



**HAL**  
open science

# Number of points on abelian and Jacobian varieties over finite fields

Yves Aubry, Safia Haloui, Gilles Lachaud

► **To cite this version:**

Yves Aubry, Safia Haloui, Gilles Lachaud. Number of points on abelian and Jacobian varieties over finite fields. 2012. hal-00662352v3

**HAL Id: hal-00662352**

**<https://hal.science/hal-00662352v3>**

Preprint submitted on 2 May 2012

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# ON THE NUMBER OF POINTS ON ABELIAN AND JACOBIAN VARIETIES OVER FINITE FIELDS

YVES AUBRY, SAFIA HALOUI, AND GILLES LACHAUD

ABSTRACT. We give upper and lower bounds for 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.

## CONTENTS

1.	Introduction	1
2.	Abelian varieties	3
2.1.	Upper bounds	3
2.2.	Lower bounds	6
2.3.	Lower bound for the harmonic mean	9
2.4.	Convexity	10
3.	Jacobians	11
3.1.	Jacobians as abelian varieties	11
3.2.	Virtual zeta functions	13
3.3.	Specific bounds for Jacobians	16
3.4.	Discussing the bounds	21
4.	Jacobian surfaces	22
	References	27

## 1. INTRODUCTION

This article has roughly a threefold aim. The first is to provide a series of upper and lower bounds for the number of points on an abelian variety defined over a finite field. A simple typical result is

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

(Corollary 2.10 and 2.2). Here  $A$  is an abelian variety of dimension  $g$  defined over the field  $\mathbb{F}_q$  of  $q$  elements, and  $m$  is the integer part of  $2q^{1/2}$ . This inequality improves on

$$(q + 1 - 2q^{1/2})^g \leq |A(\mathbb{F}_q)| \leq (q + 1 + 2q^{1/2})^g,$$

which is an immediate consequence of Weil's inequality. We provide as well bounds for  $|A(\mathbb{F}_q)|$  depending on the trace of  $A$ . If, by chance,  $A$  is the Jacobian of a curve or the Prym variety of a covering of curves, the trace is easily expressed in terms of the number of rational points on the corresponding curves. We obtain two other lower bounds depending on the *harmonic mean*  $\eta = \eta(A)$  of the numbers  $q + 1 + x_i$ , namely

$$\frac{1}{\eta} = \frac{1}{g} \sum_{i=1}^g \frac{1}{q + 1 + x_i},$$

---

*Date:* May 2, 2012.

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

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

where

$$f_A(t) = \prod_{i=1}^g (t^2 + x_i t + q)$$

is the *Weil polynomial* of  $A$ . Our second aim is to obtain specific lower bounds in the special case where  $A = J_C$  is the Jacobian of a smooth, projective, absolutely irreducible algebraic curve  $C$  defined over  $\mathbb{F}_q$ . M. Martin-Deschamps and the third author proved in [7] that

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

where  $g$  is the genus of  $C$  and  $N = |C(\mathbb{F}_q)|$ . This article offers several improvements to this bound : for instance,

$$|J(\mathbb{F}_q)| \geq \left(1 - \frac{2}{q}\right) \left(q + 1 + \frac{N - (q + 1)}{g}\right)^g,$$

and also

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

The third aim is to give exact values for the maximum and the minimum number of rational points on Jacobian varieties of dimension 2, namely, to calculate, in the case  $g = 2$ , the numbers

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

where  $C$  ranges over the set of equivalence classes of smooth curves of genus  $g$  over  $\mathbb{F}_q$ . These numbers are the analogues for Jacobians of the numbers

$$N_q(g) = \max_C |C(\mathbb{F}_q)| \quad \text{and} \quad n_q(g) = \min_C |C(\mathbb{F}_q)|,$$

introduced by J.-P. Serre. One has

$$(q + 1 - m)^2 \leq j_q(2), \quad J_q(2) \leq (q + 1 + m)^2,$$

and these bounds are attained in most cases, with exceptions occurring when  $q$  is special. It is worthwhile to point out that S. Ballet and R. Rolland obtained recently [2] asymptotic lower bounds on the number of points on Jacobian varieties; these results are distinct from those presented here.

The contents of this article are as follows. Section 2 is devoted to the number of points on general abelian varieties. In § 2.1, we first prove an upper bound (Theorem 2.1) obtained by H. G. Quebbemann in the case of Jacobians, and M. Perret in the case of Prym varieties. Then we state three sharper upper bounds, depending on the defect of  $A$  or on a specific parameter  $r$ .

The lower bounds we discuss in § 2.2 are based on auxiliary results, predominantly on inequalities between classical means, and depend on the trace of  $A$ . The first one (Theorem 2.7) is based on Specht's inequality, and is symmetric to the upper bound of Theorem 2.1. Another important result is Theorem 2.9, and Corollary 2.10 gives the unconditional lower bound stated at the beginning of this introduction.

The bounds stated in Theorem 2.11 and Proposition 2.12 are expressed in terms of the harmonic mean  $\eta$ . In order to compare these bounds, we show in § 2.3 that if  $q \geq 8$ , then  $\eta \geq q + 1 - m$  (Proposition 2.13). The convexity method of Perret is used in § 2.4 to give two other bounds in Theorem 2.14 and Proposition 2.15.

We discuss Jacobians in Section 3. The previous inequalities apply to Jacobians, depending on the number of points on the related curve, and this is stated in § 3.1. The bounds for the number of points on Jacobians given in [7] depends on the identity

$$\frac{g}{\eta} |J_C(\mathbb{F}_q)| = \sum_{n=0}^{g-1} A_n + \sum_{n=0}^{g-2} q^{g-1-n} A_n,$$

where  $A_n$  is the number of positive divisors on  $C$  which are rational over  $\mathbb{F}_q$ . In § 3.2, this identity is proved in an abstract framework, free of any geometric setting (Theorem 3.5).

By using the combinatorics of the exponential formula, various inequalities for the numbers  $A_n$  are obtained in § 3.3, depending on two conditions **(B)** and **(N)** which are satisfied by Jacobians. We discuss these conditions by giving in Propositions 3.7 and 3.8 some results on the number  $B_n$ , which, in the case of Jacobians, is the number of rational prime cycles of degree  $n$  on the curve. For instance, for a curve of genus  $g$ ,

$$nB_n \geq (q^{n/4} + 1)^2((q^{n/4} - 1)^2 - 2g).$$

This leads to three new lower bounds. All of these are gathered in §3.4, where we compare them, and discuss their accuracy.

In section 4, the last one, the complete calculation of  $J_q(2)$  in Theorem 4.1 and of  $j_q(2)$  in Theorem 4.2 are worked out.

## 2. ABELIAN VARIETIES

**2.1. Upper bounds.** 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 *Weil polynomial*  $f_A(t)$  of  $A$  is the characteristic polynomial of its Frobenius endomorphism  $F_A$ . Let  $\omega_1, \dots, \omega_g, \bar{\omega}_1, \dots, \bar{\omega}_g$  be the complex roots of  $f_A(t)$ , with  $|\omega_i| = q^{1/2}$  by Weil's inequality. For  $1 \leq i \leq g$ , we put  $x_i = -(\omega_i + \bar{\omega}_i)$ , and we say that  $A$  is of *type*  $[x_1, \dots, x_g]$ . The type of  $A$  only depends on the isogeny class of  $A$ . Let

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

The integer  $\tau$  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

$$(1) \quad |A(\mathbb{F}_q)| = \prod_{i=1}^g (q + 1 + x_i)$$

since

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

Since  $|x_i| \leq 2q^{1/2}$ , one deduces from (1) the classical bounds:

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

The arithmetic-geometric inequality states that

$$(c_1 \dots c_k)^{1/k} \leq \frac{1}{k}(c_1 + \dots + c_k)$$

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 obtain the following upper bound, proved by H. G. Quebbemann [11] in the case of Jacobians, and M. Perret [10] in the case of Prym varieties:

**Theorem 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  $[x, \dots, x]$ .* □

Let  $m = [2q^{1/2}]$  where  $[\alpha]$  denotes the integer part of the real number  $\alpha$ . Using the arithmetic-geometric inequality, J.-P. Serre [14] proved that

$$(2) \quad |\tau| \leq gm,$$

hence, by Theorem 2.1:

**Corollary 2.2.** *Let  $A/\mathbb{F}_q$  be an abelian variety of dimension  $g$ . Then*

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

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

We say that  $A$  (or  $\tau$ ) has defect  $d$  if  $\tau = gm - d$ .

**Proposition 2.3.** *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 [16] 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,

$$\begin{aligned} \varphi_1 &= (-1 + \sqrt{5})/2, & \varphi_2 &= (-1 - \sqrt{5})/2, \\ \omega_i &= 1 - 4 \cos^2 \frac{i\pi}{7}, & i &= 1, 2, 3. \end{aligned}$$

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

$d$	$[x_1, \dots, x_g]$	$\beta_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  $b = q + 1 + m$ .

Now assume  $g \geq 2$ . The following result generalizes somehow Proposition 2.3. Let

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

in such a way that  $r$  is the remainder of the division of  $\tau$  by  $g$ .

