BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 39(4), 587-595

On the size of the Jacobians of curves over finite fields

Igor Shparlinski

Abstract. Given a smooth curve of genus $g \geq 1$ which admits a smooth projective embedding of dimension m over the ground field $\mathbb{F}_q$ of q elements, we obtain the asymptotic formula $q^{g+o(g)}$ for the size of set of the $\mathbb{F}_q$-rational points on its Jacobian in the case when m and q are bounded and $g \to \infty$. We also obtain a similar result for curves of bounded gonality. For example, this applies to the Jacobian of a hyperelliptic curve of genus $g \to \infty$.

Keywords: $\mathbb{F}_q$-rational points on Jacobian, uniform distribution.

Mathematical subject classification: 11G20, 11K38, 14H40.

1 Introduction

Let C be a smooth absolutely irreducible curve of genus $g \geq 1$ defined over a finite field $\mathbb{F}_q$ of q elements. We denote by $\mathcal{J}_C$ the set of the $\mathbb{F}_q$-rational points on its Jacobian.

By the Weil theorem, there are some complex numbers $\lambda_1, \ldots, \lambda_{2g}$, called the *eigenvalues of the Frobenius endomorphism* with

$$|\lambda_j| = q^{1/2}, \quad \lambda_{j+g} = \overline{\lambda}_j, \qquad j = 1, \ldots, g, \tag{1}$$

(where $\overline{\lambda}$ means complex conjugate of λ) and such that

$$\#\mathcal{J}_C = \prod_{j=1}^{2g} (1 - \lambda_j) \tag{2}$$

see [1, Corollary 5.70 and Theorem 5.76] or [8, Corollary VIII.6.3].

Received 21 May 2008.

In particular, we immediately derive from (2) that

$$\left(q^{1/2}-1\right)^{2g} \le \#\mathcal{J}_C \le \left(q^{1/2}+1\right)^{2g}$$

which is tight in the case of $g = 1$ (that is, for elliptic curves) due to the classical result of M. Deuring [2].

Some improvements of this bound are given in [9, 10, 11, 12] (see also the references therein). For example, M. Tsfasman [12] has shown that when q is fixed then

$$g \log q + o(g) \le \log \#\mathcal{J}_C \le g \left(\log q + (q^{1/2}-1) \log \frac{q}{q-1} \right) + o(g)$$

as $g \to \infty$. A. Stein and E. Teske [11] concentrate on the case of hyperelliptic curves of small genus but defined over a large field.

Here we define the $\mathbb{F}_q$-*dimension* of C as the lowest dimension m of a smooth projective embedding of C over $\mathbb{F}_q$.

We show that if m is not too large compared to the genus g and the cardinality of the field q is fixed, then $\log \#\mathcal{J}_C \sim g \log q$ as $g \to \infty$.

We also obtain similar results for curves C of small *gonality* which is the smallest integer d such that C admits a non-constant map of degree d to the projective line over the ground field $\mathbb{F}_q$. So hyperelliptic curves are, by definition, curves of gonality $d = 2$. In particular, for a hyperelliptic curve we have

$$\log \#\mathcal{J}_C = g \left(\log q + O(1/\log g) \right). \tag{3}$$

Our approach can be applied to estimating a number of other parameters of curves. For example, following Y. Ihara [6] we consider the *Euler-Kronecker* constant γ_C of C which is defined as

$$\gamma_C = \lim_{s \to 1} \left(\frac{\zeta_C'(s)}{\zeta_C(s)} + \frac{1}{s-1} \right),$$

where

$$\zeta_C(s) = \frac{1}{(1-q^{-s})(1-q^{-s+1})} \prod_{j=1}^{2g} \left(1 - \lambda_j q^{-s}\right)$$

is the ζ-function of the curve C. Here, in particular, it follows from [6, Theorems 1 and 2] that for a fixed q and any curve of genus $g \to \infty$ the following bounds hold

$$(2 + o(1)) \log g \ge \gamma_C \ge -\left(\frac{\log q}{q} + o(1) \right) g. \tag{4}$$

Throughout the paper, the implied constants in the symbols O and $\ll$ may depend on the base field $\mathbb{F}_q$ (that is, on q), but not on the other parameters such as g and m. We recall that the notations $U = O(V)$ and $U \ll V$ are equivalent to the assertion that the inequality $|U| \le cV$ holds with some positive constant c.

