CLOSED POINTS ON CURVES OVER FINITE FIELDS

Yves Aubry, Fabien Herbaut, Julien Monaldi

[1]

CLOSED POINTS ON CURVES OVER FINITE FIELDS

YVES AUBRY, FABIEN HERBAUT, AND JULIEN MONALDI

Abstract. We are interested in the quantity $\rho(q,g)$ defined as the smallest positive integer such that $r \geq \rho(q,g)$ implies that any absolutely irreducible smooth projective algebraic curve defined over $\mathbb{F}_q$ of genus g has a closed point of degree r. We provide general upper bounds for this number and its exact value for $g = 1, 2$ and 3. We also improve the known upper bounds on the number of closed points of degree 2 on a curve.

1. Introduction

In the whole paper we consider a power q of a prime, $\mathbb{F}_q$ the finite field with q elements and $\overline{\mathbb{F}}_q$ its algebraic closure. Let X be an absolutely irreducible smooth projective algebraic curve (just called curve from now on) defined over $\mathbb{F}_q$ of genus g. This article deals with the notion of closed point, that is an orbit under the action of $\mathrm{Gal}\left(\overline{\mathbb{F}}_q/\mathbb{F}_q\right)$ 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 as the cardinality of the orbit, or equivalently as the dimension over $\mathbb{F}_q$ of the residue field, that is the quotient of the local ring $\mathcal{O}_{P,X}$ by its maximal ideal $\mathcal{M}_{P,X}$. Clearly the numbers $B_r(X)$ (B_r for short) of closed points of degree r are related to the numbers $N_r(X) = \sharp X(\mathbb{F}_{q^r})$ (N_r for short) of rational points over $\mathbb{F}_{q^r}$ by the following formula:

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

The aim of the article is to study the quantity $\rho(q,g)$ introduced in Problem 3.2.13 of [13] by Tsfasman, Vlăduţ and Nogin and defined as the smallest positive integer such that $r \geq \rho(q,g)$ implies that $B_r(X) \geq 1$ for any genus g curve X defined over $\mathbb{F}_q$.

They ask to find its exact value. In this paper we contribute to this issue by determining the exact value of $\rho(q,g)$ for $g = 1, 2, 3$. We also establish a new upper bound for the number $B_2(X)$ of closed points of degree 2. We summarize our contributions in the following theorem.

[1]This work is partially supported by the French Agence Nationale de la Recherche through the Barracuda project under Contract ANR-21-CE39-0009-BARRACUDA.

Date: October 16, 2023.

2010 *Mathematics Subject Classification.* Primary 14H25; Secondary 11G20.

Key words and phrases. Algebraic curves, finite fields, closed points, diophantine stability.

Theorem. *(Proposition 3.1,Theorem 4.1, Theorem 5.2, Theorem 6.1) Let g be a positive integer and X be a genus g curve defined over $\mathbb{F}_q$.*

(i) An upper bound on $B_2(X)$ is given by

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

(ii) The values of $\rho(q,g)$ for $g = 1, 2$ and 3 are as follows

g \ q	2	3	4	5	7	8	9	11	13	16	17	19	23	25	27	29	31	32	≥ 37
1	5	3	3	1	$\cdots$													$\cdots$	1
2	4	4	2	3	2	2	2	2	1	$\cdots$								$\cdots$	1
3	7	5	3	3	2	2	3	2	2	2	2	2	2	2	1	2	1	2	1

TABLE 1. Values of $\rho(q,g)$ for $g = 1, 2$ and 3.

Let us stress the connection between the topic and the notion of Diophantine stability introduced (over number fields) by Mazur and Rubin in [11]: a variety V defined over a field K is said to be diophantine-stable for the field extension L/K if $V(K) = V(L)$. When r is a prime number and X is a curve defined over $\mathbb{F}_q$ which is diophantine-stable for the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ then Formula (1) implies $\rho(q,g) > r$. Curves with Diophantine stability (also called DS-curves) over finite fields have been studied by Lario who provides in [8] the complete list of isomorphism classes of DS-curves up to genus 3. Vrioni has studied in [14] curves and surfaces with Diophantine stability over finite fields.

