MATHEMATICS OF COMPUTATION
Volume 71, Number 238, Pages 837–861
S 0025-5718(01)01385-0
Article electronically published on October 4, 2001

EXPLICIT BOUNDS AND HEURISTICS ON CLASS NUMBERS IN HYPERELLIPTIC FUNCTION FIELDS

ANDREAS STEIN AND EDLYN TESKE

Abstract. In this paper, we provide tight estimates for the divisor class number of hyperelliptic function fields. We extend the existing methods to any hyperelliptic function field and improve the previous bounds by a factor proportional to g with the help of new results. We thus obtain a faster method of computing regulators and class numbers. Furthermore, we provide experimental data and heuristics on the distribution of the class number within the bounds on the class number. These heuristics are based on recent results by Katz and Sarnak. Our numerical results and the heuristics imply that our approximation is in general far better than the bounds suggest.

1. Introduction

Two important invariants of a hyperelliptic function field are the regulator and the divisor class number. Since the divisor class number and the regulator represent the size of the key space of the hyperelliptic cryptosystems in [Kob88] and [SSW96], respectively, they are of cryptographic relevance, and it is of major interest to have fast algorithms for computing them. Since there exist effective subexponential methods for large genus hyperelliptic function fields (see [ADH94, MST99]), one restricts the cryptographic applications to the case that the genus of the hyperelliptic function field is relatively small. For a survey on hyperelliptic curves and function fields we refer to [Poo96].

For a general hyperelliptic function field K over a finite field k, the fastest effective algorithms in current implementations make use of a method of approximating the divisor class number h of K by truncated Euler products. The basic idea of these techniques is to find integers E and L such that $|h-E| < L^2$, i.e., an interval such that $h \in]E-L^2, E+L^2[$. Having found such an interval of length $2L^2-1$, we can search for h in this interval by a baby step–giant step method [SW99, SW98] or by Pollard's kangaroo method [STb] in $O(L)$ operations. In this paper, we provide considerably better bounds on $|h-E|$ than in [SW99]. For instance, let $K/\mathbb{F}_q$ be a hyperelliptic function field of odd genus g, where $g \equiv 3 \pmod 5$. Then our new bound on $|h-E|$ is by a factor of $(2g+3)(2g+4)/(5(2g+1))$ smaller than the bound in [SW99] assuming that q is large compared to g. The improved bounds, which are given in Theorem 4.1 and Theorem 4.3, can be derived from

Received by the editor July 27, 1999 and, in revised form, August 2, 2000.
2000 *Mathematics Subject Classification.* Primary 11Y16, 11Y40, 11R29, 11R58; Secondary 11M38, 11R65.
Key words and phrases. Hyperelliptic function field, class numbers, regulator, truncated Euler products.

Theorem 1.1. *Let $K = k(X)(\sqrt{D})$ be a hyperelliptic function field of genus g over the finite field k of odd characteristic, where $D \in k[X]$ is squarefree. Then the following statements are true for all integers $n \geq 1$:*

1. *If $\deg(D) = 2g+2$ and the leading coefficient of D is a square in k^*, then we have*

$$\sum_{\nu|n} \nu \sum_{\deg(P)=\nu} \chi(P)^{n/\nu} = -1 - \sum_{i=1}^{2g} \omega_i^n \ . \tag{1.1}$$

2. *If $\deg(D) = 2g+1$, then we have*

$$\sum_{\nu|n} \nu \sum_{\deg(P)=\nu} \chi(P)^{n/\nu} = -\sum_{i=1}^{2g} \omega_i^n \ . \tag{1.2}$$

3. *If $\deg(D) = 2g+2$ and the leading coefficient of D is not a square in k^*, then we have*

$$\sum_{\nu|n} \nu \sum_{\deg(P)=\nu} \chi(P)^{n/\nu} = (-1)^{n+1} - \sum_{i=1}^{2g} \omega_i^n \ . \tag{1.3}$$

Here, the complex numbers ω_i $(i = 1, \ldots, 2g)$ are the reciprocals of the roots of the zeta-function $Z(u, K)$ in $u = q^{-s}$. Further, $\chi(P)$ denotes the polynomial Legendre symbol $[D/P]$ and P runs through all monic prime polynomials of degree ν.

Furthermore, via Möbius inversion, this theorem relates the reciprocals of the roots of $Z(u, K)$ to the character sums of the form $\sum_{\deg(P)=n} \chi(P)$.

We now proceed as follows. We first summarize results on the ζ-functions of algebraic function fields. In Section 3, we apply these results to hyperelliptic function fields and prove Theorem 1.1. The improved bounds on $|h - E|$ and the estimates are discussed in Section 4. Hereby, we present two possible approximations for the divisor class number h. The first approximation is theoretically better than the second one. However, numerical results show that the second approximation is in general more accurate. In Section 5, we show how the improved bounds can be used to produce a faster algorithm for computing the regulator and the divisor class number of a hyperelliptic function field. In Section 6, we present experimental and heuristic results on the distribution of $|h - E|/L^2$ in the case of real quadratic function fields and we provide an explanation of these results. Our conclusions and further discussions can be found in Section 7.

2. ζ-function and l-polynomial in algebraic function fields

For an introduction to function fields, we refer to [Sti93, Deu73]. Let K/k be an algebraic function field of genus g over the finite field $k = \mathbb{F}_q$. We denote by $\mathrm{Div}_0(K)$ the group of divisors of degree 0. The group of principal divisors $P(K)$ is a subgroup of $\mathrm{Div}_0(K)$ and the factor group $\mathrm{Cl}_0(K) = \mathrm{Div}_0(K)/P(K)$ is called the *divisor class group (of degree 0)* of K. Its order $h = |\mathrm{Cl}_0(K)|$ is said to be the *divisor class number* of K. If $\mathfrak{P}$ is a prime divisor of K, then the *absolute norm* of $\mathfrak{P}$ is defined by the integer $N(\mathfrak{P}) = q^{f_\mathfrak{P}}$, where $f_\mathfrak{P}$ is the degree of $\mathfrak{P}$. The *absolute norm* of a divisor $\mathfrak{A} = \sum a_\mathfrak{P} \mathfrak{P}$ is defined to be $N(\mathfrak{A}) = q^{f_\mathfrak{A}}$, where $f_\mathfrak{A} = \sum a_\mathfrak{P} f_\mathfrak{P}$

denotes the degree of $\mathfrak{A}$. The ζ-function of K is defined by

$$\zeta(s,K)=\sum_{\mathfrak{A}}\frac{1}{N(\mathfrak{A})^s}\quad(\Re(s)>1)\ ,$$

where the summation is over all integral divisors $\mathfrak{A}$ of K. We set $u=q^{-s}$. Then, the Euler product for $\zeta(s,K)$ reads

$$\zeta(s,K)=\prod_{\mathfrak{P}}\frac{1}{1-\frac{1}{N(\mathfrak{P})^s}}=\prod_{\mathfrak{P}}\frac{1}{1-u^{f_{\mathfrak{P}}}}\ ,$$

where the product is over all prime divisors of K. It is well-known that $\zeta(s,K)$ is a rational function in u that is periodic with period $2\pi i/\log q$ and analytic in the whole plane with the exception of simple poles at $s=l\cdot 2\pi i/\log q$ and $s=1+l\cdot 2\pi i/\log q$ ($l\in\mathbb{Z}$). More precisely, we have (see, for instance, [Sti93, Theorem V.1.15 and V.2.1])

$$\zeta(s,K)=Z(u,K)=\frac{L(u,K)}{(1-u)\,(1-qu)}=\frac{\prod_{i=1}^{2g}(1-\omega_i u)}{(1-u)\,(1-qu)}\ , \tag{2.1}$$

where $|\omega_i|=\sqrt{q}$ for $i=1,2,\dots,2g$. Furthermore, we know that

$$h=L(1,K)=\prod_{i=1}^{2g}(1-\omega_i)=q^g L(1/q,K)\ . \tag{2.2}$$

It immediately follows that

$$(\sqrt{q}-1)^{2g}\le h\le(\sqrt{q}+1)^{2g}\ . \tag{2.3}$$

Let $X\in K$ be a transcendental element such that $K/k(X)$ is a separable extension of degree n. Denote by R_X, h_X, respectively, the regulator and the number of ideal classes in the corresponding order $\mathcal{O}(X)$, i.e., the integral closure of $k[X]$ in K. If $\infty_1,\dots,\infty_r$ denote the infinite places of K with respect to $\mathcal{O}(X)$ of degree $f_1,\dots,f_r$, then we derive from [Sch31] (see also [MM80]) that

$$f_X\cdot h=h_X\cdot R_X\ , \tag{2.4}$$

where $f_X=\gcd(f_1,\dots,f_r)$. Furthermore, we have

$$\zeta(s,K)=\zeta_\infty(s,K)\cdot\zeta_X(s,K)\ , \tag{2.5}$$

where

$$\zeta_\infty(s,K)=Z_\infty(u,K)=\prod_{i=1}^{r}\frac{1}{1-u^{f_i}}$$

and

$$\zeta_X(s,K)=Z_X(u,K)=\prod_{\mathfrak{p}}\frac{1}{1-\frac{1}{|N(\mathfrak{p})|^s}}=\prod_{\mathfrak{p}}\frac{1}{1-u^{f_{\mathfrak{p}}}}\ .$$

Here, $\mathfrak{p}$ runs through all prime ideals of K with respect to $\mathcal{O}(X)$ and $f_{\mathfrak{p}}=\deg\mathfrak{p}$. Clearly, if e_i denotes the ramification index of ∞_i over $k(X)$ ($i=1,\dots,r$), then $n=\sum_{i=1}^{r}e_i f_i$.