**Proposition 2.4.** *If  $r = 1$  or  $r = g - 1$ , then*

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

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

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

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

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

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

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

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

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

Now choose  $k = g - r$ . Then

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

Hence, according to the arithmetic-geometric inequality,

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

where the second inequality follows from Lemma 2.5 below. To complete the proof of Proposition 2.4, it remains to establish that  $r(g-r) < g$  if and only if  $r = 1$  or  $r = g-1$ . Observe that the inequality  $r(g-r) < g$  holds in every case if  $g \leq 3$ . Now assume that  $g \geq 4$  and let

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

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  $g-2 < r_+(g) < g-1$ .  $\square$

**Lemma 2.5.** *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  $(a, \log a)$  and  $(b, \log b)$  with the weights  $g-r$  and  $r$  is

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

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

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

and the result follows from the concavity of the logarithm.  $\square$

If  $\tau$  has defect 1, then

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

and Proposition 2.4 reduces to Proposition 2.3.

**Corollary 2.6.** *If  $\tau = gm - g + 1$  (defect  $g - 1$ ), then*

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

*Proof.* Here

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

and the result follows.  $\square$

*Remark.* Smyth's Theorem [18, p. 2] asserts that if  $x$  is a totally positive algebraic integer, then with finitely many exceptions, explicitly listed,

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

From this one deduces that the conclusion of Proposition 2.4 holds true for every  $r$  if  $g \leq 7$  and if the polynomials  $x - 1$  and  $x^2 - 3x + 1$  does not divide  $f_{g-r}$ .

**2.2. Lower bounds.** The first lower bound for  $|A(\mathbb{F}_q)|$  is symmetrical to the upper bound given in Theorem 2.1, and depends on *Specht's ratio*, defined for  $h \geq 1$  as

$$S(h) = \frac{h^{1/(h-1)}}{e \log h^{1/(h-1)}}, \quad S(1) = 1.$$

It is the least upper bound of the ratio of the arithmetic mean to the geometric mean of numbers  $c_1, \dots, c_n \in [a, b]$  with  $0 < a < b$  and  $h = b/a > 1$ , see [19], [5]. That is, the following *Specht's inequality* holds:

$$\frac{c_1 + \dots + c_n}{n} \leq S(h)(c_1 \dots c_n)^{1/n},$$

as a reverse of the arithmetic-geometric inequality.

**Theorem 2.7.** *If  $q \geq 2$ , let  $M(q) = 1/S(h(q))$ , where  $S(h)$  is Specht's ratio and*

$$h(q) = \left( \frac{q^{1/2} + 1}{q^{1/2} - 1} \right)^2.$$

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

(i) *We have*

$$|A(\mathbb{F}_q)| \geq M(q)^g \left( q + 1 + \frac{\tau}{g} \right)^g.$$

(ii) *In particular,*

$$|A(\mathbb{F}_q)| \geq \left(1 - \frac{2}{q}\right)^g \left( q + 1 + \frac{\tau}{g} \right)^g,$$

*where  $1 - 2/q$  has to be replaced by 0.261 if  $q = 2$ .* □

*Proof.* According to (1), we apply Specht's inequality with  $c_i = q + 1 + x_i$ ,  $1 \leq i \leq g$ . Then

$$h = h(q), \quad c_1 \dots c_g = |A(\mathbb{F}_q)|, \quad \frac{c_1 + \dots + c_g}{g} = q + 1 + \frac{\tau}{g},$$

and this gives (i). The function  $M(q)$  is increasing, and  $M(2) = 0.261 \dots$ . Also,

$$M(q) = 1 - \frac{2}{q} + \frac{10}{9q^2} + O(q^{-3}) \quad \text{if } q \rightarrow \infty,$$

and one checks that

$$M(q) \geq 1 - \frac{2}{q} \quad \text{if } q \geq 2.$$

Hence, (ii) follows from (i). □

Theorems 2.1 and 2.7(ii) are summarized in the relation

$$(3) \quad \left(1 - \frac{2}{q}\right) \left( q + 1 + \frac{\tau}{g} \right) \leq |A(\mathbb{F}_q)|^{1/g} \leq q + 1 + \frac{\tau}{g}.$$

It is natural to ask whether  $|A(\mathbb{F}_q)|$  has a lower bound symmetrical to Corollary 2.2, and the answer turns out to be in the affirmative.

**Lemma 2.8.** Let  $\lambda_1, \dots, \lambda_n$  be non-negative real numbers, and

$$F(T) = \prod_{i=1}^n (T + \lambda_i) \in \mathbb{R}[T].$$

Let

$$\pi = \left( \prod_{i=1}^n \lambda_i \right)^{1/n}, \quad \sigma = \frac{1}{n} \sum_{i=1}^n \lambda_i,$$

and assume that  $t \geq 0$  and  $0 \leq \lambda \leq \pi$ .

(i) We have

$$F(t) \geq (t + \lambda)^n + n(\sigma - \lambda)t^{n-1},$$

and in particular  $F(t) \geq (t + \lambda)^n$ .

(ii) Moreover

$$F'(t) \geq n(t + \lambda)^{n-1} + n(n-1)(\sigma - \lambda)t^{n-2},$$

and in particular  $F'(t) \geq n(t + \lambda)^{n-1}$ .

These inequalities are strict unless  $\lambda_1 = \dots = \lambda_n$  and  $\lambda = \pi$ .

*Proof.* We exclude the case where  $\lambda_1 = \dots = \lambda_n$ . Let  $\mathfrak{P}_k$  be the set of subsets of  $\{1, \dots, n\}$  with  $k$  elements, and put

$$p_k = \prod_{H \in \mathfrak{P}_k} \prod_{i \in H} \lambda_i.$$

For  $1 \leq i \leq n$ , the coefficient of  $\lambda_i$  in  $p_k$  is equal to the number of subsets in  $\mathfrak{P}_k$  containing  $i$ , and this number is equal to  $\binom{n-1}{k-1}$ . Therefore

$$p_k = \prod_{i=1}^n \lambda_i^{\binom{n-1}{k-1}} = \pi^{\binom{n-1}{k-1}n} \geq \lambda^{\binom{n-1}{k-1}n}, \quad \text{hence } p_k^{1/\binom{n}{k}} \geq \lambda^k.$$

For  $0 \leq k \leq n$ , let

$$s_k = \sum_{H \in \mathfrak{P}_k} \prod_{i \in H} \lambda_i$$

be the *elementary symmetric function* of degree  $k$  in the numbers  $\lambda_1, \dots, \lambda_n$ . The arithmetic-geometric inequality implies

$$p_k^{1/\binom{n}{k}} < \binom{n}{k}^{-1} s_k, \quad \text{hence } \binom{n}{k} \lambda^k < s_k.$$

Putting  $s_0 = 1$ , and since  $s_1 = n\sigma$ , we obtain

$$\begin{aligned} F(t) &= \sum_{k=0}^n s_k t^{n-k} = \sum_{k=0}^n \binom{n}{k} \lambda^k t^{n-k} + \sum_{k=0}^n \left( s_k - \binom{n}{k} \lambda^k \right) t^{n-k} \\ &> (t + \lambda)^n + n(\sigma - \lambda)t^{n-1}, \end{aligned}$$

which proves the first inequality of (i), and of course the second, since  $\sigma - \lambda \geq 0$ . Also,

$$F'(t) = \sum_{k=0}^{n-1} (n-k) s_k t^{n-1-k},$$

and (ii) is proved along the lines of the proof of (i). □

*Remark.* With the notation of Lemma 2.8, the basic inequality

$$F(t) \geq (t + \lambda)^n$$



is just a consequence of the following Hölder's inequality, where  $x_1, \dots, x_n$  and  $y_1, \dots, y_n$  are non negative real numbers:

$$\prod_{i=1}^n (x_i + y_i) > \left( \prod_{i=1}^n x_i^{1/n} + \prod_{i=1}^n y_i^{1/n} \right)^n,$$

unless  $x_1 = \dots = x_n$  and  $y_1 = \dots = y_n$ .

The *real Weil polynomial* of  $A$  is

$$h_A(t) = \prod_{i=1}^g (t + x_i).$$

Then  $f_A(t) = t^g h_A(t + qt^{-1})$  and  $|A(\mathbb{F}_q)| = h_A(q + 1)$ .

**Theorem 2.9.** *Let  $A/\mathbb{F}_q$  be an abelian variety of dimension  $g$  and trace  $-\tau$ . Then*

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

*Proof.* We apply Lemma 2.8 to the polynomial

$$F(t) = h_A(t + m + 1) = \prod_{i=1}^g (t + m + 1 + x_i).$$

Here  $\lambda_i = m + 1 + x_i$ , and

$$\pi = \prod_{i=1}^g (m + 1 + x_i)^{1/g} > 0.$$

Then  $\pi^g \in \mathbb{Z}$ , since this number is left invariant by  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ , hence  $\pi \geq 1$ . Now apply Lemma 2.8(i) with  $\lambda = 1$  and  $t = q - m$ . We get

$$h_A(q + 1) = F(q - m) \geq (q - m + 1)^g + g(q - m)^{g-1}(\sigma - 1),$$

and the result follows by observing that  $g(\sigma - 1) = gm + \tau$ .  $\square$

*Remark.* For  $g = 1$ , the inequality of Theorem 2.9 is an equality (if  $q \leq 4$  then  $q - m = 0$  and we use the convention  $0^0 = 1$ ).