2. Known bounds on B_r and $\rho(q,g)$

We collect in this section the known general bounds on B_r and $\rho(q,g)$ as well as existence results for points of given degree. In this direction we also propose one contribution, namely Proposition 2.3, which sometimes slighty improve the known bounds and which prove useful to save some cases in the study of the last three sections.

The zeta function Z_X of a curve X of genus g defined over $\mathbb{F}_q$ is defined by

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

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

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

and the Riemann Hypothesis, proved by Hasse for elliptic curves and by Weil for curves of any genus, says that the ω_j's are complex numbers of absolute value $\sqrt{q}$. We obtain from the two previous expressions of the zeta function

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

for any $n \geq 1$, and the Riemann Hypothesis implies that:

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

When r is a prime, one can combine the equality $B_r = (N_r - N_1)/r$ with the Weil bounds (3) to obtain the following Lemma.

Lemma 2.1. *Let X be an absolutely irreducible smooth projective algebraic curve of genus g defined over $\mathbb{F}_q$ and let r be a prime number. If $g < \frac{\sqrt{q^r}-\sqrt{q}}{2}$ then $B_r(X) > 0$.*

More broadly, for any integer $r \geq 1$, the Möbius inversion formula, and the Weil bounds lead to the following inequality (see for instance Proposition 3.2.10 in [13])

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

The asymptotic expansion $B_r = q^r/r + O(\sqrt{q^r}/r)$ follows, for a fixed genus g and for large values of q. As a second consequence of (4), we can deduce that if $g = 0$ then $B_r(X) > 0$ for any $r \geq 1$. Therefore for any q we have

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

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

As a third consequence of (4), one can deduce the Corollary 3.2.11 in [13] which reads (where $\lceil x \rceil$ stands for the smallest integer greater than or equal to a real number x)

$$\rho(q, g) \leq \left\lceil 2\log_q\Big(\frac{2g+1}{\sqrt{q}-1}\Big) + 1 \right\rceil \tag{5}$$

and from which one can deduce the uniform bound $\rho(q, g) \leq 4g + 3$. Combining the Möbius inversion formula and the Weil bounds is also the point

of departure of inequalities obtained by Elkies et al. in [3]. For instance, Lemma 2.1 in their paper states for every $r > 0$ the lower bound

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

and provides the following uniform inequality which applies for $g \geq 2$

$$\rho(q,g) \leq 2g+1. \tag{7}$$

When $r \geq 2$ the first author with Haloui and Lachaud manage to improve Bound (6). In Proposition 3.7. of [1] they study similar bounds in the context of abelian varieties, but the proof adapts *mutatis mutandis* if we consider a curve rather than an abelian variety. More precisely, they start from the same Möbius inversion formula $B_r = \frac{1}{r}\sum_{d|r} \mu(r/d)N_d$ where μ is the Möbius function and thus replace the numbers N_d by their expression in function of the roots ω_j's. They prove $rB_r > G(q^{r/4})$ where $G(x) = (x+1)^2\left((x-1)^2 - 2g\right)$ and so the second point of Proposition 3.7 in [1] remains true when the inequality becomes strict, that is

$$B_r > \frac{(q^{r/4}+1)^2\Big((q^{r/4}-1)^2 - 2g\Big)}{r}. \tag{8}$$

A consequence is that if $g \geq 1$, $r \geq 2$ and $(q^{r/4}-1)^2 \geq 2g$ then $B_r > 0$. We have thus checked that point (i) of Proposition 3.8 in [1] is still valid even if $g \geq 1$ and we can state:

Proposition 2.2. *(Aubry, Haloui and Lachaud, Proposition 3.8 in* [1]*)*
If $g \geq 1$ then

$$\rho(q,g) \leq \mathrm{Max}\left(2, \left\lceil 4\log_q(1+\sqrt{2g})\right\rceil\right). \tag{9}$$

One can also notice that Bound (4) on B_r involves a second degree polynomial in $q^{r/2}$ whose study leads to a quite efficient bound on $\rho(q,g)$.

Proposition 2.3. *If $g \geq 2$ or if $g = 1$ and $q \leq 9$, then:*

$$\rho(q,g) \leq \left\lfloor 2\log_q\Big(\frac{A+\sqrt{A(A-4)}}{2}\Big) + 1 \right\rfloor \tag{10}$$

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.

In particular, with the same conditions on g and q, if $g < \frac{\sqrt{q}}{2}\Big(1 - \frac{\sqrt{q}-1}{q-1}\Big)$ then $\rho(q,g) = 1$.

