



HAL
open science

On the Number of Rational Points of Jacobians over Finite Fields

Philippe Lebacque, Alexey Zykin

► **To cite this version:**

Philippe Lebacque, Alexey Zykin. On the Number of Rational Points of Jacobians over Finite Fields. 2014. hal-01081468

HAL Id: hal-01081468

<https://hal.science/hal-01081468>

Preprint submitted on 7 Nov 2014

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 RATIONAL POINTS OF JACOBIANS OVER FINITE FIELDS

PHILIPPE LEBACQUE AND ALEXEY ZYKIN

ABSTRACT. In this article we prove lower and upper bounds for class numbers of algebraic curves defined over finite fields. These bounds turn out to be better than most of the previously known bounds obtained using combinatorics. The methods used in the proof are essentially those from the explicit asymptotic theory of global fields. We thus provide a concrete application of effective results from the asymptotic theory of global fields and their zeta-functions.

1. INTRODUCTION

1.1. **Notation.** We introduce the following notation. Let

X	be a smooth projective absolutely irreducible curve defined over \mathbb{F}_q ,
g	the genus of X ,
K	the function field of X ,
Φ_{q^f}	the number of places of K of degree f ,
h	the class number of X (the number of \mathbb{F}_q -points of the Jacobian of X),
$Z_X(T)$	the zeta function of X which is a rational function of T ,
$\omega_i\sqrt{q}$	the inverse roots of the numerator of the zeta function $Z_X(T)$,
κ	the residue of $Z_X(q^{-s}) = \zeta_X(s)$ at $s = 1$,
\log	the Neperian logarithm \log_e .

By a *curve* we always mean a smooth projective absolutely irreducible curve.

1.2. **Existing lower bounds for the class number.** Our goal is to provide estimates for the number of rational points on the Jacobian of a smooth projective curve that use the information on the number of points on this curve defined over \mathbb{F}_q or over its extensions. The starting point for all such estimates is the interpretation of the class number as the value at 1 of the numerator of the zeta function of the curve. In order to estimate it, one uses properties of the zeta function, such as its functional equation and the Riemann Hypothesis (Weil bounds).

From the work of Weil, we know that the class number h of a smooth projective absolutely irreducible curve X of genus g defined over \mathbb{F}_q is bounded by :

$$(\sqrt{q} - 1)^{2g} \leq h \leq (\sqrt{q} + 1)^{2g} .$$

Considerable efforts have been devoted to sharpening these bounds. Let us quote some works in this direction. Lachaud and Martin-Deschamps first obtained the lower bound

$$h \geq h_{LMD} = q^{g-1} \frac{(q-1)^2}{(q+1)(g+1)},$$

The two authors were partially supported by ANR Globes ANR-12-JS01-0007-01 and the second author by AG Laboratory NRU HSE, RF government grant, ag. 11.G34.31.0023.

using a formula which is a consequence of the functional equation for the zeta function:

$$h = \frac{\sum_{n=0}^{g-1} A_n + \sum_{n=0}^{g-2} q^{g-1-n} A_n}{\sum_{i=1}^g |1 - \omega_i \sqrt{q}|^2},$$

where A_n is the number of effective divisors of degree n on X . Ever since, methods from combinatorics were used to give good bounds for the numerator and the denominator of this fraction.

In a series of papers [2],[3], Ballet, Rolland, and Tutdere used this approach in order to prove rather elaborate lower bounds on h . Some of these bounds turn out to be asymptotically optimal when $g \rightarrow \infty$, meaning that they converge to the lower bound from the generalized Brauer–Siegel theorem for function fields ([9]).

The best of their lower bounds is given by the following theorem:

Theorem 1.1 (Ballet–Rolland–Tutdere). *Let X/\mathbb{F}_q be a curve defined over \mathbb{F}_q of genus $g \geq 2$ and of class number h . Let D_1, D_2 be finite sets of integers, $(\ell_r)_{r \in D_1}, (m_r)_{r \in D_2}$ be families of integers such that*

- (1) $D_1 \subseteq \{1, \dots, g-1\}$;
- (2) $D_2 \subseteq \{1, \dots, g-2\}$;
- (3) for any $r \in D_1$, $\Phi_{q^r} \geq 1$;
- (4) for any $r \in D_2$, $\Phi_{q^r} \geq 1$;
- (5) $l_r \geq 0$ and $\sum_{r \in D_1} r l_r \leq g-1$;
- (6) $m_r \geq 0$ and $\sum_{r \in D_2} r m_r \leq g-2$.

