Closed points on curves over finite fields

Yves Aubry

Institut de Mathématiques de Toulon (IMATH - UTLN)
and
Institut de Mathématiques de Marseille (I2M - AMU)
France

(joint work with **Fabien Herbaut** (Univ. Nice, France) and **Julien Monaldi** (Univ. Toulon, France))

AGC^2T'2023, CIRM (France), June 5th 2023

Rational points

Let X be an absolutely irreducible smooth projective algebraic curve (just called **curve** until now) defined over $\mathbb{F}_q$ of genus g.

We denote by $X(\mathbb{F}_{q^r})$ the **set** of rational points over $\mathbb{F}_{q^r}$ of X.

We denote by $N_r(X) = \sharp X(\mathbb{F}_{q^r})$ its **number** of rational points over $\mathbb{F}_{q^r}$.

Closed points

Let $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$.

A **closed point** of X is an **orbit** under the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on $X(\overline{\mathbb{F}}_q)$ (or equivalently a **place** of the corresponding function field).

If P is a closed point of X, we define its **degree** to be the cadinality of the orbit (or equivalently the dimension of the residue field $\mathcal{O}_P/\mathcal{M}_P$ over $\mathbb{F}_q$).

Let $B_d(X)$ be the **number of closed points** of degree d of X.
We have :

$$N_r(X) = \sum_{d|r} dB_d(X). \tag{1}$$

Closed points : example

Let $\mathcal{F}$ be the **Fermat cubic** curve over $\mathbb{F}_2$ of equation

$$X^3 + Y^3 + Z^3 = 0.$$

The $\mathbb{F}_2$-**rational points** of $\mathcal{F}$ are the three points $(1:1:0), (1:0:1)$ and $(0:1:1)$.

Let $\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha^2\}$ with $\alpha^2 + \alpha + 1 = 0$.

There are three $\mathbb{F}_2$-rational **closed points of degree 2**, namely $\{(1:\alpha:0), (1:\alpha^2:0)\}, \{(0:\alpha:1), (0:\alpha^2:1)\}$ and $\{(\alpha:0:1), (\alpha^2:0:1)\}$.

Finally, the number of $\mathbb{F}_4$-**rational points** of $\mathcal{F}$ is

$$N_2 = 9 = B_1 + 2B_2 = 3 + 2 \times 3.$$

Zeta function

Let X be a curve of genus g defined over $\mathbb{F}_q$ with **zeta function**

$$Z_X(T) = \exp\Big(\sum_{n=1}^{\infty} \sharp X(\mathbb{F}_{q^n}) \frac{T^n}{n}\Big).$$

It is well-known that it is a **rational fraction** of the form

$$Z_X(T) = \frac{\prod_{j=1}^{g}(1-\omega_j T)(1-\overline{\omega_j} T)}{(1-T)(1-qT)}.$$

From the two previous expressions, we obtain for any $n \geq 1$:

$$N_n(X) = \sharp X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{j=1}^{g}(\omega_j^n + \overline{\omega_j}^n). \qquad (2)$$

Bounds on the number of rational points

The **Riemann Hypothesis** says that $|\omega_j| = \sqrt{q}$.

It implies the famous **Weil bounds** :

$$q^n + 1 - 2gq^{n/2} \leq N_n(X) \leq q^n + 1 + 2gq^{n/2}. \qquad (3)$$

Bounds on the number of closed points

$$B_r(X)$$

Bounds on the number of closed points

Starting with the formula

$$N_r = \sum_{d|r} dB_d$$

and using the Möbius inversion formula, one obtain :

$$B_r = \frac{1}{r} \sum_{d|r} \mu\left(\frac{r}{d}\right) N_d.$$

Then we derive that for any $r \geq 1$ (see for instance Proposition 3.2.10 of [Tsfasman-Vlăduț -Nogin's Algebraic Geometric Codes : Basic Notions]) :

$$|B_r(X) - \frac{q^r}{r}| \leq \left(\frac{q}{q-1} + 2g\frac{\sqrt{q}}{\sqrt{q}-1}\right)\frac{q^{r/2}-1}{r} < (2+7g)\frac{q^{r/2}}{r}. \quad (4)$$

Lower bounds on the number of closed points

Elkies, Howe, Kresch, Poonen, Wetherell and Zieve proved (Duke Math. J., 2004) that for every $d > 0$ we have

$$B_r > (q^r - (6g+3)q^{r/2})/r. \tag{5}$$

Furthermore, the first author with Haloui and Lachaud proved (Acta Arith., 2013) a result on abelian varieties whose proof *mutatis mutandis* gives, for $r \geq 2$:

$$B_r > (q^{r/4}+1)^2\Big((q^{r/4}-1)^2 - 2g\Big)/r. \tag{6}$$

Upper bounds on the number of closed points of degree 2

We focus on closed points of degree 2.