Proof. When setting $X = q^{r/2}$, the lower bound of Inequality (4) yields $rB_r \geq X^2 - AX + A$ where A is as in the statement. The discriminant of

the rigth hand side is $A(A-4)$ which is positive if $g \geq 2$, or if $g = 1$ and $q \geq 9$. In these cases we see that if $r > 2\log_q\left(\frac{A+\sqrt{A(A-4)}}{2}\right)$ then $B_r \geq 1$ and the bound follows.

An easy computation shows that $2\log_q\left(\frac{A+\sqrt{A(A-4)}}{2}\right) < 1$ if and only if $A < \frac{q}{\sqrt{q}-1}$, which is equivalent to $g < \frac{\sqrt{q}}{2}\left(1 - \frac{\sqrt{q}-1}{q-1}\right)$. Hence the previous condition on g implies by Inequality (10) that $\rho(q,g) = 1$.

□

Now one can deduce bounds on $\rho(q,g)$ for small values of g and large values of q as stated in the following corollary. These bounds will prove useful to reduce the work of Sections 4, 5 and 6 to a finite number of cases.

Corollary 2.4. *We have $\rho(q,1) = 1$ for any $q \geq 8$, $\rho(q,2) \leq 2$ for any $q \geq 7$ and $\rho(q,3) \leq 2$ for any $q \geq 37$.*

Proof. If $q \in \{8,9\}$ then Proposition 2.3 asserts that $\rho(q,1) = 1$. Moreover, if $q \geq 11$ then $A(A-4) < 0$ and thus $B_r \geq 1$ for any r, which implies that $\rho(q,1) = 1$. Finally, the proof of the cases of genus 2 and 3 is straightforward by Proposition 2.3. □

To conclude this section one should also mention that the Stöhr-Voloch theory leads to specific upper and lower bounds on B_r for irreducible plane curves. See for instance Theorem 9.62 and Theorem 9.63 in [5].

3. Upper bound for B_2

In this section we focus on the number of closed points of degree 2 for which we improve the known upper bounds.

We begin by summarizing the upper bounds obtained in the most natural ways. The first idea is to specialize Inequality (4) for $r = 2$ to obtain

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

For comparisons it is interesting to adopt the asymptotic viewpoint for a fixed genus g and for large values of q. This way the asymptotic expansion of the upper bound reads

$$B_2 \leq \frac{q^2}{2} + (g+\frac{1}{2})q + O(\sqrt{q}). \tag{11}$$

Another natural idea is to start from Formula (1), namely $N_2 = B_1 + 2B_2$. Then the Weil upper bound for N_2 yields to the following bound which involves N_1:

$$B_2 = \frac{N_2 - N_1}{2} \leq \frac{q^2+1+2gq}{2} - \frac{N_1}{2}. \tag{12}$$

Again from the Weil lower bound for N_1, one deduces the following bound which only depends on q:

$$B_2 \leq \begin{cases} \frac{q^2+1+2gq}{2} & \text{if } \ g \geq \frac{q+1}{2\sqrt{q}} \\ \frac{q^2-q+2g(q+\sqrt{q})}{2} & \text{otherwise.} \end{cases} \tag{13}$$

If we adopt the same asymptotic point of view for large values of q we get

$$B_2 \leq \frac{q^2}{2} + (g - \frac{1}{2})q + O(\sqrt{q}). \tag{14}$$

Let us now present our new upper bound.

Proposition 3.1. *Let X be a curve of genus $g > 0$ defined over $\mathbb{F}_q$.*

We have:

$$B_2(X) \leq \begin{cases} \frac{q^2+1+2gq}{2} - \frac{(q+1)^2}{2g} & \textit{if } \ g \geq 2q+2 \\ \frac{q^2+1+2gq}{2} - \frac{4(q+1)-g}{8} & \textit{otherwise.} \end{cases} \tag{15}$$

The following recent result is the point of departure to prove Proposition 3.1. It has been interpreted by Hallouin and Perret as a consequence of an inequality of Euclidean geometry in the numerical space $Num(X \times X)_{\mathbb{R}}$.