Then $h \geq h_{BRT}$ with

$$h_{BRT} = \frac{(q-1)^2}{(g+1)(q+1) - \Phi_q} \left(\prod_{r \in D_1} \binom{\Phi_{q^r} + \ell_r}{\ell_r} + q^g \prod_{r \in D_2} \left[\left(\frac{q^r}{q^r - 1} \right)^{\phi_{q^r}} - \Phi_{q^r} \binom{\Phi_{q^r} + m_r}{m_r} \int_0^{q^{-r}} \frac{(q^{-r} - t)^{m_r}}{(1-t)^{\Phi_{q^r} + m_r + 1}} dt \right] \right).$$

From now on we denote by h_{BRT} the best possible lower bound from this theorem. In a recent article dealing with estimates for the number of points on general abelian varieties, Aubry, Haloui, and Lauchaud [1] obtained certain lower bounds on class numbers that can be very sharp when the curve in question has many rational points compared to its genus. However, these bounds are all rather poor from the asymptotic point of view when $g \rightarrow \infty$. Let us recall their results concerning Jacobian of curves.

Theorem 1.2 (Aubry–Haloui–Lachaud). *Under the same assumptions as in theorem 1.1, we have:*

$$(1) \ h \geq M(q)^g \left(q+1 + \frac{\Phi_q - (q+1)}{g} \right)^g, \text{ with } M(q) = \frac{e \log x^{\frac{1}{x}-1}}{x^{\frac{1}{x}} - 1}, \text{ where}$$

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

$$(2) \ h \geq \frac{q-1}{q^g - 1} \left[\binom{\Phi_q + 2g - 2}{2g - 1} + \sum_{r=2}^{2g-1} \Phi_{q^r} \binom{\Phi_q + 2g - 2 - r}{2g - 1 - i} \right].$$

(3) If $\Phi_q \geq g(\sqrt{q} - 1) + 1$ then

$$h \geq \binom{\Phi_q + g - 1}{g} - q \binom{\Phi_q + g - 3}{g - 2}.$$

$$(4) h \geq \frac{(g-1)^2}{(g+1)(q+1) - \Phi_q} \left[\binom{\Phi_q + g - 2}{g - 2} + \sum_{r=0}^{g-1} q^{g-1-1} \binom{\Phi_q + r - 1}{r} \right].$$

We denote by h_{AHL} the best possible lower bound for h given by (1) – (4) of this theorem. We remark that the estimate (3) can be very sharp when g is small and Φ_q is large. We will come back to that in §3.

1.3. The aim of this paper is to show how the Mertens theorem and the explicit Brauer–Siegel theorem lead to improvements of these bounds in many cases, most notably when g is large. This is done in §2 (Corollary 2.3). To do so we use the asymptotic theory of global fields and more precisely the technique of explicit formulae. The third section is devoted to numerical experiments. We compare the bounds in several examples provided by recursive asymptotically good towers of function fields. Finally, in the fourth section we discuss further research directions and open problems.

Acknowledgements. We would like to thank Stéphane Ballet, Julia Pielant and Michael Tsfasman for helpful discussions.

2. EXPLICIT FORMULAE AND THEIR LINK TO CLASS NUMBERS

2.1. **Explicit formulae.** Our starting point is the Mertens theorem ([6]) for curves and its relation to the generalized Brauer–Siegel theorem. Our exposition differs slightly from [6]: we take the opportunity to sharpen (and sometimes correct) the corresponding bounds.

Let us recall Serre’s explicit formulae from [8].