3. ζ-function and l-polynomial in hyperelliptic function fields

In this section, let K be a hyperelliptic function field over a finite field $k = \mathbb{F}_q$ of odd characteristic. Then, there exists $X \in K$ such that K is a quadratic extension of $k(X)$, i.e., $K = k(X)(\sqrt{D})$, where $D = D(X) \in k[X]$ is squarefree. We have $\mathcal{O}(X) = k[X][\sqrt{D}]$. Let $P = P(X)$ represent any prime polynomial in $k[X]$ and let $\chi(P)$ be the quadratic character $\chi(P) = [D/P]$, where $[D/P]$ denotes the Legendre symbol for polynomials of D over P. We then have (see [Art24]) that

$$\zeta_X(s,K) = Z_X(u,K) = \frac{1}{(1-qu)} \cdot \prod_P \frac{1}{1-\chi(P)u^{\deg(P)}} \ , \tag{3.1}$$

where P runs through all monic prime polynomials of $k[X]$. Now, since $[K : k(X)] = 2$, we distinguish between three cases (see [Art24, WZ91]) which correspond to 1, 2, and 3 in Theorem 1.1. In the first case, there are two conjugate places at infinity of degree one, $r = 2$, $f_1 = f_2 = 1$, $e_1 = e_2 = 1$, and D is a squarefree polynomial of degree $2g+2$ whose leading coefficient is a square in k^*. Then $K = k(X)(\sqrt{D})$ is called a *real quadratic function field* over k. In the remaining two cases, we call K an *imaginary quadratic function field* over k. In the second case, there is one ramified place at infinity of degree one, $r = 1$, $f_1 = 1$, $e_1 = 2$, and D is a squarefree polynomial of degree $2g+1$. In the last case, $r = 1$, $f_1 = 2$, $e_1 = 1$, and D is a squarefree polynomial of degree $2g+2$ whose leading coefficient is not a square in $\mathbb{F}_q^*$. It follows that

$$\zeta_\infty(s,K) = Z_\infty(u,K) = \frac{1}{(1-u)^r} \cdot \frac{1}{(1+u)^{r_2}} \ ,$$

where r_2 is the number of infinite places of degree 2. By combining this result with (2.5) and (3.1), we obtain

$$\prod_{i=1}^{2g} (1-\omega_i u) = L(u,K) = \frac{1}{(1-u)^{r-1}} \cdot \frac{1}{(1+u)^{r_2}} \prod_P \frac{1}{1-\chi(P)u^{\deg(P)}} \ . \tag{3.2}$$

If we put

$$S_\nu(j) = \sum_{\deg(P)=\nu} \chi(P)^j \quad (\nu, j \geq 1) \ ,$$

then Theorem 1.1 reads

$$\sum_{\nu|n} \nu \, S_\nu\left(\frac{n}{\nu}\right) = -1 - \sum_{i=1}^{2g} \omega_i^n \quad (n \geq 1) \ , \tag{3.3}$$

in the case that $\deg(D) = 2g+2$ and the leading coefficient of D is a square in k^*, i.e., $r = 2$ and $r_2 = 0$.

If $\deg(D) = 2g+1$, i.e., $r = 1$ and $r_2 = 0$, then Theorem 1.1 reads

$$\sum_{\nu|n} \nu \, S_\nu\left(\frac{n}{\nu}\right) = -\sum_{i=1}^{2g} \omega_i^n \quad (n \geq 1) \ . \tag{3.4}$$

In the final case, we have $r = 1 = r_2$, and Theorem 1.1 states that

$$\sum_{\nu|n} \nu \, S_\nu\left(\frac{n}{\nu}\right) = (-1)^{n+1} - \sum_{i=1}^{2g} \omega_i^n \quad (n \geq 1) \ . \tag{3.5}$$

Proof of Theorem 1.1. By (3.2), we have

$$(1-u)^{r-1}(1+u)^{r_2}\prod_{i=1}^{2g}(1-\omega_i u)=\prod_P \frac{1}{1-\chi(P)u^{\deg(P)}}\ .$$

Taking formal logarithms yields

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{u^n}{n}\Big(1-r+(-1)^{n+1}r_2-\sum_{i=1}^{2g}\omega_i^n\Big) &= \sum_{n=1}^{\infty}\sum_P \chi(P)^n\,\frac{u^{n\deg(P)}}{n}\\ &= \sum_{n=1}^{\infty}\frac{u^n}{n}\sum_{\nu|n}\nu\,S_\nu\left(\frac{n}{\nu}\right)\ ,\end{aligned}$$

where ν runs through all positive divisors of n. If we equate coefficients at u^n for any $n\geq 1$, then we obtain

$$1-r+(-1)^{n+1}r_2-\sum_{i=1}^{2g}\omega_i^n=\sum_{\nu|n}\nu\,S_\nu\left(\frac{n}{\nu}\right)\ . \tag{3.6}$$

This gives the desired results, since

$$1-r+(-1)^{n+1}r_2=\begin{cases}-1 & \text{if } r=2 \text{ and } r_2=0\\ 0 & \text{if } r=1 \text{ and } r_2=0\\ (-1)^{n+1} & \text{if } r=1 \text{ and } r_2=1.\end{cases} \tag{3.7}$$

□

With the help of this theorem, we are able to provide improved bounds on the error in our approximations of h. Hereby, it is essential to estimate $nS_n(1)$ for any positive integer n. For $n=1$, we know immediately from Theorem 1.1 that

$$S_1(1)=\sum_{\deg(P)=1}\chi(P)=-\sum_{i=1}^{2g}\omega_i+\begin{cases}-1 & \text{if } r=2 \text{ and } r_2=0\\ 0 & \text{if } r=1 \text{ and } r_2=0\\ 1 & \text{if } r=1 \text{ and } r_2=1.\end{cases} \tag{3.8}$$

Corollary 3.1. *We have for $n\geq 2$*

$$nS_n(1)=n\sum_{\deg(P)=n}\chi(P)=\rho(n)-\sum_{\substack{\nu|n\\ n/\nu \text{ odd}}}\mu\left(\frac{n}{\nu}\right)\sum_{i=1}^{2g}\omega_i^\nu-\sum_{\substack{\nu|n\\ n/\nu=2^l,\,l\geq 1}}\nu\,S_\nu(2)\ ,$$

where $\rho(n)=0$, if n is not a power of 2, and for $t\geq 1$

$$\rho(2^t)=\begin{cases}-1 & \text{if } r=2 \text{ and } r_2=0\\ 0 & \text{if } r=1 \text{ and } r_2=0\\ -1 & \text{if } r=1 \text{ and } r_2=1.\end{cases}$$

Proof. Let $n\geq 2$. First note that

$$\sum_{\substack{\nu|n\\ n/\nu \text{ odd}}}\mu\left(\frac{n}{\nu}\right)=\sum_{\substack{\nu|n\\ n/\nu \text{ odd}}}\mu\left(\frac{n}{\nu}\right)(-1)^\nu=\begin{cases}1 & \text{if } n=2^t,\ t\geq 1\ ,\\ 0 & \text{otherwise}\ .\end{cases}$$

From (3.6), we derive that

$$\sum_{\substack{\nu|n \\ n/\nu \text{ odd}}} \nu\, S_\nu(1) = 1 - r + (-1)^{n+1} r_2 - \sum_{i=1}^{2g} \omega_i^n - \sum_{\substack{\nu|n \\ n/\nu \text{ even}}} \nu\, S_\nu(2)\ .$$

By special Möbius inversion,[1] we see that

$$\begin{aligned} nS_n(1) &= \sum_{\substack{\nu|n \\ n/\nu \text{ odd}}} \mu\left(\frac{n}{\nu}\right) \Big(1 - r - (-1)^\nu r_2 - \sum_{i=1}^{2g} \omega_i^\nu - \sum_{\substack{\nu|n \\ n/\nu \text{ even}}} \nu\, S_\nu(2)\Big) \\ &= \rho(n) - \sum_{\substack{\nu|n \\ n/\nu \text{ odd}}} \mu\left(\frac{n}{\nu}\right) \sum_{i=1}^{2g} \omega_i^\nu - \sum_{\substack{\nu|n \\ n/\nu \text{ odd}}} \mu\left(\frac{n}{\nu}\right) \sum_{\substack{j|\nu \\ \nu/j \text{ even}}} j\, S_j(2)\ . \end{aligned}$$

The assertion then follows from the fact that

$$\sum_{\substack{\nu|n \\ n/\nu \text{ odd}}} \mu\left(\frac{n}{\nu}\right) \sum_{\substack{j|\nu \\ \nu/j \text{ even}}} j\, S_j(2) = \sum_{\substack{\nu|n \\ n/\nu = 2^l,\, l \geq 1}} \nu\, S_\nu(2)\ .$$

□

Before we provide bounds on $nS_n(1)$, we mention two special cases. If $n > 1$ is odd, then

$$nS_n(1) = -\sum_{\nu|n} \mu\left(\frac{n}{\nu}\right) \sum_{i=1}^{2g} \omega_i^\nu\ ,$$

and if $n > 1$ is a power of 2, then

$$nS_n(1) = -\sum_{i=1}^{2g} \omega_i^n - \sum_{\nu|\frac{n}{2}} \nu\, S_\nu(2) - \begin{cases} 1 & \text{if } r = 2 \text{ and } r_2 = 0 \\ 0 & \text{if } r = 1 \text{ and } r_2 = 0 \\ 1 & \text{if } r = 1 \text{ and } r_2 = 1. \end{cases}$$

4. New improved estimates for h

4.1. **The idea.** One wants to find integers E and L such that

$$|h - E| < L^2\ .$$

Of course, L should be as small as possible so that the approximation is as accurate as possible. Assume h to be given in the form

$$h = E' \cdot e^B \quad (E', B \in \mathbb{R})\ ,$$

and put $E = \text{round}(E')$, where $\text{round}(y)$ denotes the nearest integer to y.[2] Thus,

$$B = \log h - \log E'$$

and

$$|h - E| \leq E' |e^B - 1| + \tfrac{1}{2}\ .$$

[1] If f is an arithmetic function and $F(n) = \sum_{\substack{\nu|n \\ n/\nu \text{ odd}}} f(\nu)$, then $f(n) = \sum_{\substack{\nu|n \\ n/\nu \text{ odd}}} \mu(n/\nu) F(\nu)$.

[2] $\text{round}(y)$ is the unique integer such that $-\frac{1}{2} < y - \text{round}(y) \leq \frac{1}{2}$.