Serre's inequality (2) implies  $gm + \tau \geq 0$ , hence :

**Corollary 2.10.** *Let  $A/\mathbb{F}_q$  be an abelian variety of dimension  $g$ . Then*

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

*with equality if and only if  $A$  is of type  $[-m, \dots, -m]$ .*  $\square$

The *harmonic mean*  $\eta = \eta(A)$  of the numbers  $q + 1 + x_i$  is defined by

$$\frac{1}{\eta} = \frac{1}{g} \sum_{i=1}^g \frac{1}{q + 1 + x_i},$$

hence

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

The classical inequality between harmonic and geometric means leads to:

**Theorem 2.11.** *Let  $A/\mathbb{F}_q$  be an abelian variety of dimension  $g$ . Then*

$$|A(\mathbb{F}_q)| \geq \eta^g. \quad \square$$

The next proposition is similar to Theorem 2.9.

**Proposition 2.12.** *Let  $A/\mathbb{F}_q$  be an abelian variety of dimension  $g$ . Then*

$$|A(\mathbb{F}_q)| \geq \eta(q + 1 - m)^{g-1} + \eta \frac{g-1}{g} (q - m)^{g-2} (gm + \tau).$$

*Proof.* Since

$$\frac{h'_A(t)}{h_A(t)} = \sum_{i=1}^g \frac{1}{t + x_i},$$

we have

$$|A(\mathbb{F}_q)| = \frac{\eta}{g} h'_A(q + 1).$$

By applying Lemma 2.8(ii) with  $F(t)$  as in the proof of Theorem 2.9, we obtain

$$h'_A(q + 1) \geq g(q + 1 - m)^{g-1} + (g - 1)(q - m)^{g-2}(gm + \tau).$$

leading to the second inequality.  $\square$

**2.3. Lower bound for the harmonic mean.** In order to compare the results of the previous section, a lower bound for  $\eta$  is needed. The proof of the forthcoming proposition makes use of a simple observation, following C. Smyth [18] and J.-P. Serre [17]: let

$$P(t) = \prod_{i=1}^g (t - \alpha_i) \in \mathbb{Z}[t]$$

and  $F \in \mathbb{Z}[t]$ . The resultant  $\text{res}(P, F)$  is an integer, and if  $\text{res}(P, F) \neq 0$ , then

$$(4) \quad \sum_{i=1}^g \log|F(\alpha_i)| = \log|\text{res}(P, F)| \geq 0.$$

**Proposition 2.13.** *If  $q \geq 8$ , then*

$$\eta(A) \geq q + 1 - m.$$

*Proof.* (a) Assume  $c > 2$ . If  $-1 < t \leq c(c - 2)$ , then

$$\log(1 + t) \leq \frac{ct}{c + t}.$$

Indeed, if

$$f(t) = \frac{ct}{c + t} - \log(1 + t)$$

then

$$f'(t) = \frac{t(c^2 - 2c - t)}{(1 + t)(c + t)^2}.$$

Thus  $f'(t) \leq 0$  if  $-1 \leq t < 0$  and  $f'(t) \geq 0$  if  $0 \leq t \leq c(c - 2)$ . This proves our statement, since  $f(-1) = +\infty$  and  $f(0) = 0$ .

(b) If  $q \geq 8$ , and if  $|x| \leq m + 1$ , then

$$\log(x + m + 1) \leq (q + 1 - m) \left(1 - \frac{q + 1 - m}{q + 1 + x}\right).$$

Let  $c = q + 1 - m$ . If  $q > 5$ , then  $q + 1 - m > 2$ , and if  $q \geq 11$ , then

$$2m + 1 \leq (q + 1 - m)(q - 1 - m).$$

Putting  $t = x + m$ , the hypotheses of (a) are satisfied, and

$$\log(x + m + 1) \leq \frac{(q + 1 - m)(x + m)}{q + 1 + x} = (q + 1 - m) \left(1 - \frac{q + 1 - m}{q + 1 + x}\right).$$

(c) Now use (4) with  $F(t) = t + m + 1$  and  $P(t) = (-1)^g h_A(-t)$ . Obviously  $\text{res}(P, F) \neq 0$ , hence

$$\sum_{i=1}^g \log(x_i + m + 1) \geq 0.$$

One deduces from (b) that

$$\sum_{i=1}^g \left(1 - \frac{q+1-m}{q+1+x_i}\right) \geq 0, \quad \text{hence} \quad (q+1-m) \sum_{i=1}^g \frac{1}{q+1+x_i} \leq g.$$

Finally, the conclusion is obvious if  $q = 9$  (a square), and verified by brute force if  $q = 8$ .  $\square$

*Remarks.* (i) Proposition 2.13 shows that Theorem 2.11 is stronger than Theorem 2.10 if  $q \geq 8$ . (ii) It can happen that  $\eta < q+1-m$ . Take  $q = 2$  for instance. As explained in section 4, there is an abelian surface  $A/\mathbb{F}_2$  with

$$f_A(t) = t^4 - t^3 - 2t + 4, \quad \text{and} \quad |A(\mathbb{F}_2)| = 2.$$

Hence,  $A$  is of type  $[x_+, x_-]$ , with  $x_{\pm} = (-1 \pm \sqrt{17})/2$ , and  $\eta = 4/5$ , but  $q+1-m = 1$ .

**2.4. Convexity.** Another way to obtain lower bounds for  $|A(\mathbb{F}_q)|$  is to use convexity methods as performed by M. Perret. We give the statement of [10, Th. 3], slightly rectified.

**Theorem 2.14.** *Let  $A/\mathbb{F}_q$  be an abelian variety of dimension  $g$  and trace  $-\tau$ . Then*

$$|A(\mathbb{F}_q)| \geq (q-1)^g \left(\frac{q^{1/2}+1}{q^{1/2}-1}\right)^{\omega-2\delta}, \quad \text{where } \omega = \frac{\tau}{2q^{1/2}},$$

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

$$\left\{ (x_1, \dots, x_g) \in [-2q^{1/2}, 2q^{1/2}]^g \mid x_1 + \dots + x_g = \tau \right\}.$$

Let

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

The problem reduces to minimizing the function

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

on the polytope

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

The set of points in  $P$  where  $F$  is minimal is invariant under permutations. Since  $F$  is strictly concave, the points in this set are vertices of  $P$ . But at most one of the coordinates of a vertex of  $P$  is different from  $\pm 1$ . 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 respective numbers of occurrences of 1 and of  $-1$  in  $\gamma$ , and set  $\delta = 1$  if  $\beta$  is in the open interval  $(-1, 1)$  and 0 otherwise. Then

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

and adding these equations, it follows that if  $\delta = 0$  then  $g + \omega$  is an even integer. The converse is true: if  $\delta = 1$  then  $\beta$  is in the open interval  $(-1, 1)$ , and either  $\beta \neq 0$  and  $g + \omega$  is not an integer, or  $\beta = 0$  and  $g + \omega = 2u + 1$ . Hence,

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

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

It is possible to improve Theorem 2.14 by computing more explicitly the coordinates of the extremal points of  $P$  in the above proof.

**Proposition 2.15.** *Let*

$$r = \left\lfloor \frac{g + [\omega]}{2} \right\rfloor, \quad s = \left\lfloor \frac{g - 1 - [\omega]}{2} \right\rfloor, \quad \text{where } \omega = \frac{\tau}{2q^{1/2}}.$$

Then

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

*Proof.* We keep the notation and results from the proof of Theorem 2.14. If  $\gamma \neq (1, \dots, 1)$ , we denote by  $r$  and  $s$  the number of occurrences of 1 and of  $-1$  respectively in  $\gamma$  but now, without eventually counting  $\beta$ . Then  $r - s = \omega - \beta$ , thus  $\beta$  must be equal to  $\{\omega\} = \omega - [\omega]$  or  $\{\omega\} - 1$  (after perhaps a permutation of  $\beta$  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  $r = g$  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

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

Proceeding as in the proof of Theorem 2.14, we obtain

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

Then

$$|A(\mathbb{F}_q)| \geq (q - 1)^{g-1} \left( q + 1 + 2q^{1/2}(\{\omega\} - \epsilon) \right) \left( \frac{q^{1/2} + 1}{q^{1/2} - 1} \right)^{\frac{[\omega]+\epsilon}{2}}$$

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

*Remark.* If  $q$  is not a square, the bound of Proposition 2.15 is reached only if  $r = s$  (which implies that  $|\tau| < 2q^{1/2}$ ) and  $\tau$  is the trace of some elliptic curve. If  $q$  is a square, this bound is not reached only if  $\tau - 2(r - s)q^{1/2}$  is not the trace of an elliptic curve (in particular, it is reached if  $\tau$  is coprime to  $p$ ).