Theorem 2.1 (Explicit Formula). *For any sequence (v_n) such that the radius of convergence ρ of the series $\sum v_n t^n$ is strictly positive, put $\psi_{m,v}(t) = \sum_{n=1}^{+\infty} v_{mn} t^{mn}$, and $\psi_v(t) = \psi_{1,v}(t)$. Then for $t < q^{-1}\rho$, we have the following explicit formula:*

$$\sum_{f=1}^{+\infty} f \Phi_{q^f} \psi_{f,v}(t) = \psi_v(t) + \psi_v(qt) - \sum_{j=1}^{2g} \psi_v(\sqrt{q}\omega_j t).$$

We choose $N \in \mathbb{N}$ and take $v_n = \frac{1}{n}$ if $n \leq N$ and 0 otherwise. Applying theorem 2.1 with $t = q^{-1}$, we obtain the following identity:

$$S_0(N) = S_1(N) + S_2(N) + S_3(N),$$

where

$$S_0(N) = \sum_{n=1}^N n^{-1} q^{-n} \sum_{m|n} m \Phi_{q^m} = \sum_{f=1}^N \frac{1}{f q^f} |X(\mathbb{F}_{q^f})|,$$

$$S_1(N) = \sum_{n=1}^N \frac{1}{n}, \quad S_2(N) = \sum_{n=1}^N \frac{1}{n q^n}, \quad S_3(N) = - \sum_{j=1}^{2g} \sum_{n=1}^N \frac{1}{n} (q^{-\frac{1}{2}} \omega_j)^n.$$

We transform it in order to make the desired quantities appear. For any $N \geq 1$,

$$\begin{aligned}
S_0 - \underbrace{\sum_{f=1}^N \Phi_{q^f} \log \left(\frac{q^f}{q^f - 1} \right)}_{\varepsilon_0} + \sum_{f=1}^N \Phi_{q^f} \log \left(\frac{q^f}{q^f - 1} \right) &= \\
&= S_1 + \underbrace{S_2 - \log \frac{q}{q-1}}_{\varepsilon_2} + \log \frac{q}{q-1} \\
&\quad + \underbrace{S_3 - \log(\kappa \log q)}_{\varepsilon_3} + \log \frac{q}{q-1} + \log(\kappa \log q) - \log \frac{q}{q-1}.
\end{aligned}$$

In order to get bounds for h we will not need estimates on ε_0 and ε_2 , however they are useful for proving the Mertens theorem recalled later.

We have the following bounds for ε_i :

$$\begin{aligned}
-\frac{c_1(q)}{N q^{\frac{N}{2}}} - \frac{c_2(q)g}{N q^{\frac{3N}{4}}} &\leq \varepsilon_0 \leq 0, \\
-\frac{1}{(q-1)(N+1)q^N} &\leq \varepsilon_2 \leq 0, \quad 0 \leq |\varepsilon_3| \leq \frac{2g}{(\sqrt{q}-1)(N+1)q^{\frac{N}{2}}},
\end{aligned}$$

with

$$c_1(q) = \frac{2q(q+1)}{(q-1)^2} \leq 12 \quad \text{and} \quad c_2(q) = \frac{2q}{q-1} \left(\frac{\sqrt{q}}{\sqrt{q}-1} + \frac{q^{\frac{3}{2}}}{q^{\frac{3}{2}}-1} \right) \leq 20.$$

Indeed, note the inequalities that hold for $x > 1$ and $N > 0$:

$$0 \leq \log \left(\frac{x}{x-1} \right) - \sum_{n=1}^N \frac{1}{nx^n} = \sum_{n=N+1}^{+\infty} \frac{1}{nx^n} \leq \frac{1}{(N+1)x^{N+1}} \sum_{n=0}^{+\infty} \frac{1}{x^n} \leq \frac{1}{(N+1)x^N(x-1)}.$$

This implies the bounds for ε_2 . The one for ε_3 is derived from the classical formula ([9, Corollary 3.1.13]):

$$\log(\kappa \log q) - \log \frac{q}{q-1} = \sum_{i=1}^{2g} \log \left(1 - \frac{\omega_j}{\sqrt{q}} \right).$$

