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.archives-ouvertes.fr/hal-01081468
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

- $X$ the genus of $X$,
- $K$ the function field of $X$,
- $\Phi_q(f)$ 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 $Z_X(T)$,
- $\kappa$ 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 Tuñedere used this approach in order to prove rather elaborate lower bounds on \( h \). Some of these bounds turn out to be asymptotically optimal when \( g \to \infty \), 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–Tuñedere). 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. \( D_1 \subseteq \{1, \ldots, g - 1\} \);
2. \( D_2 \subseteq \{1, \ldots, g - 2\} \);
3. for any \( r \in D_1 \), \( \Phi_q \ell_r \geq 1 \);
4. for any \( r \in D_2 \), \( \Phi_q m_r \geq 1 \);
5. \( \ell_r \geq 0 \) and \( \sum_{r \in D_1} r \ell_r \leq g - 1 \);
6. \( m_r \geq 0 \) and \( \sum_{r \in D_2} r m_r \leq g - 2 \).

Then \( h \geq h_{BRT} \) with

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

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 \( g \to \infty \). Let us recall their results concerning Jacobian of curves.

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

1. \( h \geq M(q)^g \left( q + 1 + \frac{\Phi_q - (q + 1)}{g} \right)^g \), with \( M(q) = \frac{e \log x^{1/2} - 1}{x^{1/2} - 1} \), where
   \[
x = \left( \frac{\sqrt{q} + 1}{\sqrt{q} - 1} \right)^2.
\]
2. \( h \geq \frac{q - 1}{q^g - 1} \left[ \Phi_q + 2g - 2 \right] + \sum_{r=2}^{2g-1} \Phi_q \left( \frac{\Phi_q + 2g - 2 - r}{2g - 1 - i} \right). \)
If \( \Phi_q \geq g(\sqrt{q} - 1) + 1 \) then
\[
h \geq \left( \frac{\Phi_q + g - 1}{g} \right) - q\left( \frac{\Phi_q + g - 3}{g - 2} \right).
\]

(4) \( h \geq \frac{(q - 1)^2}{(g + 1)(q + 1) - \Phi_q} \left[ \left( \frac{\Phi_q + g - 2}{g - 2} \right)^{g - 1} + \sum_{r=0}^{g-1} q^{g-1-1} \left( \frac{\Phi_q + r - 1}{r} \right) \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 \( \Phi_q \) 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 Pieltant 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 \( \rho \) of the series \( \sum v_n t^n \) is strictly positive, put \( \psi_{m,v}(t) = \sum_{n=1}^{\infty} v_m t^n \), and \( \psi_v(t) = \psi_{1,v}(t) \). Then for \( t < q^{-1} \rho \), we have the following explicit formula:
\[
\sum_{f=1}^{+\infty} f^{\Phi_q} \psi_{f,v}(t) = \psi_v(t) + \psi_v(qt) - \sum_{j=1}^{2g} \psi_v(\sqrt{q} \omega_j t).
\]

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
\[
S_0(N) = \sum_{n=1}^{N} n^{-1} q^{-n} \sum_{m | n} m^{\Phi_q} = \sum_{f=1}^{N} \frac{1}{f q^f} |X(F_{q^f})|,
\]
\[
S_1(N) = \sum_{n=1}^{N} \frac{1}{n}, \quad S_2(N) = \sum_{n=1}^{N} \frac{1}{n q^n}, \quad S_3(N) = -\sum_{j=1}^{2g} \sum_{n=1}^{N} \frac{1}{n} (q^{-\frac{1}{2}} \omega_j)^n.
\]
We transform it in order to make the desired quantities appear. For any $N \geq 1$,
\[
S_0 - \sum_{f=1}^{N} \Phi_q f \log \left( \frac{q^f}{q^f - 1} \right) + \sum_{f=1}^{N} \Phi_q f \log \left( \frac{q^f}{q^f - 1} \right) =
\]
\[
= S_1 + S_2 - \log \frac{q}{q - 1} + \log \frac{q}{q - 1}
\]
\[
+ S_3 - \log (\kappa \log q) + \log \frac{q}{q - 1} + \log (\kappa \log q) - \log \frac{q}{q - 1}.
\]

In order to get bounds for $h$ we will not need estimates on $\varepsilon_0$ and $\varepsilon_2$, however they are useful for proving the Mertens theorem recalled later.