### 3. JACOBIANS

**3.1. Jacobians as abelian varieties.** Let  $C$  denotes a nonsingular, projective, absolutely irreducible curve defined over  $\mathbb{F}_q$ , with Jacobian  $J_C$ . 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  $g$ . Theorem 2.10 implies

$$(q + 1 - m)^g \leq j_q(g) \leq |J_C(\mathbb{F}_q)| \leq J_q(g) \leq (q + 1 + m)^g.$$

Let  $N = |C(\mathbb{F}_q)|$  be the number of  $\mathbb{F}_q$ -rational points on  $C$ . If  $J_C$  has trace  $-\tau$ , then  $N = q + 1 + \tau$ , and (3) implies

$$\left(1 - \frac{2}{q}\right) \left(q + 1 + \frac{N - (q + 1)}{g}\right)^g \leq |J_C(\mathbb{F}_q)| \leq \left(q + 1 + \frac{N - (q + 1)}{g}\right)^g.$$

Hence,

$$\left(1 - \frac{2}{q}\right) \left(q + 1 + \frac{N_q(g) - (q + 1)}{g}\right)^g \leq J_q(g) \leq \left(q + 1 + \frac{N_q(g) - (q + 1)}{g}\right)^g,$$

where  $N_q(g)$  stands for the maximum number of rational points on a curve defined over  $\mathbb{F}_q$  of genus  $g$ . The quantity  $J_q(g)$  has the following asymptotic behaviour. Define, as usual,

$$A(q) = \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g}.$$

The preceding inequalities imply

$$\left(1 - \frac{2}{q}\right)(q + 1 + A(q)) \leq \limsup J_q(g)^{1/g} \leq q + 1 + A(q).$$

On the one hand, the Drinfeld-Vlăduț upper bound [23, p. 146]

$$A(q) \leq q^{1/2} - 1$$

implies

$$\limsup_{g \rightarrow \infty} (J_q(g))^{1/g} \leq q + q^{1/2}$$

(the Weil bound would only give the upper bound  $q + 1 + 2q^{1/2}$ ). On the other hand, S. Vlăduț has proved [24] that if  $q$  is a square, then

$$q\left(\frac{q}{q-1}\right)^{q^{1/2}-1} \leq \limsup_{g \rightarrow \infty} (J_q(g))^{1/g}.$$

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

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

*Remark.* Some observations are worthwhile to point out on the relationship between  $N_q(g)$  and  $J_q(g)$ . The number of points on the Jacobian of a maximal curve, that is, with  $N_q(g)$  points, does not necessarily reach  $J_q(g)$ . For instance, J.-P. Serre [16, p. Se47] has shown that there exist two curves of genus 2 over  $\mathbb{F}_3$  with  $N_3(2) = 8$  points whose Jacobians have 35 points and 36 points respectively.

We shall see in Section 4 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 remain true if  $g > 2$ ). A curve reaching the Serre-Weil bound (i.e. with  $q + 1 + m$  points) has type  $[m, \dots, m]$  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.

We record the consequences for Jacobians of the results of section 2. Theorem 2.7(i) implies, with  $M(q)$  as defined there:

**Proposition 3.1.** *If  $C$  is a curve of genus  $g$  over  $\mathbb{F}_q$  as above, then*

$$(I) \quad |J_C(\mathbb{F}_q)| \geq M(q)^g \left( q + 1 + \frac{N - (q + 1)}{g} \right)^g.$$

Proposition 2.9 implies

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

and Proposition 2.15 leads to:

**Proposition 3.2.** *If  $C$  is a curve of genus  $g$  over  $\mathbb{F}_q$  as above, then*

$$(II) \quad |J_C(\mathbb{F}_q)| \geq (N - 2(r - s)q^{1/2})(q + 1 + 2q^{1/2})^r (q + 1 - 2q^{1/2})^s,$$

with

$$r = \left\lfloor \frac{g + [\omega]}{2} \right\rfloor, \quad s = \left\lfloor \frac{g - 1 - [\omega]}{2} \right\rfloor, \quad \text{where } \omega = \frac{N - q - 1}{2q^{1/2}}. \quad \square$$

**3.2. Virtual zeta functions.** The usual numerical sequences associated to a curve over  $\mathbb{F}_q$  (number of points, number of effective and prime divisors) occur in expressions involving the numerator of its zeta function. These sequences are defined and their main properties are obtained here by taking as starting point a polynomial satisfying suitable conditions, without any geometric reference. If  $A$  is an abelian variety of dimension  $g$  over  $\mathbb{F}_q$ , with characteristic polynomial  $f_A(t)$ , the reciprocal Weil polynomial  $P(t) = P_A(t) = t^{2g} f_A(t^{-1})$  fulfills the following conditions :

(i)  $P(t)$  satisfies the functional equation

$$P(t) = q^g t^{2g} P\left(\frac{1}{qt}\right),$$

(ii)  $P(0) = 1$  and  $P(1) \neq 0$ .

The inverse roots of  $P$  have modulus  $q^{1/2}$ , but we do not need this condition now. Condition (i) means that if

$$P(t) = \sum_{n=0}^{2g} a_n t^n$$

then  $a_{2g-n} = q^{g-n} a_n$  for  $0 \leq n \leq 2g$ , in other words the sequence  $q^{-n/2} a_n$  is *palindromic*. This condition implies that the possible multiplicity of  $\pm q^{1/2}$  is even, as shown by H. Stichtenoth in the proof of [21, Th. 5.1.15(e)]. Now, let  $q \in \mathbb{N}$  with  $q \geq 2$ , and denote by  $\mathbf{P}_g(q)$  the set of polynomials of degree  $2g$  in  $\mathbb{Z}[t]$  satisfying (i) and (ii). If  $P \in \mathbf{P}_g(q)$ , the *virtual zeta function* with numerator  $P$  is the power series

$$(5) \quad Z(t) = Z_P(t) = \frac{P(t)}{(1-t)(1-qt)} \in \mathbb{Z}[[t]],$$

which is convergent if  $|t| < q^{-1}$ . For  $n \geq 0$ , define  $A_n = A_n(P) \in \mathbb{Z}$  and  $N_n = N_n(P) \in \mathbb{Q}$  as the coefficients of the power series

$$(6) \quad Z(t) = \sum_{n=0}^{\infty} A_n t^n, \quad \log Z(t) = \sum_{n=1}^{\infty} N_n \frac{t^n}{n},$$

and put

$$B_n = B_n(P) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) N_d \in \mathbb{Q},$$

where  $\mu$  is the Möbius function. The Möbius inversion formula implies

$$(7) \quad N_n = \sum_{d|n} dB_d.$$

We recall now a result of Schur [13]:

**Lemma 3.3.** *Let  $P \in \mathbf{P}_g(q)$ . With the previous notation:*

(i) *We have*

$$Z(t) = \prod_{n=1}^{\infty} (1-t^n)^{-B_n}.$$

(ii) *The numbers  $B_n$  and  $N_n$  are in  $\mathbb{Z}$  for any  $n \geq 1$ .*

(iii) *If  $n \geq 1$ , then*

$$(8) \quad A_n = \prod_{b \in \mathcal{P}_n} \prod_{i=1}^n \binom{B_i + b_i - 1}{b_i},$$

*with*

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

*Proof.* First, (i) is a consequence of (7). 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

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

are the *generalized binomial coefficients*, we get (iii) from (i) by comparison of the coefficients of these power series. We prove (ii) by induction. First, (i) implies  $A_1 = B_1$ , and also

$$Z(t) \prod_{i=1}^{n-1} (1-t^i)^{B_i} = \prod_{i=n}^{\infty} (1-t^i)^{-B_i} = 1 + B_n t^n \pmod{t^{n+1}}.$$

If  $B_i \in \mathbb{Z}$  for  $1 \leq i \leq n-1$ , the left hand side is a power series with coefficients in  $\mathbb{Z}$ , and in particular the coefficient of  $t^n$ . Then  $N_n \in \mathbb{Z}$  by (7).  $\square$