If $\psi \in \mathbb{R}$ such that $\psi > |B|$, then $|e^B - 1| < e^\psi - 1$; notice that if $B < 0$, by this estimate we lose a factor of e^ψ, even if ψ is a good upper bound for $|B|$. However, it turns out that our values for ψ are significantly smaller than 1, and then $e^\psi \sim 1+\psi$, i.e., $e^\psi - 1 \sim \psi$. So let ψ be a bound on $|B|$. Then

$$|h - E| < E'(e^\psi - 1) + \tfrac{1}{2} \ ,$$

so that we can put

$$L = \left\lceil \sqrt{E'(e^\psi - 1) + \tfrac{1}{2}} \right\rceil$$

to receive a good upper bound L^2 on $|h - E|$. The main idea is to make use of the analogue of the analytic class number formula for hyperelliptic function fields. Namely, from (2.2) and (3.2), we derive that

$$h = q^g L(1/q, K) = q^g \prod_P \frac{1}{1 - \chi(P) q^{-\deg(P)}} \cdot \begin{cases} \dfrac{q}{q-1} & \text{if } r = 2 \text{ and } r_2 = 0 \\ 1 & \text{if } r = 1 \text{ and } r_2 = 0 \\ \dfrac{q}{q+1} & \text{if } r = 1 \text{ and } r_2 = 1. \end{cases}$$

As in the proof of Theorem 1.1, it follows that

$$\log h = A(D) + \sum_{n=1}^{\infty} \frac{1}{nq^n} \sum_{\nu | n} \nu \, S_\nu \left(\frac{n}{\nu}\right) \ , \tag{4.1}$$

where $A(D) = (g + r - 1 + r_2) \log q - (r-1) \log(q-1) - r_2 \log(q+1)$. Note that

$$A(D) = \begin{cases} (g+1) \log q - \log(q-1) & \text{if } r = 2 \text{ and } r_2 = 0 \\ g \log q & \text{if } r = 1 \text{ and } r_2 = 0 \\ (g+1) \log q - \log(q+1) & \text{if } r = 1 \text{ and } r_2 = 1. \end{cases}$$

We now consider two possible choices for the approximation of h dependent on a parameter $\lambda \in \mathbb{N}$.[3] We will determine λ later to obtain an optimal overall complexity of the baby step–giant step algorithm. The first possibility is to define $E_1' = E_1'(\lambda, D)$ and $B_1 = B_1(\lambda, D)$ by

$$\log E_1'(\lambda, D) := A(D) + \sum_{n=1}^{\lambda} \frac{1}{nq^n} \sum_{\nu | n} \nu \, S_\nu \left(\frac{n}{\nu}\right) \tag{4.2}$$

and

$$B_1(\lambda, D) := \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \sum_{\nu | n} \nu \, S_\nu \left(\frac{n}{\nu}\right) \ . \tag{4.3}$$

If we put $E_1(\lambda, D) := \mathrm{round}(E_1'(\lambda, D))$, then $E_1(\lambda, D)$ is an approximation of h. Note that $B_1(\lambda, D) = \log h - \log E_1'(\lambda, D)$. To estimate the error in this approximation, we have to bound $B_1(\lambda, D)$. Below, we will show that

$$|B_1(\lambda, D)| < \frac{2g q^{-\frac{(\lambda+1)}{2}}}{\lambda + 1} + O\left(\frac{g q^{-\frac{(\lambda+2)}{2}}}{\lambda}\right) \ .$$

[3] $\mathbb{N}$ denotes the set of positive integers.

The second possibility is to proceed as in [SW99] and define $E_2' = E_2'(\lambda, D)$ and $B_2 = B_2(\lambda, D)$ by

$$\log E_2'(\lambda, D) := A(D) + \sum_{n=1}^{\lambda} \frac{1}{nq^n} \sum_{\nu|n} \nu\, S_\nu\left(\frac{n}{\nu}\right) + \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu\le\lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right) \ , \tag{4.4}$$

or, equivalently,

$$E_2'(\lambda, D) = q^g \prod_{\substack{P \\ \deg(P)\le\lambda}} \frac{1}{1-\chi(P)q^{-\deg(P)}} \cdot \begin{cases} \dfrac{q}{q-1} & \text{if } r = 2 \text{ and } r_2 = 0 \\ 1 & \text{if } r = 1 \text{ and } r_2 = 0 \\ \dfrac{q}{q+1} & \text{if } r = 1 \text{ and } r_2 = 1 \end{cases}$$

and

$$B_2(\lambda, D) := \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right) \ . \tag{4.5}$$

We then let $E_2(\lambda, D) := \mathrm{round}(E_2'(\lambda, D))$ and obtain that $E_2(\lambda, D)$ is an approximation of h. Note that $B_2(\lambda, D) = \log h - \log E_2'(\lambda, D)$, i.e., $B_2(\lambda, D)$ is the logarithm of the tail of the truncated Euler product. Our aim is to find a good upper bound on $|B_2(\lambda, D)|$. We will improve results in [SW99] by proving that

$$|B_2(\lambda, D)| < \frac{(2g + \epsilon(\lambda))q^{-\frac{(\lambda+1)}{2}}}{\lambda+1} + O\left(\frac{gq^{-\frac{(\lambda+2)}{2}}}{\lambda}\right) \ ,$$

where $\epsilon(n) = 0$ or 1, respectively, depending on whether $n \in \mathbb{N}$ is even or odd. It turns out that the second choice of the approximation is more accurate in practice, although the bound on $|B_1(\lambda, D)|$ is smaller than the one on $|B_2(\lambda, D)|$.

4.2. **A first estimate.** Here, we investigate the approximation $E_1'(\lambda, D)$ of h as defined in (4.2) for any $\lambda \ge 1$. From (4.1)-(4.3) it follows that

$$B_1(\lambda, D) = \log h - \log E_1'(\lambda, D) = \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \sum_{\nu|n} \nu\, S_\nu\left(\frac{n}{\nu}\right) \ .$$

In order to find a good upper bound for $|B_1(\lambda, D)|$, we make use of Theorem 1.1 and find that

$$\begin{aligned} \Big|\sum_{\nu|n} \nu\, S_\nu\left(\frac{n}{\nu}\right)\Big| &\le 1 + \Big|\sum_{i=1}^{2g} \omega_i^n\Big| \\ &\le 1 + 2gq^{\frac{n}{2}} \ , \end{aligned} \tag{4.6}$$

since $|\omega_i| = \sqrt{q}$. Putting

$$\psi_1(\lambda, D) = 2g \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^{\frac{n}{2}}} + \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \ , \tag{4.7}$$

we obtain that $|B_1(\lambda, D)| < \psi_1(\lambda, D)$. Moreover,

$$\begin{aligned}\psi_1(\lambda, D) &< \frac{2gq^{-\frac{(\lambda+1)}{2}}}{\lambda+1} + \frac{2g}{\lambda+2}\sum_{n=\lambda+2}^{\infty} q^{-\frac{n}{2}} + \frac{1}{\lambda+1}\sum_{n=2\lambda+2}^{\infty} q^{-\frac{n}{2}} \\ &\le \frac{2gq^{-\frac{(\lambda+1)}{2}}}{\lambda+1} + \frac{2gq^{-\frac{(\lambda+1)}{2}}}{(\lambda+2)(\sqrt{q}-1)} + \frac{q^{-\frac{(2\lambda+1)}{2}}}{(\lambda+1)(\sqrt{q}-1)} \\ &\le \frac{2gq^{-\frac{(\lambda+1)}{2}}}{\lambda+1}\Big(1 + \frac{1}{\sqrt{q}-1}\Big) = \frac{2g}{(\lambda+1)}\,\frac{\sqrt{q}}{(\sqrt{q}-1)}\,q^{-\frac{(\lambda+1)}{2}}\ ,\end{aligned}$$

where in the last inequality we used that $2gq^{\frac{\lambda}{2}} \ge \lambda + 2$ for $\lambda \ge 1$. We summarize this in the following

Theorem 4.1. *For any $\lambda \in \mathbb{N}$, let $E_1(\lambda, D) = \mathrm{round}(E_1'(\lambda, D))$ and*

$$L_1(\lambda, D) = \left\lceil \sqrt{E_1'(\lambda, D)(e^{\psi_1(\lambda, D)} - 1) + \tfrac{1}{2}} \right\rceil\ ,$$

where $E_1'(\lambda, D)$, $\psi_1(\lambda, D)$ are defined in (4.2) *and* (4.7)*, respectively. Then, we have*

$$|h - E_1(\lambda, D)| < L_1^2(\lambda, D)\ .$$

Furthermore, we have

$$|\log h - \log E_1'(\lambda, D)| < \frac{2g}{(\lambda+1)}\,\frac{\sqrt{q}}{(\sqrt{q}-1)}\,q^{-\frac{(\lambda+1)}{2}}\ .$$

For the computation of $\psi_1(\lambda, D)$ we notice that

$$\psi_1(\lambda, D) = 2g\Big(\log\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big) - \sum_{n=1}^{\lambda}\frac{1}{nq^{\frac{n}{2}}}\Big) + \log\Big(\frac{q}{q-1}\Big) - \sum_{n=1}^{\lambda}\frac{1}{nq^n}\ .$$

Finally, we have to show that $E_1(\lambda, D)$ does not become too large in order to guarantee that our algorithm is effective. Since we are mainly interested in the case that q is large and g is small, the following theorem is sufficient.

