Towards maximal singular curves over finite fields

Annamaria Iezzi
(Joint work with Yves Aubry)

Institut des Mathématiques de Marseille, Université d'Aix-Marseille, France

AGCT, 18 May 2015

Notation

- $\mathbb{F}_q$ the finite field with q elements.
- The word "curve" will always stand for an absolutely irreducible projective algebraic curve.

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

- $\mathbb{F}_q(X)$ the function field of X;
- $\sharp X(\mathbb{F}_q)$, the number of rational points on X over $\mathbb{F}_q$;
- $\tilde{X}$ the normalization of X and $\nu : \tilde{X} \to X$ the normalization map (regular finite and birational): $\mathbb{F}_q(X) = \mathbb{F}_q(\tilde{X})$;
- 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 in $\mathbb{F}_q(X)$ associated to 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 $\mathcal{O}_Q$. $\overline{\mathcal{O}_Q}/\mathcal{O}_Q$ 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, $\pi = \frac{(d-1)(d-2)}{2}$.

Smooth curves

If X is smooth ($\pi = g$), the integers $q, \sharp X(\mathbb{F}_q)$ and g satisfy the **Serre-Weil inequality**:

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

Let us denote by

$$N_q(g)$$

the maximal number of rational points over $\mathbb{F}_q$ that a smooth curve of genus g can have. We have:

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

Bounds for singular curves

In 1996, Aubry and Perret find relations between a curve and its normalization:

$$Z_X(T) = Z_{\tilde{X}}(T) \prod_{P \in \operatorname{Sing} X} \left(\frac{\prod_{Q \in \nu^{-1}(P)} (1 - T^{\deg Q})}{1 - T^{\deg P}} \right)$$

$$|\sharp \tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)| \leq \pi - g,$$

As a consequence we get the analogous of Serre-Weil bound for singular curves (**Aubry-Perret bound**):

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

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 maximal number of rational points over $\mathbb{F}_q$ that a curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π can have.

Obviously we have

$$N_q(g, g) = N_q(g),$$

$$N_q(g, \pi) \leq N_q(g) + \pi - g,$$

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

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

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

Fukasawa, Homma and Kim's curve

In 2011, Fukasawa, Homma and Kim consider and study the rational plane curve B over $\mathbb{F}_q$ defined by the image of

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

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

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

<u>Remark:</u> 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, $\Phi^{-1}(\Phi(P)) = \{P, P^q\}$.

δ-optimal and maximal curves

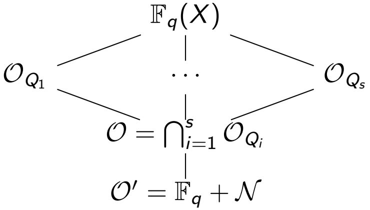
Proposition

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

1. *the normalization $\tilde{X}$ is an optimal (maximal) curve;*
2. $\text{Sing}(X) \subset X(\mathbb{F}_q)$;
3. *if P is a singular point on X, then $\nu^{-1}(P) = \{Q\}$, with Q 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. $Z_X(T) = Z_{\tilde{X}}(T)(1+T)^{\pi-g}$.

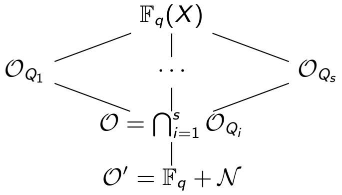
Construction of a prescribed singularity

Let start from a smooth curve X over $\mathbb{F}_q$ and let $S = \{Q_1, \ldots, Q_s\}$ be a non-empty finite set of closed points on X.



$\mathcal{O}$ is a semi-local ring with maximal ideals $\mathcal{N}_{Q_i} := \mathcal{M}_{Q_i} \cap \mathcal{O}$ for $i = 1, \ldots, s$.
Let $n_1, \ldots, n_s$ be s positive integers, let us set $\mathcal{N} := \mathcal{N}_{Q_1}^{n_1} \cdots \mathcal{N}_{Q_s}^{n_s}$ and let us consider:

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

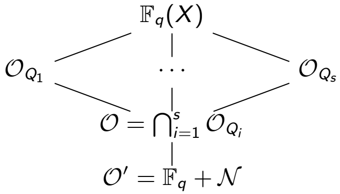


Proposition

$\mathcal{O}' = \mathbb{F}_q + \mathcal{N}$ 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 residual field $\mathcal{O}'/\mathcal{N} \cong \mathbb{F}_q$.*
3. *$\mathcal{O}/\mathcal{O}'$ is a $\mathbb{F}_q$-vector space such that*

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



Theorem

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

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

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

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

$$|$$

$$\mathcal{O} = \mathcal{O}_Q$$

$$|$$

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

Proposition

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

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

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

Theorem

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

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

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

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 normalization 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 of $d-1$.

Let us denote by

$\mathcal{X}_q(g)$: the set of optimal smooth curves X 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 case of rational curves: g=0

Proposition

We have

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

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

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

g=1

Proposition

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

Spectrum of maximal curves

Proposition

Assume q is square. If X is a maximal curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π, then:

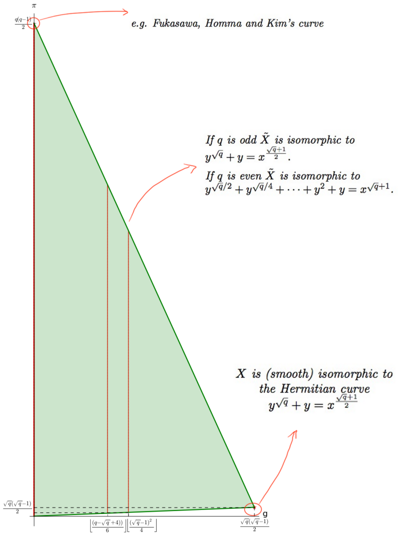
$$\pi \leq g + \frac{q^2 + (2g-1)q - 2g\sqrt{q}(2\sqrt{q}+1)}{2} = (-q - \sqrt{q} + 1)g + \frac{q(q-1)}{2},$$

$$g \leq \frac{\sqrt{q}(\sqrt{q}-1)}{2}$$

and

$$\pi \leq \frac{q(q-1)}{2}.$$

Spectrum of maximal curves



Merci !

Thank you very much for the attention!