We have the following bounds for $\varepsilon_i$:
\[
-\frac{c_1(q)}{N q^{\frac{2}{x}}} - \frac{c_2(q)q}{N q^{\frac{2}{x}}} \leq \varepsilon_0 \leq 0,
\]
\[
-\frac{1}{(q - 1)(N + 1)q^x} \leq \varepsilon_2 \leq 0, \quad 0 \leq |\varepsilon_3| \leq \frac{2g}{(\sqrt{q} - 1)(N + 1)q^{\frac{2}{x}}},
\]
with
\[
c_1(q) = \frac{2q(q + 1)}{(q - 1)^2} \leq 12 \quad \text{and} \quad c_2(q) = \frac{2q}{q - 1} \left( \frac{\sqrt{q}}{\sqrt{q} - 1} + \frac{q^{\frac{3}{2}}}{q^{x} - 1} \right) \leq 20.
\]

Indeed, note the inequalities that hold for $x > 1$ and $N > 0$:
\[
0 \leq \log \left( \frac{x}{x - 1} \right) - \sum_{n=1}^{N} \frac{1}{n x^n} = \sum_{n=N+1}^{+\infty} \frac{1}{n x^n} \leq \frac{1}{(N + 1) x^{N+1}} \sum_{n=0}^{+\infty} \frac{1}{n x^n} \leq \frac{1}{(N + 1) x^{N}(x - 1)}.
\]

This implies the bounds for $\varepsilon_2$. The one for $\varepsilon_3$ is derived from the classical formula ([9, Corollary 3.1.13]):
\[
\log (\kappa \log q) - \log \frac{q}{q - 1} = \sum_{i=1}^{2g} \log \left( 1 - \frac{\omega_i}{\sqrt{q}} \right).
\]

It gives us
\[
|\varepsilon_3| = \left| - \sum_{j=1}^{2g} \sum_{n=1}^{N} \frac{1}{n} (q^{\frac{1}{2}} \omega_j)^n - \log (\kappa \log q) + \log \frac{q}{q - 1} \right|
\]
\[
= \sum_{j=1}^{2g} \left| - \log \left( 1 - \frac{\omega_j}{\sqrt{q}} \right) - \sum_{n=1}^{N} \frac{1}{n} \left( \frac{\omega_j}{\sqrt{q}} \right)^n \right|
\]
and, since $|\omega_j| = 1$,
\[
|\varepsilon_3| \leq \sum_{j=1}^{2g} \frac{1}{(N + 1) \sqrt{q} N |\sqrt{q} - \omega_j|} \leq \frac{2g}{(\sqrt{q} - 1)(N + 1)q^{\frac{2}{x}}}.\]
2.2. **Bounds for the class number.** Using the calculations from the previous section and applying the class number formula
\[
\kappa \log q = \frac{hq^{1-g}}{q-1},
\]
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 \(N \geq 1\):
\[
\log h = g \log q + \sum_{f=1}^{N} \frac{1}{fq^f} |X(\mathbb{F}_{q^f})| - \sum_{n=1}^{N} \frac{1 + q^{-n}}{n} - \varepsilon_3(N),
\]
or equivalently,
\[
\log h = g \log q + \sum_{r=1}^{N} \left( \Phi_{q^r} \sum_{f=1}^{N} \frac{1}{fq^f} \right) - \sum_{n=1}^{N} \frac{1 + q^{-n}}{n} - \varepsilon_3(N),
\]
where \(\varepsilon_3(N)\) satisfies \(|\varepsilon_3(N)| \leq \frac{2g}{(\sqrt{q} - 1)(N + 1)q^{N^2}}\).