Theorem 4.2. *For any $\lambda \in \mathbb{N}$, we have*

$$E_1'(\lambda, D) \le q^g\Big(\frac{q}{q-1}\Big)^r\Big(\frac{q}{q+1}\Big)^{r_2}\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)^{2g}\ .$$

Proof. From (4.6), it follows that

$$\begin{aligned}\Big|\sum_{n=1}^{\lambda}\frac{1}{nq^n}\sum_{\nu|n}\nu\,S_\nu\Big(\frac{n}{\nu}\Big)\Big| &\le \sum_{n=1}^{\lambda}\frac{2gq^{\frac{n}{2}}+1}{nq^n} < 2g\sum_{n=1}^{\infty}\frac{1}{nq^{\frac{n}{2}}} + \sum_{n=1}^{\infty}\frac{1}{nq^n} \\ &= 2g\log\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big) + \log\Big(\frac{q}{q-1}\Big)\ .\end{aligned}$$

Thus, by (4.2),

$$\begin{aligned}\log E_1'(\lambda, D) &\le A(D) + 2g\log\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big) + \log\Big(\frac{q}{q-1}\Big) \\ &= g\log q + r\log\Big(\frac{q}{q-1}\Big) + r_2\log\Big(\frac{q}{q+1}\Big) + 2g\log\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)\ ,\end{aligned}$$

and the assertion is proved. □

It follows that if g is not too large compared to q, we have $E_1(\lambda, D) = O(q^g)$, since $q/(q+1) \leq 1$, $q/(q-1) \leq 3/2$, and $\sqrt{q}/(\sqrt{q}-1) \to 1$, if $q \to \infty$. In particular, if $2g \leq \sqrt{q} - 1$, then

$$2g \log\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big) = 2g \sum_{n=1}^{\infty} \frac{1}{nq^{\frac{n}{2}}} \leq \frac{2g}{\sqrt{q}-1} \leq 1 \ .$$

In this case, we have $E_1'(\lambda, D) \leq e(3/2)^r \cdot q^g$. Also, notice that if $\psi_1(\lambda, D) < 1$, then $e^{\psi_1(\lambda,D)} - 1 \sim \psi_1(\lambda, D)$ and for sufficiently small values of g it follows that $L_1(\lambda, D) = O(q^{g/2-(\lambda+1)/4})$.

4.3. **A second estimate.** Let $\lambda \in \mathbb{N}$ and let $E_2'(\lambda, D)$ be the approximation of h as in (4.4). By (4.5), we have

$$B_2(\lambda, D) = \frac{S_{\lambda+1}(1)}{q^{\lambda+1}} + \sum_{n=\lambda+2}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu \, S_\nu\Big(\frac{n}{\nu}\Big) \ . \tag{4.8}$$

We denote by n_ν the number of monic prime polynomials of degree ν. We know that

$$\sum_{l|\nu} l n_l = q^\nu \tag{4.9}$$

and that $\nu n_\nu = \sum_{l|\nu} \mu(\nu/l) q^l$. It is easy to see that $0 \leq S_\nu(2) \leq n_\nu$, and n_ν and $S_\nu(2)$ differ only by the number of prime factors of D of degree ν, i.e.,

$$S_\nu(2) = n_\nu + O(g) \ . \tag{4.10}$$

Lemma 4.1. *We have for $n \in \mathbb{N}$, $n \geq 2$,*

$$n|S_n(1)| < \frac{(2g + \epsilon(n-1))q^{\frac{n+1}{2}}}{\sqrt{q}-1} \ ,$$

where $\epsilon(n) = 0$ or 1, respectively, depending on whether n is even or odd.

Proof. Let $n \in \mathbb{N}$, $n \geq 2$. By Corollary 3.1, we know that

$$nS_n(1) = \rho(n) - \sum_{\substack{\nu|n \\ n/\nu \text{ odd}}} \mu\Big(\frac{n}{\nu}\Big) \sum_{i=1}^{2g} \omega_i^\nu - \sum_{\substack{\nu|n \\ n/\nu = 2^l, \, l \geq 1}} \nu \, S_\nu(2) \ ,$$

where $|\rho(n)| \leq 1$. Note that the last sum on the right hand side of this equation is zero if n is odd. If n is even, we calculate

$$\Big| \sum_{\substack{\nu|n \\ n/\nu = 2^l, \, l \geq 1}} \nu \, S_\nu(2) \Big| \leq \sum_{\substack{\nu|n \\ n/\nu = 2^l, \, l \geq 1}} \nu \, n_\nu \leq \sum_{\nu|(n/2)} \nu \, n_\nu = q^{\frac{n}{2}} \ .$$

Since $|\omega_i| = \sqrt{q}$, it follows that

$$\Big| \sum_{\substack{\nu|n \\ n/\nu \text{ odd}}} \mu\Big(\frac{n}{\nu}\Big) \sum_{i=1}^{2g} \omega_i^\nu \Big| \leq \sum_{\substack{\nu|n \\ n/\nu \text{ odd}}} 2gq^{\frac{\nu}{2}} \leq 2g \sum_{\nu=1}^{n} q^{\frac{\nu}{2}} < \frac{2gq^{\frac{n+1}{2}}}{\sqrt{q}-1} - 1 \ .$$

Summarizing, we obtain

$$n|S_n(1)| < \frac{2gq^{\frac{n+1}{2}}}{\sqrt{q}-1} + \epsilon(n-1)q^{\frac{n}{2}} < \frac{(2g+\epsilon(n-1))q^{\frac{n+1}{2}}}{\sqrt{q}-1} \ .$$

□

Note that the bound in the above lemma can be minimally improved by considering only the odd factors in the sum. But, for our purposes the estimate is sufficient, since for large values of q there is no noticeable difference.

Lemma 4.2. *For $\lambda, \beta \in \mathbb{N}$ such that $\beta > \lambda \geq 1$, we have*

$$\Big|\sum_{n=\beta}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu\, S_\nu\Big(\frac{n}{\nu}\Big)\Big| < \frac{(2g+2)}{\beta}\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)^3 q^{-\frac{\beta}{2}} \ .$$

Proof. First, we see that

$$\Big|\sum_{\substack{\nu|n \\ \nu>\lambda \\ n/\nu \text{ even}}} \nu\, S_\nu\Big(\frac{n}{\nu}\Big)\Big| \leq \sum_{\substack{\nu|n \\ n/\nu \text{ even}}} \nu\, S_\nu(2) \leq \sum_{\nu|(n/2)} \nu\, n_\nu = q^{\frac{n}{2}} \ . \tag{4.11}$$

Then we make use of Lemma 4.1 to find that

$$\begin{aligned}\Big|\sum_{\substack{\nu|n \\ \nu>\lambda \\ n/\nu \text{ odd}}} \nu\, S_\nu\Big(\frac{n}{\nu}\Big)\Big| &\leq \sum_{\substack{\nu|n \\ \nu>\lambda \\ n/\nu \text{ odd}}} \nu|S_\nu(1)| < \sum_{\nu=1}^{n} \frac{(2g+\epsilon(n-1))q^{\frac{n+1}{2}}}{\sqrt{q}-1} \\ &< \frac{(2g+1)q^{\frac{n+2}{2}}}{(\sqrt{q}-1)^2} = (2g+1)\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)^2 q^{\frac{n}{2}} \ .\end{aligned}$$

Thus,

$$\Big|\sum_{\substack{\nu|n \\ \nu>\lambda}} \nu\, S_\nu\Big(\frac{n}{\nu}\Big)\Big| < (2g+2)\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)^2 q^{\frac{n}{2}} \ .$$

Summing up we can conclude that

$$\begin{aligned}\Big|\sum_{n=\beta}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu\, S_\nu\Big(\frac{n}{\nu}\Big)\Big| &< (2g+2)\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)^2 \sum_{n=\beta}^{\infty} \frac{1}{nq^{\frac{n}{2}}} \\ &< \frac{(2g+2)}{\beta}\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)^3 q^{-\frac{\beta}{2}} \ .\end{aligned}$$

□

Lemmas 4.1 and 4.2 provide us with improved bounds on $B_2(\lambda, D)$ as follows. We define $\psi_2(\lambda, D)$ as

$$\psi_2(\lambda, D) = \frac{(2g+\epsilon(\lambda))q^{-\frac{\lambda}{2}}}{(\lambda+1)(\sqrt{q}-1)} + \frac{(2g+2)q^{-\frac{\lambda-1}{2}}}{(\lambda+2)(\sqrt{q}-1)^3} \tag{4.12}$$

and find that $|B_2(\lambda, D)| < \psi_2(\lambda, D)$ since

$$\begin{aligned}|B_2(\lambda, D)| &\le \frac{(\lambda+1)|S_{\lambda+1}(1)|}{(\lambda+1)q^{\lambda+1}} + \Big| \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right) \Big| \\ &< \frac{(2g+\epsilon(\lambda))q^{-\frac{\lambda}{2}}}{(\lambda+1)(\sqrt{q}-1)} + \frac{(2g+2)}{(\lambda+2)}\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)^3 q^{-\frac{\lambda+2}{2}} \\ &= \psi_2(\lambda, D)\ .\end{aligned}$$

We proved the following

Theorem 4.3. *For any $\lambda \in \mathbb{N}$, let $E_2(\lambda, D) = \mathrm{round}(E_2'(\lambda, D))$ and*

$$L_2(\lambda, D) = \left\lceil \sqrt{E_2'(\lambda, D)(e^{\psi_2(\lambda, D)} - 1) + \tfrac{1}{2}} \right\rceil\ ,$$

where $E_2'(\lambda, D)$, $\psi_2(\lambda, D)$ are defined in (4.4) *and* (4.12)*, respectively. Then, we have*

$$|h - E_2(\lambda, D)| < L_2^2(\lambda, D)\ .$$

Furthermore, we have

$$|\log h - \log E_2'(\lambda, D)| < \frac{(2g+\epsilon(\lambda))q^{-\frac{\lambda}{2}}}{(\lambda+1)(\sqrt{q}-1)} + \frac{(2g+2)q^{-\frac{\lambda-1}{2}}}{(\lambda+2)(\sqrt{q}-1)^3}\ .$$

How accurate is the bound on $|B_2(\lambda, D)| = |\log h - \log E_2'(\lambda, D)|$? We notice that $S_{\lambda+1}(1)/q^{\lambda+1}$ is the dominant term for $B_2(\lambda, D)$. For instance, let $K = k(X)(\sqrt{D})$, where D is a monic, squarefree polynomial of degree $2g+2$ with no linear factors in $k[X]$, and let $\lambda = 1$. Then, $r = 2$, $r_2 = 0$, $S_1(2) = q$, and

$$2S_2(1) = -\sum_{i=1}^{2g} \omega_i^2 - 1 - S_1(2) = -\sum_{i=1}^{2g} \omega_i^2 - q - 1\ .$$

It follows that

$$\frac{|S_{\lambda+1}(1)|}{q^{\lambda+1}} = \frac{|S_2(1)|}{q^2} \le \frac{(2g+1)}{2} q^{-1} + O(q^{-2}) = \frac{(2g+1)}{\lambda+1} q^{-\frac{\lambda+1}{2}} + O(q^{-2})\ .$$

If it happens that $\omega_i = -\sqrt{q}$ for $i = 1, \ldots, 2g$, i.e., K is a *maximal function field* (see [Sti93, pp. 182, 197]), then we even have $2S_2(1) = -(2g+1)q - 1$, and

$$\frac{|S_2(1)|}{q^2} = \frac{(2g+1)}{\lambda+1} q^{-\frac{\lambda+1}{2}} + O(q^{-\frac{\lambda+3}{2}})\ .$$

This means that, in this case, the bound on $|B_2(\lambda, D)|$ is sharp.