It gives us

$$\begin{aligned}
|\varepsilon_3| &= \left| - \sum_{j=1}^{2g} \sum_{n=1}^N \frac{1}{n} (q^{-\frac{1}{2}} \omega_j)^n - \log(\kappa \log q) + \log \frac{q}{q-1} \right| \\
&= \left| \sum_{j=1}^{2g} \left(- \log \left(1 - \frac{\omega_j}{\sqrt{q}} \right) - \sum_{n=1}^N \frac{1}{n} \left(\frac{\omega_j}{\sqrt{q}} \right)^n \right) \right|
\end{aligned}$$

and, since $|\omega_j| = 1$,

$$|\varepsilon_3| \leq \sum_{j=1}^{2g} \frac{1}{(N+1)\sqrt{q}^N |\sqrt{q} - \omega_j|} \leq \frac{2g}{(\sqrt{q}-1)(N+1)q^{\frac{N}{2}}}.$$

2.2. Bounds for the class number. Using the calculations from the previous section and applying the class number formula

$$\kappa \log q = \frac{h q^{1-g}}{q-1},$$

we get the following theorem.

Theorem 2.2. *Let X be a smooth projective absolutely irreducible curve defined over \mathbb{F}_q of class number h . Then h is given by the following formula valid for any $N \geq 1$:*

$$\log h = g \log q + \sum_{f=1}^N \frac{1}{f q^f} |X(\mathbb{F}_{q^f})| - \sum_{n=1}^N \frac{1+q^{-n}}{n} - \varepsilon_3(N),$$

or equivalently,

$$\log h = g \log q + \sum_{r=1}^N \left(\Phi_{q^r} \sum_{f=1}^{\lfloor \frac{N}{r} \rfloor} \frac{1}{f q^{rf}} \right) - \sum_{n=1}^N \frac{1+q^{-n}}{n} - \varepsilon_3(N),$$

where $\varepsilon_3(N)$ satisfies $|\varepsilon_3(N)| \leq \frac{2g}{(\sqrt{q}-1)(N+1)q^{\frac{N}{2}}}$.

Corollary 2.3. *(Bounds for the class number) The number of rational points h on the Jacobian of X satisfies $h_{\min}(N) \leq h \leq h_{\max}(N)$, where*

$$h_{\min}(N) = q^g \exp \left(\sum_{f=1}^N \frac{1}{f q^f} |X(\mathbb{F}_{q^f})| - \sum_{n=1}^N \frac{1+q^{-n}}{n} - \frac{2g}{(\sqrt{q}-1)(N+1)q^{\frac{N}{2}}} \right),$$

$$h_{\max}(N) = q^g \exp \left(\sum_{f=1}^N \frac{1}{f q^f} |X(\mathbb{F}_{q^f})| - \sum_{n=1}^N \frac{1+q^{-n}}{n} + \frac{2g}{(\sqrt{q}-1)(N+1)q^{\frac{N}{2}}} \right).$$

Remark 2.4. *The knowledge of a given (small) number of Φ_{q^f} 's allows us, nevertheless, to apply corollary 2.3 for any N . For example, in the case of lower bounds, one can bound from below the unknown Φ_{q^f} by 0 or by the quantities arising from the Weil bounds, depending which one is better. We thus get a family of bounds parametrized by N and we can choose the best one.*

2.3. Mertens theorem and class numbers. Putting together estimates from section 2.1, we find once again:

Theorem 2.5. *(Mertens theorem, [6]) Let X be a smooth projective absolutely irreducible curve of genus g defined over \mathbb{F}_q . Then*

$$\sum_{f=1}^N \Phi_{q^f} \log \left(\frac{q^f}{q^f - 1} \right) = \log(\kappa \log q) - \varepsilon_0 + \varepsilon_2 + \varepsilon_3 - \sum_{n=1}^N \frac{1}{n}.$$

For any $N \geq 1$, we can deduce from it a weaker form of our bound, which might be easier compared to Ballet–Rolland–Tutdere's bound:

$$\log h = g \log q + \left[\sum_{f=1}^N \Phi_{q^f} \log \left(\frac{q^f}{q^f - 1} \right) \right] - \sum_{n=1}^N \frac{1+q^{-n}}{n} + \varepsilon_0 - \varepsilon_3.$$

Remark 2.6. *Theorem 2.5 implies that our bounds on h are asymptotically optimal. More precisely, recall that a family of curves $\{X_i\}$ over \mathbb{F}_q of genus $g_i \rightarrow \infty$ is asymptotically exact if the limits $\phi_{q^r} = \lim_{i \rightarrow \infty} \frac{\Phi_{q^r}(X_i)}{g_i}$ exist for all r . For asymptotically exact families of curves the generalized Brauer–Siegel theorem ([9]) affirms that*

$$\lim_{i \rightarrow \infty} \frac{\log h(X_i)}{g_i} = \log q + \sum_{r=1}^{\infty} \phi_{q^r} \log \left(\frac{q^r}{q^r - 1} \right).$$

We see that when $N \rightarrow \infty$ the bounds $h_{\min}(N)$ and $h_{\max}(N)$ from corollary 2.3 converge to the right hand side of the above equality being divided by g_i .