2 Our Results and Approach

Theorem 1. *For any smooth absolutely irreducible curve C of genus $g \ge 1$ and $\mathbb{F}_q$-dimension m*

$$\log \#\mathcal{J}_C = g\left(\log q + O\left(\frac{m}{\log g}\right)\right)$$

as $g \to \infty$.

We also have a similar statement in terms of gonality.

Theorem 2. *For any smooth absolutely irreducible curve C of genus $g \ge 1$ and gonality d*

$$\log \#\mathcal{J}_C = g\left(\log q + O\left(\frac{1}{\log(g/d)}\right)\right)$$

as $g \to \infty$.

For example, for hyperelliptic curves we have $d = 2$ and for smooth plane curves we have $m = 2$. Thus, in both cases, Theorem 2 implies (3). We note that it seems that the "explicit formulas" approach of M. Tsfasman [12] provides an alternative to proving that $\log \#\mathcal{J}_C = g \log q + o(g)$ under the conditions of Theorem 1. However our proof appears to be more general (as it may be applied to a variety of other characteristics of algebraic curves) and immediately leads to an explicit error term.

More precisely, one of the main ingredients of the proof is the bound $O\big(mg/\log g\big)$ on the discrepancy of the distribution of the arguments of $\lambda_1, \ldots, \lambda_{2g}$, which in turn generalises a similar result of D. Faifman and Z. Rudnick [4] (but is based on slightly different arguments). This bound can be of independent interest and can be applied to several other problems. Then this bound is combined with of some standard tools from the theory of uniform distribution, such as the Koksma–Hlawka inequality.

It is also interesting to know that M. Tsfasman [12] gives examples of families of curves with the number of $\mathbb{F}_q$-rational points of the Jacobian is not asymptotic to $g \log q$ (and hence with unbounded m and d).

For the Euler-Kronecker constant, in the case when the $\mathbb{F}_q$-dimension m of C small we obtain lower bounds which are stronger than that of (4) (our bounds is both-sided but it is weaker the upper bound in (4)).

Theorem 3. *For any smooth absolutely irreducible curve C of genus $g \geq 1$ and $\mathbb{F}_q$-dimension m*

$$\gamma_C = O\left(\frac{mg}{\log g}\right)$$

as $g \to \infty$.

As in the case of the Jacobian, we also have an analogue of Theorem 4 in terms of gonality.

Theorem 4. *For any smooth absolutely irreducible curve C of genus $g \geq 1$ and gonality d*

$$\gamma_C = O\left(\frac{g}{\log(g/d)}\right)$$

as $g \to \infty$.

3 Preliminaries

Given a smooth absolutely irreducible curve C of genus $g \geq 1$ over $\mathbb{F}_q$, we see from (1) that the eigenvalues of the Frobenius endomorphism on C can be written as

$$\lambda_j = q^{1/2} \exp(2\pi i \vartheta_j), \qquad j = 1, \ldots, 2g, \tag{5}$$

where

$$\vartheta_j = -\vartheta_{g+j} \in [0, 1/2], \qquad j = 1, \ldots, g.$$

We now need a result showing that the angles $\vartheta_1, \ldots, \vartheta_{2g}$ are uniformly distributed in $[0, 1]$. For the case of hyperelliptic curves it has been obtained by D. Faifman and Z. Rudnick [4]. Here we use a slightly different argument to extend this result to arbitrary curves.

As usual, for a sequence of N real numbers $\gamma_1, \ldots, \gamma_N$ the *discrepancy* is defined by

$$D = \max_{0 \leq \gamma \leq 1} |T(\gamma) - \gamma N|,$$

where $T(\gamma)$ is the number of $n \leq N$ such that the fractional part $\{\gamma_n\}$ satisfies the inequality $\{\gamma_n\} \leq \gamma$, see [3, 7].

We now recall the *Erdös–Turán inequality* (see [3, 7]), which links the discrepancy with exponential sums.

Lemma 5. *For any integer $K \ge 1$, the discrepancy D of a sequence of N real numbers $\gamma_1, \ldots, \gamma_N \in [0, 1)$ satisfies the inequality*

$$D \ll \frac{N}{K} + \sum_{k=1}^{K} \frac{1}{k} \left| \sum_{n=1}^{N} \exp(2\pi i k \gamma_n) \right|.$$

We are now ready to estimate the discrepancy of the set of angles.

