Number of points on abelian and Jacobians varieties over finite fields

Yves Aubry, Safia Haloui, Gilles Lachaud

NUMBER OF POINTS ON ABELIAN AND JACOBIANS VARIETIES OVER FINITE FIELDS

YVES AUBRY, SAFIA HALOUI, AND GILLES LACHAUD

Abstract. We give upper and lower bounds on the number of points on abelian varieties over finite fields, and lower bounds specific to Jacobian varieties. We also determine exact formulas for the maximum and minimum number of points on Jacobian surfaces.

1. Introduction

Let A be an abelian variety of dimension g defined over the finite field $\mathbb{F}_q$ of characteristic p, with $q = p^n$. The characteristic polynomial $f_A(t)$ of A is defined as the characteristic polynomial of its Frobenius endomorphism F_A. Let $\omega_1, \dots, \omega_g, \overline{\omega}_1, \dots, \overline{\omega}_g$ be the complex roots of $f_A(t)$, with $|\omega_i| = \sqrt{q}$, as proved by A. Weil. For $1 \leq i \leq g$, we put $x_i = -(\omega_i + \overline{\omega}_i)$, and we say that A is *of type* $[x_1, \dots, x_g]$. The type of A only depends on the isogeny class of A, by the Honda-Tate Theorem. Let

$$\tau = -\sum_{i=1}^{g} (\omega_i + \overline{\omega}_i) = \sum_{i=1}^{g} x_i.$$

The integer τ is the opposite of the trace of F_A, and we say that A *has trace* $-\tau$. The number of rational points on A is $\#A(\mathbb{F}_q) = f_A(1)$, and

$$\#A(\mathbb{F}_q) = \prod_{i=1}^{g} (q + 1 + x_i), \tag{1}$$

since

$$f_A(t) = \prod_{i=1}^{g} (t - \omega_i)(t - \overline{\omega}_i) = \prod_{i=1}^{g} (t^2 + x_i t + q).$$

Since $|x_i| \leq 2\sqrt{q}$, we deduce from (1) the classical bounds:

$$(q + 1 - 2\sqrt{q})^g \leq \#A(\mathbb{F}_q) \leq (q + 1 + 2\sqrt{q})^g.$$

Moreover, if J_C is the Jacobian of a smooth, projective, absolutely irreducible algebraic curve C defined over $\mathbb{F}_q$ of genus g and with N rational points, M. Martin-Deschamps and the third author proved in [4] the lower bound

$$\#J_C(\mathbb{F}_q) \geq (\sqrt{q} - 1)^2 \frac{q^{g-1} - 1}{g} \frac{N + q - 1}{q - 1}.$$

The purpose of this article is to give a series of inequalities, contributing to improve the classical bounds for abelian varieties and the aforementioned lower bound for Jacobians. We then compare the bounds obtained. Furthermore, we study the special case of Jacobian varieties of dimension 2 and we give exact values for the maximum and the minimum number of rational points on such varieties.

It is worthwile to point out that S. Ballet and R. Rolland obtained recently in [1] some exact and asymptotic lower bounds on the number of points of Jacobian varieties. The methods and the results are different from those of the present article.

2000 *Mathematics Subject Classification.* 14G15, 11G10, 11G25.

Key words and phrases. Abelian varieties over finite fields, Jacobians, zeta functions.

2. Abelian varieties

Let $A/\mathbb{F}_q$ be an abelian variety of dimension g and trace $-\tau$. The arithmetic-geometric inequality states that

$$\sqrt[k]{c_1 \dots c_k} \leq \frac{1}{k}(c_1 + \dots + c_k)$$

if $c_1, \dots, c_k$ are non negative real numbers, with equality if and only if $c_1 = \dots = c_k$. Applying this inequality to (1), we get the following majoration, proved by H. G. Quebbemann [8] in the case of Jacobians, and M. Perret [7] in the case of Prym varieties:

Proposition 2.1. *Let $A/\mathbb{F}_q$ be an abelian variety of dimension g and trace $-\tau$. Then*

$$\#A(\mathbb{F}_q) \leq \left(q + 1 + \frac{\tau}{g}\right)^g$$

with equality if and only if A is of type $[x, \dots, x]$. □

We put $m = [2\sqrt{q}]$. Using the arithmetic-geometric inequality, J.-P. Serre [11] proved that

$$|\tau| \leq gm, \tag{2}$$

hence, Prop. 2.1 implies

$$\#A(\mathbb{F}_q) \leq (q + 1 + m)^g. \tag{3}$$

with equality if and only if A is of type $[m, \dots, m]$. We say that A (or τ) has *defect* d if $\tau = gm - d$.

Proposition 2.2. *If A has defect d, with $d = 1$ or $d = 2$, then*

$$\#A(\mathbb{F}_q) \leq (q + m)^d (q + 1 + m)^{g-d}.$$

Proof. J.-P. Serre gives in [13] the list of types $[x_1, \dots, x_g]$ such that $d = 1$ or $d = 2$, and we prove the proposition by inspection. The various possibilities are described in Table 1 below. In this table,

$$\varphi_1 = (-1 + \sqrt{5})/2, \quad \varphi_2 = (-1 - \sqrt{5})/2,$$

$$\omega_i = 1 - 4\cos^2 \frac{i\pi}{7}, \quad i = 1, 2, 3.$$

Moreover, B_d is the right hand side of the inequality, and $b = q + 1 + m$. □

d	$[x_1, \dots, x_g]$	$B_d - \#A(\mathbb{F}_q)$
1	$(m, \dots, m, m-1)$	0
	$(m, \dots, m, m+\varphi_1, m+\varphi_2)$	b^{g-2}
2	$(m, \dots, m, m-1, m-1)$	0
	$(m, \dots, m, m-2)$	b^{g-2}
	$(m, \dots, m, m+\sqrt{2}-1, m-\sqrt{2}-1)$	$2b^{g-2}$
	$(m, \dots, m, m+\sqrt{3}-1, m-\sqrt{3}-1)$	$3b^{g-2}$
	$(m, \dots, m, m-1, m+\varphi_1, m+\varphi_2)$	$b^{g-3}(b-1)$
	$(m, \dots, m, m+\varphi_1, m+\varphi_2, m+\varphi_1, m+\varphi_2)$	$b^{g-4}(2b^2-2b-1)$
	$(m, \dots, m, m+\omega_1, m+\omega_2, m+\omega_3)$	$b^{g-3}(2b-1)$

Table 1. Types with defect 1 or 2, with $b = q + 1 + m$.

We now assume $g \geq 2$, and prove a result generalizing somehow Prop. 2.2. Let

$$y_i = x_i - \left[\frac{\tau}{g}\right] \ (1 \leq i \leq g), \quad r = \sum_{i=1}^{g} y_i = \tau - g\left[\frac{\tau}{g}\right],$$

in such a way that r is the remainder of the division of τ by g.

Proposition 2.3. *If $r = 1$ or $r = g - 1$, then*

$$\#A(\mathbb{F}_q) \leq \left(q + 1 + \left[\frac{\tau}{g}\right]\right)^{g-r} \left(q + 2 + \left[\frac{\tau}{g}\right]\right)^{r}.$$

Proof. Take an integer k with $1 \leq k \leq g-1$. If H belongs to the set $\mathfrak{P}_k$ of subsets of $\{1, \ldots, g\}$ with k elements, we define

$$y_H = \sum_{i \in H} y_i \quad \text{and } f_k(T) = \prod_{H \in \mathfrak{P}_k} (T - y_H)$$

The polynomials f_k are in $\mathbb{Z}[T]$, since the family (x_i) is stable under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Moreover

$$\frac{\operatorname{Tr} y_H}{\deg f_k} = \frac{1}{\binom{g}{k}} \sum_{H \in \mathfrak{P}_k} y_H = \frac{1}{\binom{g}{k}} \binom{g-1}{k-1} \sum_{i=1}^{g} y_i = \frac{kr}{g}.$$

Now recall that if y is a totally positive algebraic integer, then the arithmetic-geometric inequality implies

$$\operatorname{Tr} y \geq \deg y.$$

Hence, if $y_H > 0$ for every $H \in \mathfrak{P}_k$, then $kr \geq g$. This shows that if $kr < g$, then, by possibly renumbering the numbers x_i, we have

$$\sum_{i=1}^{k} y_i \leq 0, \quad \text{i.e. } \sum_{i=1}^{k} x_i \leq k \left[\frac{\tau}{g}\right].$$