3. NUMERICAL COMPUTATIONS

In this section, we compare the lower bound $h_{\min}(N)$ given by our theorem 2.2 with h_{BRT} and h_{AHL} in the situation of recursive towers. We denote by h_{LZ} the bound from theorem 2.2 for the optimal choice of N . Such a number N is found by computer-aided calculations where the missing information on the number of points on a curve X over \mathbb{F}_{q^r} is obtained either from the inequality $X(\mathbb{F}_{q^r}) \geq X(\mathbb{F}_{q^d})$ when $d \mid r$, or from the Serre’s bound $X(\mathbb{F}_{q^r}) \geq q^r + 1 - g \lfloor 2q^{r/2} \rfloor$, depending on which one is more precise. We follow closely [3, Section 5].

Recall that a *tower* of function fields over \mathbb{F}_q is an infinite sequence $\{F_k/\mathbb{F}_q\}_{k \in \mathbb{N}}$ of function fields such that for all k the ground field \mathbb{F}_q is algebraically closed in F_k , $F_k \subset F_{k+1}$, and the genus $g(F_k) \rightarrow \infty$. A *recursive tower* is a tower $\{F_k\}$ of function fields over \mathbb{F}_q such that $F_0 = \mathbb{F}_q(x_0)$ is a rational function field and $F_{k+1} = F_k(x_{k+1})$ where x_{k+1} satisfy the equation $f(x_k, x_{k+1}) = 0$ for a given polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$.

3.1. The first tower of Garcia–Stichtenoth. Assume that q^r is a square and consider the tower $\{H_k\} = \mathcal{H}/\mathbb{F}_{q^r}$ defined recursively by the polynomial

$$f(X, Y) = Yq^{\frac{r}{2}} Xq^{\frac{r}{2}-1} + Y - Xq^{\frac{r}{2}} \in \mathbb{F}_q[X, Y].$$

We also consider the recursive tower $\{F_k\} = \mathcal{F}/\mathbb{F}_q$ of function fields defined by the same polynomial starting with the rational function field $\mathbb{F}_q(x_0)$. The base change of F_k to \mathbb{F}_{q^r} gives H_k .

We compare the numerical estimates from [3, Section 5.1] with what we obtain using our bound h_{LZ} . We take $q = 2, r = 2$ and consider the fields H_2, H_3 , and H_4 . Note an error in [3, Section 5.1] where for $k = 3$ the genus is erroneously taken to be equal to 14 instead of 13 (this was pointed out by Julia Pielant).

Step k	$g(H_k)$	$B_1(H_k)$	h_{BRT}	h_{AHL}	h_{LZ}	N
2	5	16	7434	12240	9230	10
3	13	30	16 911 279 581	16 271 525 520	26 274 427 880	33
4	33	56	1.43×10^{25}	0.075×10^{25}	4.149×10^{25}	83

Here is a similar comparison for $q = 2$ and the tower \mathcal{F} .

Step k	$g(F_k)$	$B_1(F_k)$	$B_2(F_k)$	h_{BRT}	h_{LZ}	N
2	5	2	7	7	30	12
3	13	2	14	10453	42898	26
4	33	2	27	343 733 443 618	1 543 267 494 985	74

We notice that our bound is better than the other ones except for the case of H_2/\mathbb{F}_4 where we can not beat the h_{AHL} bound. The situation changes, however, if we use some additional information on the places of H_2/\mathbb{F}_4 . Namely, one can calculate that $B_2(H_2) = 0$ and $B_3(H_2) = 24$. These values give the bound $h_{LZ} = 13430$ reached for $N = 11$. Using MAGMA we calculated that the exact value of the class number is 16200.