Inequality (4) given by TVN for $r = 2$ gives :

$$B_2 \leq \frac{q^2 + 1 + 2gq}{2} + \frac{q - 1 + 2g\sqrt{q}}{2}.$$

But one obtain a better bound writing that $B_2 = \frac{N_2 - N_1}{2}$ and using the Weil upper bound for N_2 and the Weil lower bound for N_1 :

$$B_2 \leq \begin{cases} \frac{q^2+1+2gq}{2} & \text{if } \ g \geq \frac{q+1}{2\sqrt{q}} \\ \frac{q^2-q+2g(q+\sqrt{q})}{2} & \text{otherwise.} \end{cases} \tag{7}$$

New upper bound on B_2

Proposition (Y.A., F. Herbaut, J. Monaldi (2023))

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

$$B_2(X) \leq \begin{cases} \frac{q^2+1+2gq}{2} - \frac{(q+1)^2}{2g} & \text{if } g \geq 2q+2 \\ \frac{q^2+1+2gq}{2} - \frac{4(q+1)-g}{8} & \text{otherwise.} \end{cases}$$

Comparisons

The new bounds of our proposition are always **better** than the bounds obtained using the Weil bounds.

Furthermore, the new bounds of our proposition are **reached** for many values of g and q as quoted in the following table for some values :

Comparisons between the upper bounds for B_2

	Weil	AHM	Curve reaching AHM
$g = 1,\ q = 2$	4	3	$y^2 + xy = x^3 + x^2 + x$
$g = 2,\ q = 3$	11	9	$y^2 = 2x^6 + x^4 + 2x^3 + x^2 + 2$
$g = 2,\ q = 4$	16	14	$y^2 + (x^2 + x)y = x^5 + x^3 + x^2 + x$
$g = 2,\ q = 5$	23	20	$y^2 = 4x^6 + x^5 + x^4 + x^3 + x^2 + x + 4$
$g = 2,\ q = 7$	39	35	$y^2 = 3x^6 + 3x^3 + 3$
$g = 2,\ q = 11$	83	77	$y^2 = 7x^6 + 5x^5 + 9x^4 + 8x^3 + 5x^2 + 6x$
$g = 3,\ q = 2$	7	8	$x^4 + x^2y^2 + x^2yz + x^2z^2 + xy^2z + xyz^2$

New upper bound on B_2 : sketch of the proof I

Let us recall the Euclidean viewpoint used by Weil in "Variétés abéliennes et courbes algébriques" (1946) and by Grothendieck in "Sur une note de Mattuck-Tate" (J. für die reine und angewandte Math., 1958).

Consider the smooth algebraic **surface** $X \times X$ and the Néron-Severi group $\mathrm{NS}(\mathrm{X} \times \mathrm{X})$ (the group $\mathrm{Div}(\mathrm{X} \times \mathrm{X})$ modulo algebraic equivalence) which is a finitely generated abelian group.

The intersection pairing on $\mathrm{Div}(\mathrm{X} \times \mathrm{X})$ induces a symmetric bilinear pairing on $\mathrm{NS}(\mathrm{X} \times \mathrm{X})$.

Let $\mathrm{Num}(\mathrm{X} \times \mathrm{X})$ be the quotient of $\mathrm{NS}(\mathrm{X} \times \mathrm{X})$ by the kernel of this pairing.

Then consider the $\mathbb{R}$-vector space $\mathrm{Num}(\mathrm{X} \times \mathrm{X}) \otimes_{\mathbb{Z}} \mathbb{R}$.

New upper bound on B_2 : sketch of the proof II

The **Hodge index theorem** says that the bilinear form induced by the intersection pairing on $NS(X \times X) \otimes_{\mathbb{Z}} \mathbb{R}$ is non-degenerate, definite negative on the orthogonal supplement of any ample divisor on the surface $X \times X$.

New upper bound on B_2 : sketch of the proof III

Following Hallouin and Perret (Transactions AMS, 2019), we set for $i \geq 1$:

$$x_i := \frac{(q^i + 1) - N_i}{\sqrt{q^i}}.$$

Considering the definite positivity of the Gram matrix of the graphs of the iterated Frobenius endomorphisms, they obtain several bounds on the x_i's, including the following one

$$2g^2 + gx_2 - x_1^2 \geq 0.$$

It gives, for non-zero genus curves :

$$\sharp X(\mathbb{F}_{q^2}) - (q^2 + 1) \leq 2gq - \frac{1}{g}\big(\sharp X(\mathbb{F}_q) - (q + 1)\big)^2. \qquad (8)$$

New upper bound on B_2 : sketch of the proof IV

The previous inequality gives

$$B_2 \leq \frac{q^2+1+2gq}{2} - \frac{N_1}{2} - \frac{(N_1-(q+1))^2}{2g}$$

and a study of maxima of functions gives the result.

