2, \ldots$ one has $(x_1, \ldots, x_n) \in \mathcal{C}_n \cap \mathcal{W}_n \cap \mathcal{H}_n^{q,g}$

Hallouin and Perret showed that, increasing the dimension n, the set $\mathcal{C}_n \cap \mathcal{W}_n \cap \mathcal{H}_n^{q,g}$ provides an increasingly sharper lower bound for x_1 (and hence an increasingly sharper upper bound for $\sharp X(\mathbb{F}_q)$) if g is large enough compared to q.

Bounds for the number of points of degree 2

Let X be a smooth curve defined over $\mathbb{F}_q$ of genus g. We have

$$B_2(X) = \frac{\sharp X(\mathbb{F}_{q^2}) - \sharp X(\mathbb{F}_q)}{2}.$$

We can write $B_2(X)$ as a function of x_1 and x_2

$$B_2(X) = g\sqrt{q}(x_1 - \sqrt{q}x_2) + \frac{q^2 - q}{2}$$

and study this function in the domain $\mathcal{C}_n \cap \mathcal{W}_n \cap \mathcal{H}_n^{q,g}$ for different values of n.

We note that any lower bound for x_2 implies an upper bound for $B_2(X)$, possibly depending on x_1.

First order: $n = 1$

$$B_2(X) \leq \frac{q^2 - q}{2} + g(q + \sqrt{q}) =: M'(q, g).$$

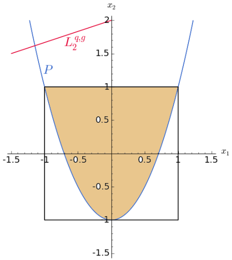
q \ g	2	3	4	5	6
2	7	11	14	18	21
3	12	17	21	26	31
2^2	18	24	30	36	42

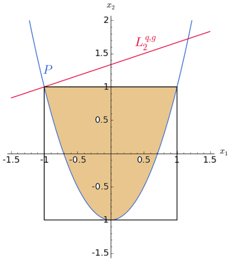
Table: First-order upper bounds for $B_2(\mathcal{X}_q(g))$ given by $M'(q, g)$.

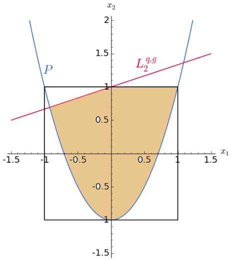
Second order : $n = 2$

$$\mathcal{C}_2 \cap \mathcal{W}_2 \cap \mathcal{H}_2^{q,g} \longrightarrow \begin{cases} 2x_1^2 - 1 \leq x_2 \leq 1 \\ x_2 \leq \frac{x_1}{\sqrt{q}} + \frac{q-1}{2g}. \end{cases}$$

Table: The region $\mathcal{C}_2 \cap \mathcal{W}_2 \cap \mathcal{H}_2^{q,g}$, respectively for $g < g_2$, $g = g_2$ and $g > g_2$.







$$x_2 \geq 2x_1^2 - 1 \Rightarrow B_2(X) \leq g\sqrt{q}(x_1 - \sqrt{q}(2x_1^2 - 1)) + \frac{q^2 - q}{2}.$$

Second order : $n = 2$

Let X be a smooth curve of genus $g > 0$ over $\mathbb{F}_q$. We have:

$$B_2(X) \leq \frac{q^2 + 1 + 2gq - \frac{1}{g}\left(\sharp X(\mathbb{F}_q) - (q+1)\right)^2 - \sharp X(\mathbb{F}_q)}{2}.$$

$$M''(q,g) := \frac{q^2 + 1 + 2gq - \frac{1}{g}\left(N_q(g) - (q+1)\right)^2 - N_q(g)}{2}$$

$$\Downarrow$$

$$B_2(\mathcal{X}_q(g)) \leq M''(q,g).$$

Second order : $n = 2$

g / q	2	3	4	5	6
2	1	2	3	4	5
3	3	3	3	5	7
2^2	5	0	4	5	3

Table: Second-order upper bounds for $B_2(\mathcal{X}_q(g))$ given by $M''(q, g)$.

Third order: $n = 3$

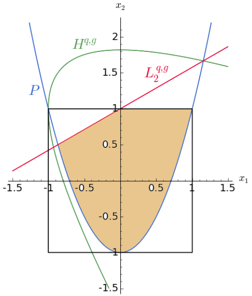
$$\mathcal{C}_3 \cap \mathcal{W}_3 \cap \mathcal{H}_3^{q,g} \longrightarrow \begin{cases} 2x_1^2 - 1 \le x_2 \le 1 \\ -1 + \frac{(x_1+x_2)^2}{1+x_1} \le x_3 \le 1 - \frac{(x_1-x_2)^2}{1-x_1} \\ 1 + 2x_1x_2x_3 - x_3^2 - x_1^2 - x_2^2 \ge 0 \\ x_2 \le \frac{x_1}{\sqrt{q}} + \frac{q-1}{2g} \\ x_3 \le \frac{x_1}{q} + \frac{q^2-1}{2g\sqrt{q}}. \end{cases}$$