3.2. The tower of Bassa–Garcia–Stichtenoth. Consider the tower $\{H_k\} = \mathcal{H}/\mathbb{F}_{q^3}$ defined recursively by the polynomial

$$f(X, Y) = (Y^q - Y)^{q-1} + 1 + \frac{X^{q(q-1)}}{(X^{q-1} - 1)^{q-1}} \in \mathbb{F}_q[X, Y]$$

and let $\{F_k\} = \mathcal{F}/\mathbb{F}_q$ be the same recursive tower over \mathbb{F}_q . We have the following numerical estimates for the class numbers when $q = 2$, that is over \mathbb{F}_8 for H_k and over \mathbb{F}_2 for F_k . The value of h_{BRT} bound is taken from [3, Section 5.1].

Step k	$g(H_k)$	$B_1(H_k)$	h_{BRT}	h_{LZ}	N
2	5	24	125 537	126832	9
3	13	48	2.556×10^{13}	4.039×10^{13}	29
4	29	96	2.010×10^{30}	5.778×10^{30}	11

Step k	$g(F_k)$	$B_3(F_k)$	h_{BRT}	h_{LZ}	N
2	5	8	3	3	5
3	13	16	771	1623	19
4	29	32	212 127 395	751 622 136	61

3.3. Composite towers. The next example is the composite tower $\{E_k/\mathbb{F}_{q^2}\}$ constructed in [4]. It is obtained as a composite of the tower of Garcia and Stichtenoth from section 3.1 with a certain explicitly given function field. The details can be found in [3, Propositions 5.11]. The following table combines the estimates for $q^2 = 4$.

Step k	$g(E_k)$	$B_1(E_k)$	$B_2(E_k)$	$B_3(E_k)$	h_{BRT}	h_{LZ}	N
2	55	1	12	12	3.657×10^{31}	23.55×10^{31}	14
3	132	1	24	24	9.198×10^{77}	121.02×10^{77}	15

For another two composite towers $\{E_k/\mathbb{F}_2\}$ and $\{E'_k/\mathbb{F}_8\}$ this time based on the tower from section 3.2 (see [3, Proposition 5.17] for a detailed description) we get the following numerical data:

Step k	$g(E_k)$	$B_3(E_k)$	$B_6(E_k)$	h_{BRT}	h_{LZ}	N
2	17	16	8	10 254	27563	30
3	49	32	16	1.718×10^{14}	9.173×10^{14}	94

Step k	$g(E'_k)$	$B_1(E'_k)$	$B_2(E'_k)$	h_{BRT}	h_{LZ}	N
2	17	48	24	1.002×10^{17}	2.304×10^{17}	35
3	49	96	48	2.426×10^{48}	13.08×10^{48}	10

One more composite tower E_k/\mathbb{F}_4 introduced in [10] (see also [3, Proposition 5.18]) gives us the following table:

Step k	$g(E_k)$	$B_1(E_k)$	$B_2(E_k)$	$B_3(E_k)$	h_{BRT}	h_{LZ}	N
2	30	1	9	9	4.625×10^{16}	18.329×10^{16}	52
3	89	1	27	27	2.236×10^{52}	21.39×10^{52}	16

For the composite tower E_k/\mathbb{F}_9 from [3, Proposition 5.20] we obtain.

Step k	$g(E_k)$	$B_1(E_k)$	$B_2(E_k)$	h_{BRT}	h_{LZ}	N
2	15	36	4	8.563×10^{14}	18.76×10^{14}	30
3	46	72	8	7.470×10^{45}	41.64×10^{45}	10

Finally, for yet another composite tower E_k/\mathbb{F}_4 from [3, Proposition 5.22] we get.

Step k	$g(E_k)$	$B_1(E_k)$	$B_2(E_k)$	h_{BRT}	h_{LZ}	N
2	25	36	9	1.415×10^{18}	3.835×10^{18}	56
3	124	108	27	3.501×10^{86}	36.23×10^{86}	16

In all these examples with one exception we manage to improve on the previously known bounds.

4. OPEN QUESTIONS

Several natural questions arise in connection with the bounds obtained in this paper.