Again, we have to guarantee that $E_2(\lambda, D)$ does not become too large. In essentials, this was already proved in [SW99]. It was shown that $E_2(\lambda, D) = O(\lambda q^g)$ and if $\psi_2(\lambda, D) < 1$, then $e^{\psi_2(\lambda, D)} - 1 \sim \psi_2(\lambda, D)$. For sufficiently small values of g and w it follows that $L_2(\lambda, D) = O(q^{g/2-(\lambda+1)/4})$. For completeness, we mention a similar result as in Theorem 4.2.

Theorem 4.4. *For any $\lambda \ge 1$, we have*

$$E_2'(\lambda, D) \le q^g \Big(\frac{q}{q-1}\Big)^r \Big(\frac{q}{q+1}\Big)^{r_2} \Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big)^{2g} e^{\psi_2(\lambda, D)}\ .$$

Proof. By (4.4), we have

$$\log E_2'(\lambda, D) = A(D) + \sum_{n=1}^{\lambda} \frac{1}{nq^n} \sum_{\nu|n} \nu\, S_\nu\left(\frac{n}{\nu}\right) + \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu\le\lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right) .$$

If we use that

$$\sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu\le\lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right) = \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n}\Big(\sum_{\nu|n} \nu\, S_\nu\left(\frac{n}{\nu}\right) - \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right)\Big) ,$$

we can proceed as in the proof of Theorem 4.2 to obtain

$$\log E_2'(\lambda, D) < g\log q + r\log\Big(\frac{q}{q-1}\Big) + r_2\log\Big(\frac{q}{q+1}\Big) + 2g\log\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big) + \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n}\Big| \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right)\Big| .$$

The last sum on the right side can be bounded by $\psi_2(\lambda, D)$ which gives the desired result. □

If $\psi_2(\lambda, D) < 1$ and g is sufficiently small compared to q, it follows that $E_2(\lambda, D) = O(q^g)$ and $L_2(\lambda, D) = O(q^{g/2-(\lambda+1)/4})$. For instance, if $2g \le \sqrt{q} - 2$, then $\psi_2(\lambda, D) < 1$ and $E_2'(\lambda, D) < e^2(3/2)^r \cdot q^g$. In the next section, we apply the improved bounds to get a faster method for computing the regulator R_X and the divisor class number h of hyperelliptic function fields.

5. Computation of R_X and h

Let $K = k(X)(\sqrt{D})$ be an imaginary quadratic function field over the finite field $k = \mathbb{F}_q$ of odd characteristic. We then know that $R_X = 1$, and we only need to compute h. In the case that D is a squarefree polynomial of even degree whose leading coefficient is not a square in k^*, we have $h_X = 2h$. Furthermore, a constant field extension of degree 2 over k leads to a real quadratic function field. In the second imaginary case, $D = D(X)$ is a squarefree polynomial of odd degree. Without loss of generality, we may assume that D is monic. For convenience, we also assume that $q \gg g^2$. Then K can be represented as a real quadratic function field $K = k(T)(\sqrt{F})$ over the same finite field k by applying the following birational transformation:

$$T = \frac{1}{X - \beta} \quad , \quad F(T) = T^{2g+2} D\left(\beta + \tfrac{1}{T}\right) ,$$

where β is a suitable element of k such that the leading coefficient of $F(T)$ is a square in k^*. For further discussions, we refer to [CF96, PR99]. Note that $\deg(F) = 2g + 2$ and that the divisor class number h does not change under this transformation. Here and throughout the remainder of this paper, we therefore consider $K = k(X)(\sqrt{D})$ to be a real quadratic function field over the finite field $k = \mathbb{F}_q$ of odd characteristic with q elements, where D is a squarefree polynomial of degree $2g+2$ whose leading coefficient is a square in k^*. We now sketch the idea of computing the regulator R_X of K. Hereby, we proceed in three steps and provide an analysis of the complexity. Mainly, we follow the ideas in [SW98, SW99].

5.1. **The idea of the algorithm.** In the first step, we compute an approximation E of h such that $|h - E| < L^2$ for some integer L. If $g \leq 2$, we make use of (2.3) and we immediately obtain a good estimate. For $g \geq 3$, we put $E' = E_2'(\lambda, D)$, $E = \text{round}(E_2'(\lambda, D))$, and $L = L_2(\lambda, D)$ as in (4.4) and Theorem 4.3. Thus, E and L can be computed in $O(q^\lambda)$ operations in k. In the second step, we compute a multiple $h_0 = h^* R_X$ of R_X in the interval $]E - L^2, E + L^2[$. Here, we may use a baby step–giant step method as in [SW98, SW99] or Pollard's kangaroo method (see [STb]). Since the length of the interval $]E - L^2, E + L^2[$ is $2L^2 - 1$, and we do not know *a priori* how much better the approximation of h is in practice, the search for a multiple of the regulator can be done in $O(L(\lambda, D)) = O(q^{g/2-(\lambda+1)/4})$ baby steps and giant steps. If $g = 1$ or 2, respectively, then a multiple of the regulator can be found in $O(q^{1/4})$, $O(q^{3/4})$ baby steps and giant steps. In the final step, one determines h^* by factoring h_0 in subexponential running time and performing a simple test with all the prime divisors of h_0. Once having computed h^*, one knows $R_X = h_0/h^*$. In general, we expect R_X to be greater than $2L^2 - 2$, in which case $h_0 = h$ and $h^* = h_X$. If $R_X \leq 2L^2 - 2$, some additional steps will produce the values of h and h_X. We see that the complexity of this algorithm[4] is $\max\{O(q^\lambda), O(q^{g/2-(\lambda+1)/4})\}$, since it is mainly determined by the first and the second step. It follows that the optimal choice of λ is

$$\lambda = \begin{cases} \lfloor (2g-1)/5 \rfloor & \text{if } g \equiv 2 \pmod 5 , \\ \text{round}((2g-1)/5) & \text{otherwise} , \end{cases} \tag{5.1}$$

which yields a total running time of

$$O(q^{\text{round}((2g-1)/5)+\eta}) , \ g \geq 3 ,$$

where

$$\eta = \begin{cases} -\frac{1}{4} & \text{if } g \equiv 2 \pmod 5 , \\ 0 & \text{if } g \equiv 0, 3 \pmod 5 , \\ \frac{1}{4} & \text{if } g \equiv 1 \pmod 5 , \\ \frac{1}{2} & \text{if } g \equiv 4 \pmod 5 . \end{cases}$$

Notice that this choice of λ is in fact different from the choice in [SW99]. If $g = 1$ or 2, respectively, then the total running time is $O(q^{1/4})$, $O(q^{3/4})$.

5.2. **Using divisors of h_X.** We now assume that we have computed an approximation E' of h such that $h = E' e^B$ and $|h - E| < L^2$ for some integers E and L, where $E = \text{round}(E')$, $|B| < \psi$, and $L = \lceil \sqrt{E'(e^\psi - 1) + \frac{1}{2}} \rceil$. First, we show how to lower the bound given that we know a divisor $\tilde{h}$ of the ideal class number h_X. Second, we discuss how one might obtain such a divisor. Let $\tilde{h} | h_X$, and let $h_X = \tilde{h}\, H$ for some positive integer H, i.e., $h = \tilde{h}\, H R_X$. We put

$$E'' = \frac{E'}{\tilde{h}} \quad , \quad L'' = \left\lceil \frac{L}{\sqrt{\tilde{h}}} \right\rceil .$$

Then,

$$|H R_X - E''| = \frac{|h - E'|}{\tilde{h}} < \frac{L^2}{\tilde{h}} \leq (L'')^2$$

[4]Note that if one uses Pollard's kangaroo method in the second step of the algorithm, then we have a probabilistic algorithm of *expected* running time as indicated.

and $HR_X = E''e^B$, where $|B| < \psi$. Thus, we can search for a multiple (that might be HR_X) of the regulator R_X in a new interval of length $2(L'')^2 - 1$ which is by a factor of approximately $\tilde{h}$ smaller than the interval $]E - L^2, E + L^2[$. Note that if $R_X \geq 2(L'')^2$, then $H = \text{round}(E''/R_X)$. Moreover, we put $\tilde{H} = \text{round}(E''/R_X)$ and $F = E''/R_X - \text{round}(E''/R_X)$. If $\psi < \log((\tilde{H}+1)/(\tilde{H}+|F|))$, then $H = \tilde{H}$. To find a divisor of h_X we may apply a theorem of Zhang [Zha87]. Let D be a product of s distinct prime polynomials in $k[X]$. Then the 2-rank of the ideal class group of $k(X)(\sqrt{D})$ is $s-2$, if D contains a prime factor of odd degree, and $s-1$ otherwise. It follows that if D is not a prime polynomial or not a product of two odd degree prime polynomials, then a power of 2 divides the ideal class number h_X. Another way of finding a divisor of h_X is to randomly pick reduced ideals and determine the order of the subgroup of the ideal class group generated by these ideals (see [DW85]).