Choose now $k = g - r$. Then

$$\sum_{i=g-r+1}^{g} x_i \geq r(\left[\frac{\tau}{g}\right] + 1).$$

Hence, according to the arithmetic-geometric inequality,

$$\begin{aligned} \#A(\mathbb{F}_q) = \prod_{i=1}^{g} (q + 1 + x_i) &\leq \left(q + 1 + \frac{1}{g-r} \sum_{i=1}^{g-r} x_i\right)^{g-r} \left(q + 1 + \frac{1}{r} \sum_{i=g-r+1}^{g} x_i\right)^{r} \\ &\leq \left(q + 1 + \left[\frac{\tau}{g}\right]\right)^{g-r} \left(q + 2 + \left[\frac{\tau}{g}\right]\right)^{r}, \end{aligned}$$

where we use Lemma 2.4 below for the second inequality. The proof of Prop. 2.3 will be achieved by establishing that $r(g-r) < g$ if and only if $r = 1$ or $r = g-1$. In order to prove this, observe that the inequality $r(g-r) < g$ holds in every case if $g \leq 3$. Assume now $g \geq 4$, and let

$$r_{\pm}(g) = \frac{1}{2}(g \pm \sqrt{g^2 - 4g}).$$

The inequality holds if and only if $r < r_-(g)$ or $r > r_+(g)$. If $g = 4$, then $r_-(4) = r_+(4) = 2$. If $g \geq 5$, then $1 < r_-(g) < 2$ and $g - 2 < r_+(g) < g - 1$. □

Lemma 2.4. *Let $0 \leq a \leq c \leq d \leq b$. If $(g-r)a + rb = (g-r)c + rd$, then*

$$a^{g-r} b^r \leq c^{g-r} d^r.$$

Proof. The barycenter of $(a, \ln a)$ and $(b, \ln b)$ with the weights $g - r$ and r is

$$\left(\frac{(g-r)a + rb}{g}, \frac{(g-r)\ln a + r \ln b}{g}\right)$$

and that of $(c, \ln c)$ and $(d, \ln d)$ with the same weights is

$$\left(\frac{(g-r)c + rd}{g}, \frac{(g-r)\ln c + r \ln d}{g}\right) = \left(\frac{(g-r)a + rb}{g}, \frac{(g-r)\ln c + r \ln d}{g}\right),$$

and we conclude using the concavity of the logarithm. □

If τ has defect 1, then

$$\frac{\tau}{g} = m - \frac{1}{g}, \quad \left[\frac{\tau}{g}\right] = m - 1, \quad r = (gm - 1) - (gm - g) = g - 1,$$

and Prop. 2.3 reduces to Prop. 2.2. Moreover:

Corollary 2.5. *If $\tau = gm - g + 1$ (defect $g - 1$), then*

$$\#A(\mathbb{F}_q) \leq (q + m)^{g-1}(q + 1 + m).$$

Proof. Here

$$\frac{\tau}{g} = m - 1 + \frac{1}{g}, \quad \left[\frac{\tau}{g}\right] = m - 1, \quad r = gm - g + 1 - (gm - g) = 1.$$

□

Remark. Smyth's Theorem [14, p. 2], asserts that if x is a totally positive algebraic integer, then with finitely many exceptions, explicitly listed,

$$\operatorname{Tr} x \geq 1.7719 \deg x.$$

From this one deduces that the conclusion of Prop. 2.3 holds true for every r if $g \leq 7$ and if no one of the polynomials $x - 1$ or $x^2 - 3x + 1$ divides f_{g-r}.

It is natural to ask whether $\#A(\mathbb{F}_q)$ has a lower bound analogous to Serre's upper bound (3), and the answer turns out to be in the affirmative.

Theorem 2.6. *Let $A/\mathbb{F}_q$ be an abelian variety of dimension g. Then*

$$(q + 1 - m)^g \leq \#A(\mathbb{F}_q) \leq (q + 1 + m)^g,$$

and the lower (resp. upper) bound is reached if and only if A is of type $[-m, \ldots, -m]$ (resp. $[m, \ldots, m]$).

Proof. Only the first inequality has to be proved. For $k = 0, \ldots, g$, let t_k be the k-th symmetric function of the $(m + 1 + x_i)$'s, for $i = 1, \ldots, g$, that is,

$$\prod_{i=1}^{g}(t + (m + 1 + x_i)) = \sum_{k=0}^{g} t_k t^{g-k}.$$

If $1 \leq k \leq g$, define

$$T_k = \prod_{H \in \mathfrak{P}_k} \prod_{i \in H} (m + 1 + x_i).$$

The number T_k is a non zero integer, since it is left invariant by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Thus

$$T_k \geq 1.$$

On the other hand, using the arithmetic-geometric inequality, we obtain

$$T_k^{1/\binom{g}{k}} \leq \frac{1}{\binom{g}{k}} \sum_{H \in \mathfrak{P}_k} \prod_{i \in H} (m + 1 + x_i) = \frac{1}{\binom{g}{k}} t_k.$$

Combining these two inequalities, we get

$$\binom{g}{k} \leq t_k. \tag{4}$$

Moreover, (4) remains true for $k = 0$. Multiplying both sides of (4) by $(q - m)^{g-k}$ and adding the inequalities obtained for $k = 0, \ldots, g$ we obtain

$$\sum_{k=0}^{g} \binom{g}{k} (q - m)^{g-k} \leq \sum_{k=0}^{g} t_k (q - m)^{g-k}$$

from which the result follows. □

The inequality (4) implies as well a lower bound on $\#A(\mathbb{F}_q)$ related to the trace:

Proposition 2.7. *Let $A/\mathbb{F}_q$ be an abelian variety of dimension g and trace $-\tau$. Then*

$$\#A(\mathbb{F}_q) \geq (q+1-m)^g + (gm+\tau)(q-m)^{g-1}.$$

Proof. With the notations of the proof of Th. 2.6,

$$\begin{aligned}\#A(\mathbb{F}_q) &= \sum_{k=0}^{g}\binom{g}{k}(q-m)^{g-k} + \sum_{k=0}^{g}(t_k - \binom{g}{k})(q-m)^{g-k} \\ &= (q+1-m)^g + \sum_{k=0}^{g}(t_k - \binom{g}{k})(q-m)^{g-k} \\ &\geq (q+1-m)^g + (t_1 - g)(q-m)^{g-1}\end{aligned}$$

where the last inequality comes from (4). □

Remark. By (2), we know that $gm+\tau \geq 0$, hence

$$(q+1-m)^g + (gm+\tau)(q-m)^{g-1} \geq (q+1-m)^g.$$

Moreover, for $g=1$ (if $q \leq 4$ then $q-m=0$ and we use the convention $0^0=1$) the lower bound of Prop. 2.7 is an equality.

Another way to get lower bounds for $\#A(\mathbb{F}_q)$ is to use real analysis methods as preformed by Perret. We give the statement of [7, Th. 3], with a slightly rectified proof.

Theorem 2.8. *We have*

$$\#A(\mathbb{F}_q) \geq (q-1)^g\Big(\frac{\sqrt{q}+1}{\sqrt{q}-1}\Big)^{\omega-2\delta}, \quad \text{where } \omega = \frac{\tau}{2\sqrt{q}},$$

and where $\delta = 0$ if $g+\omega$ is an even integer and 1 otherwise.

Proof. The idea is to find the minimum of the function

$$(x_1,\dots,x_g) \mapsto \prod_{i=1}^{g}(q+1+x_i)$$

on the set

$$\{(x_1,\dots,x_g) \in [-2\sqrt{q},2\sqrt{q}]^g \mid x_1+\cdots+x_g = \tau\}.$$

Let

$$y_i = \frac{x_i}{2\sqrt{q}}, \quad c = \frac{q+1}{2\sqrt{q}}.$$

The problem is reduced to minimize the function

$$F(y_1,\dots,y_g) = \sum_{i=1}^{g}\ln(c+y_i)$$

on the polytope

$$P = \{(y_1,\dots,y_g) \in [-1,1]^g \mid y_1+\cdots+y_g = \omega\}.$$

The set of points of P where F is minimum is invariant under permutations. Since F is strictly concave, the points of this set are vertices of P. But at most one of the coordinates of a vertex of P is different from ± 1. Hence the minimum of F is attained at a vertex

$$\gamma = (1,\dots,1,-1,\dots,-1,\beta), \quad \text{with } \beta \in [-1,1].$$

Denote by u and v the number of 1 and of -1 in γ and set $\delta = 1$ if $\beta \in]-1,1[$ and 0 otherwise. Then

$$u+v+\delta = g, \quad u-v+\delta\beta = \omega,$$

and adding these equations, we see that if $\delta = 0$ then $g + \omega$ is an even integer. The converse is true: if $\delta = 1$ then $\beta \in]-1, 1[$, and either $\beta \neq 0$ and $g + \omega$ is not an integer, or $\beta = 0$ and $g + \omega = 2u + 1$. Hence,

$$\begin{aligned}\min_{(y_1,\dots,y_g)\in P} \exp F(y_1,\dots,y_g) &= (c+\beta)^\delta (c+1)^u (c-1)^v \\ &= (c+\beta)^\delta (c^2-1)^{\frac{u+v}{2}} \Big(\frac{c+1}{c-1}\Big)^{\frac{u-v}{2}} \\ &= (c+\beta)^\delta (c^2-1)^{\frac{g-\delta}{2}} \Big(\frac{c+1}{c-1}\Big)^{\frac{\omega-\delta\beta}{2}},\end{aligned}$$

and $c + \beta \geq c - 1$ and $\omega - \delta\beta \geq \omega - \delta$. □

It is possible to improve Th. 2.8 by computing more explicitly the coordinates of the extremal points of P in the above proof.