Lemma 6. *For any smooth absolutely irreducible curve C of genus $g \ge 1$ and $\mathbb{F}_q$-dimension m, the discrepancy D_C of the sequence $\vartheta_1, \ldots, \vartheta_{2g}$ satisfies the inequality*

$$D_C \ll \frac{mg}{\log g}.$$

Proof. Let $N_{k,C}$ denotes the number of $\mathbb{F}_{q^k}$-rational points on the projective model of the curves C. We recall that

$$N_{k,C} - q^k - 1 = -\sum_{j=1}^{2g} \lambda_j = -q^{k/2} \sum_{j=1}^{2g} \exp(2\pi i k \vartheta_j), \tag{6}$$

see [1, Section 8.1.1] or [8, Section VIII.5.8].

Clearly, if the curve C is defined by a system of polynomial equations in m variables then $N_{k,C}$ does not exceed the number of points of the m-dimensional projective space over $\mathbb{F}_{q^k}$. Therefore,

$$N_{k,C} \le \sum_{\nu=0}^{m} q^{k\nu}. \tag{7}$$

Therefore from (6) and (7) we see that for any integer $k \ge 1$ the bound

$$\left| \sum_{j=1}^{2g} \exp(2\pi i k \vartheta_j) \right| \le \sum_{\nu=0}^{m} q^{k\nu} + q^k + 1 \le 2 \sum_{\nu=0}^{m} q^{k\nu} \le 4q^{km}. \tag{8}$$

Using (8) in a combination with Lemma 5, we see that for any integer $K \ge 1$,

$$D_C \ll \frac{g}{K} + \sum_{k=1}^{K} \frac{1}{k} q^{km} \ll \frac{g}{K} + \frac{1}{K} q^{Km}. \tag{9}$$

Taking

$$K = \left\lceil \frac{\log g}{2m \log q} \right\rceil$$

we conclude the proof. □

Corollary 7. *For any smooth absolutely irreducible curve C of genus $g \ge 1$ and $\mathbb{F}_q$-dimension m, the discrepancy $\widetilde{D}_C$ of the sequence $2\vartheta_1, \ldots, 2\vartheta_g$ satisfies the inequality*

$$\widetilde{D}_C \ll \frac{mg}{\log g}.$$

Lemma 8. *For any smooth absolutely irreducible curve C of genus $g \ge 1$ and gonality d, the discrepancy D_C of the sequence $\vartheta_1, \ldots, \vartheta_{2g}$ satisfies the inequality*

$$D_C \ll \frac{g}{\log(g/d)}.$$

Proof. The proof is fully analogous to that of Lemma 6 as for a curve of gonality d we have

$$N_{k,C} \le d(q^k + 1).$$

instead of (7). Therefore instead of (9), we obtain

$$D_C \ll \frac{g}{K} + d\sum_{k=1}^{K} \frac{1}{k} q^k \ll \frac{g}{K} + \frac{d}{K} q^K.$$

Taking

$$K = \left\lceil \frac{\log(g/d)}{\log q} \right\rceil$$

we conclude the proof. □

Corollary 9. *For any smooth absolutely irreducible curve C of genus $g \ge 1$ and gonality d, the discrepancy $\widetilde{D}_C$ of the sequence $2\vartheta_1, \ldots, 2\vartheta_g$ satisfies the inequality*

$$\widetilde{D}_C \ll \frac{g}{\log(g/d)}.$$

Finally, to link the discrepancy bound with $\#J_C$ we need the *Koksma–Hlawka inequality*, see [3, Theorem 1.14], which allows us to estimate average values of various functions at uniformly distributed the points.

Lemma 10. *For any continuous function $f(z)$ on the unit interval $z \in [0, 1]^s$ and a sequence of N real numbers $\gamma_1, \ldots, \gamma_N \in [0, 1]$ with the discrepancy D, the following bound holds:*

$$\frac{1}{N}\sum_{j=1}^{N} f(\gamma_j) = \int_0^1 f(z)dz + O_f\left(DN^{-1}\right),$$

where the implied constant in O_f depends only on the function f.