Theorem. *(Hallouin and Perret, Proposition 12 in* [4]*) Let X be a curve of genus g defined over $\mathbb{F}_q$. Then*

$$\sharp X(\mathbb{F}_{q^2}) - (q^2+1) \leq 2gq - \frac{1}{g}\big(\sharp X(\mathbb{F}_q) - (q+1)\big)^2. \tag{16}$$

Proof. The previous theorem gives immediately (see also Proposition 3.1. in [2] where it has already been noticed):

$$B_2 \leq \frac{q^2+1+2gq}{2} - \frac{N_1}{2} - \frac{(N_1-(q+1))^2}{2g} \tag{17}$$

which clearly improves Bound (12). Now we consider the function $x \mapsto -\frac{1}{2g}(x-(q+1))^2 - \frac{x}{2}$. If $g \geq 2q+2$ this function reaches its maximum for $x = 0$ which implies $B_2 \leq \frac{q^2+1+2gq}{2} - \frac{(q+1)^2}{2g}$. If $g \leq 2q+2$ it reaches its maximum for $x = \frac{2q+2-g}{2}$ and thus we deduce $B_2 \leq \frac{q^2+1+2gq}{2} - \frac{4(q+1)-g}{8}$. □

Straightforward computations in the three intervals $[1, \frac{q+1}{2\sqrt{q}}]$, $[\frac{q+1}{2\sqrt{q}}, 2q+2]$, and $[2q+2, \infty)$ enable us to check that the new bounds of Proposition 3.1 are always better than Bound (13) deduced from the Weil bounds.

Let us come back to the asymptotic viewpoint for a fixed genus g and for large values of q to compare Bound (13) with our new bound (15) which reads

$$B_2 \leq \frac{q^2}{2} + (g - \frac{1}{2})q + O(1). \tag{18}$$

In the asymptotic expansion of the upper bound we have managed to replace a $O(\sqrt{q})$ by a $O(1)$.

We now provide examples to show that the integer part of the new bound (15) of Proposition 3.1 is reached for different values of g and q. The third and fourth columns of the following table enable us to compare the bound (13) deduced from the Weil bounds to our new bound (15) for some values q and g. The fifth column provides equations of curves which attain our new bound. To describe the curves we sometimes need to introduce a generator a of the multiplicative group $\mathbb{F}_q^*$. We also give the numbers of rational points N_1 and N_2 over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ of the given curve.

g	q	Bound (13)	Bound (15)	Curves reaching bound (15) of Proposition (3.1)	N_1	N_2
1	2	4	3	$y^2+xy=x^3+x^2+1$	2	8
1	3	7	6	$y^2=x^3+x^2-1$	3	15
1	4	12	10	$y^2+xy=x^3+a$	4	24
2	3	11	9	$y^2=2x^6+x^4+2x^3+x^2+2$	2	20
2	4	16	14	$y^2+(x^2+x)y=x^5+x^3+x^2+x$	3	31
2	5	23	20	$y^2=4x^6+x^5+x^4+x^3+x^2+x+4$	4	44
2	7	39	35	$y^2=3x^6+3x^3+3$	6	76
2	8	48	44	$y^2+(x^2+x)y=a^2x^5+a^2x^3+ax^2+ax$	7	95
2	9	59	54	$y^2=2ax^6+ax^5+2ax^4+ax^2+ax+a$	8	116
2	11	83	77	$y^2=7x^6+5x^5+9x^4+8x^3+5x^2+6x+7$	10	164
3	2	8	7	$x^4+x^2y^2+x^2yz+x^2z^2+xy^2z+xyz^2+y^4+y^2z^2+z^4=0$	0	14

TABLE 2. Ex. of curves which attain the bound of Proposition 3.1.
In column 5 we denote by a a generator of $\mathbb{F}_q^*$

4. Elliptic curves

In this section we consider an elliptic curve X defined over $\mathbb{F}_q$.

Theorem 4.1. *The values of $\rho(q,1)$ are as follows.*

(i) $\rho(2,1)=5$ *(ii)* $\rho(3,1)=3$

(iii) $\rho(4,1)=3$ *(iv)* $\rho(q,1)=1$ *for any* $q\geq 5$

Proof. (i) First we consider the case where $q=2$. Proposition 2.2 leads to $\rho(2,1)\leq 6$. Lemma 2.1 also applies and ensures the existence of a degree 5 point, so $\rho(2,1)\leq 5$. Note that a curve X defined over $\mathbb{F}_2$ satisfies $B_4(X)=0$

if and only if it is a DS-curve for the extension $\mathbb{F}_{2^4}/\mathbb{F}_{2^2}$. As Lario indicates in [8] the elliptic curve of equation $y^2+y=x^3$ is an example of such a curve and we can conclude that $\rho(2,1)=5$.