Proposition 2.9. *Let*

$$r = \left[\frac{g + [\omega]}{2}\right], \quad s = \left[\frac{g - 1 - [\omega]}{2}\right], \quad \textit{where } \omega = \frac{\tau}{2\sqrt{q}}.$$

Then

$$\#A(\mathbb{F}_q) \geq (q + 1 + \tau - 2(r - s)\sqrt{q})(q + 1 + 2\sqrt{q})^r (q + 1 - 2\sqrt{q})^s.$$

Proof. We keep the notation and results of the proof of Th. 2.8. If $\gamma \neq (1, \dots, 1)$, we denote by r and s the number of 1 and of -1 of γ but now, without eventually counting β. We have $r - s = \omega - \beta$, thus β must be equal to $\{\omega\} = \omega - [\omega]$ or $\{\omega\} - 1$ (after perhaps a permutation of β with one of the coordinate equal to -1 in the case where $\beta = 1$). Thus,

$$r + s = g - 1, \quad r - s = [\omega] + \epsilon, \quad \beta = \{\omega\} - \epsilon,$$

where $\epsilon \in \{0, 1\}$. If $\gamma = (1, \dots, 1)$, the previous identities remain true if we set $r = g$ and $s = -1$. The equations $2r = g - 1 + [\omega] + \epsilon$ and $2s = g - 1 - [\omega] - \epsilon$ show that $\epsilon = 1$ if and only if $g + [\omega]$ is even, and that

$$r = \Big[\frac{g + [\omega]}{2}\Big] \quad \text{and} \quad s = \Big[\frac{g - 1 - [\omega]}{2}\Big].$$

Proceeding as in the proof of Th. 2.8, we obtain

$$\min_{(y_1,\dots,y_g)\in P} \exp F(y_1,\dots,y_g) = (c + \{\omega\} - \epsilon)(c^2 - 1)^{\frac{g-1}{2}} \Big(\frac{c+1}{c-1}\Big)^{\frac{[\omega]+\epsilon}{2}}.$$

Then

$$\#A(\mathbb{F}_q) \geq (q-1)^{g-1} \Big(q + 1 + 2\sqrt{q}(\{\omega\} - \epsilon)\Big) \Big(\frac{\sqrt{q}+1}{\sqrt{q}-1}\Big)^{\frac{[\omega]+\epsilon}{2}}$$

where $\epsilon = 1$ if $g + [\omega]$ is even and 0 otherwise, from which the result follows. □

Remark. If q is not a square, the bound of Prop. 2.9 is reached only if $r = s$ (which implies that $|\tau| < 2\sqrt{q}$) and τ is the trace of some elliptic curve. If q is a square, this bound is not reached only if $\tau - 2(r - s)\sqrt{q}$ is not the trace of an elliptic curve (in particular, it is reached if τ is coprime to p).

3. Jacobians

In this section, we denote by C a nonsingular, projective, absolutely irreducible curve defined over $\mathbb{F}_q$, and we focus on the Jacobian J_C of such curves. We define

$$J_q(g) = \max_C \#J_C(\mathbb{F}_q) \quad \text{and} \quad j_q(g) = \min_C \#J_C(\mathbb{F}_q),$$

where C ranges over the set of curves of genus g. Th. 2.6 implies

$$(q + 1 - m)^g \leq j_q(g) \leq J_q(g) \leq (q + 1 + m)^g.$$

3.1. **Jacobians as abelian varieties.** Let $N = \#C(\mathbb{F}_q)$ the number of rational points of C over $\mathbb{F}_q$. If J_C has trace $-\tau$, then

$$N = q + 1 + \tau.$$

By Prop. 2.1, we get

$$\#J_C(\mathbb{F}_q) \leq \Big(q + 1 + \frac{N - (q+1)}{g}\Big)^g,$$

hence,

$$J_q(g) \leq \Big(q + 1 + \frac{N_q(g) - (q+1)}{g}\Big)^g,$$

where $N_q(g)$ stands for the maximal number of rational points of a curve defined over $\mathbb{F}_q$ of genus g. The quantity $J_q(g)$ has the following asymptotic behaviour. On one hand, the Drinfeld-Vlăduţ upper bound [17, p. 146]

$$\limsup_{g\to\infty} N_q(g)/g \leq \sqrt{q} - 1$$

implies

$$\limsup_{g\to\infty} (J_q(g))^{1/g} \leq q + \sqrt{q}$$

(the Weil bound would only give the upper bound $q + 1 + 2\sqrt{q}$). On the other hand, S. Vlăduţ has proved [18] that if q is a square, then

$$q(\frac{q}{q-1})^{\sqrt{q}-1} \leq \limsup_{g\to\infty} (J_q(g))^{1/g}.$$

Observe that, when $q \to \infty$,

$$q(\frac{q}{q-1})^{\sqrt{q}-1} = q + \sqrt{q} - \frac{1}{2} + O(\frac{1}{\sqrt{q}}).$$

Remark (On the links between $N_q(g)$ and $J_q(g)$). The number of points of the Jacobian of a maximal curve (i.e. with $N_q(g)$ points) does not necessarily reach $J_q(g)$. For instance, J.-P. Serre [13, p. Se47] has shown that there exists two curves of genus 2 over $\mathbb{F}_3$ with $N_3(2) = 8$ points whose Jacobians have respectively 35 and 36 points.
We shall see below that a maximal Jacobian surface, that is, with $J_q(2)$ points, is always the Jacobian of a maximal curve (but there is no reason that this could remains true when $g > 2$). A curve reaching the Serre-Weil bound (i.e. with $q + 1 + m$ points) has type $[m, \ldots, m]$ by (2), hence, in the case where the Serre-Weil bound is reached for curves of genus g, a curve of genus g is maximal if and only if its Jacobian is maximal.

Prop. 2.7 implies

$$\#J_C(\mathbb{F}_q) \geq (q + 1 - m)^g + (gm + N - (q+1))(q - m)^{g-1},$$

and Prop. 2.9 leads to our first lower bound for Jacobians:

Proposition 3.1. *We have*

(**I**) $$\#J_C(\mathbb{F}_q) \geq (N - 2(r-s)\sqrt{q})(q + 1 + 2\sqrt{q})^r (q + 1 - 2\sqrt{q})^s,$$

with

$$r = \left[\frac{g + [\omega]}{2}\right], \quad s = \left[\frac{g - 1 - [\omega]}{2}\right], \quad \textit{where } \omega = \frac{N - q - 1}{2\sqrt{q}}.$$

3.2. **Specific bounds for Jacobians.** If $k \in \mathbb{N}$ and $k \geq 1$, we set $N_k = \#C(\mathbb{F}_{q^k})$, in such a way that $N_1 = N$. The *zeta function* of C is

$$Z_C(t) = \exp\Big(\sum_{k=1}^{+\infty} N_k \frac{t^k}{k}\Big).$$

Let $\omega_1, \ldots, \omega_{2g}$ be the roots of the characteristic polynomial of the Jacobian J_C of C, ordered in such a way that $\omega_{g+i} = \overline{\omega}_i$. Then

$$Z_C(t) = \frac{1}{(1-t)(1-qt)} \prod_{i=1}^{2g} (1 - \omega_i t).$$

If $n \in \mathbb{N}$, We denote by A_n the number of effective divisors of C of degree n and by B_n the number of points of C of degree n. Observe that $A_0 = 1, A_1 = B_1 = N$, and

$$N_k = \sum_{d|k} dB_d.$$

We have

$$Z_C(t) = \prod_{k=1}^{\infty} (1 - t^k)^{-B_k} = \sum_{n=0}^{+\infty} A_n t^n. \tag{5}$$

By using the negative binomial formula

$$(1-t)^{-M} = \sum_{n=0}^{+\infty} \binom{M+n-1}{n} t^n,$$

where $M \in \mathbb{C}$ and

$$\binom{r}{0} = 1, \quad \binom{r}{k} = \frac{r(r-1)\ldots(r-k+1)}{k!} \quad (r \in \mathbb{Z}, k \in \mathbb{N})$$

are the *generalized binomial coefficients*, the second equality of (5) gives, for $n \geq 1$:

$$A_n = \sum_{b \in \mathcal{P}_n} \prod_{i=1}^{n} \binom{B_i + b_i - 1}{b_i}, \tag{6}$$

with

$$\mathcal{P}_n = \{b = (b_1, \ldots, b_n) \in \mathbb{N}^n \mid b_1 + 2b_2 + \cdots + nb_n = n\}.$$

Mireille Martin-Deschamps and the third author proved in [4], with the help of Riemann-Roch theorem, the following results: if $g \geq 2$, then

$$A_{n+g} = q^{n+1} A_{g-n-2} + \#J_C(\mathbb{F}_q) \frac{q^{n+1} - 1}{q - 1} \qquad \text{for } 0 \leq n \leq g-2, \tag{7}$$

$$A_{n+g} = \#J_C(\mathbb{F}_q) \frac{q^{n+1} - 1}{q - 1} \qquad \text{for } n \geq g-1. \tag{8}$$

In particular,

$$\#J_C(\mathbb{F}_q) = \frac{q-1}{q^g - 1} A_{2g-1}. \tag{9}$$

We begin by proving a lower bound for A_n.

