On the maximal number of points on singular curves over finite fields

Annamaria Iezzi
(Joint work with Yves Aubry)

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

YACC, 11 Juin 2014

Notation

- $\mathbb{F}_q$ the finite field with q elements.
- With the word "curve" we will always refer to an absolutely irreducible projective algebraic curve.

Smooth curves over finite fields

Let X be a smooth curve over $\mathbb{F}_q$. We can associate to X two nonnegative integers:

- $\sharp X(\mathbb{F}_q)$: the number of rational points on X over $\mathbb{F}_q$;
- g: the genus of X.

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 curve of genus g can have. Clearly we have:

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

… and if X is singular?

If now we remove the hypothesis of smoothness for X, can we still say something about $\sharp X(\mathbb{F}_q)$?

Yes, but we have to introduce another invariant for X,

the arithmetic genus π.

To define π we have to recall some local properties of curves.

Points and local rings

Let X be a curve over $\mathbb{F}_q$ and let $\mathbb{F}_q(X)$ be the function field of X. Let Q be a point on X and let us define

$$\mathcal{O}_Q := \{f \in \mathbb{F}_q(X) \mid f \text{ is regular at } Q\}.$$

$\mathcal{O}_Q$ is a local ring with maximal ideal

$$\mathcal{M}_Q := \{f \in \mathcal{O}_Q \mid f \text{ vanishes at } Q\}$$

Moreover we have:

$$[\mathcal{O}_Q/\mathcal{M}_Q : \mathbb{F}_q] = \deg Q.$$

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

$$\Downarrow$$

X is smooth if and only if $\mathcal{O}_Q$ is integrally closed for every Q on X.

Normalization of a singular curve

Let $\tilde{X}$ be the **normalization** of X, i.e. the smooth curve together with a regular map

$$\nu : \tilde{X} \to X$$

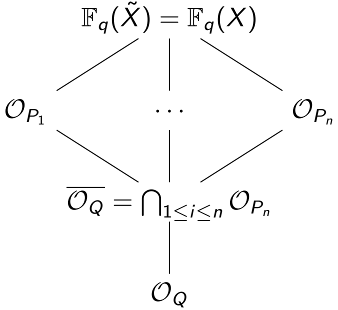
such that ν is finite and birational.

In particular X and $\tilde{X}$ have the same function field:

$$\mathbb{F}_q(X) = \mathbb{F}_q(\tilde{X}).$$

Diagram

Let Q be a point on X and let $P_1, \dots, P_n$ be the points on $\tilde{X}$ such that $\nu(P_i) = Q$ for all $i = 1, \dots, n$.



$\overline{\mathcal{O}_Q}$ is the integral closure of $\mathcal{O}_Q$.

The arithmetic genus

$\overline{\mathcal{O}_Q}/\mathcal{O}_Q$ is a finite dimensional $\mathbb{F}_q$-vectorial space. We set:

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

We can now define the **arithmetic genus** π of a curve X as the integer:

$$\pi := g + \sum_{Q \in \mathrm{Sing}\, X(\overline{\mathbb{F}_q})} \delta_Q,$$

where g is the genus of the normalization $\tilde{X}$ of X (g is called the **geometric genus** of X).

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

Bounds for singular curves

In 1996, Aubry and Perret give the following result on singular curves:

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

from which they obtain directly the equivalent of Serre-Weil bound for singular curves:

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

The quantity $N_q(g,\pi)$

We define 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

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

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

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

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

Properties of B:

1. B is a rational curve of degree $q+1 \Rightarrow g = 0, \pi = \frac{q^2-q}{2}$;
2. For $P \in \mathbb{P}^1$, $\Phi(P) \in \mathrm{Sing}(B)$ if and only if $P \in \mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mathbb{P}^1(\mathbb{F}_q) \Rightarrow B$ has $\frac{q^2-q}{2}$ ordinary double points.
3. $\sharp B(\mathbb{F}_q) = q + 1 + \frac{q^2-q}{2} \Rightarrow$ B attains the Aubry-Perret bound!!

$$\Downarrow$$

$$N(0, \frac{q^2-q}{2}) = N_q(0) + \frac{q^2-q}{2}$$

Question

Does there exist other different values of g and π for which

$$N_q(g, \pi) = N_q(g) + \pi - g\,?$$

To try to answer this question we need to find some way to construct singular curves with prescribed geometric genus g and arithmetic genus π and "many" rational points.

Singular curves with many points

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' (so that X' has geometric genus g) 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 $d-1$.

Sketch of the proof

Without loss of generality we can limit ourselves to the affine case; the general case will follow directly by covering X by affine opens.