(ii) For $q=3$ we use Proposition 2.3 to get $\rho(3,1)\leq 3$. Lario gives in [8] a DS-curve of genus 1 for the extension $\mathbb{F}_9/\mathbb{F}_3$, namely the curve of equation $y^2=x^3+2x+1$. So there exists an elliptic curve defined over $\mathbb{F}_3$ with no closed point of degree 2, and thus we have that $\rho(3,1)\geq 3$ which gives the result.

(iii) For $q=4$ Proposition 2.3 gives $\rho(4,1)\leq 3$ and as the elliptic curve of equation $y^2+y=x^3$ defined in [8] has no closed point of degree 2 we can conclude that $\rho(4,1)=3$.

(iv) We use Proposition 2.3 to get $\rho(5,1)\leq 2$ and $\rho(7,1)\leq 2$. But any elliptic curve over a finite field has a rational point, so $\rho(5,1)=1$ and $\rho(7,1)=1$. At last, Corollary 2.4 shows that for any $q\geq 8$ we have $\rho(q,1)=1$, which concludes the proof. □

5. Genus 2 curves

In this section we consider a curve X of genus 2 defined over $\mathbb{F}_q$. To make the proof of Theorem 5.2 more readable we first establish the following lemma.

Lemma 5.1. *Any absolutely irreducible smooth projective algebraic curve X of genus 2 defined over $\mathbb{F}_2$ (respectively over $\mathbb{F}_4$) admits at least one closed point of degree 4 (respectively of degree 2 and 3).*

Proof. We can relate the issue to the existence of a DS-curve and thus conclude with [8]. □

As an important ingredient of the following theorem we will also make use of the classification of genus 2 curves over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism and quadratic twist provided by Maisner and Nart in [10].

Theorem 5.2. *The values of $\rho(q,2)$ are as follows.*

(i) $\rho(2,2)=4$ *(ii)* $\rho(4,2)=2$ *(v)* $\rho(q,2)=2$ *for* $7\leq q\leq 11$

(iii) $\rho(3,2)=4$ *(iv)* $\rho(5,2)=3$ *(vi)* $\rho(q,2)=1$ *for any* $q\geq 13$

Proof. First, Corollary 2.4 implies that for $q\geq 7$ we have $\rho(q,2)\leq 2$. On the other hand Theorem 3.2. in [10] ensures that there is no genus 2 pointless curve defined over $\mathbb{F}_q$ if $q>11$. Hence we conclude that $\rho(q,2)=1$ for any $q\geq 13$ and point (vi) follows.

The same reference provides an example of a pointless genus 2 curve defined over $\mathbb{F}_q$ for any $q \leq 11$. It implies that $\rho(q,2) \geq 2$ for $q \leq 11$, and thus point (v) is proved.

Now we consider the case where $q = 2$. The genus 2 curve X described in Table 2 of [10] by the equation $y^2+y = x^5+x^2$ satisfies $N_1(X) = N_3(X) = 5$, which means that $B_3(X) = 0$, and thus $\rho(2,2) \geq 4$. Lemma (5.1) ensures the existence of a closed point of degree 4 on any curve whereas (7) gives $\rho(2,2) \leq 5$. We can conclude that $\rho(2,2) = 4$.

When $q = 3$, Proposition 2.2 asserts that $\rho(3,2) \leq 4$. The genus 2 curve X defined in Table 3 in [10] and also in [8] by the equation $y^2 = (1+x^2)(-1+x+x^2)(-1-x+x^2)$ is such that $N_3(X) = N_1(X) = 8$, and so $B_3(X) = 0$ which implies $\rho(3,2) = 4$.

If $q = 4$ we use Proposition 2.2 to get $\rho(4,2) \leq 4$ and Lemma 5.1 to conclude.

Now suppose that $q = 5$. Proposition 2.2 gives $\rho(5,2) \leq 3$ but the genus 2 curve X defined in [8] by the equation $y^2 = x^5 + 4x$ satisfies $B_2(X) = 0$, and the other inequality follows.