6. Experimental results and heuristics

We first discuss the results of experiments we did to compare our estimates for h and $|h - E|$ with the actual respective values. Since any hyperelliptic function field can be represented as a real quadratic function field, and since the corresponding birational transformation preserves h, E and L, we restrict ourselves to real quadratic function fields. From now on, let λ be defined as in (5.1) (with the exceptions as mentioned in Table 1). The approximation $E_2'(\lambda, D)$ from (4.4) turned out to be a better approximation of h than $E_1'(\lambda, D)$ from (4.2). Hence, in the following let $E_2 = E_2(\lambda, D)$, $L_2 = L_2(\lambda, D)$, and we consider only the estimate for $|h - E_2|$ in Theorem 4.3. This estimate is very good. Indeed, for $k = \mathbb{F}_{10009}$ and

$$\begin{aligned} D(X) =& X^8 + 4527X^7 + 3555X^6 + 7911X^5 + 5059X^4 + 10005X^3 \\ &+ 3823X^2 + 1276X + 9036 \end{aligned}$$

(hence, $g = 3$ and $\lambda = 1$) we find that $E_2 = 984388508397$, $L_2 = 18721$ and $h = 984086389784$. That is, $|h - E_2|/L_2^2 > 0.862$. However, in the large majority of cases, the actual value of $|h - E_2|$ is much smaller than L_2^2. For example, for characteristic $q = 10009$ and genus $g = 3$ we found that among 100000 distinct monic, squarefree polynomials $D = D(X)$ of degree eight, 99% of all values $|h - E_2|$ were smaller than $0.5L_2^2$, and 50% were even smaller than $0.15L_2^2$. The average value of $|h - E_2|/L_2^2$ was 0.161. Similar results were obtained with various other values for q between 17 and 100003 and g between 3 and 9. In fact, the higher the genus was, the smaller $|h - E_2|/L_2^2$ tended to be; for example, for $q = 17$ and $g = 9$, the average value of $|h - E_2|/L_2^2$ was only 0.055.

On the other hand, we found that there exists no lower bound on $|h - E_2|$ in Theorem 4.3. For every value of q and g, we computed examples, where h and E_2 were very close together, i.e., $|h - E_2|$ was very small. For instance, for characteristic $q = 97$ and

$$D(X) = X^8 + 40X^7 + 11X^6 + 42X^5 + 35X^4 + 62X^3 + 76X^2 + 17X + 16$$

we observed that $h = E_2 = 819035$, i.e., $|h - E_2| = 0$.

The detailed experimental results are shown in Table 1. Here, the first and second columns indicate the characteristic q of the constant field and the genus g, while the last column shows how many distinct monic squarefree polynomials have been considered. In the third and forth columns, μ and σ denote the average

TABLE 1. On the distribution of $|h - E_2|/L_2^2$

q	g	μ	σ/μ	min.	max.	0.05	0.1	0.2	50%	95%	99%	#
97	3	0.13	0.73	0	0.611	23.4	45	78	0.11	0.31	0.4	100000
199	3	0.141	0.74	0.16e-3	0.584	22.2	42.3	73.8	0.12	0.33	0.44	1000
991	3	0.161	0.72	0.55e-3	0.608	18.9	36	67.1	0.14	0.38	0.49	1000
10009	3	0.157	0.76	0.2e-4	0.733	20.6	38.3	67.4	0.13	0.39	0.5	1000
10009	3	0.161	0.73	0.312e-5	0.862	18.8	37.1	67.4	0.14	0.38	0.49	100000
100003	3	0.16	0.72	0.12e-3	0.741	17.8	36.2	67.3	0.14	0.37	0.5	1000
1000003	3	0.165	0.72	0.32e-3	0.602	18	35.6	66.3	0.14	0.39	0.5	1000
37	4	0.116	0.73	0.9e-4	0.395	27.2	51.4	82.2	0.1	0.28	0.35	1000
97	4	0.136	0.76	0.1e-3	0.566	23	45.6	76.9	0.12	0.33	0.45	1000
199	4	0.147	0.74	0.47e-3	0.59	21.4	40.6	71.3	0.13	0.35	0.45	1000
991	4	0.116	0.77	0.14e-3	0.584	26.8	52.3	83	0.1	0.29	0.39	1000
37	5	0.94e-1	0.76	0.4e-4	0.391	32.6	59.4	90.8	0.8e-1	0.23	0.3	1000
97	5	0.107	0.75	0.26e-3	0.445	27.9	54.5	86	0.9e-1	0.26	0.34	1000
199	5	0.119	0.75	0.5e-4	0.544	24.4	50.9	82.7	0.1	0.29	0.39	1000
991	5	0.133	0.75	0.266e-5	0.6	22.3	45	77.9	0.11	0.34	0.43	1000
37	6	0.81e-1	0.75	0.9e-4	0.328	37.5	69.4	94.6	0.7e-1	0.2	0.26	1000
97	6	0.96e-1	0.76	0.7e-4	0.44	31.2	58.2	90.4	0.8e-1	0.23	0.32	1000
199	6	0.1	0.75	0.13e-3	0.36	31	57.4	88.2	0.8e-1	0.25	0.31	1000
37	7	0.74e-1	0.74	0.3e-4	0.298	39.6	71.7	97.1	0.6e-1	0.18	0.23	1000
97	7	0.89e-1	0.71	0.24e-3	0.371	33.1	62.4	93.8	0.8e-1	0.21	0.27	1000
17	8	0.52e-1	0.73	0.7e-4	0.199	54.1	88.6	100	0.5e-1	0.13	0.16	1000
17	9	0.55e-1	0.73	0.9e-4	0.244	52.4	84.9	99.7	0.5e-1	0.13	0.16	1000

value and the standard deviation of $|h - E_2|/L_2^2$, respectively. Notice that the ratio σ/μ was essentially the same for all pairs (q, g), which suggests that the probability distribution of $|h - E_2|/L_2^2$ is qualitatively independent of q and g. The next two columns show the minimum and maximum values for $|h - E_2|/L_2^2$. Then columns 7–9 show the percentage of cases for which $|h - E_2|/L_2^2$ was bounded by 0.05, 0.1 and 0.2, respectively, while columns 10 – 12 show which bound B was the smallest possible such that 50%, 95% and 99%, respectively, of all values $|h-E_2|/L_2^2$ were less than or equal to B. In general, we hence find that the large majority of the values for $|h-E_2|/L_2^2$ are much smaller than one, and that large values for $|h-E_2|/L_2^2$ are very rare. We remark that, different from the definition in (5.1), we used $\lambda = 3$ for $g = 7$ and $\lambda = 4$ for $g = 9$, since for the given values of q we were able to compute a better approximation.

We denote by $\alpha(g, q)$ the average value for $|h - E_2|/L_2^2$ for fixed values of g and q. Our aim is to find $\alpha(g) = \lim_{q\to\infty} \alpha(g, q)$. For instance, our experimental results suggest that $\alpha(3) \approx 0.161$. Having determined the correct value of $\alpha(g)$, we then know that the bound L_2^2 is, *on average*, by a factor of $1/\alpha(g)$ too large. We try to explain these observations, and go back to Theorem 4.3 where we derived the bound $\psi_2(\lambda, D)$ on $|B_2(\lambda, D)| = |\log h - \log E_2|$. As noted at the beginning of Section 4, a sharp bound $\psi_2(\lambda, D)$ on $|B_2(\lambda, D)|$ leads to a sharp value of L_2^2 if $\psi_2(\lambda, D) \ll 1$; in general, for $B_2(\lambda, D) < 0$, we lose a factor of $e^{\psi_2(\lambda,D)}$. From (4.12) we see that the largest values for $\psi_2(\lambda, D)$ occur for small values of q. This explains why the average and maximum values for $|h - E_2|/L_2^2$ in Table 1 have a tendency to grow for q increasing and g fixed. In our examples above, the largest value for $\psi_2(\lambda, D)$ occurs for $g = 4$, $q = 37$: then $\lambda = 1$ and $\psi_2(\lambda, D) = 0.15476$, so that for $B_2(\lambda, D) < 0$ the bound L_2^2 on $|h - E_2|$ is by at least a factor of approximately 1.167 too large. For most of our examples, however, we have $\psi_2(\lambda, D) < 0.05$ so that we do not lose much at that step of the estimate.

From (4.8) and Lemma 4.2 we see that

$$B_2(\lambda, D) = \frac{S_{\lambda+1}(1)}{q^{\lambda+1}} + O(q^{-\frac{\lambda+2}{2}}) \ ,$$

where we recall that

$$S_{\lambda+1}(1) = \sum_{\deg(P)=\lambda+1} \chi(P) \ .$$

Now, from Corollary 3.1 we see that $S_{\lambda+1}(1)$ contains at least one term of magnitude $q^{(\lambda+1)/2}$, namely

$$\frac{1}{(\lambda+1)} \sum_{j=1}^{2g} \omega_j^{\lambda+1} \ .$$

If λ is even, this is the only term of this magnitude. If λ is odd, we also have to consider the term

$$\frac{1}{\lambda+1} \sum_{\substack{\nu|(\lambda+1) \\ (\lambda+1)/\nu=2^l,\, l\geq 1}} \nu\, S_\nu(2) \ .$$

From (4.11), (4.10) and (4.9) it is easy to see that

$$\frac{1}{\lambda+1} \sum_{\substack{\nu|(\lambda+1) \\ (\lambda+1)/\nu=2^l,\, l\geq 1}} \nu\, S_\nu(2) = \frac{S_{(\lambda+1)/2}(2)}{2} + O(q^{\frac{\lambda+1}{4}}) = \frac{q^{\frac{\lambda+1}{2}}}{\lambda+1} + O(q^{\frac{\lambda+1}{4}}) \ .$$