For  $n \in \mathbb{Z}$  we define  $\pi_n = (q^{n+1} - 1)/(q - 1)$ , in such a way that  $\pi_{-1} = 0$  and

$$\frac{1}{(1-t)(1-qt)} = \sum_{n=0}^{\infty} \pi_n t^n.$$

The definition of  $Z(t)$  implies

$$(9) \quad A_n = \sum_{k=0}^{\min(n, 2g)} a_k \pi_{n-k}, \quad n \geq 0.$$

**Lemma 3.4.** *Let  $P \in \mathbf{P}_g(q)$ , and assume  $g \geq 2$ . If  $n \in \mathbb{Z}$ , then*

$$(10) \quad A_n = q^{n+1-g} A_{2g-2-n} + P(1) \pi_{n-g},$$

*assuming that  $A_n = 0$  si  $n < 0$ . In particular,*

$$(11) \quad A_n = P(1) \pi_{n-g}, \quad n \geq 2g-1.$$

*Proof.* Since (10) is invariant by  $n \mapsto 2g - n - 2$ , and trivial if  $n = g - 1$ , it is sufficient to prove (10) if  $n \geq g$ . This is performed in three steps. (a) If  $n \in \mathbb{Z}$ , then

$$\begin{aligned} (q-1) \sum_{k=0}^{2g} a_k \pi_{n-k} &= \sum_{k=0}^{2g} a_k (q^{n-k+1} - 1) = q^{n+1} \sum_{k=0}^{2g} a_k q^{-k} - \sum_{k=0}^{2g} a_k \\ &= q^{n+1} P(q^{-1}) - P(1) = (q^{n+1-g} - 1) P(1) = (q-1) P(1) \pi_{n-g}, \end{aligned}$$

since  $P(q^{-1}) = q^{-g} P(1)$ , hence

$$\sum_{k=0}^{2g} a_k \pi_{n-k} = P(1) \pi_{n-g}.$$

This proves (11), since the left hand side is equal to  $A_n$  (if  $n = 2g - 1$ , notice that the term with subscript  $k = 2g$  is zero), and  $A_{2g-2-n} = 0$ , since  $2g - 2 - n \leq -1$ . (b) If  $0 \leq n \leq 2g - 2$ , then

$$\begin{aligned} q^{n+1-g} A_{2g-n-2} &= \frac{q^{n+1-g}}{q-1} \sum_{k=0}^{2g-n-2} a_k (q^{2g-n-1-k} - 1) \\ &= \frac{-1}{q-1} \sum_{k=0}^{2g-n-2} a_k q^{g-k} (q^{n-2g+k+1} - 1) = - \sum_{k=0}^{2g-n-2} a_{2g-k} \pi_{n-2g+k} = - \sum_{k=n+2}^{2g} a_k \pi_{n-k}. \end{aligned}$$

(c) If  $0 \leq n \leq 2g - 2$ , we deduce from (a) :

$$A_n = \sum_{k=0}^n a_k \pi_{n-k} = \sum_{k=0}^{2g} a_k \pi_{n-k} - a_{n+1} \pi_{-1} - \sum_{k=n+2}^{2g} a_k \pi_{n-k}.$$

The first term is equal to  $P(1)\pi_{n-g}$  by (a), the second is zero, and the third is equal to  $q^{n+1-g}A_{2g-n-2}$  by (b).  $\square$

As in the case of the zeta function of a curve [7], we deduce from Lemma 3.4 that if  $g \geq 2$ , then

$$(12) \quad \sum_{n=0}^{g-1} A_n t^n + \sum_{n=0}^{g-2} q^{g-1-n} A_n t^{2g-2-n} = Z_P(t) - \frac{P(1)t^g}{(1-t)(1-qt)}.$$

In particular, if  $t = q^{-1/2}$ ,

$$(13) \quad A_{g-1} + 2q^{(g-1)/2} \sum_{n=0}^{g-2} A_n q^{-n/2} = q^{(g-1)/2} Z_P(q^{-1/2}) + \frac{P(1)}{(q^{1/2} - 1)^2}.$$

If  $P \in \mathbf{P}_g(q)$ , the map  $\omega \mapsto q/\omega$  is a permutation of the inverse roots of  $P$ , and we order them in a sequence  $(\omega_i)_{1 \leq i \leq 2g}$  such that  $\omega_{g+i} = q/\omega_i$  for  $1 \leq i \leq g$ . We put

$$x_i = -(\omega_i + \frac{q}{\omega_i}), \quad 1 \leq i \leq g.$$

As in § 2.2, we define  $\eta = \eta(P) \in \mathbb{Q}$  by

$$\frac{1}{\eta} = \frac{1}{g} \sum_{i=1}^g \frac{1}{q+1+x_i}.$$

Since  $P(1) \neq 0$ , we are sure that  $q+1+x_i \neq 0$ . As in the case of the zeta function of a curve [7], the evaluation at  $t = 1$  of (12) leads to

**Theorem 3.5.** *Assume  $g \geq 2$ . With notation as above, if  $P \in \mathbf{P}_g(q)$ , then*

$$\frac{g}{\eta} P(1) = \sum_{n=0}^{g-1} A_n + \sum_{n=0}^{g-2} q^{g-1-n} A_n. \quad \square$$

We recall now the *exponential formula*, see R.P. Stanley [20], which goes back to Euler. Let  $\mathbf{y} = (y_n)_{n \in \mathbb{N}}$  be a sequence of indeterminates. To an element  $b = (b_1, \dots, b_n) \in \mathbb{N}^n$  one associates the monomial  $\mathbf{y}^b = y_1^{b_1} \dots y_n^{b_n}$  in the ring  $\mathbb{Q}[[\mathbf{y}]]$ . Then

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

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

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

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

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

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

$$\exp\left(\sum_{n=1}^{+\infty} y_n \frac{t^n}{n}\right) = \sum_{n=0}^{+\infty} C_n(\mathbf{y}) t^n.$$



The coefficients of  $C_n(\mathbf{y})$  are natural numbers, since

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

where the summation is over the symmetric group  $\mathfrak{S}_n$ , where  $\beta(\sigma) = (b_1(\sigma), \dots, b_n(\sigma))$  and  $b_k(\sigma)$  is the number of cycles of length  $k$  in the cycle decomposition of  $\sigma$  as a product of disjoint cycles. Now come back to the zeta function  $Z_P(t)$  of a polynomial  $P \in \mathbf{P}_g(q)$ . From (6), we deduce

$$(14) \quad A_n = \mathcal{C}_n(N_1, \dots, N_n).$$

**3.3. Specific bounds for Jacobians.** All the results of § 3.2 apply if we take for  $P$  the reciprocal Weil polynomial  $P_A$  of an abelian variety  $A$  over  $\mathbb{F}_q$ , and  $|A(\mathbb{F}_q)| = P_A(1)$ . We put

$$Z_A(t) = Z_P(t), \quad A_n(A) = A_n(P), \quad B_n(A) = B_n(P), \quad N_n(A) = N_n(P)$$

( $N_n(A)$  should not be confused with  $|A(\mathbb{F}_{q^n})|$ ). If  $A$  is of dimension  $g$  and trace  $-\tau$ , then

$$P_A(t) = \sum_{n=0}^{2g} a_n t^n, \quad |a_n| \leq \binom{2g}{n} q^{n/2}, \quad a_1 = \tau.$$

We deduce from (9) that, roughly speaking, if  $q$  is large with respect to  $g$ , then

$$(15) \quad A_n = \pi_n + \pi_{n-1}\tau + O(q^{n-1}) = q^n + q^{n-1}\tau + O(q^{n-1}),$$

where the involved constants depends only on  $n$  and  $g$ . Now consider a curve  $C$  over  $\mathbb{F}_q$  with Jacobian  $J$  as above, and take  $P = P_J$ . Then  $Z_J(t) = Z_C(t)$  is the zeta function of  $C$ . Moreover,  $A_n$  and  $B_n$  are respectively the number of effective and prime rational divisors of degree  $n$  of  $C$ , and  $N_n = |C(\mathbb{F}_{q^n})|$ . We record for future use that in this case the following conditions hold:

$$(B) \quad B_n \geq 0 \quad \text{for } 1 \leq n \leq 2g,$$

$$(N) \quad N_n \geq N_1 \geq 0 \quad \text{for } 1 \leq n \leq 2g.$$

The reality is that these conditions hold for any  $n \geq 1$ , and more precisely  $N_n \geq N_d$  if  $d|n$ . The Jacobian of a curve satisfies (B) and (N), unlike a general abelian variety. Notice that (B) is stronger than (N), since if (B) holds, one deduces from (7):

$$nB_n \leq N_n - N_1 \quad \text{for } n \geq 2.$$

We discuss below some lower bounds for  $N_n$  and  $B_n$  which are valid for any abelian variety. The results show that (B) and (N) can be peculiar to Jacobians only if  $g$  is sufficiently large with respect to  $q$ .

**Lemma 3.6.** *Let  $A$  be an abelian variety of dimension  $g \geq 1$  over  $\mathbb{F}_q$ . If  $g \leq q/m$ , then  $N_1 = B_1 \geq 1$ . If*

$$g \leq \frac{q - q^{1/2}}{2}, \quad \text{then } N_n \geq N_1 \quad \text{for } n \geq 1,$$

and, hence,  $B_n \geq 0$  if  $n$  is prime.

*Proof.* The first statement comes from Serre's inequality. By Weil's inequality,  $N_n - N_1 \geq f_q(g)$ , with

$$f_q(g) = q^n - q - 2g(q^{n/2} + q^{1/2}),$$

and  $g \mapsto f_q(g)$  is decreasing. If  $g \leq g_0 = (q - q^{1/2})/2$ , then

$$f_q(g) \geq f_q(g_0) = (q^{n/2} + q^{1/2})(q^{n/2} - q),$$

hence,  $f_q(g) \geq 0$  if  $n \geq 2$ . □

The following two propositions improve some results of N. Elkies and al. [4, Lem. 2.1(i)].