Question 4.1. *Is it possible to compare the bounds h_{BRT} , h_{AHL} , and h_{LZ} ?*

We would like to have a more or less explicit description of the cases when each of the bounds is the best one. In the above examples our bound h_{LZ} always turned out to be better than h_{BRT} . However, we were not able to establish this fact in general. Comparing the bounds h_{LZ} and h_{BRT} does not seem to be straight forward in particular due to the fact that the number N corresponding to optimal $h_{min}(N)$ can vary significantly and does not correspond at all to the number of known Φ_{q^r} 's.

Question 4.2. *Can one improve (or even optimize) the bound h_{LZ} using different test functions in the explicit formulae?*

Oesterlé managed to get the best possible bounds for $|X(\mathbb{F}_{q^r})|$ available from explicit formulae using the linear programming approach (see [8]). This technique, however, does not seem to be applicable directly in our case due to the non-linearity of the problem in question. The optimization seeming difficult, it would be interesting at least to find examples where different choice of test functions in the explicit formulae leads to better bounds than h_{LZ} .

Question 4.3. *What are the analogues of the above bounds in the number field case?*

This question seems to be more directly accessible than the previous ones, since there are both the Mertens theorem and an explicit version of the Brauer–Siegel theorem available in the number field case ([6], [7]). Nevertheless, analytic component in the proofs will certainly be more substantial and the application of the Generalized Riemann Hypothesis might be necessary in certain cases.

REFERENCES

- [1] Y. Aubry, S. Haloui, G. Lachaud. Sur le nombre de points rationnels des variétés abéliennes et des Jacobiennes sur les corps finis. *C. R. Acad. Sci. Paris*, Ser. I 350, 907–910, 2012.
- [2] S. Ballet, R. Rolland. Lower bounds on the class number of algebraic function field defined over any finite field. *J. Théor. Nombres Bordeaux*, 24(3), 505–540, 2012.
- [3] S. Ballet, R. Rolland, S. Tutdere. Lower Bounds on the number of rational points of Jacobians over finite fields and application to algebraic function fields in towers. *arXiv:1303.5822*
- [4] Florian Hess, Henning Stichtenoth, and Seher Tutdere. On invariants of towers of function fields over finite fields. *Journal of Algebra and Its Applications*, 12(4), 477–487, 2013.
- [5] G. Lachaud, M. Martin-Deschamps. Nombre de points des jacobiennes sur un corps fini. *Acta Arith.*, 56(4): 329–340, 1990.
- [6] P. Lebacque. Generalised Mertens and Brauer-Siegel theorems. *Acta Arith.*, 130(4):333–350, 2007.
- [7] P. Lebacque, A. Zykin. On logarithmic derivatives of zeta functions in families of global fields. *International Journal of Number Theory*, 7(8), 2139–2156, 2011.
- [8] J.-P. Serre, Rational Points on Curves over Finite Fields, Lecture Notes, Harvard University, 1985
- [9] M. A. Tsfasman, S. G. Vlăduț, D. Nogin. Algebraic geometric codes: basic notions, Mathematical Surveys and Monographs, **139**, American Mathematical Society, Providence, RI, 2007.
- [10] Jörg Wulftange. Zahme Türme algebraischer Funktionenkörper. PhD thesis, Essen University, 2002.

PHILIPPE LEBACQUE

LABORATOIRE DE MATHÉMATIQUES DE BESANÇON, UFR SCIENCES ET TECHNIQUES
16, ROUTE DE GRAY 25 030 BESANÇON, FRANCE

E-mail address: philippe.lebacque@univ-fcomte.fr

ALEXEY ZYKIN

LABORATOIRE GAATI, UNIVERSITÉ DE LA POLYNÉSIE FRANÇAISE, BP 6570 — 98702 FAA'A,
TAHITI, POLYNÉSIE FRANÇAISE

DEPARTMENT OF MATHEMATICS OF THE NATIONAL RESEARCH UNIVERSITY HIGHER SCHOOL OF
ECONOMICS

AG LABORATORY NRU HSE

LABORATOIRE PONCELET (UMI 2615)

INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS OF THE RUSSIAN ACADEMY OF
SCIENCES

E-mail address: alzykin@gmail.com