Hence, with $\omega_j = q^{1/2} e^{i\varphi_j}$, $\varphi_j \in [0, 2\pi[$, $j = 1, \dots, 2g$,

$$|B_2(\lambda, D)| = \left| \frac{q^{-\frac{\lambda+1}{2}}}{\lambda+1} \Big(\epsilon(\lambda) + \sum_{j=1}^{2g} e^{i(\lambda+1)\varphi_j} \Big) \right| + O(\max\{q^{-\frac{\lambda+2}{2}}, q^{-\frac{3(\lambda+1)}{4}}\}) \ ,$$

where $\epsilon(\lambda) = 0$ if λ is even and $\epsilon(\lambda) = 1$ if λ is odd. Recall that $\lambda + 1 \geq 2$. To derive the bound $\psi_2(\lambda, D)$ on $|B_2(\lambda, D)|$, we estimated

$$\Big| \sum_{j=1}^{2g} e^{i(\lambda+1)\varphi_j} \Big| \leq 2g \ , \tag{6.1}$$

which led to the bounds in Theorem 4.3. We have equality in (6.1) if and only if $\varphi_j = 0$ for $j = 1, \dots, 2g$ or $\varphi_j = \pi$ for $j = 1, \dots, 2g$. For the latter case, this means that the ω_j satisfy the condition

$$\omega_j = -\sqrt{q}, \qquad j = 1, \dots, 2g \ ,$$

which happens for *maximal function fields* (see [Sti93]). (However, such function fields do not occur if q is a prime.) Looking at (6.1), we do not find it surprising that large values for $|h - E_2|/L_2^2$ are so rare: we simply do not expect all φ_j to be close to 0, or all of them to be close to π. On the other hand, our definition $\alpha(g, q) = \mathrm{Mean}(|h - E_2|/L_2^2)$ for fixed values of g and q reads as

$$\mathrm{Mean}\Big(|S_{\lambda+1}(1)|/q^{\frac{\lambda+1}{2}} \Big) \approx \alpha(g, q) \cdot \frac{2g + \epsilon(\lambda)}{\lambda+1} \ , \tag{6.2}$$

where $\mathrm{Mean}(Y)$ stands for the mean value of Y. Notice that, clearly, the φ_j cannot be viewed as random numbers in the interval $[0, 2\pi[$: The ω_j occur as pairs (ω_j, ω_{j+g}) $(j = 1, \dots, g)$, where $\omega_{j+g} = \overline{\omega_j}$. Therefore, we put

$\varphi_{j+g} = -\varphi_j \pmod{2\pi}$ for $j = 1, \ldots, g$ and henceforth assume that $0 \leq \varphi_j \leq \pi$ for $j = 1, \ldots, g$. For any $n \geq 1$ we define

$$F_n(\,\varphi_1, \ldots, \varphi_g\,) = \left|\epsilon(n) + \sum_{j=1}^{2g} e^{i(n+1)\varphi_j}\right| = \left|\epsilon(n) + 2\sum_{j=1}^{g} \cos((n+1)\varphi_j)\right| .$$

Taking $q \to \infty$, (6.2) is equivalent to saying that

$$\text{Mean}(\,F_\lambda\,) \;\approx\; \alpha(g) \cdot (2g + \epsilon(\lambda)) \;. \tag{6.3}$$

Notice that for even λ, i.e., $\epsilon(\lambda) = 0$, the last equation is a statement about the distribution of the reciprocals of the roots of the zeta-function $Z(u, K)$ in $u = q^{-s}$, i.e., about the absolute value of the trace of the Frobenius in a constant field extension of degree $\lambda + 1$ (see [Sti93]).

By evaluating $\sum_{\deg(P)=1} \chi(P)$ and $\sum_{\deg(P)=2} \chi(P)$ for various choices of q and g and $D = D(X)$, we computed the average values of $|S_{\lambda+1}(1)|/q^{\frac{\lambda+1}{2}}$, for $\lambda = 0$ and $\lambda = 1$. In these cases, we know from (3.8) and Corollary 3.1 that

$$\sum_{j=1}^{2g} \omega_j = -1 - \sum_{\deg(P)=1} \chi(P)$$

and

$$\sum_{j=1}^{2g} \omega_j^2 = -1 - q + \theta(D) - 2 \sum_{\deg(P)=2} \chi(P) \;,$$

where $\theta(D)$ denotes the number of linear factors of D. Using these equations, we simultaneously determined the corresponding average values for $|\sum_{j=1}^{2g} {\omega_j}^\nu|$ for $\nu = 1, 2$. A selection of our results is shown in Table 2. All average values are taken over 1000 examples with the exception of $g = 3$ and $q = 10009$, where only 100 distinct monic, squarefree polynomials D have been considered. For instance, if $g = 3$, computation of $\text{Mean}(|\sum \omega_j^\nu|)/q^{\nu/2}$ via Riemann sums [Ser99] yield the values 0.80 and 1.40, respectively, for $\nu = 1$ and 2. Note that these theoretical mean values fit with our numerical experiments. Although we included the average values of $|S_1(1)|/\sqrt{q}$ for various values of q and g, we remark that $S_1(1)$ is irrelevant in our application, since $B_2(\lambda, D)$ is only defined for $\lambda \geq 1$.

In the remainder of this section we discuss our experimental observations. In particular, we explain (6.3) and show how to find the correct values for $\alpha(g)$. Hereby, we make use of recent results of Katz and Sarnak [KS99b, KS99a]. We remark that our explanation is basically due to [Ser99].

The main idea is to find a measure μ_g such that for any $n \geq 1$ we have

$$\text{Mean}(\,F_n\,) = \int_A F_n \, d\,\text{Haar} = \int_{[0,\pi]^g} F_n(\,\varphi_1, \ldots, \varphi_g\,)\, \mu_g(d\varphi_1, \ldots, d\varphi_g) \;,$$

where Haar denotes the Haar measure of a subgroup of the symplectic group $\text{Sp}(2g)$, and the latter integral is a Riemann integral which can be evaluated. We see that it is important to find the measure μ_g, i.e., to find the correct equidistribution. For instance, numerically, we find that the $\varphi_1, \ldots, \varphi_g$ are not uniformly distributed at random in the interval $[0, 2\pi[$. Since, otherwise, the expected value of $\text{Mean}(\,F_\lambda\,)$ would grow with $\sqrt{g}$ for even n rather than staying close to one.

TABLE 2. On the average values of $|S_{\lambda+1}(1)|/q^{(\lambda+1)/2}$ for $\lambda = 0, 1$

q	g	$\frac{\text{Mean}(\lvert\sum\omega_j\rvert)}{\sqrt{q}}$	$\frac{\text{Mean}(\lvert S_1(1)\rvert)}{\sqrt{q}}$	$\frac{\text{Mean}(\lvert\sum\omega_j^2\rvert)}{q}$	$\frac{\text{Mean}(\lvert S_2(1)\rvert)}{q}$
97	3	0.773	0.770	0.138e1	0.572
97	4	0.795	0.792	0.142e1	0.575
97	5	0.790	0.784	0.138e1	0.559
97	6	0.824	0.821	0.139e1	0.586
97	7	0.779	0.776	0.138e1	0.547
97	8	0.806	0.802	0.145e1	0.566
97	9	0.789	0.787	0.137e1	0.572
199	3	0.801	0.806		
199	4	0.792	0.793		
199	7	0.797	0.794		
991	3	0.802	0.801		
991	4	0.790	0.791		
991	7	0.800	0.801		
10009	3	0.853	0.853	0.148e1	0.549
10009	4	0.778	0.778		
10009	7	0.806	0.806		
100003	3	0.773	0.773		
100003	4	0.759	0.759		
100003	7	0.810	0.810		

Fortunately, there exist results on such equidistributions, from which we can derive results on Mean(F_n) for any n, and, in particular, for $n = \lambda$ as defined in (5.1). For $g = 1$ Birch [Bir68] (see also [Yos73]) proved that φ_1 is equidistributed relative to the Sato-Tate measure (see [Tat65]), which is given as $\mu_1(d\varphi_1) = \frac{2}{\pi}\sin^2(\varphi_1)d\varphi_1$. We then have that

$$\begin{aligned}\text{Mean}(\, F_1\,) &= \int_0^\pi F_1(\,\varphi_1\,)\,\mu_1(d\varphi_1)\\ &= \tfrac{2}{\pi}\int_0^\pi |1+2\cos(2\varphi_1)|\sin^2(\varphi_1)d\varphi_1\\ &= 3\sqrt{3}/2\pi \;\approx\; 0.82699\ldots .\end{aligned}$$

The case $g > 1$ was done more recently, when Katz and Sarnak [KS99a, Theorem 10.8.2, p.321] showed that the equidistribution of $\varphi_1, \ldots, \varphi_g$ takes place relative to the measure μ_g which is basically the Haar measure of a maximal compact subgroup of the symplectic group $\text{Sp}(2g)$. The explicit formula for μ_g is provided in [KS99a, 5.0.4, p.107] and is due to Weyl [Wey68, p.591]: If $0 \le \varphi_j \le \pi$ and $\varphi_{j+g} = -\varphi_j$ for $j = 1, \ldots, g$, then

$$\mu_g(d\varphi_1, \ldots, d\varphi_g) = (\tfrac{1}{g!})\prod_{j=1}^{g}(\tfrac{2}{\pi})\sin^2(\varphi_j)\prod_{i<j}4(\cos(\varphi_i)-\cos(\varphi_j))^2 d\varphi_1\cdots d\varphi_g\ .$$

TABLE 3. Approximate values of $\mathrm{Mean}(F_\lambda)$ and $\alpha(g)$ for $3 \le g \le 7$

g	λ	N	$\mathrm{Mean}(F_\lambda)$	$\alpha(g)$
3	1	150	1.144	0.163
4	1	70	1.128	0.125
5	2	50	1.389	0.139
6	2	40	1.382	0.115
7	2	30	1.381	0.099