4 Proofs of Theorems 1 and 2

Using (1), for every $j = 1, \dots, g$, we obtain

$$\begin{aligned}(1-\lambda_j)(1-\lambda_{j+g}) &= (1-\lambda_j)(1-\overline{\lambda}_j) = 1-\lambda_j-\overline{\lambda}_j+q\\ &= 1-q^{1/2}\left(\exp(2\pi i\vartheta_j)+\exp(-2\pi i\vartheta_j)\right)+q\\ &= 1-q^{1/2}\left(\exp(2\pi i\vartheta_j)+\exp(-2\pi i\vartheta_j)\right)+q\\ &= 1-2q^{1/2}\cos(4\pi\vartheta_j)+q.\end{aligned}$$

Therefore, using Lemma 10 and Corollary 7 we derive from (2)

$$\frac{1}{g}\log \#\mathcal{J}_C = \int_0^1 \log\left(1-2q^{1/2}\cos(2\pi z)+q\right)\mathrm{d}z + O\left(\frac{m}{\log g}\right).$$

We now recall that for any $a > 1$,

$$\begin{aligned}&\int_0^1 \log\left(1-2q^{1/2}\cos(2\pi z)+q\right)\mathrm{d}z\\ &\qquad = \frac{1}{2\pi}\int_0^{2\pi}\log\left(1-2q^{1/2}\cos(z)+q\right)\mathrm{d}z = \log q,\end{aligned}$$

see [5, Section 4.224(15)], which concludes the proof of Theorem 1.

Using Corollary 9 instead of Corollary 7 we obtain the bound of Theorem 2.

5 Proofs of Theorems 3 and 4

The proof is analogous to the proof of Theorem 1, except that it uses the formula

$$\gamma_C = \left((q-1)\rho_C - g + 1 - \frac{q+1}{2(q-1)}\right)\log q = ((q-1)\rho_C - g)\log q + O(1),$$

where

$$\rho_C = \sum_{j=1}^{g}\frac{1}{(1-\lambda_j)(1-\overline{\lambda}_j)} = \sum_{j=1}^{g}\frac{1}{1-2q^{1/2}\cos(4\pi\vartheta_j)+q},$$

see [6, Equation (0.5)] and the integral identity

$$\begin{aligned}&\int_0^1 \frac{1}{1-2q^{1/2}\cos(2\pi z)+q}\mathrm{d}z\\ &\qquad = \frac{1}{2\pi}\int_0^{2\pi}\frac{1}{1-2q^{1/2}\cos(z)+q}\mathrm{d}z = \frac{1}{q-1},\end{aligned}$$

see [5, Section 3.616(2)]. In particular, by Lemma 10 and Corollary 7 we have

$$\rho_C = \frac{g}{q-1} + O\left(\frac{mg}{\log g}\right),$$

which concludes the proof of Theorem 3.

As before, using Corollary 9 instead of Corollary 7 we obtain the bound of Theorem 4.

Acknowledgments. The author is very grateful to the referee for many very helpful suggestions, in particular for the idea of using the notion of gonality.

The author would also like to thank Par Kurlberg, Zeev Rudnick and Michael Tsfasman for a number of fruitful discussions.

During the preparation of this paper, the author was supported in part by ARC grant DP0881473.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren. *Elliptic and hyperelliptic curve cryptography: Theory and practice*. CRC Press (2005).

[2] M. Deuring. 'Die Typen der Multiplikatorenringe elliptischer Funktionenkörper'. *Abh. Math. Sem. Hansischen Univ.*, **14** (1941), 197–272.

[3] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*. Springer (1997).

[4] D. Faifman and Z. Rudnick. 'Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field'. *Preprint*, 2008 (available from `http://arxiv.org/abs/0803.3534`).

[5] I.S. Gradshteyn and I.M. Ryzhik. *Table of integrals, series, and products*. Academic Press (2000).

[6] Y. Ihara. 'On the Euler-Kronecker constants of global fields and primes with small norms'. *Algebraic Geometry and Number Theory*. Progress in Math., Vol. 850, Birkhäuser, Boston, Cambridge, MA, (2006), 407–451.

[7] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Wiley-Interscience (1974).

[8] D. Lorenzini. *An invitation to arithmetic geometry*. Amer. Math. Soc. (1996).

[9] H.-G. Quebbemann. 'Estimates of regulators and class numbers in function fields'. *J. Reine Angew. Math.*, **419** (1991), 79–87.

[10] M.Y. Rosenbloom and M.A. Tsfasman. 'Multiplicative lattices in global fields'. *Invent. Math.*, **101** (1990), 687–696.

[11] A. Stein and E. Teske. 'Explicit bounds and heuristics on class numbers in hyperelliptic function fields'. *Math. Comp.*, **71** (2002), 837–861.

[12] M. Tsfasman. 'Some remarks on the asymptotic number of points'. *Coding theory and algebraic geometry (Luminy, 1991).* Lect. Notes in Math., vol. 1518, Springer, (1992), 178–192.

Igor Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109
AUSTRALIA

E-mail: igor@ics.mq.edu.au