Let us take on the curve X:

- a_2 closed points of degree $2: \; S_2 = \{Q_1^{(2)}, Q_2^{(2)}, \ldots, Q_{a_2}^{(2)}\}$;
- a_3 closed points of degree $3: \; S_3 = \{Q_1^{(3)}, Q_2^{(3)}, \ldots, Q_{a_3}^{(3)}\}$;

  $\vdots$
- a_n closed points of degree $n: \; S_n = \{Q_1^{(n)}, Q_2^{(n)}, \ldots, Q_{a_n}^{(n)}\}$;

$\Downarrow$

$S := S_2 \cup S_3 \cup \cdots \cup S_n$.

Sketch of the proof

Let $\mathcal{O}$ be the sheaf of local rings of X. Starting from $\mathcal{O}$ we are going now to define a new sheaf of local rings in the following way:

- for every $Q \in X - S$ we put $\mathcal{O}'_Q := \mathcal{O}_Q$.
- for every $Q \in S$ we set $\mathcal{O}'_Q := \mathbb{F}_q + \mathcal{M}_Q$;

The set of $\mathcal{O}'_Q$, for $Q \in X$, form a subsheaf $\mathcal{O}'$ of $\mathcal{O}$.

In particular for every $Q \in S$ we have:

- $\mathcal{O}'_Q$ is local with maximal ideal $\mathcal{M}_Q$ and

$$\left[\mathcal{O}'_Q/\mathcal{M}_Q : \mathbb{F}_q\right] = 1;$$

- $\mathcal{O}_Q$ is the integral closure of $\mathcal{O}'_Q$;
- $\mathcal{O}_Q/\mathcal{O}'_Q$ is an $\mathbb{F}_q$-vectorial space of dimension $\deg Q - 1$.

Sketch of the proof

Let us denote

$$A' := \bigcap_{Q \in X} \mathcal{O}'_Q.$$

A' is a $\mathbb{F}_q$-algebra of finite type corresponding to an affine irreducible curve X' defined over $\mathbb{F}_q$.

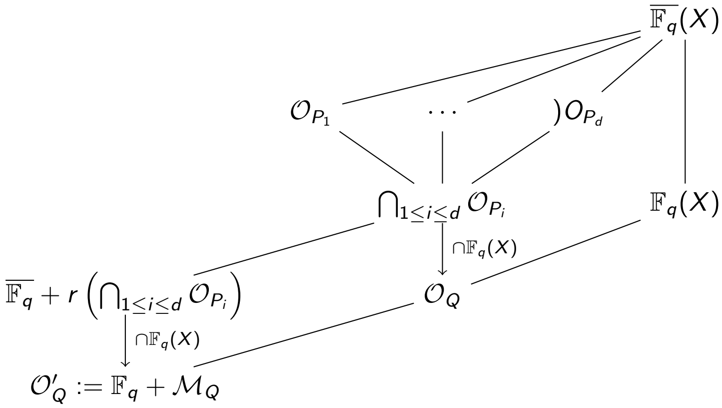
By construction we obtain that:

- $\tilde{X}'$=X so that X' has geometric genus g;
- $\sharp X'(\mathbb{F}_q) = \sharp X(\mathbb{F}_q) + |S| = \sharp X(\mathbb{F}_q) + a_2 + a_3 + \cdots + a_n$;
- X' has arithmetic genus $\pi = g + a_2 + 2a_3 + 3a_4 + \cdots + (n-1)a_n$.

Remarks

- Unfortunately this construction is not explicit;
- this construction corresponds to a glueing of points on the curve obtained from X by extension of the base field to its algebraic closure.

Diagram



$\overline{\mathbb{F}_q}(X)$
$\mathcal{O}_{P_1}$
$\cdots$
$)O_{P_d}$
$\bigcap_{1\leq i\leq d}\mathcal{O}_{P_i}$
$\mathbb{F}_q(X)$
$\cap\mathbb{F}_q(X)$
$\overline{\mathbb{F}_q}+r\left(\bigcap_{1\leq i\leq d}\mathcal{O}_{P_i}\right)$
$\mathcal{O}_Q$
$\cap\mathbb{F}_q(X)$
$\mathcal{O}'_Q:=\mathbb{F}_q+\mathcal{M}_Q$

The case of rational curves

Let start from $X = \mathbb{P}^1$, the projective line, over a finite field $\mathbb{F}_q$. As

$$B_2(\mathbb{P}^1) = \frac{q^2 - q}{2},$$

we have:

Proposition

For any $\pi \leq \frac{q^2-q}{2}$, there exists a (singular) rational curve X' over $\mathbb{F}_q$ of arithmetic genus π that attains the Aubry-Perret bound, i.e.

$$\sharp X(\mathbb{F}_q) = q + 1 + \pi.$$

In other terms we have

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

Maximal curves

Definition

A (not necessarily smooth) curve X defined over $\mathbb{F}_q$ is called maximal if

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

Proposition

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

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

In particular, for a maximal rational curve (and for q not necessarily square), this proposition implies:

$$\pi \leq \frac{q^2 - q}{2}$$

Proposition

We have

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

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

With this proposition we completely answer the question when $g = 0$.