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

**Remark 2.4.** The knowledge of a given (small) number of \(\Phi_{q^f}\)'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 \(\Phi_{q^f}\) 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 chose 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 $g_i \to \infty$ is asymptotically exact if the limits $\phi_{q^r}(X_i) = \lim_{i \to \infty} \frac{\log h(X_i)}{g_i}$ exist for all $r$. For asymptotically exact families of curves the generalized Brauer–Siegel theorem ([9]) affirms that

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

We see that when $N \to \infty$ the bounds $h_{\text{min}}(N)$ and $h_{\text{max}}(N)$ 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 $h_{\text{min}}(N)$ given by our theorem 2.2 with $h_{\text{BRT}}$ and $h_{\text{AHL}}$ in the situation of recursive towers. We denote by $h_{\text{LZ}}$ 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 $d | r$, or from the Serre’s bound $X(\mathbb{F}_{q^r}) \geq q^r + 1 - (2q^{r/2}]$, 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 $g(F_k) \to \infty$. 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 $\{H_k\} = H/\mathbb{F}_{q^r}$ defined recursively by the polynomial

$$f(X, Y) = Y^{q^{r/2}} X^{q^{r/4} - 1} + Y - X^{q^{r/2}} \in \mathbb{F}_q[X, Y].$$

We also consider the recursive tower $\{F_k\} = \mathcal{F}/\mathbb{F}_{q^r}$ of function fields defined by the same polynomial starting with the rational function field $\mathbb{F}_{q^r}(x_0)$. 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 $h_{\text{LZ}}$. 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 Pieliant).

<table>
<thead>
<tr>
<th>Step $k$</th>
<th>$g(H_k)$</th>
<th>$B_1(H_k)$</th>
<th>$h_{\text{BRT}}$</th>
<th>$h_{\text{AHL}}$</th>
<th>$h_{\text{LZ}}$</th>
<th>$N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
<td>16</td>
<td>7434</td>
<td>12240</td>
<td>9230</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td>30</td>
<td>16 941 279 581</td>
<td>16 271 525 520</td>
<td>26 274 427 880</td>
<td>33</td>
</tr>
<tr>
<td>4</td>
<td>33</td>
<td>56</td>
<td>$1.43 \times 10^{32}$</td>
<td>$0.075 \times 10^{32}$</td>
<td>$4.149 \times 10^{32}$</td>
<td>83</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step $k$</th>
<th>$g(F_k)$</th>
<th>$B_1(F_k)$</th>
<th>$B_2(F_k)$</th>
<th>$h_{\text{BRT}}$</th>
<th>$h_{\text{LZ}}$</th>
<th>$N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
<td>2</td>
<td>7</td>
<td>7</td>
<td>30</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td>2</td>
<td>14</td>
<td>10453</td>
<td>42898</td>
<td>26</td>
</tr>
<tr>
<td>4</td>
<td>33</td>
<td>2</td>
<td>27</td>
<td>343 733 443 618</td>
<td>1 543 267 494 985</td>
<td>74</td>
</tr>
</tbody>
</table>
We notice that our bound is better than the other ones except for the case of \( H_2/F_4 \) where we can not beat the \( h_{AHL} \) bound. The situation changes, however, if we use some additional information on the places of \( H_2/F_4 \). 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].

<table>
<thead>
<tr>
<th>Step k</th>
<th>( g(H_k) )</th>
<th>( B_1(H_k) )</th>
<th>( h_{BRT} )</th>
<th>( h_{LZ} )</th>
<th>( N )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
<td>24</td>
<td>125 537</td>
<td>126832</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td>48</td>
<td>2.556 \times 10^{13}</td>
<td>4.039 \times 10^{13}</td>
<td>29</td>
</tr>
<tr>
<td>4</td>
<td>29</td>
<td>96</td>
<td>2.010 \times 10^{30}</td>
<td>5.778 \times 10^{30}</td>
<td>11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step k</th>
<th>( g(F_k) )</th>
<th>( B_3(F_k) )</th>
<th>( h_{BRT} )</th>
<th>( h_{LZ} )</th>
<th>( N )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
<td>8</td>
<td>3</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td>16</td>
<td>771</td>
<td>1623</td>
<td>19</td>
</tr>
<tr>
<td>4</td>
<td>29</td>
<td>32</td>
<td>212 127 395</td>
<td>751 622 136</td>
<td>61</td>
</tr>
</tbody>
</table>

### 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, Proposition 5.11]. The following table combines the estimates for \( q^2 = 4 \).