Lemma 3.2. *If $n \geq 2$,*

$$A_n \geq \binom{N+n-1}{n} + \sum_{i=2}^{n} B_i \binom{N+n-i-1}{n-i}.$$

Proof. All the terms in the right hand side of (6) are ≥ 0. In order to get a lower bound, we sum over the subset of $\mathcal{P}_n$ consisting of

$$(n, 0, \ldots, 0), (n-2, 1, 0, \ldots, 0), (n-3, 0, 1, 0, \ldots, 0), \ldots, (1, 0, \ldots, 0, 1, 0), (0, \ldots, 0, 1).$$

□

From (9) and Lemma 3.2 we deduce:

Proposition 3.3. *We have*

$$\#J_C(\mathbb{F}_q) \geq \frac{q-1}{q^g-1}\left[\binom{N+2g-2}{2g-1} + \sum_{i=2}^{2g-1} B_i \binom{N+2g-2-i}{2g-1-i}\right].$$

In particular:

(II) $$\#J_C(\mathbb{F}_q) \geq \frac{q-1}{q^g-1}\binom{N+2g-2}{2g-1}. \quad \square$$

The lower bound (**II**) is obtained using the inequality $B_i \geq 0$ for $2 \leq i \leq 2g-1$.

We recall now some general facts on the exponential formula [9, 15]. Let $\mathbf{y} = (y_n)_{n\in\mathbb{N}}$ be a sequence of indeterminates. To an element $b = (b_1, \ldots, b_n) \in \mathbb{N}^n$ we associate the monomial $\mathbf{y}^b = y_1^{b_1} \ldots y_n^{b_n}$ in the ring $\mathbb{Q}[[\mathbf{y}]]$. We verify that

$$\begin{aligned}\exp\Big(\sum_{n=1}^{\infty} y_n \frac{t^n}{n}\Big) &= \prod_{n=1}^{\infty} \exp\Big(y_n \frac{t^n}{n}\Big) = \prod_{n=1}^{\infty}\sum_{b_n=0}^{\infty} \frac{1}{b_n!}\Big(y_n\frac{t^n}{n}\Big)^{b_n} \\ &= \sum_{b_1,\ldots b_k\in\mathbb{N}} \frac{\mathbf{y}^b}{b_1!\ldots b_k!}\frac{t^{b_1+2b_2+\cdots+kb_k}}{2^{b_2}\ldots k^{b_k}}.\end{aligned}$$

Let $C_0(\mathbf{y}) = 1$ and for $n \in \mathbb{N}$, $n \geq 1$:

$$C_n(\mathbf{y}) = \sum_{b\in\mathcal{P}_n} c(b)\mathbf{y}^b, \quad c(b) = \frac{n!}{b_1!\ldots b_n!}\frac{1}{2^{b_2}\ldots n^{b_n}}$$

where $\mathcal{P}_n$ is as above. We put

$$\mathcal{C}_n(\mathbf{y}) = \frac{C_n(\mathbf{y})}{n!}.$$

The previous computations show that the following equality, called the *exponential formula*, holds in the ring $\mathbb{Q}[[\mathbf{y}]][[t]]$:

$$\exp\Big(\sum_{n=1}^{+\infty} y_n \frac{t^n}{n}\Big) = \sum_{n=0}^{+\infty} \mathcal{C}_n(\mathbf{y})t^n.$$

The polynomial $C_n(\mathbf{y})$ has positive integer coefficients, more precisely,

$$C_n(\mathbf{y}) = \sum_{\sigma\in\mathfrak{S}_n} \mathbf{y}^{\beta(\sigma)}$$

where the summation is over the symmetric group $\mathfrak{S}_n$, where $\beta(\sigma) = (b_1(\sigma), \ldots, b_n(\sigma))$ and $b_k(\sigma)$ is the number of cycles of length k in the cycle decomposition of σ as a product of disjoint cycles [9, 15]. We recall now two classical results. Let $\mathbf{y} = (y_n)_{n\in\mathbb{N}}$ and $\mathbf{z} = (z_n)_{n\in\mathbb{N}}$ be two sequences of indeterminates, and take $n \in \mathbb{N}$. Firstly, by applying the exponential formula to

$$\exp\Big(\sum_{n=1}^{+\infty}(y_n+z_n)\frac{t^n}{n}\Big) = \exp\Big(\sum_{n=1}^{+\infty} y_n\frac{t^n}{n}\Big)\exp\Big(\sum_{n=1}^{+\infty} z_n\frac{t^n}{n}\Big).$$

and expanding the right hand side, we obtain:

$$\mathcal{C}_n(\mathbf{y}+\mathbf{z}) = \sum_{k=0}^{n} \mathcal{C}_k(\mathbf{y})\mathcal{C}_{n-k}(\mathbf{z}). \tag{10}$$

Secondly, if $M \in \mathbb{N}$, then

$$\exp\Big(\sum_{n=1}^{+\infty} M\frac{t^n}{n}\Big) = \exp\Big(\sum_{n=1}^{+\infty} \frac{t^n}{n}\Big)^M = (1-t)^{-M} = \sum_{n=0}^{+\infty} \binom{M+n-1}{n} t^n.$$

hence,

$$\mathcal{C}_n(M,\dots,M) = \binom{M+n-1}{n}. \tag{11}$$

Since the zeta function $Z_C(t)$ of a curve C over $\mathbb{F}_q$ as above is equal to the power series defined by the right-hand-side of (5), we deduce from the very definition of $Z_C(t)$ that

$$A_n = \mathcal{C}_n(N_1,\dots,N_n). \tag{12}$$

We define

$$\mathbf{n} = (N, N, \dots), \quad \mathbf{d} = (0, N_2 - N, N_3 - N, \dots),$$

and put, if $k \geq 2$,

$$\begin{aligned} \mathcal{X}_k(N) &= \binom{N+k-1}{k} - q\binom{N+k-3}{k-2} \\ &= \binom{N+k-3}{k-2}\left[\left(\frac{N-1}{k}+1\right)\left(\frac{N-1}{k-1}+1\right) - q\right]. \end{aligned}$$

Proposition 3.4. *If $k \geq 0$, then $\mathcal{C}_k(\mathbf{n}) \geq 0$, $\mathcal{C}_k(\mathbf{d}) \geq 0$, and*

$$\#J_C(\mathbb{F}_q) = \mathcal{C}_g(\mathbf{d}) + (N-1)\mathcal{C}_{g-1}(\mathbf{d}) + \sum_{k=2}^{g} \mathcal{X}_k(N)\,\mathcal{C}_{g-k}(\mathbf{d}).$$

Proof. The coordinates of $\mathbf{n}$ and $\mathbf{d}$ are ≥ 0, and this implies our first assertion. Let $\mathbf{y}$ and $\mathbf{z}$ be two sequences of indeterminates. By (10),

$$\begin{aligned} \mathcal{C}_g(\mathbf{y}+\mathbf{z}) - q\mathcal{C}_{g-2}(\mathbf{y}+\mathbf{z}) &= \sum_{k=0}^{g} \mathcal{C}_k(\mathbf{y})\mathcal{C}_{g-k}(\mathbf{z}) - q\sum_{k=0}^{g-2} \mathcal{C}_k(\mathbf{y})\mathcal{C}_{g-2-k}(\mathbf{z}) \\ &= \sum_{k=0}^{g} \mathcal{C}_k(\mathbf{y})\mathcal{C}_{g-k}(\mathbf{z}) - q\sum_{k=2}^{g} \mathcal{C}_{k-2}(\mathbf{y})\mathcal{C}_{g-k}(\mathbf{z}) \\ &= \mathcal{C}_0(\mathbf{y})\mathcal{C}_g(\mathbf{z}) + \mathcal{C}_1(\mathbf{y})\mathcal{C}_{g-1}(\mathbf{z}) + \sum_{k=2}^{g} (\mathcal{C}_k(\mathbf{y}) - q\mathcal{C}_{k-2}(\mathbf{y}))\mathcal{C}_{g-k}(\mathbf{z}). \end{aligned}$$

Now

$$\#J_C(\mathbb{F}_q) = A_g - qA_{g-2} = \mathcal{C}_g(\mathbf{n}+\mathbf{d}) - q\mathcal{C}_{g-2}(\mathbf{n}+\mathbf{d}),$$

by applying (7) with $n = 0$, and using (12). Replacing $\mathbf{y}$ by $\mathbf{n}$ and $\mathbf{z}$ by $\mathbf{d}$, and since (11) implies

$$\mathcal{C}_k(\mathbf{n}) = \binom{N+k-1}{k},$$

we get the required expression for $\#J_C(\mathbb{F}_q)$. □

Now, we are ready to state the second lower bound for Jacobians.