□

6. Genus 3 curves

We would like to emphaze two of the main ingredients of the proof of the main theorem of this section. First we will make use of the *L-functions and modular forms database* (sometimes refered as LMFDB, see [9]). Second, we will exploit the Theorem 1.1. proved by Howe, Lauter and Top in [6] which ensures that there exists a pointless genus 3 curve defined over $\mathbb{F}_q$ if and only if either $q = 32$, $q = 29$ or $q \leq 25$. Hence for such values of q we know that $\rho(q,3) \geq 2$.

Theorem 6.1. *The values of $\rho(q,3)$ are as follows.*

(i) $\rho(2,3) = 7$ *(ii)* $\rho(3,3) = 5$ *(iii)* $\rho(4,3) = 3$ *(iv)* $\rho(5,3) = 3$

(v) $\rho(7,3) = 2$ *(vi)* $\rho(8,3) = 2$ *(vii)* $\rho(9,3) = 3$ *(viii)* $\rho(q,3) = 2$ *for* $11 \leq q \leq 25$

(ix) $\rho(27,3) = 1$ *(x)* $\rho(29,3) = 2$ *(xi)* $\rho(31,3) = 1$ *(xii)* $\rho(32,3) = 2$

(xiii) $\rho(q,3) = 1$ *for any* $q \geq 37$

Proof. As already mentioned, Theorem 1.1 of [6] implies that $\rho(q,3) \geq 2$ for $q \leq 25$, $q = 29$ and $q = 32$.

(i) The inequality (7) yields $\rho(2,3) \leq 7$. Moreover, LMFDB provides the curve X of equation $x^4+x^2y^2+x^2yz+x^2z^2+xy^2z+xyz^2+y^4+y^2z^2+z^4 = 0$ which satisfies $B_6(X) = 0$, and thus $\rho(2,3) = 7$.

(ii) By Proposition 2.2 we have $\rho(3,3) \leq 5$. But the curve $x^3z+xz^3+y^4 = 0$ given in [9] is a curve of genus 3 over $\mathbb{F}_3$ without points of degree 4, so $\rho(3,3) > 4$ and we are done.

(iii) Proposition 2.2 gives $\rho(4,3) \leq 4$ whereas the curve $x^3y + x^3z + x^2y^2 + xz^3 + y^3z + y^2z^2 = 0$ defined over $\mathbb{F}_4$ and provided by [9] has genus 3 and no points of degree 2. So $\rho(4,3) \geq 3$. Furthermore, the Weil bounds (3) yield $N_1 \leq 17 \leq N_3$. But, there does not exist a curve over $\mathbb{F}_4$ of genus 3 with 17 rational points since $N_4(3) = 14$ (see Table 1 in [12]). Now use $B_3 = (N_3 - N_1)/3$ to get $B_3 > 0$ and the desired result.

(iv) Here Proposition 2.3 improves Proposition (2.2) and we get $\rho(5,3) \leq 3$. Moreover, the curve $y^2 = x^7 + x^5 + 3x^3 + x$ found in [9] has no points of degree 2, so $\rho(5,3) \geq 3$.

(v) Proposition 2.2 gives $\rho(7,3) \leq 3$. Moreover, by Theorem 1 of [14], there does not exist a DS-curve for the extension $\mathbb{F}_{7^2}/\mathbb{F}_7$. So one can conclude that $\rho(7,3) = 2$.

(vi) Proposition 2.2 leads to $\rho(8,3) \leq 3$. And by [9] there is no genus 3 curve X defined over $\mathbb{F}_8$ such that $B_2(X) = 0$. One can see the coherence with results provided in [8]: Lario states that there does not exist a DS-curves for the field extension $\mathbb{F}_{64}/\mathbb{F}_8$.

(vii) By Proposition 2.2 again we have $\rho(9,3) \leq 3$. Moreover, the genus 3 curve X of equation $x^4 + y^4 + z^4 = 0$ defined over $\mathbb{F}_9$ proposed in [8] has no degree 2 points since $N_1(X) = N_2(X) = 28$. This implies $\rho(9,3) = 3$.

(viii) We use the bound of Proposition (2.2) to find $\rho(q,3) \leq 2$ for $11 \leq q \leq 25$. But for such values of q Theorem 1.1. of [6] states that there exists a pointless curve of genus 3.