□

The TVN quantity

$$\rho(q, g)$$

The TVN quantity : definition

Tsfasman, Vlăduț and Nogin introduced in Problem 3.2.13 of their book *Algebraic Geometric Codes : Basic Notions* the quantity

$$\rho(q, g)$$

defined as the smallest integer ≥ 1 such that $r \geq \rho(q, g)$ implies that $B_r(X) \geq 1$ for any curve X defined over $\mathbb{F}_q$ of genus g.

The TVN quantity : genus 0 case

Recall that Tsfasman, Vlăduț and Nogin proved that for any $r \geq 1$, we have :

$$|B_r(X) - \frac{q^r}{r}| \leq \left(\frac{q}{q-1} + 2g\frac{\sqrt{q}}{\sqrt{q}-1}\right)\frac{q^{r/2}-1}{r} < (2+7g)\frac{q^{r/2}}{r}.$$

As a first consequence, one obtain that if $g = 0$ then $B_r(X) \geq 0$ for any $r \geq 1$, and thus we obtain that for any q :

$$\rho(q, 0) = 1.$$

The case of genus zero curves is thus solved and we will now consider curves of **positive** genus.

The TVN quantity : general bound

As a second consequence, one can obtain that for any r such that $2g+1 \leq q^{\frac{r-1}{2}}(\sqrt{q}-1)$ there exists at least one point of degree r, and, in particular, if $r \geq 4g+3$ then $B_r(X) \geq 1$. It implies that

$$\rho(q,g) \leq \left\lceil 2\log_q\left(\frac{2g+1}{\sqrt{q}-1}\right)+1 \right\rceil \tag{9}$$

where $\lceil x \rceil$ stands for the least integer greater than or equal to a real number x, and in particular

$$\rho(q,g) \leq 4g+3. \tag{10}$$

The TVN quantity : improvement

Moreover, the bound proved by Elkies et al. implies

$$\rho(q, g) \leq 2g + 1.$$

The TVN quantity : our general result

Theorem (Y.A., F. Herbaut, J. Monaldi (2023))

1) If $g \geq 2$ and q is any power of a prime, or if $g = 1$ and $q \leq 10$, then : If q is a power of a prime and g a positive integer then :

$$\rho(q,g) \leq \left\lfloor 2\log_q\left(\frac{A+\sqrt{A(A-4)}}{2}\right)+1 \right\rfloor \tag{11}$$

where $A := \frac{q}{q-1} + 2g\frac{\sqrt{q}}{\sqrt{q}-1}$ and $\lfloor x \rfloor$ stands for the integer part of a real number x.
Moreover, $\rho(q,1) = 1$ for any $q \geq 11$.
2) If $g \geq 1$ and $r \geq 2$ then for any q we have :

$$\rho(q,g) \leq \left\lceil 4\log_q(1+\sqrt{2g}) \right\rceil . \tag{12}$$

Genus 1

Proposition (Y.A., F. Herbaut, J. Monaldi (2023))

$$\rho(2,1) = 5 \qquad \rho(4,1) = 3$$

$$\rho(3,1) = 3 \quad \rho(q,1) = 1 \text{ for any } q \geq 5$$

Genus 1 : proofs

We use three principal ingredients :

- The general upper bound given in our theorem ;

- the **Deuring-Waterhouse theorem** which gives the possible zeta functions of elliptic curves ;

- the notion of **Diophantine Stability** :
a curve X defined over $\mathbb{F}_q$ such that $X(\mathbb{F}_{q^n}) = X(\mathbb{F}_q)$ is said to be diophantine-stable for the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ and is called a DS-curve.

Lario gives in his webpage the complete list of DS-curves over finite fields of genus 1, 2 and 3.

Genus 1 over $\mathbb{F}_2$

What is the value of $\rho(2,1)$?

- By the previous theorem, Bound (11) or (12), we deduce that $\rho(2,1) \leq 6$.

- Moreover we have by Weil : $\sharp X(\mathbb{F}_{q^5}) \geq q^5 + 1 - 2gq^{5/2}$ and $\sharp X(\mathbb{F}_q) \leq q + 1 + 2gq^{1/2}$ and thus

$$B_5(X) = \frac{\sharp X(\mathbb{F}_{q^5}) - \sharp X(\mathbb{F}_q)}{5} \geq \frac{q^5 - q - 2g\sqrt{q}(q^2+1)}{5}.$$

So if $g < \frac{\sqrt{q}(q^2-1)}{2}$ then $B_5(X) > 0$, and thus $\rho(2,1) \leq 5$.