**Proposition 3.7.** *Let  $A$  be an abelian variety of dimension  $g \geq 1$  over  $\mathbb{F}_q$ . If  $n \geq 2$ , then*

$$|nB_n - q^n| \leq (2g + 2)q^{n/2} + 4gq^{n/4} - (4g + 2),$$

and

$$nB_n \geq (q^{n/4} + 1)^2((q^{n/4} - 1)^2 - 2g).$$

*Proof.* Since

$$N_n = q^n + 1 + \tau_n, \quad \text{where} \quad \tau_n = - \sum_{i=1}^g (\omega_i^n + \bar{\omega}_i^n),$$

we find

$$\begin{aligned} nB_n &= \sum_{d|n} \mu\left(\frac{n}{d}\right)(q^d + 1 + \tau_d) = \sum_{d|n} \mu\left(\frac{n}{d}\right)q^d + 0 + \sum_{d|n} \mu\left(\frac{n}{d}\right)\tau_d \\ |nB_n - q^n| &\leq \sum_{d|n, d < n} |\mu\left(\frac{n}{d}\right)|q^d + \sum_{d|n} |\mu\left(\frac{n}{d}\right)| |\tau_d| \\ &\leq \sum_{d|n, d < n} |\mu\left(\frac{n}{d}\right)|q^d + 2g \sum_{d|n} q^{d/2} \leq 2gq^{n/2} + \sum_{d|n, d < n} (q^d + 2gq^{d/2}). \end{aligned}$$

Since  $q/(q-1) \leq 2$ , we have

$$\sum_{d|n, d < n} q^d \leq q + q^2 + \dots + q^{[n/2]} = \frac{q^{[n/2]+1} - 1}{q - 1} - 1 \leq \frac{q}{q-1}(q^{n/2} - 1) \leq 2q^{n/2} - 2,$$

and

$$\sum_{d|n, d < n} (q^d + 2gq^{d/2}) \leq 2q^{n/2} + 4gq^{n/4} - (4g + 2).$$

This implies the first statement, and hence,  $nB_n \geq F(q^{n/4})$ , where

$$\begin{aligned} F(x) &= x^4 - (2g + 2)x^2 - 4gx + 4g + 2 = G(x) + 6g + 1, \\ G(x) &= (x + 1)^2((x - 1)^2 - 2g). \end{aligned}$$

Since  $F(x) > G(x)$  for any real number  $x$ , the second statement follows.  $\square$

**Proposition 3.8.** *Let  $A$  be an abelian variety of dimension  $g \geq 2$  over  $\mathbb{F}_q$ , and let  $n \geq 2$ .*

(i) *If  $n > 4 \log_q(1 + (2g)^{1/2})$ , that is, if*

$$g < \frac{(q^{n/4} - 1)^2}{2}, \quad \text{then} \quad B_n \geq 1.$$

(ii) *If*

$$g \leq \frac{q - q^{1/2}}{2}, \quad \text{then} \quad B_n \geq 0.$$

(iii) *If  $n \geq g$ , then  $B_n \geq 1$ , unless  $2 \leq g \leq 9$  and  $q \leq 5$ .*

(iv) *If  $n \geq 2g$ , then  $B_n \geq 1$ , unless  $2 \leq g \leq 3$  and  $q = 2$ . If so,  $B_n \geq 1$  if  $n \geq 2g + 1$ .*

*Proof.* The second statement of Proposition 3.7 implies (i), since  $B_n \in \mathbb{Z}$ . In the proof of (ii), we can assume  $n \geq 4$ , since Lemma 3.6 implies  $B_2 \geq 0$  and  $B_3 \geq 0$ . But  $q - q^{1/2} < (q^{n/4} - 1)^2$  if  $n \geq 4$ , and (i) implies (ii). Let

$$f_q(g) = 4 \log_q(1 + (2g)^{1/2}).$$

Then  $q \mapsto f_q(g)$  is decreasing, and  $g \mapsto f_q(g)$  is increasing. If  $g \geq 10$ , then  $g > f_2(g)$  and (i) implies  $B_n \geq 1$  for every  $n \geq g$ . On the other hand, if  $g \geq 3$  and  $q \geq 7$ , then  $g > f_7(g)$  as well. It is easy to see that a ‘‘strict’’ version of (ii) holds, namely, if  $2g < q - q^{1/2}$ , and in particular if  $g = 2$  and  $q \geq 7$ , then  $B_n > 0$  for every  $n \geq 2$ . This proves (iii). If  $g \geq 4$ , then  $2g > f_2(g)$  and (i) implies that  $B_n \geq 1$  for every  $n \geq g$ . On the other hand, if  $g \geq 2$  and  $q \geq 3$ , then  $2g > f_3(g)$ , hence  $q = 2$  and  $g \leq 3$  if the statement is false, and this proves the first statement of (iv). If

$n \geq 2g + 2$ , then  $B_n \geq 1$ , because, firstly,  $2g + 2 > f_2(g)$  if  $g \geq 3$ , and secondly, with  $F(x)$  as above, and if  $g = 2$ , then  $F(2^{3/2}) = 2(13 - 8\sqrt{2}) > 0$ , and  $F(q)$  is increasing if  $q \geq 2$ . In the two remaining cases, if  $n = 2g + 1$ , we use Serre's inequality: if  $g = 2$  then  $B_5 \geq 4$ , and if  $g = 3$  then  $B_7 \geq 54$ . This proves (iv).  $\square$

*Example.* Here are two instances of the exceptional cases appearing in (iv). Consider the elliptic curves over  $\mathbb{F}_2$ :

$$E_1 : y^2 + y = x^3, \quad E_2 : y^2 + xy = x^3 + x^2 + 1.$$

Then  $f_{E_1}(t) = t^2 + 2$  and  $f_{E_2}(t) = t^2 - t + 2$ . If  $A = E_1 \times E_2$ , then  $B_4(A) = -1$  and  $N_4(A) - N_1(A) = 6$ . If  $A = E_2 \times E_2 \times E_2$ , then  $B_6(A) = 0$  and  $N_6(A) - N_1(A) = 38$ .

We shall use the results of § 3.2 in order to obtain lower bounds for the number of rational points on the Jacobian of a curve. To do that, we consider an abelian variety, and assume that Condition **(B)** or Condition **(N)** is satisfied.

**Lemma 3.9.** *Assume that **(B)** holds. If  $n \geq 2$ ,*

$$A_n \geq \binom{N_1 + n - 1}{n} + \sum_{i=2}^n B_i \binom{N_1 + n - i - 1}{n - i}.$$

*Proof.* All the terms in the right hand side of (8) are  $\geq 0$ . In order to get a lower bound, we sum over the subset of  $\mathcal{P}_n$  consisting of

$$(n, 0, \dots, 0), (n - 2, 1, 0, \dots, 0), (n - 3, 0, 1, 0, \dots, 0), \dots, (1, 0, \dots, 0, 1, 0), (0, \dots, 0, 1). \quad \square$$

From (11) we deduce

$$(16) \quad |A(\mathbb{F}_q)| = \frac{q - 1}{q^g - 1} A_{2g-1}.$$

From (16) and Lemma 3.9 we deduce:

**Proposition 3.10.** *Let  $A$  be an abelian variety, and assume that **(B)** holds. Then*

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

*In particular:*

$$(17) \quad |A(\mathbb{F}_q)| \geq \frac{q - 1}{q^g - 1} \binom{N + 2g - 2}{2g - 1}. \quad \square$$

*Remarks.* (i) Notice that the bound **(III)** can be made more explicit, using Proposition 3.7.  
(ii) The bound (17) is not optimal for  $g \geq 10$  or  $q \geq 7$ , by Lemma 3.8(iii).

**Lemma 3.11.** *Let  $A$  be an abelian variety, and assume that **(N)** holds. Then*

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

*Proof.* We recall 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

$$\exp\left(\sum_{n=1}^{+\infty} (y_n + z_n) \frac{t^n}{n}\right) = \exp\left(\sum_{n=1}^{+\infty} y_n \frac{t^n}{n}\right) \exp\left(\sum_{n=1}^{+\infty} z_n \frac{t^n}{n}\right),$$

and expanding the right hand side, we obtain:

$$(18) \quad \mathcal{C}_n(\mathbf{y} + \mathbf{z}) = \sum_{k=0}^n \mathcal{C}_k(\mathbf{y}) \mathcal{C}_{n-k}(\mathbf{z}).$$

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

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

hence,

$$(19) \quad \mathcal{C}_n(M, \dots, M) = \binom{M+n-1}{n}.$$

We define

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

Then, by (14), (18) and (19),

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

We put, if  $k \geq 2$ ,

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

**Lemma 3.12.** *Let  $A$  be an abelian variety, and assume that  $(\mathbf{N})$  holds. If  $k \geq 0$ , then  $\mathcal{C}_k(\mathbf{n}) \geq 0$ ,  $\mathcal{C}_k(\mathbf{d}) \geq 0$ , and*

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

*Proof.* By Condition  $(\mathbf{N})$ , the coordinates of  $\mathbf{n}$  and  $\mathbf{d}$  are  $\geq 0$ , and this implies our first assertion. Let  $\mathbf{y}$  and  $\mathbf{z}$  be two sequences of indeterminates. By (18),