(ix), (x), (xi) and (xii) We first use Proposition 2.2 to learn that $\rho(q,3) \leq 2$ for $q \in \{27, 29, 31, 32\}$. Moreover, by Theorem 1.1. of [6], there exists a pointless curve defined over $\mathbb{F}_{29}$ nor $\mathbb{F}_{32}$ whereas there does not exist such a curve neither over $\mathbb{F}_{27}$ nor $\mathbb{F}_{31}$.

(xiii) Corollary 2.4 enables us to check that for any $q \geq 37$ we have $\rho(q,3) \leq 2$. But by Theorem 1.1. of [6], there does not exist a genus 3 pointless curve for such values of q, so $\rho(q,3) = 1$. □

Acknowledgement. The authors would like to thank Joan-C. Lario for a useful discussion on Diophantine Stability.

References

[1] Y. Aubry, S. Haloui and G. Lachaud. On the number of points on abelian and Jacobian varieties over finite fields, Acta Arith. 160.3 (2013), 201–242.
[2] Y. Aubry and A. Iezzi. Optimal and maximal singular curves, Contemp. Math. Vol. 686, pp 31–43, A.M.S. (2017).
[3] N. D. Elkies, E. W. Howe, A. Kresch, B. Poonen, J. L. Wetherell and M. E. Zieve. Curves of every genus with many points. II. Asymptotically good families, Duke Math. J. 122 (2004), 399–422.
[4] E. Hallouin and M. Perret. A unified viewpoint for upper bounds for the number of points of curves over finite fields via euclidean geometry and semi-definite symmetric Toeplitz matrices, Trans. A.M.S., Volume 372, Number 8, 15 October 2019, pp 5409–5451.
[5] J.W.P. Hirschfeld, G. Korchmáros and F. Torres. Algebraic curves over a finite field, Princeton Ser. Appl. Math. Princeton University Press, Princeton, NJ, 2008.
[6] E. Howe, K. Lauter and J. Top. Pointless curves of genus three and four, Arithmetic, geometry and coding theory (AGCT 2003), 125–141, Sémin. Congr., 11, Soc. Math. France, Paris, 2005.
[7] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo Sect. IA Math., 28(3) : 721–724 (1982), 1981.
[8] J-C. Lario. Curves over finite fields with Diophantine stability, `https://web.mat.upc.edu/joan.carles.lario/DS.html#`
[9] The LMFDB Collab., The L-functions and modular forms database, http://www.lmfdb.org (2022).
[10] D. Maisner and E. Nart , with an Appendix by E. Howe. Abelian surfaces over finite fields as Jacobians, Experiment. Math. 11 (2002), no.3, 321–337.
[11] B. Mazur and K. Rubin , with an Appendix by M. Larsen. Diophantine stability, American J. Math. Vol. 140, Number 3 (2018), pp. 571–616.
[12] J.- P. Serre. Rational points on curves over finite fields, Doc. Math. (Paris), vol. 18 Soc. Math. France (2020).
[13] M. Tsfasman, S. Vlăduţ and D. Nogin. Algebraic geometric codes: basic notions, Mathematical Surveys and Monographs, 139. American Mathematical Society, Providence, RI, 2007.
[14] B. Vrioni. A census for curves and surfaces with Diophantine Stability over finite fields, Ph.D. thesis from Polytechnic University of Catalonia, School of Mathematics and Statistics, 2021.
[15] W. C. Waterhouse. Abelian varieties over finite fields, Ann. Sc. E. N. S. (4), **2** (1969), 521–560.

(Aubry) Institut de Mathématiques de Toulon - IMATH, Université de Toulon, France

(Aubry) Institut de Mathématiques de Marseille - I2M, Aix Marseille Univ, CNRS, Centrale Marseille, France
Email address: `yves.aubry@univ-tln.fr`

(Herbaut) INSPE Nice-Toulon, Université Côte d'Azur, France

(Herbaut) Institut de Mathématiques de Toulon - IMATH, Université de Toulon, France
Email address: fabien.herbaut@univ-cotedazur.fr

(Monaldi) Institut de Mathématiques de Toulon - IMATH, Université de Toulon, France
Email address: julien.monaldi@ac-nice.fr