- Furthermore, the Fermat cubic curve is a DS-curve for the extension $\mathbb{F}_{2^4}/\mathbb{F}_{2^2}$ (because $N_4 = N_2$) and thus is such that $B_4 = 0$ i.e. there exists an elliptic curve defined over $\mathbb{F}_2$ with no closed point of degree 4, so we can conclude that $\rho(2,1) = 5$.

□

Genus 2

Proposition (Y.A., F. Herbaut, J. Monaldi (2023))

$$\rho(2,2) = 4 \quad \rho(4,2) = 2 \quad \rho(q,2) = 2 \text{ for } 7 \leq q \leq 11$$

$$\rho(3,2) = 4 \quad \rho(5,2) = 3 \quad \rho(q,2) = 1 \text{ for any } q \geq 13$$

Genus 2 : proofs

• Bound (11) of our theorem implies that for $q \geq 7$ we have $\rho(q, 2) \leq 2$.
Moreover Maisner and Nart (Experiment. Math., 2002) proved that if a genus 2 curve defined over $\mathbb{F}_q$ is **pointless**, then $q \leq 11$.
Hence we conclude that $\rho(q, 2) = 1$ for any $q \geq 13$

• The Lario list of **DS-curves**.
But the case where $B_6 = 0$ does not corresponds to DS-curves.

• Then we use the **explicit determination** of the representatives of the quotient set of classes of curves of genus 2 up to $\mathbb{F}_q$-isomorphism and quadratic twist given by Maisner and Nart.
Then we prove the non-existence of a genus 2 curve over $\mathbb{F}_2$ with $B_6 = 0$ i.e. with $N_6 = N_2 - N_1 + N_3$.

Genus 3

Proposition (Y.A., F. Herbaut, J. Monaldi (2023))

$\rho(2,3) = 7$ $\quad$ $\rho(8,3) = 2$ $\quad$ $\rho(31,3) = 1$

$\rho(3,3) = 5$ $\quad$ $\rho(9,3) = 3$ $\quad$ $\rho(32,3) = 2$

$\rho(4,3) = 3$ $\quad$ $\rho(q,3) = 2$ *for* $11 \leq q \leq 25$ $\quad$ $\rho(q,3) = 1$ *for any* $q \geq 37$

$\rho(5,3) = 3$ $\quad$ $\rho(27,3) = 1$

$\rho(7,3) = 2$ $\quad$ $\rho(29,3) = 2$

Genus 3 : proofs

Howe, Lauter and Top proved (AGCT' 2003, SMF 2005) that there exists a **pointless genus-3 curve** over $\mathbb{F}_q$ if and only if either $q \leq 25$ or $q = 29$ or $q = 32$, which means that

$$\rho(q, 3) \geq 2$$

for such values of q.

We will also make use of the *L-functions and modular forms database* (**LMFDB**).

The end

Appendix I

Let us come back to the **Hallouin-Perret bound** for non-zero genus curves :

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

which states that for a non-rational curve X, any lower bound for the deviation of $\sharp X(\mathbb{F}_q)$ from $(q+1)$ yields to a better upper bound than the Weil one for $\sharp X(\mathbb{F}_{q^2})$.

Appendix II

Let us call **HP-max** any non-zero genus curve X defined over $\mathbb{F}_q$ reaching this bound, i.e. such that :

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

A curve X defined over $\mathbb{F}_q$ is HP-max iff it has an **optimal** $\sharp X(\mathbb{F}_{q^2})$ for a given $\sharp X(\mathbb{F}_q)$.

It is straighforward that any **elliptic curve** is HP-max.

Appendix III

Proposition (Y.A., F. Herbaut, J. Monaldi (2023))

A curve X defined over $\mathbb{F}_q$ of genus $g > 1$ is HP-max iff its zeta function is of the form

$$Z_X(T) = \frac{(1 - 2\alpha T + qT^2)^g}{(1 - T)(1 - qT)}$$

where $\alpha = \frac{q+1-\sharp X(\mathbb{F}_q)}{2g}$.

Appendix IV

Proposition (Y.A., F. Herbaut, J. Monaldi (2023))

A curve X defined over $\mathbb{F}_q$ of genus $g > 1$ is Ihara-max or Ihara-min iff X is HP-max and DS$(\mathbb{F}_{q^2}/\mathbb{F}_q)$ iff its zeta function is of the form

$$Z_X(T) = \frac{(1 - 2\alpha T + qT^2)^g}{(1 - T)(1 - qT)}$$

where $\alpha = \frac{1}{4} \mp \frac{\sqrt{g^2+4g(q^2+q(2g-1)}}{4g}$.