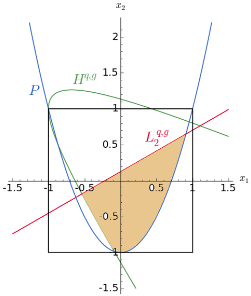
$$\downarrow$$

$$\text{projection over } \langle x_1, x_2 \rangle \quad \begin{cases} 2x_1^2 - 1 \le x_2 \le 1 \\ -1 + \frac{(x_1+x_2)^2}{1+x_1} \le \frac{x_1}{q} + \frac{q^2-1}{2g\sqrt{q}} \\ x_2 \le \frac{x_1}{\sqrt{q}} + \frac{q-1}{2g}. \end{cases}$$

Third order: $n = 3$

Table: The projection of $\mathcal{C}_3 \cap \mathcal{W}_3 \cap \mathcal{H}_3^{q,g}$ on the plane $< x_1, x_2 >$ respectively for $g < g_3$ and $g > g_3$.





$$x_2 \geq -x_1 - \sqrt{\frac{1}{q}x_1^2 + \left(\frac{1}{q} + 1 + \frac{q^2-1}{2g\sqrt{q}}\right)x_1 + 1 + \frac{q^2-1}{2g\sqrt{q}}}$$

Third order: $n = 3$

Proposition

Let X be a smooth curve of genus $g \geq \frac{\sqrt{q}(q-1)}{\sqrt{2}}$ over $\mathbb{F}_q$. We have:

$$B_2(X) \leq \sqrt{1/4\left(\sharp X(\mathbb{F}_q)\right)^2 + \alpha(q,g)\sharp X(\mathbb{F}_q) + \beta(q,g)} - \frac{(1+\sqrt{q})}{2}\sharp X(\mathbb{F}_q) + \frac{q^2+1+\sqrt{q}(q+1)}{2},$$

où

$$\begin{cases} \alpha(q,g) = -\frac{1}{4}((2q\sqrt{q}+2\sqrt{q})g + q^3 + q + 2) \\ \beta(q,g) = \frac{1}{4}(4q^2g^2 + 2\sqrt{q}(q^3+q^2+q+1)g + q^4 + q^3 + q + 1). \end{cases}$$

$$M'''(q,g) := \sqrt{1/4\left(N_q(g)\right)^2 + \alpha(q,g)N_q(g)) + \beta(q,g)} - \frac{(1+\sqrt{q})}{2}N_q(g)) + \frac{q^2+1+\sqrt{q}(q+1)}{2}$$

$$\Downarrow$$

$$B_2(\mathcal{X}_q(g)) \leq M'''(q,g).$$

Third order: $n = 3$

q \ g	2	3	4	5	6
2	0	0	1	1	1
3		2	1	2	3
2^2				4	1

Table: Third-order upper bounds for $B_2(\mathcal{X}_q(g))$ given by $M'''(q,g)$.

Upper bounds for $B_2(\mathcal{X}_q(g))$

q \ g	2	3	4	5	6
2	7	11	14	18	21
3	12	17	21	26	31
2^2	18	24	30	36	42

$\downarrow$

q \ g	2	3	4	5	6
2	0	0	1	1	1
3	3	2	1	2	3
2^2	5	0	4	4	1

Table: Upper bounds for $B_2(\mathcal{X}_q(g))$.

Some exact values for $N_q(g, \pi)$

Proposition

Let q be a power of a prime number p. We have:

1. $N_q(0, \pi) = q + 1 + \pi$ *if and only if* $0 \leq \pi \leq \frac{q^2 - q}{2}$.
2. *If p does not divide $[2\sqrt{q}]$, or q is a square, or $q = p$, then* $N_q(1, \pi) = q + [2\sqrt{q}] + \pi$ *if and only if* $1 \leq \pi \leq 1 + \frac{q^2 + q - [2\sqrt{q}]([2\sqrt{q}] + 1)}{2}$. *Otherwise,* $N_q(1, \pi) = q + [2\sqrt{q}] + \pi - 1$ *if and only if* $1 \leq \pi \leq 1 + \frac{q^2 + q + [2\sqrt{q}](1 - [2\sqrt{q}])}{2}$.
3. *If* $g < \frac{\sqrt{q}(\sqrt{q} - 1)}{2}$ *and* $g \leq \pi \leq \frac{q^2 - q}{2} - g(q + \sqrt{q} - 1)$ *then* $N_q(g, \pi) = N_q(g) + \pi - g$.
4. $N_2(2, 3) = 6$.
5. $N_2(3, 4) = 7$.
6. $N_{2^2}(4, 5) = 14$.