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

Now, by applying (10) with  $n = 0$ , we get

$$(20) \quad |A(\mathbb{F}_q)| = A_g - qA_{g-2},$$

and using (14),

$$|A(\mathbb{F}_q)| = \mathcal{C}_g(\mathbf{n} + \mathbf{d}) - q\mathcal{C}_{g-2}(\mathbf{n} + \mathbf{d}).$$

Replacing  $\mathbf{y}$  by  $\mathbf{n}$  and  $\mathbf{z}$  by  $\mathbf{d}$ , and since (19) implies

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

we get the required expression for  $|A(\mathbb{F}_q)|$ .  $\square$

**Proposition 3.13.** *Assume  $g \geq 2$ . Let  $A$  be an abelian variety. Assume that  $(\mathbf{N})$  holds and that*

$$(21) \quad \left( \frac{N-1}{g} + 1 \right) \left( \frac{N-1}{g-1} + 1 \right) - q > 0.$$

Then

$$(IV) \quad |A(\mathbb{F}_q)| \geq \binom{N+g-1}{g} - q \binom{N+g-3}{g-2}.$$

*Proof.* The right hand side of (IV) is equal to  $\mathcal{X}_g(N)$ , and  $\mathcal{X}_g(N) > 0$  if and only if (21) holds, in which case  $N \geq 1$ . For  $k = 2, \dots, g$ , 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 (21). Applying Lemma 3.12 we deduce

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

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

*Remarks.* (i) The condition (21) is satisfied if  $N \geq g(q^{1/2} - 1) + 1$ . This inequality has to be compared to the Drinfeld-Vlăduț upper bound.

(ii) Notice that Proposition 3.13 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  $b = (0, \dots, 0, 1)$ , 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 (21) 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 (IV).

(iii) Lemma 3.4 provides some others identities than (16) and (20), for instance

$$A_{2g-2} = |A(\mathbb{F}_q)|\pi_{g-2} + q^{g-1}.$$

On the other hand,  $Z_A(t) < 0$  if  $q^{-1} < t < 1$ , because  $f_A(t) \geq 0$  for any  $t \in \mathbb{R}$ , and one deduces from (13) the inequality

$$A_{g-1} \leq \frac{|A(\mathbb{F}_q)|}{(q^{1/2} - 1)^2} - 2q^{(g-1)/2},$$

as established by S. Ballet, C. Ritzenthaler and R. Rolland in [1]. These relations lead to lower bounds similar to (III) and (IV).

Assume  $g \geq 2$ . From Theorem 3.5, we know that

$$(22) \quad \frac{g}{\eta} |A(\mathbb{F}_q)| = \sum_{n=0}^{g-1} A_n + \sum_{n=0}^{g-2} q^{g-1-n} A_n,$$

where  $\eta = \eta(A)$  is the harmonic mean of the numbers  $q+1+x_i$ , as in § 2.2. We recall from [7] that

$$(23) \quad \eta \geq (q^{1/2} - 1)^2,$$

$$(24) \quad \eta \geq \frac{g(q-1)^2}{(g+1)(q+1) - N},$$

and (24) is always tighter than (23), though it does depend on  $N$ . Moreover, if  $q \geq 8$ , by Proposition 2.13, we know that

$$\eta \geq q + 1 - m.$$

This lower bound is better than the uniform lower bound deduced from (24), namely

$$\eta \geq \frac{g(q-1)^2}{(g+1)(q+1) - N} \geq \frac{(q-1)^2}{q+1+m} = q+1-m - \frac{4q-m^2}{q+1+m}.$$

**Theorem 3.14.** *If  $g \geq 2$ , and if  $(\mathbf{N})$  holds, then*

$$(\mathbf{V}) \quad |A(\mathbb{F}_q)| \geq \frac{\eta}{g} \left[ \binom{N+g-2}{g-2} + \sum_{n=0}^{g-1} q^{g-1-n} \binom{N+n-1}{n} \right]$$

*Proof.* Since  $(\mathbf{N})$  holds, we apply the inequality of Lemma 3.11 in (22). Noticing that

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

we obtain the result. □

*Remark.* The expression in brackets is  $\geq q^{g-1}$ . Since  $N \geq 0$ , we recover as a corollary the bound [7, 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 of  $(\mathbf{V})$  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 Theorem 3.14:

**Corollary 3.15.** *If  $g \geq 2$ , then*

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

**3.4. Discussing the bounds.** Let  $C$  be a curve of genus  $g \geq 2$  over  $\mathbb{F}_q$ , with  $N = |C(\mathbb{F}_q)|$ . We recall the lower bounds for the number of rational points on  $J = J_C$ , respectively obtained from Proposition 3.1 (with  $M(q)$  as defined there), Proposition 3.2 (with  $r$  and  $s$  as defined there),

Proposition 3.10, Proposition 3.13, and Theorem 3.14:

$$\begin{aligned}
\text{(I)} \quad |J(\mathbb{F}_q)| &\geq M(q)^g \left( q + 1 + \frac{N - (q + 1)}{g} \right)^g \\
\text{(II)} \quad |J(\mathbb{F}_q)| &\geq (N - 2(r - s)q^{1/2})(q + 1 + 2q^{1/2})^r (q + 1 - 2q^{1/2})^s \\
\text{(III)} \quad |J(\mathbb{F}_q)| &\geq \frac{q - 1}{q^g - 1} \left[ \binom{N + 2g - 2}{2g - 1} + \sum_{i=2}^{2g-1} B_i \binom{N + 2g - 2 - i}{2g - 1 - i} \right] \\
\text{(IV)} \quad |J(\mathbb{F}_q)| &\geq \binom{N + g - 1}{g} - q \binom{N + g - 3}{g - 2} \\
\text{(V)} \quad |J(\mathbb{F}_q)| &\geq \frac{\eta}{g} \left[ \binom{N + g - 2}{g - 2} + \sum_{n=0}^{g-1} q^{g-1-n} \binom{N + n - 1}{n} \right]
\end{aligned}$$

(i) When  $q$  is large with respect to  $g$ , we have, for any abelian variety of dimension  $g$ ,

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

and **(I)** and **(II)** are the only bounds to be consistent with this estimate. More precisely, since **(II)** is usually reached for abelian varieties when  $q$  is a square, this bound is probably the best one as soon as  $g \leq (q - q^{1/2})/2$ .

(ii) Assume that **(N)** holds. Then (22), joint to the inequality  $A_n \geq N$  for  $n \geq 1$ , gives

$$\frac{g}{\eta} |A(\mathbb{F}_q)| \geq (q^{g-1} - 1) \frac{N + q - 1}{q - 1}.$$

Using (23), we recover [7, Th. 2(2)]:

$$(25) \quad |A(\mathbb{F}_q)| \geq (q^{1/2} - 1)^2 \frac{q^{g-1} - 1}{g} \frac{N + q - 1}{q - 1}.$$

But if  $n \geq 1$  and  $N \geq 1$ , the inequality in Lemma 3.11 is better than  $A_n \geq N$ , since

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

Hence, **(V)** is always better than (25).

(iii) The tables in [7] provide numerical evidence that these bounds can be better than those which hold for general abelian varieties, at least when  $q$  is not too large.

(iv) Assume  $q \geq 4$ , and let  $A$  be any abelian variety of dimension  $g \leq (q - q^{1/2})/2$  with  $N_1 \geq 0$ . Then the bounds **(IV)** and **(V)** hold for  $A$ , by Lemma 3.6. Likewise, the bound **(III)** holds for  $A$ , by Proposition 3.8(ii).

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

#### 4. 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 [3], [25]): if  $q = p^n$ , then

$$J_q(1) = \begin{cases} q + 1 + m & \text{if } n = 1, n \text{ is even, or } p \nmid m, \\ q + m & \text{otherwise,} \end{cases}$$

$$j_q(1) = \begin{cases} q + 1 - m & \text{if } n = 1, n \text{ is even, or } p \nmid m, \\ q + 2 - m & \text{otherwise.} \end{cases}$$

The description of the set of characteristic polynomials of abelian surfaces has been given by H.G. Rück in [12]. 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 [14], [15], [16], whose aim was to determine  $N_q(2)$ . A complete answer to this question was finally given by E. Howe, E. Nart, and C. Ritzenthaler in [6]. In the remainder 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 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 [12] 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  $q^{1/2}$ ) is equivalent to

$$(26) \quad |a_1| \leq 2m \quad \text{and} \quad 2|a_1|q^{1/2} - 2q \leq a_2 \leq \frac{a_1^2}{4} + 2q.$$

We have

$$(27) \quad |A(\mathbb{F}_q)| = f_A(1) = q^2 + 1 + (q + 1)a_1 + a_2.$$

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

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

$a_1$	$a_2$	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  $b = q + 1 + m$ .

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  $[-2m, 2m - 3]$ ).



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 (26) 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  $b' = q + 1 - m$ .