Theorem 3.5. *If $g \geq 2$, then*

$$\#J_C(\mathbb{F}_q) \geq \binom{N+g-1}{g} - q\binom{N+g-3}{g-2}, \tag{**III**}$$

and the right-hand side is > 0 if and only if

$$\left(\frac{N-1}{g}+1\right)\left(\frac{N-1}{g-1}+1\right) - q > 0. \tag{13}$$

Proof. The right hand side of (**III**) is equal to $\mathcal{X}_g(N)$, and $\mathcal{X}_g(N) > 0$ if and only if (13) holds, in which case $N \geq 1$. We therefore assume that $\mathcal{X}_g(N) > 0$ (otherwise there is nothing to prove). For $k = 2, \ldots, g$, we have

$$\mathcal{X}_k(N) \geq \binom{N+k-3}{k-2} \left(\left(\frac{N-1}{g} + 1 \right) \left(\frac{N-1}{g-1} + 1 \right) - q \right) \geq 0,$$

where the second inequality comes from (13). Applying Prop. 3.4 we deduce

$$\#J_C(\mathbb{F}_q) \geq \mathcal{C}_0(\mathbf{n})\mathcal{C}_g(\mathbf{d}) + \mathcal{C}_1(\mathbf{n})\mathcal{C}_{g-1}(\mathbf{d}) + \mathcal{X}_g\,\mathcal{C}_0(\mathbf{d}) \geq \mathcal{X}_g\,\mathcal{C}_0(\mathbf{d}),$$

and the result follows, since $\mathcal{C}_0(\mathbf{d}) = 1$. □

Remarks. (i) The condition (13) is satisfied if $N \geq g(\sqrt{q} - 1) + 1$. This inequality has to be compared to the Drinfeld-Vlăduţ upper bound.
(ii) Notice that Th. 3.5 can be improved: since

$$C_n(\mathbf{d}) = \sum_{b \in \mathcal{P}_n} c(b)\mathbf{d}^b \geq \frac{N_n - N}{n},$$

because the right hand side is the term of the sum corresponding to $b = (0, \ldots, 0, 1)$, we get

$$\mathcal{C}_0(\mathbf{n})\mathcal{C}_g(\mathbf{d}) \geq \frac{N_g - N}{g} \quad \text{and} \quad \mathcal{C}_1(\mathbf{n})\mathcal{C}_{g-1}(\mathbf{d}) \geq N\frac{N_{g-1} - N}{g-1}.$$

Therefore if (13) holds, then

$$\#J_C(\mathbb{F}_q) \geq \frac{N_g - N}{g} + N\frac{N_{g-1} - N}{g-1} + \binom{N+g-1}{g} - q\binom{N+g-3}{g-2},$$

and the numbers N_g and N_{g-1} can be replaced by their standard lower bounds in order to get a bound improving (**III**).

From [4], we know that

$$\sigma\,\#J_C(\mathbb{F}_q) = \sum_{n=0}^{g-2} A_n + \sum_{n=0}^{g-1} q^{g-1-n} A_n, \tag{14}$$

where

$$\sigma = \sum_{i=1}^{g} \frac{1}{|1 - \omega_i|^2}\,.$$

Moreover

$$\frac{1}{\sigma} \geq \frac{(\sqrt{q}-1)^2}{g}, \tag{15}$$

$$\frac{1}{\sigma} \geq \frac{(q-1)^2}{(g+1)(q+1) - N}, \tag{16}$$

the last one being always better than the first one (but depending on N). The identity (14), joint to the inequality $A_n \geq N$ for $n \geq 1$, gives

$$\sigma\#J_C(\mathbb{F}_q) \geq (q^{g-1} - 1)\frac{N+q-1}{q-1}\,.$$

Using (15), we obtain [4, Th. 2(2)]:

$$\#J_C(\mathbb{F}_q) \geq (\sqrt{q}-1)^2 \frac{q^{g-1}-1}{g}\frac{N+q-1}{q-1}\,. \tag{**A**}$$

Now, instead of the inequality $A_n \geq N$, we use the inequality of Lemma 3.2 in (14). We find that if $g \geq 4$, then

$$\sigma\,\#J_C(\mathbb{F}_q) \geq \sum_{n=0}^{g-2}\binom{N+n-1}{n} + \sum_{n=2}^{g-2}\sum_{i=2}^{n} B_i\binom{N+n-i-1}{n-i} + \sum_{n=0}^{g-1} q^{g-1-n}\binom{N+n-1}{n} + \sum_{n=2}^{g-1} q^{g-1-n}\sum_{i=2}^{n} B_i\binom{N+n-i-1}{n-i}.$$

Noticing that

$$\sum_{n=0}^{g-2}\binom{N+n-1}{n} = \binom{N+g-2}{g-2},$$

and using the inequality $B_i \geq 0$ for $2 \leq i \leq g-1$, we obtain:

$$\sigma\,\#J_C(\mathbb{F}_q) \geq \binom{N+g-2}{g-2} + \sum_{n=0}^{g-1} q^{g-1-n}\binom{N+n-1}{n}.$$

If $g < 4$, one checks directly from (14) that the above inequality still holds. Namely,

$$\begin{array}{lcll} \sigma\,\#J_C(\mathbb{F}_q) & = & 1+q+N & \text{if} \quad g=2, \\ \sigma\,\#J_C(\mathbb{F}_q) & \geq & 1+N+q^2+Nq+\binom{N+1}{2} & \text{if} \quad g=3. \end{array}$$

Using finally (16) instead of (15), we have proved:

Theorem 3.6. *If $g \geq 2$, then*

$$\textbf{(IV)} \qquad \#J_C(\mathbb{F}_q) \geq \left[\binom{N+g-2}{g-2} + \sum_{n=0}^{g-1} q^{g-1-n}\binom{N+n-1}{n}\right]\frac{(q-1)^2}{(g+1)(q+1)-N}. \quad \square$$

Remark. The expression in brackets is $\geq q^{g-1}$. Since $N \geq 0$, we obtain as a corollary the following bound [4, Th. 2(1)], which does not depend on N:

$$\#J_C(\mathbb{F}_q) \geq q^{g-1}\frac{(q-1)^2}{(q+1)(g+1)}.$$

The right hand side in (**IV**) is cumbersome. Here is a simpler lower bound using the partial sums of the exponential series. Let

$$e_n(x) = \sum_{j=0}^{n}\frac{x^j}{j!}, \quad n \in \mathbb{N}, \quad x > 0.$$

Then

$$e_n(x) = e^x\frac{\Gamma(n+1,x)}{n!}, \quad \text{where} \quad \Gamma(n,x) = \int_x^\infty t^{n-1}e^{-t}dt$$

is the incomplete Gamma function. Since

$$\binom{N+n-1}{n} \geq \frac{N^n}{n!},$$

we get from Th. 3.6:

Corollary 3.7. *If $g \geq 2$, then*

$$\#J_C(\mathbb{F}_q) \geq \left[\binom{N+g-2}{g-2} + q^{g-1}e_{g-1}(q^{-1}N)\right]\frac{(q-1)^2}{(g+1)(q+1)-N}. \quad \square$$

4. Comparing the bounds

Let C be a curve of genus g defined over $\mathbb{F}_q$ as in section 3, with $N = \#C(\mathbb{F}_q)$. We recall the lower bounds obtained respectively in Prop. 3.1 (with r and s as defined there), Prop. 3.3, Th. 3.5, and Th. 3.6, for the number of rational points of J_C:

$$\textbf{(I)} \quad \#J_C(\mathbb{F}_q) \geq (N - 2(r-s)\sqrt{q})(q+1+2\sqrt{q})^r(q+1-2\sqrt{q})^s$$

$$\textbf{(II)} \quad \#J_C(\mathbb{F}_q) \geq \frac{q-1}{q^g-1}\binom{N+2g-2}{2g-1}$$

$$\textbf{(III)} \quad \#J_C(\mathbb{F}_q) \geq \binom{N+g-1}{g} - q\binom{N+g-3}{g-2}$$

$$\textbf{(IV)} \quad \#J_C(\mathbb{F}_q) \geq \left[\binom{N+g-2}{g-2} + \sum_{n=0}^{g-1} q^{g-1-n}\binom{N+n-1}{n}\right] \frac{(q-1)^2}{(g+1)(q+1)-N}$$

(i) Observe that (**IV**) is always better than (**A**): if $n \geq 1$ and $N \geq 1$ are two integers, then

$$\binom{N+n-1}{n} \geq N,$$

thus the lower bound $A_n \geq \binom{N+n-1}{n}$ is better than $A_n \geq N$.