<table>
<thead>
<tr>
<th>Step k</th>
<th>( g(E_k) )</th>
<th>( B_1(E_k) )</th>
<th>( B_2(E_k) )</th>
<th>( B_3(E_k) )</th>
<th>( h_{BRT} )</th>
<th>( h_{LZ} )</th>
<th>( N )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>55</td>
<td>1</td>
<td>12</td>
<td>12</td>
<td>3.65 \times 10^{14}</td>
<td>23.55 \times 10^{14}</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>132</td>
<td>1</td>
<td>24</td>
<td>24</td>
<td>9.198 \times 10^{17}</td>
<td>121.02 \times 10^{17}</td>
<td>15</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step k</th>
<th>( g(E'_k) )</th>
<th>( B_3(E'_k) )</th>
<th>( h_{BRT} )</th>
<th>( h_{LZ} )</th>
<th>( N )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>17</td>
<td>48</td>
<td>1.002 \times 10^{14}</td>
<td>2.304 \times 10^{14}</td>
<td>35</td>
</tr>
<tr>
<td>3</td>
<td>49</td>
<td>48</td>
<td>2.426 \times 10^{18}</td>
<td>13.08 \times 10^{18}</td>
<td>10</td>
</tr>
</tbody>
</table>

One more composite tower \( E_4/\mathbb{F}_4 \) introduced in [10] (see also [3, Proposition 5.18]) gives us the following table:
For the composite tower $E_k/F_3$ from [3, Proposition 5.20] we obtain.

<table>
<thead>
<tr>
<th>Step k</th>
<th>$g(E_k)$</th>
<th>$B_1(E_k)$</th>
<th>$B_2(E_k)$</th>
<th>$B_3(E_k)$</th>
<th>$h_{BRT}$</th>
<th>$h_{LZ}$</th>
<th>$N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>30</td>
<td>1</td>
<td>9</td>
<td>9</td>
<td>$4.625 \times 10^{16}$</td>
<td>$18.329 \times 10^{16}$</td>
<td>52</td>
</tr>
<tr>
<td>3</td>
<td>89</td>
<td>1</td>
<td>27</td>
<td>27</td>
<td>$2.236 \times 10^{16}$</td>
<td>$21.39 \times 10^{16}$</td>
<td>16</td>
</tr>
</tbody>
</table>

Finally, for yet another composite tower $E_k/F_4$ from [3, Proposition 5.22] we get.

<table>
<thead>
<tr>
<th>Step k</th>
<th>$g(E_k)$</th>
<th>$B_1(E_k)$</th>
<th>$B_2(E_k)$</th>
<th>$h_{BRT}$</th>
<th>$h_{LZ}$</th>
<th>$N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>15</td>
<td>36</td>
<td>4</td>
<td>$8.563 \times 10^{14}$</td>
<td>$18.76 \times 10^{14}$</td>
<td>30</td>
</tr>
<tr>
<td>3</td>
<td>46</td>
<td>72</td>
<td>8</td>
<td>$7.470 \times 10^{45}$</td>
<td>$41.64 \times 10^{45}$</td>
<td>10</td>
</tr>
</tbody>
</table>

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 straightforward 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 $\Phi_q$’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 $|X(F_q)|$ 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 then 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


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
Laboratory NRU HSE
Laboratoire Poncelet (UMI 2615)
Institute for Information Transmission Problems of the Russian Academy of Sciences
E-mail address: alzykin@gmail.com