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

(notice that the function  $x \mapsto (q+1)x + 2|x|q^{1/2}$  is increasing on the interval  $[-2m+3, 2m]$ ). Most cases of Theorem 4.1 and 4.2 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 H.-G. Rück [12] who solved the problem of describing characteristic polynomials of abelian surfaces, in particular the fact that if  $(a_1, a_2)$  satisfy (26) 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 [6] where we can find a characterization of isogeny classes of abelian surfaces containing a Jacobian.

The determination of  $J_q(2)$  in Theorem 4.1 is closely related to that of  $N_q(2)$ , as done by J.-P. Serre [16]. In order to simplify the proof of Theorem 4.2, 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 Theorem 4.1.

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  $m = \lfloor 2q^{1/2} \rfloor$ ):

- (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 [15], 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 [8] for more details) that conditions (2), (3) and (4) are respectively equivalent to  $m^2 - 4q = -4, -3$  and  $-7$ .

**Theorem 4.1.** *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*

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

*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 [15], 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 (26). 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 [6]). 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 [6] 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 [16] 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  $\{2q^{1/2}\} \geq \varphi_1$ . Note that  $\{2q^{1/2}\} \geq \varphi_1$  is equivalent to  $m+\varphi_1 \leq 2q^{1/2}$ , thus it is obvious that this condition is necessary.

— If  $q$  is special,  $\{2q^{1/2}\} < \varphi_1, p \neq 2$  or  $p|m$ , then there exists a Jacobian of type  $[m-1, m-1]$ .

— If  $q$  is special,  $\{2q^{1/2}\} < \varphi_1, p = 2$  and  $p \nmid m$ , that is,  $q = 2^5$  or  $2^{13}$  (if  $q = 2^3$ , then  $\{2q^{1/2}\} \geq \varphi_1$ ), 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 [9], Prop. 2.5).  $\square$

**Theorem 4.2.** *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*

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

*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 (26). 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

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

(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 Theorem 4.1. The number of points on 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  $\{2q^{1/2}\} = 0$  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 [6]). The product of two copies of an elliptic curve of trace  $(m-1)$  is isogenous to a Jacobian (such a curve exists since  $3 \nmid (m-1)$ ).

(b) Assume that  $q$  is not a square. Using twisting arguments and the proof of Theorem 4.1, 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  $\{2q^{1/2}\} \geq \varphi_1$ .

— An abelian surface of type  $[-m, -m+1]$  is never a Jacobian.

In the remainder of the proof, we suppose that  $q$  is special and  $\{2q^{1/2}\} < \varphi_1$ .

— 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  $\{2q^{1/2}\} \geq \sqrt{3}-1$ . When  $\{2q^{1/2}\} < \varphi_1$ , 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  $\{2q^{1/2}\} \geq \sqrt{2}-1$ . 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 that J.-P. Serre used in [16]. If  $p \nmid m$ , we are done since  $p \nmid a_2 = m^2 - 2m - 1 + 2q$ .

Otherwise,  $(m - 2q^{1/2})(m + 2q^{1/2}) = m^2 - 4q \in \{-3, -4, -7\}$ , hence

$$\{2q^{1/2}\} = 2q^{1/2} - m = \frac{4q - m^2}{m + 2q^{1/2}} \leq \frac{7}{2m},$$

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  $\{2q^{1/2}\} \geq \varphi_1$ . If  $q = 3$ , then  $p|m$ . If  $q = 4, 7, 13, 17$ , then  $\{2q^{1/2}\} < \sqrt{2} - 1$ . 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 [6], we conclude that this abelian surface is isogenous to a Jacobian. — If  $\{2q^{1/2}\} < \sqrt{2} - 1$ ,  $p \nmid m$  and  $q \neq 7^3$ , then  $p \nmid (m - 2)$ . 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  $p$  also divides  $m^2 - 4 - 4q = (m + 2)(m - 2) - 4q$ . 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  $q = 7$ ,  $p \nmid (m - 2) = 5$ ), 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 [6] their product is isogenous to a Jacobian.

— Suppose that  $\{2q^{1/2}\} < \sqrt{2} - 1$  and  $p|m$ , or  $q = 7^3$ . By [25], if  $p|m$ , there does not exist an elliptic curve of trace  $m$  ( $q = 2$  and  $3$  are excluded since in those cases,  $\{2q^{1/2}\} \geq \sqrt{2} - 1$ ). 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  $\{2q^{1/2}\} < \sqrt{2} - 1$  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 Theorem 4.1.  $\square$

## REFERENCES

- [1] Ballet, Stéphane; Ritzenthaler, Christophe; Rolland, Robert. On the existence of dimension zero divisors in algebraic function fields defined over  $\mathbb{F}_q$ . *Acta Arithmetica* **143** (2010), no. 4, 377–392
- [2] Ballet, Stéphane; Rolland, Robert. Lower bounds on the class number of algebraic function fields defined over any finite field. *Journal de Théorie des Nombres de Bordeaux*, to appear. = arXiv:1103.2161
- [3] Deuring, Max. Die typen der multiplikatorenringe elliptischer funktionenkörper. *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272.
- [4] Elkies, Noam D.; Howe, Everett W.; Kresch, Andrew; Poonen, Bjorn; Wetherell, Joseph L.; Zieve, Michael E. Curves of every genus with many points. II. Asymptotically good families. *Duke Math. J.* **122** (2004), no. 2, 399–422.
- [5] Fujii, Jun Ichi; Izumino, Saichi; Seo, Yuki. Determinant for positive operators and Specht’s theorem, *Scientiae Mathematicae* **1** (1998) 307–310.
- [6] Howe, Everett; Nart, Enric; Ritzenthaler, Christophe. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourier* **59** (2009), 239–289.
- [7] Lachaud, Gilles; Martin-Deschamps, Mireille. Nombre de points des jacobiniennes sur un corps fini. *Acta Arithmetica* **16** (1990), 329–340.
- [8] Lauter, Kristin. The maximum or minimum number of rational points on genus three curves over finite fields. With an Appendix by Jean-Pierre Serre. *Compositio Math.* **134** (2002), 87–111.
- [9] Maisner, Daniel; Nart, Enric. Abelian surfaces over finite fields as jacobians. With an Appendix by Everett W. Howe. *Experiment. Math.* **11** (2002), 321–337.
- [10] Perret, Marc. Number of points of Prym varieties over finite fields. *Glasgow Math. J.* **48** (2006), 275–280.
- [11] Quebbemann, Heinz-Georg. *Lattices from curves over finite fields*. Preprint (April 1989).
- [12] Rück, Hans-Georg. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Math.* **76** (1990), 351–366.
- [13] Schur, Issai. Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung. *Compositio Math.* **4** (1937), 432–444.
- [14] Serre, Jean-Pierre. 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. = Œuvres, vol. III, No. 128, 658–663.
- [15] Serre, Jean-Pierre. Nombre de points des courbes algébriques sur  $\mathbb{F}_q$ . *Sém. de Théorie des nombres de Bordeaux* 1982/83, exp. no. 22. = Œuvres, vol. III, No. 129, 664–668.
- [16] Serre, Jean-Pierre. *Rational points on curves over finite fields*. Lectures at Harvard University, Notes by F. Gouvea, 1985.
- [17] Serre, Jean-Pierre. *Lettre à Daniel Bertrand*, 15 février 1997.

- [18] Smyth, Christopher. Totally positive algebraic integers of small trace. *Ann. Inst. Fourier* **34** (1984), no. 3, 1–28.
- [19] Specht, Wilhelm. Zur Theorie der elementaren Mittel. *Math. Zeitschr.* **74** (1960), 91–98.
- [20] Stanley, Richard P. *Enumerative combinatorics*, Vol. 2. Cambridge University Press, Cambridge, 1999.
- [21] Stichtenoth, Henning. *Algebraic function fields and codes*. Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin, 2009.
- [22] Tate, John. Classes d’isogénies de variétés abéliennes sur un corps fini (d’après T. Honda). *Séminaire Bourbaki* **21** (1968/69), Exp. 352.
- [23] Tsfasman, Michael; Vlăduț, Serge; Nogin, Dmitry. *Algebraic geometric codes: basic notions*. Vol. 139, Math. Surveys and Monographs, A.M.S, 2007.
- [24] Vlăduț, Serge. An exhaustion bound for algebro-geometric “modular” codes. *Problemy Peredachi Informatsii* **23** (1987), no. 1, 28–41.
- [25] Waterhouse, William C. 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, AIX-MARSEILLE UNIVERSITÉ / CNRS, FRANCE  
*E-mail address:* `aubry@iml.univ-mrs.fr`

INSTITUT DE MATHÉMATIQUES DE LUMINY, AIX-MARSEILLE UNIVERSITÉ / CNRS, FRANCE AND DEPARTMENT OF MATHEMATICS, TECHNICAL UNIVERSITY OF DENMARK, LYNGBY, DENMARK  
*E-mail address:* `s.haloui@mat.dtu.dk`

INSTITUT DE MATHÉMATIQUES DE LUMINY, AIX-MARSEILLE UNIVERSITÉ / CNRS , FRANCE  
*E-mail address:* `lachaud@univ-amu.fr`