(iii) When q is large with respect to g, then

$$\#J_C(\mathbb{F}_q) = q^g + O(q^{g-\frac{1}{2}}),$$

according to the Lang-Weil estimate, and (**I**) is the only bound to be consistent with this estimate. More precisely, since (**I**) is usually reached for abelian varieties when q is a square, this bound is probably the best one as soon as $g \leq (q-\sqrt{q})/2$.

(ii) If $g \leq (q-\sqrt{q})/2$, the bounds (**II**), (**III**), and (**IV**) hold for every abelian variety. In order to prove this, we associate to an abelian variety a sequence (N_k) of integers, by setting

$$N_k = q^k + 1 - \sum_{i=1}^{g} (\omega_i^k + \bar{\omega}_i^k).$$

These numbers satisfy

$$q^k + 1 - 2gq^{k/2} \leq N_k \leq q^k + 1 + 2gq^{k/2}.$$

But

$$g \leq (q-\sqrt{q})/2 \iff q+1+2g\sqrt{q} \leq q^2+1-2gq \implies q+1+2g\sqrt{q} \leq q^k+1-2gq^{k/2},$$

for all $k \geq 1$, and hence, $N_k \geq N$. In this setting, one can *define* the numbers

$$A_n = \mathcal{C}_n(N, N_2, \ldots, N_n)$$

which are positive, and the formulas (7), (8), and (14) hold true. With the notation used in Prop. 3.4, we have, by (10) and (11),

$$A_n = \mathcal{C}_n(\mathbf{n}+\mathbf{d}) = \sum_{k=0}^{n} \mathcal{C}_k(\mathbf{n})\mathcal{C}_{n-k}(\mathbf{d}) \geq \mathcal{C}_n(\mathbf{n}) = \binom{N+n-1}{n},$$

and we recover all the tools used to establish our lower bounds.

(iv) The bounds (**II**) and (**III**) are never optimal for $g \geq 9$, owing to the following result:

There is no curve of genus ≥ 9 *with* $B_2 = \cdots = B_g = 0$.

Indeed, suppose $B_2 = \cdots = B_g = 0$. Then $q + 1 + 2gq^{1/2} \geq N = N_g \geq q^g + 1 - 2gq^{g/2}$, hence

$$2g \geq \frac{q^g - q}{q^{g/2} + q^{1/2}} = q^{g/2} - q^{1/2} \geq 2^{g/2} - 2^{1/2}.$$

The function $x \mapsto 2^{x/2} - 2x - 2^{1/2}$ is increasing on $[8, +\infty[$ and take a positive value on 9 and thus the inequality $2g \geq 2^{g/2} - 2^{1/2}$ can be verified only if $g < 9$.

(v) The numerical experiments that we performed lead to the following observations. The bound (**III**) can be good even if $g \geq 9$, but, when g is large, (**IV**) seems to be better than (**II**) and (**III**), and probably (**IV**) becomes better than (**I**) when g is very large.

5. Jacobian surfaces

The characteristic polynomial of an elliptic curve determines the number of its rational points, and vice versa. Therefore, the values of $J_q(1)$ and $j_q(1)$ are given by the Deuring-Waterhouse Theorem (see [2], [19]): if $q = p^n$, then

$$J_q(1) = \begin{cases} q + 1 + m & \text{if } n = 1, n \text{ is even, or } p \not| m, \\ q + m & \text{otherwise,} \end{cases}$$

$$j_q(1) = \begin{cases} q + 1 - m & \text{if } n = 1, n \text{ is even, or } p \not| m, \\ q + 2 - m & \text{otherwise.} \end{cases}$$

The description of the set of characteristic polynomials of abelian surfaces was given by Rück in [10]. The question of describing the set of isogeny classes of abelian surfaces which contain a Jacobian has been widely studied, especially by J.-P. Serre [11], [12], [13], whose aim was to determine $N_q(2)$. A complete answer to this question was finally given by Howe, Nart, and Ritzenthaler in [3]. In the remaining of this section, we explain how to deduce from these results the value of $J_q(2)$ and $j_q(2)$. Let A be an abelian surface over $\mathbb{F}_q$ of type $[x_1, x_2]$. Its characteristic polynomial $f_A(t)$ has the form

$$f_A(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2,$$

with

$$a_1 = x_1 + x_2 \quad \text{and} \quad a_2 = x_1 x_2 + 2q.$$

By elementary computations, H.G. Rück [10] showed that the fact that the roots of $f_A(t)$ are q-Weil numbers (i.e. algebraic integers such that their images under every complex embedding have absolute value $\sqrt{q}$) is equivalent to

$$|a_1| \leq 2m \quad \text{and} \quad 2|a_1|\sqrt{q} - 2q \leq a_2 \leq \frac{a_1^2}{4} + 2q. \tag{17}$$

We have

$$\#A(\mathbb{F}_q) = f_A(1) = q^2 + 1 + (q+1)a_1 + a_2. \tag{18}$$

Table 2 gives all the possibilities for (a_1, a_2) such that $a_1 \geq 2m - 2$. Here

$$\varphi_1 = (-1 + \sqrt{5})/2, \quad \varphi_2 = (-1 - \sqrt{5})/2.$$

The numbers of points are classified in decreasing order and an abelian variety with (a_1, a_2) not in the table has a number of points strictly less than the values of the table. Indeed, if $-2m \leq a_1 < 2m - 2$, then

$$\begin{aligned} (q+1)a_1 + a_2 &\leq [(q+1)a_1 + \frac{{a_1}^2}{4} + 2q] \\ &\leq [(q+1)(2m-3) + \frac{(2m-3)^2}{4} + 2q] \\ &= (q+1)(2m-2) + (m^2 - 2m - 2 + 2q) + (3 - (q+m)) \\ &< (q+1)(2m-2) + (m^2 - 2m - 2 + 2q) \end{aligned}$$

(notice that the function $x \mapsto (q+1)x + (x^2/4)$ is increasing on the interval $[-2m, 2m-3]$).

a_1	a_2	Type	$\#A(\mathbb{F}_q)$
$2m$	m^2+2q	$[m,m]$	b^2
$2m-1$	m^2-m+2q	$[m,m-1]$	$b(b-1)$
	$m^2-m-1+2q$	$[m+\varphi_1, m+\varphi_2]$	b^2-b-1
$2m-2$	$m^2-2m+1+2q$	$[m-1,m-1]$	$(b-1)^2$
	$m^2-2m+2q$	$[m,m-2]$	$b(b-2)$
	$m^2-2m-1+2q$	$[m-1+\sqrt{2}, m-1-\sqrt{2}]$	$(b-1)^2-2$
	$m^2-2m-2+2q$	$[m-1+\sqrt{3}, m-1-\sqrt{3}]$	$(b-1)^2-3$

TABLE 2. Couples (a_1,a_2) maximizing $\#A(\mathbb{F}_q)$, with $b=q+1+m$.

In the same way, we build the table of couples (a_1,a_2) with $a_1 \leq -2m+2$. Notice that the ends of the interval containing a_2 given by (17) depend only on the value of a_1, hence the possible entries for a_2 are the same as in the previous table. Here again, the numbers of points are classified in increasing order and an abelian variety with (a_1,a_2) not in the following table has a number of points strictly greater than the values of the table. Indeed, if $-2m+2 < a_1 \leq 2m$, then

a_1	a_2	Type	$A(\mathbb{F}_q)$
$-2m$	m^2+2q	$[-m,-m]$	b'^2
$-2m+1$	$m^2-m-1+2q$	$[-m+\varphi_1, -m+\varphi_2]$	$b'^2-b'-1$
	m^2-m+2q	$[-m,-m+1]$	$b'(b'+1)$
$-2m+2$	$m^2-2m-2+2q$	$[-m+1+\sqrt{3}, -m+1-\sqrt{3}]$	$(b'+1)^2-3$
	$m^2-2m-1+2q$	$[-m+1+\sqrt{2}, -m+1-\sqrt{2}]$	$(b'+1)^2-2$
	$m^2-2m+2q$	$[-m,-m+2]$	$b'(b'+2)$
	$m^2-2m+1+2q$	$[-m+1,-m+1]$	$(b'+1)^2$

TABLE 3. Couples (a_1,a_2) minimizing $\#A(\mathbb{F}_q)$, with $b'=q+1-m$.

$$\begin{aligned}(q+1)a_1+a_2 &\geq (q+1)a_1+2|a_1|\sqrt{q}-2q\\ &\geq (q+1)(-2m+3)+2(2m-3)\sqrt{q}-2q\\ &= (q+1)(-2m+2)+(m^2-2m+1+2q)-(2\sqrt{q}-m+1)^2+(\sqrt{q}-1)^2\\ &> (q+1)(-2m+2)+(m^2-2m+1+2q)\end{aligned}$$

(notice that the function $x \mapsto (q+1)x+2|x|\sqrt{q}$ is increasing on the interval $[-2m+3, 2m]$). Most cases of Th. 5.1 and 5.2 will be proved in the following way:

(i) Look at the highest row of Table 2 or 3 (depending on the proposition being proved).
(ii) Check if the corresponding polynomial is the characteristic polynomial of an abelian variety.
(iii) When it is the case, check if this abelian variety is isogenous to a Jacobian variety.
(iv) When it is not the case, look at the following row and come back to the second step.

For the second step, we use the results of Rück [10] who solved the problem of describing characteristic polynomials of abelian surfaces, in particular the fact that if (a_1,a_2) satisfy (17)

and p does not divide a_2 then the corresponding polynomial is the characteristic polynomial of an abelian surface.
For the third step, we use [3] where we can find a characterization of isogeny classes of abelian surfaces containing a Jacobian.
The determination of $J_q(2)$ in Th. 5.1 is closely related to that of $N_q(2)$, as done by J.-P. Serre [13]. In order to simplify the proof of Th. 5.2, we use the fact that given a curve of genus 2, if we denote by (a_1, a_2) the coefficients associated to its characteristic polynomial, there exists a curve (its quadratic twist) whose coefficients are $(-a_1, a_2)$. This allows us to adapt the proof of Th. 5.1.
Let us recall the definition of special numbers introduced by J.-P. Serre. An odd power q of a prime number p is *special* if one of the following conditions is satisfied (recall that $m = [2\sqrt{q}]$):

(i) m is divisible by p,
(ii) there exists $x \in \mathbb{Z}$ such that $q = x^2 + 1$,
(iii) there exists $x \in \mathbb{Z}$ such that $q = x^2 + x + 1$,
(iv) there exists $x \in \mathbb{Z}$ such that $q = x^2 + x + 2$.

Remark. In [12], J.-P. Serre asserts that if q is prime then the only possible conditions are conditions (2) and (3). When q is not prime, then condition (2) is impossible, condition (3) is possible only if $q = 7^3$ and condition (4) is possible only if $q = 2^3$, 2^5 or 2^{13}. Moreover, using basic arithmetic, it can be shown (see [5] for more details) that conditions (2), (3) and (4) are respectively equivalent to $m^2 - 4q = -4$, -3 and -7.

Theorem 5.1. *The complete set of values of $J_q(2)$ is given by the following display.*

(a) *Assume that q is a square. Then*

$$J_q(2) = \begin{cases} (q+1+m)^2 & \text{if } q \neq 4, 9. \\ 55 & \text{if } q = 4. \\ 225 & \text{if } q = 9. \end{cases}$$

(b) *Assume that q is not a square. If q is not special, then*

$$J_q(2) = (q+1+m)^2.$$

If q is special, then

$$J_q(2) = \begin{cases} (q+1+m+\varphi_1)(q+1+m+\varphi_2) & \text{if } \{2\sqrt{q}\} \geq \varphi_1. \\ (q+m)^2 & \text{if } \{2\sqrt{q}\} < \varphi_1, p \neq 2 \text{ or } p|m. \\ (q+1+m)(q-1+m) & \text{otherwise.} \end{cases}$$

Here $\varphi_1 = (-1+\sqrt{5})/2, \varphi_2 = (-1-\sqrt{5})/2$.

Proof. (a) Assume that q is a square.
— If $q \neq 4, 9$, $N_q(2)$ is the Serre-Weil bound [12], thus there exists a curve of type $[m, m]$.
— If $q = 4$, then $m = 4$. First we prove that $J_4(2) \leq 55$. Every curve of genus 2 over $\mathbb{F}_q$ is hyperelliptic, therefore, the number of rational points is at most $2(q+1) = 10$. We deduce that a Jacobian of dimension 2 over $\mathbb{F}_4$ must have $a_1 \leq 10 - (q+1) = 5$.
If $a_1 = 5$ then $a_2 \leq 14$ by (17). An abelian surface over $\mathbb{F}_4$ with $(a_1, a_2) = (5, 14)$ is of type $[3, 2]$ and is never a Jacobian (because $x_1 - x_2 = 3 - 2 = 1$, see [3]). Thus we have $a_2 \leq 13$ and a Jacobian surface over $\mathbb{F}_4$ with $a_1 = 5$ has at most $q^2 + 1 + 5(q+1) + 13 = 55$ points. If $a_1 < 5$, then

$$q^2 + 1 + (q+1)a_1 + a_2 \leq q^2 + 1 + (q+1)a_1 + \frac{{a_1}^2}{4} + 2q \leq 49$$

(notice that the function $x \mapsto 5x + (x^2/4)$ is increasing on $[-8, 4]$, and $a_1 \geq -8$). Thus an abelian surface over $\mathbb{F}_4$ with $a_1 < 5$ has less than 55 points, hence $J_4(2) \leq 55$.
It remains to prove that $J_4(2) \geq 55$. An abelian surface over $\mathbb{F}_4$ with $(a_1, a_2) = (5, 13)$ is of type $[3 + \varphi_1, 3 + \varphi_2]$. Such an abelian surface exists (because $p = 2$ does not divide 13) and by [3] it is isogenous to a Jacobian. This Jacobian has $q^2 + 1 + 5(q+1) + 13 = 55$ points.

— If $q = 9$, then $m = 6$. Since $2(q+1) = 20$, we must have $a_1 \leq 20 - (q+1) = 10 = 2m - 2$. The highest row of Table 2 such that $a_1 = 2m-2$ is that with type $[m-1, m-1]$, and this is the type of some Jacobian with $(q+m)^2 = 225$ points.

(b) Assume that q is not a square. This part of the proof follows easily from Serre's results. He proved in [13] the following facts:
— There exists a Jacobian of type $[m, m]$ if and only if q is not special.
— An abelian surface of type $[m, m-1]$ is never a Jacobian.
— If q is special, then there exists a Jacobian of type $[m+\varphi_1, m+\varphi_2]$ if and only if $\{2\sqrt{q}\} \geq \varphi_1$. Note that $\{2\sqrt{q}\} \geq \varphi_1$ is equivalent to $m + \varphi_1 \leq 2\sqrt{q}$, thus it is obvious that this condition is necessary.
— If q is special, $\{2\sqrt{q}\} < \varphi_1$, $p \neq 2$ or $p|m$, then there exists a Jacobian of type $[m-1, m-1]$.
— If q is special, $\{2\sqrt{q}\} < \varphi_1$, $p = 2$ and $p \nmid m$, that is, $q = 2^5$ or 2^{13} (if $q = 2^3$, then $\{2\sqrt{q}\} \geq \varphi_1$), then there exists a Jacobian of type $[m, m-2]$.
It remains to prove that for $q = 2^5$ and 2^{13}, there does not exist a Jacobian of type $[m-1, m-1]$. In fact, when $q = 2^5$ and 2^{13}, an abelian variety with all x_i equal to $(m-1)$ must have a dimension respectively multiple of 5 and 13 (see [6], Prop. 2.5). □

Theorem 5.2. *The complete set of values of $j_q(2)$ is given by the following display.*

(a) *Assume that q is a square. Then*

$$j_q(2) = \begin{cases} (q+1-m)^2 & \text{if } q \neq 4, 9. \\ 5 & \text{if } q = 4. \\ 25 & \text{if } q = 9. \end{cases}$$

(b) *Assume that q is not a square. If q is not special, then*

$$j_q(2) = (q+1-m)^2.$$

If q is special, then

$$j_q(2) = \begin{cases} (q+1-m-\varphi_1)(q+1-m-\varphi_2) & \text{if } \{2\sqrt{q}\} \geq \varphi_1. \\ (q+2-m+\sqrt{2})(q+2-m-\sqrt{2}) & \text{if } \sqrt{2}-1 \leq \{2\sqrt{q}\} < \varphi_1. \\ (q+1-m)(q+3-m) & \text{if } \{2\sqrt{q}\} < \sqrt{2}-1, p \nmid m \text{ and } q \neq 7^3. \\ (q+2-m)^2 & \text{otherwise.} \end{cases}$$

Proof. (a) Assume that q is a square.
— If $q \neq 4, 9$, we saw that there exists a curve of type $[m, m]$, and its quadratic twist is of type $[-m, -m]$.
— If $q = 4$, then $m = 4$. First we prove that $j_4(2) \geq 5$. We have $a_1 \geq -5$ since the quadratic twist of a curve with $a_1 < -5$ would have $a_1 > 5$ and we saw that it is not possible.
If $a_1 = -5$ then $a_2 \geq 12$ by (17). An abelian surface over $\mathbb{F}_4$ with $(a_1, a_2) = (-5, 12)$ is of type $[-4, 1]$ and is never a Jacobian. Thus $a_2 \geq 13$ and a Jacobian surface over $\mathbb{F}_4$ with $a_1 = -5$ has at least $q^2 + 1 - 5(q+1) + 13 = 5$ points. If $a_1 > -5$, then

$$q^2 + 1 + (q+1)a_1 + a_2 \geq q^2 + 1 + (q+1)a_1 + 2|a_1|\sqrt{q} - 2q = 9 + 5a_1 + 4|a_1| \geq 5$$

(note that the function $x \mapsto 5x + 4|x|$ is increasing on $[-4, 8]$). Thus an abelian surface over $\mathbb{F}_4$ with $a_1 > -5$ has more than 5 points, hence $j_4(2) \geq 5$.
It remains to prove that $j_4(2) \leq 5$. There exists a curve with $(a_1, a_2) = (-5, 13)$: the quadratic twist of the curve with $(a_1, a_2) = (5, 13)$ in the proof of Th. 5.1. The number of points of its Jacobian is

$$q^2 + 1 - 5(q+1) + 13 = 5.$$

— If $q = 9$, then $m = 6$. Using the same argument as in the last step, we must have $a_1 \geq -2m+2$. We look at the rows of Table 3, beginning by the rows on the top, for which $a_1 = -2m+2$. The first two can be ignored since $\{2\sqrt{q}\} = 0$ is less than $\sqrt{3} - 1$ and less than $\sqrt{2} - 1$. An abelian surface of type $[-m, -m+2]$ is not a Jacobian (this is an almost ordinary abelian surface,

$m^2 = 4q$ and $m - (m-2)$ is squarefree, see [3]). The product of two copies of an elliptic curve of trace $(m-1)$ is isogenous to a Jacobian (such a curve exists since $3 \not| (m-1)$).

(b) Assume that q is not a square. Using twisting arguments and the proof of Th. 5.1, we see that:
— There exists a Jacobian of type $[-m, -m]$ if and only if q is not special.
— If q is special, there exists a Jacobian of type $[-m-\varphi_1, -m-\varphi_2]$ if and only if $\{2\sqrt{q}\} \geq \varphi_1$.
— An abelian surface of type $[-m, -m+1]$ is never a Jacobian.
In the remaining of the proof, we suppose that q is special and $\{2\sqrt{q}\} < \varphi_1$.
— In order to have the existence of an abelian surface of type $[-m+1+\sqrt{3}, -m+1-\sqrt{3}]$, it is necessary to have $\{2\sqrt{q}\} \geq \sqrt{3}-1$. When $\{2\sqrt{q}\} < \varphi_1$, this condition is never satisfied (since $\varphi_1 < \sqrt{3}-1$).
— In order to ensure the existence of an abelian surface of type $[-m+1+\sqrt{2}, -m+1-\sqrt{2}]$, it is necessary to have $\{2\sqrt{q}\} \geq \sqrt{2}-1$. Suppose that this condition holds. we shall show that there exists an abelian surface of type $[-m+1+\sqrt{2}, -m+1-\sqrt{2}]$. We use the same kind of argument as J.-P. Serre used in [13]. If $p|m$, we are done since $p \not| a_2 = m^2 - 2m - 1 + 2q$. Otherwise, $(m - 2\sqrt{q})(m + 2\sqrt{q}) = m^2 - 4q \in \{-3, -4, -7\}$, hence

$$\{2\sqrt{q}\} = 2\sqrt{q} - m = \frac{4q - m^2}{m + 2\sqrt{q}} \leq \frac{7}{2m},$$

and if $m \geq 9$, $\frac{7}{2m} < \sqrt{2}-1$. It remains to consider by hand the powers of primes of the form x^2+1, x^2+x+1 and x^2+x+2 with $m < 9$ (i.e. $q < 21$). These prime powers are precisely 2, 3, 4, 5, 7, 8, 13 and 17. If $q = 2, 8$, then $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$. If $q = 3$, then $p|m$. If $q = 4, 7, 13, 17$, then $\{2\sqrt{q}\} < \sqrt{2}-1$. If $q = 5$, then $m = 4$ and $p = 5$ do not divide $a_2 = m^2 - 2m - 1 + 2q = 17$, and we are done. Finally, using [3], we conclude that this abelian surface is isogenous to a Jacobian.
— If $\{2\sqrt{q}\} < \sqrt{2}-1$, $p \not| m$ and $q \neq 7^3$, then $p \not| (m-2)$. To see this, take $p \neq 2$ (if $p = 2$, this is obvious) and use the remark about special numbers in this section. Suppose that p divides $(m-2)$, then p divides also $m^2 - 4 - 4q = (m+2)(m-2) - 4q$. Since $p \neq 2$, we must have $m^2 - 4q \in \{-3, -4\}$. If $m^2 - 4q = -3$, p divides $-3 - 4 = -7$ thus $p = 7$. But q is not prime (since for $q = 7$, $p \not| (m-2) = 5$), therefore we must have $q = 7^3$ and this case is excluded. If $m^2 - 4q = -4$, p divides $-4 - 4 = -8$ thus $p = 2$ which contradicts our assumption. This proves our assertion, and therefore, there exist elliptic curves of trace m and $(m-2)$ and by [3] their product is isogenous to a Jacobian.
— Suppose that $\{2\sqrt{q}\} < \sqrt{2}-1$ and $p|m$, or $q = 7^3$. By [19], if $p|m$, there does not exist an elliptic curve of trace m ($q = 2$ and 3 are excluded since in those cases, $\{2\sqrt{q}\} \geq \sqrt{2}-1$). If $q = 7^3$ (thus $(m-2) = 35$) there does not exist an elliptic curve of trace $(m-2)$. Therefore, in both cases, an abelian surface of type $[-m, -m+2]$ cannot exist.
— If $\{2\sqrt{q}\} < \sqrt{2}-1$ and $p|m$, or $q = 7^3$, there exists a curve of type $[-m+1, -m+1]$: the quadratic twist of the curve of type $[m-1, m-1]$ in the proof of Th. 5.1. □

References

[1] S. Ballet, R. Rolland. Lower bounds on the class number of algebraic function fields defined over any finite field. arXiv:1103.2161
[2] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197-272.
[3] E. Howe, E. Nart, C. Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourier, Grenoble* **59** (2009), 239-289.
[4] G. Lachaud, M. Martin-Deschamps. Nombre de points des jacobiennes sur un corps fini. *Acta Arith.* **16** (1990), 329-340.
[5] K. Lauter, with an Appendix by J.-P. Serre. The maximum or minimum number of rational points on genus three curves over finite fields. *Compositio Math.* **134** (2002), 87-111.
[6] D. Maisner, E. Nart, with an Appendix by E. W. Howe. Abelian surfaces over finite fields as jacobians. *Experiment. Math.* **11** (2002), 321-337.
[7] M. Perret. Number of points of Prym varieties over finite fields. *Glasgow Math. J.* **48** (2006), 275-280.

[8] H.-G. Quebbemann. Lattices from curves over finite fields. Preprint (April 1989).
[9] J. Riordan. *Introduction to combinatorial analysis*. Wiley, New York, 1958.
[10] H.-G. Rück. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Math.* **76** (1990), 351-366.
[11] J.-P. Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris* **296** (1983), série I, 397-402.
[12] J.-P. Serre. Nombre de points des courbes algébriques sur $\mathbb{F}_q$. *Sém. de Théorie des nombres de Bordeaux* 1982/83, exp. no. 22. (Oeuvres III, no 132, 701-705).
[13] J.-P. Serre. Rational points on curves over finite fields. Lectures at Harvard University, Notes by F. Gouvea, 1985.
[14] Smyth, Christopher. *Totally positive algebraic integers of small trace*. Ann. Inst. Fourier **34** (1984), no. 3, 1–28.
[15] R. Stanley. *Enumerative combinatorics*, Vol. 2. Cambridge University Press, Cambridge, 1999.
[16] J. Tate. Classes d'isogénies de variétés abéliennes sur un corps fini (d'après T. Honda). *Sém. Bourbaki* **21** (1968/69), Exp. 352.
[17] M. Tsfasman, S. Vlăduţ, D. Nogin. *Algebraic geometric codes: basic notions*. Vol. 139, Math. Surveys and Monographs, A.M.S, 2007.
[18] S. Vlăduţ. An exhaustion bound for algebro-geometric "modular" codes. *Problemy Peredachi Informatsii* **23** (1987), no. 1, 28-41.
[19] W.C. Waterhouse. Abelian varieties over finite fields. *Ann. Sc. E.N.S.* (4), **2** (1969), 521-560.

Institut de Mathématiques de Toulon, Université du Sud Toulon-Var and Institut de Mathématiques de Luminy, CNRS/Université Aix-Marseille, France
E-mail address: aubry@iml.univ-mrs.fr

Institut de Mathématiques de Luminy, CNRS/Université Aix-Marseille, France
E-mail address: s.haloui@mat.dtu.dk

Institut de Mathématiques de Luminy, CNRS/Université Aix-Marseille, France
E-mail address: lachaud@iml.univ-mrs.fr