Note that we may remove the factor $1/(g!)$ if we arrange the φ_i in increasing order: $0 \le \varphi_1 \le \ldots \le \varphi_g \le \pi$. We thus have that

$$\begin{aligned}\mathrm{Mean}(F_n) &= \tfrac{1}{g!}\left(\tfrac{2^g}{\pi}\right)^g \int_0^\pi \int_0^\pi \ldots \int_0^\pi G_n(\varphi_1, \ldots, \varphi_g)\, d\varphi_1\, d\varphi_2 \ldots d\varphi_g \\ &= \left(\tfrac{2^g}{\pi}\right)^g \int_{\varphi_g=0}^{\pi} \int_{\varphi_{g-1}=0}^{\varphi_g} \ldots \int_{\varphi_1=0}^{\varphi_2} G_n(\varphi_1, \ldots, \varphi_g)\, d\varphi_1\, d\varphi_2 \ldots d\varphi_g\end{aligned}$$

where

$$\begin{aligned}&G_n(\varphi_1, \ldots, \varphi_g) \\ &\quad = \left|\epsilon(n) + 2\sum_{j=1}^{g} \cos((n+1)\varphi_j)\right| \prod_{j=1}^{g} \sin^2(\varphi_j) \prod_{i<j} (\cos(\varphi_i) - \cos(\varphi_j))^2 \ .\end{aligned}$$

One way to approximate the integral is to use Riemann sums. We choose a positive integer N and divide the interval $[0, \pi]$ in multiples of π/N. For reasonably large values of N this will give an approximation of the integral, i.e., $\mathrm{Mean}(F_n) = \lim_{N\to\infty} F_{n,N}$ with

$$F_{n,N}(\varphi_1, \ldots, \varphi_g) = \left(\tfrac{2^g}{N}\right)^g \sum_{\varphi_g=0}^{N-1} \sum_{\varphi_{g-1}=0}^{\varphi_g} \ldots \sum_{\varphi_1=0}^{\varphi_2} G_n\left(\tfrac{\varphi_1 \pi}{N}, \ldots, \tfrac{\varphi_g \pi}{N}\right).$$

In Table 3, we summarize the approximate values of $\mathrm{Mean}(F_\lambda)$ and $\alpha(g)$, where λ is defined in (5.1) and g takes values between 3 and 7. We also computed the approximate value of $\mathrm{Mean}(F_3)$ in the case $g = 7$, which is 1.600 for $N = 30$, yielding an approximate value of 0.107 for $\mathrm{Mean}(|h - E_2|/L_2^2)$.

Our approximation seems to be quite reasonable for our values of N. For comparison, we mention that in the case $g = 3$ we obtained for $\mathrm{Mean}(F_1)$ the value 1.144, 1.143, 1.143, and 1.144, respectively, when $N = 20$, 30, 50, and 100. This yields the value $\alpha(3) = 0.163$ for each such N and suggests that $|\alpha(3) - 0.163| < 10^{-3}$.

7. Discussion, outlook, conclusion

7.1. **Speeding up baby step–giant step and Pollard kangaroo methods.** Our improved bounds and heuristics are useful to speed up the computation of the regulator and divisor class number in hyperelliptic function fields when using the baby step–giant step method or the Pollard kangaroo method. In both cases we assume that we know an approximation E for the divisor class number h, and a number L such that $|h - E| < L^2$. We then use one of the two aforementioned methods to find the actual value of h in the interval $]E - L^2, E + L^2[$.

An important parameter in the baby step–giant step method is the number M of baby steps that are computed. Usually, in the case of hyperelliptic function fields, one chooses $M = L$. But since the distribution of $|h - E|$ seems to have an increasing hazard rate, the average total number of baby steps and giant steps is minimal when choosing $M = \lceil \sqrt{2\alpha(g)L^2} \rceil$ (see [BT00]), where $\alpha(g)$ is as in Table 3; this choice reduces the average number of baby steps and giant steps by a factor of $(1 + \alpha(g))/(3\sqrt{\alpha(g)/2})$. For example, if $g = 3$ and $\alpha(3) = 0.163$, this factor is 1.92, while for $g = 4$ and $\alpha(4) = 0.125$, we get a factor of 2.12. Notice that a further improvement can be achieved by exploiting the different computational costs of baby steps and giant steps (see [STa]).

In the Pollard kangaroo method, an important parameter is given by the mean value of the jump distances in the set of jumps. The optimal choice for this mean value is, among other things, determined by the expected value for $|h-E|$. Without heuristics, we would assume this value to be $L^2/2$. If we work with $\alpha(g)L^2$ instead, we can speed up the algorithm by a factor of 1.16 for $g = 3$ and 1.25 for $g = 4$. See [STb] for details.

7.2. **The case of characteristic 2.** In this section we show that the same results of the paper hold for fields of even characteristic. In fact, we only need to derive a formula as in (3.1) with an appropriate symbol χ and explain how to evaluate this symbol. Then, the same estimates and bounds as in Section 3 and Section 4 hold. We mention that explicit ideal arithmetic in hyperelliptic function fields of even characteristic can be found in [Zuc97].

At first, we do not need to restrict ourselves to finite fields of even characteristic. Let $k = \mathbb{F}_q$ be a finite field of characteristic p, i.e., $q = p^t$, $t \geq 1$. Let $K = k(X)(\rho)$ be a hyperelliptic function field over k, where $\rho \in K$ is a zero of the irreducible polynomial $\varphi(X, Y) = Y^2 + h(X)\,Y - f(X) \in k[X, Y]$, i.e., $\varphi(X, \rho) = 0$. Furthermore, we assume that $h(X), f(X)$ are polynomials in $k[X]$ such that the hyperelliptic curve $C : Y^2 + h(X)\,Y = f(X)$ is nonsingular. Note that $K = k(X)(\rho) = k(C)$ and $[K : k(X)] = 2$. Then the integral closure $\mathcal{O}(X)$ of $k[X]$ in K is given by $\mathcal{O}(X) = k[X, \rho] = k[X, Y]/(\varphi(X, Y))$, and $\mathcal{O}(X)$ is a Dedekind domain.

We now proceed as follows. First, we discuss the splitting behavior of the infinite place of $k(X)$ and prime ideals of $k(X)$ in K. Hereby, we introduce the symbol $\chi(P)$ for a monic, irreducible polynomial $P = P(X) \in k[X]$, and mainly apply [Lor96, Prop. 4.3, p.99] to derive formula (3.1) for any hyperelliptic function field. Then, we explain how to compute $\chi(P)$ efficiently.

In analogy to the cases in Theorem 1.1 and Section 3, we can distinguish between three possible situations depending on how the infinite place ∞ of $k(X)$ splits in K. Let r denote the number of infinite places of K and let r_2 be the number of infinite places of degree 2. In the first case, $\varphi(X, Y)$ factors in $k((\frac{1}{X}))[Y]$ into two linear factors so that $Y \in k((\frac{1}{X}))$. K is then called a *real quadratic function field* over k. We then have $r = 2$, i.e., ∞ splits completely in K, and $r_2 = 0$. Otherwise K is called *imaginary quadratic*. In the second case, the infinite place ∞ of $k(X)$ is ramified in K. It follows that $r = 1$ and $r_2 = 0$. In the last case, ∞ is inert in K which means that $r = 1$ and $r_2 = 1$.

Prime ideals $\mathfrak{p}$ of $\mathcal{O}(X)$ arise from prime ideals of $k[X]$, which are principal ideals given by prime polynomials. Let $P = P(X)$ be any monic, irreducible (prime) polynomial in $k[X]$ such that $P(X)k[X]$ is a prime ideal of $k[X]$. Then the factorization of $P(X)\mathcal{O}(X)$ is determined by the factorization of the quadratic polynomial

$\varphi(X,Y) \pmod{P(X)}$ in $(k[X]/P(X)k[X])[Y]$. Equivalently, we ask whether the equation

$$\varphi(X,Y) = Y^2 + h(X)\,Y - f(X) \equiv 0 \pmod{P(X)} \tag{7.1}$$

has 0, 1, or 2 solutions $Y \pmod{P(X)}$. The case $p > 2$ is described in detail in [Art24, p.170–171]. In this case, we may assume that $h(X) = 0$, and the solvability of $Y^2 \equiv f(X) \pmod{P(X)}$ can be easily expressed in terms of the polynomial Legendre symbol $[f(X)/P(X)]$.

Now, let $q = 2^t$, i.e., $p = 2$. For a monic, irreducible polynomial $P(X)$ in $\mathbb{F}_{2^t}[X]$ of degree $\nu = \deg P(X)$, we denote by $\chi(P)$ the following symbol

$$\chi(P) = \begin{cases} 1 & \text{if (7.1) has 2 solutions} \\ 0 & \text{if (7.1) has 1 solution} \\ -1 & \text{if (7.1) has no solution.} \end{cases} \tag{7.2}$$

We can proceed as in [Art24, p.170–171] and make use of [Lor96, Prop. 4.3, p.99] (e.g.). Recall that $(\mathbb{F}_{2^t}[X]/P(X)\mathbb{F}_{2^t}[X])$ can be identified with the finite field $\mathbb{F}_{2^{\nu t}}$. Then (7.1) is equivalent to

$$Y^2 + bY - c = 0$$

in $\mathbb{F}_{2^{\nu t}}$, where $b, c \in \mathbb{F}_{2^{\nu t}}$, respectively, denote the elements $h(X) \pmod{P(X)}$, and $f(X) \pmod{P(X)}$.

Case 1. $P(X) \mid h(X)$. Then $\varphi(X,Y) \equiv Y^2 - f(X) \equiv (Y - f(X)^{2^{\nu t-1}})^2 \pmod{P(X)}$ and (7.1) has 1 solution so that $\chi(P) = 0$. This means that $b = 0$, and in $\mathbb{F}_{2^{\nu t}}$ we have $Y^2 + bY - c = (Y + c^{2^{\nu t-1}})^2$. It follows that $P(X)\mathcal{O}(X) = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ of degree $f_\mathfrak{p} = 1$ in $\mathcal{O}(X)$ and $|N(\mathfrak{p})| = q^{f_\mathfrak{p}} = q$. In this case, $\mathfrak{p}$ is ramified.

Case 2. $P(X)$ does not divide $h(X)$ and (7.1) has no solution. Then $\chi(P) = -1$, and $\varphi(X,Y)$ is irreducible $\pmod{P(X)}$. It follows that $P(X)\mathcal{O}(X) = \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of degree $f_\mathfrak{p} = 2$ in $\mathcal{O}(X)$, and $|N(\mathfrak{p})| = q^{f_\mathfrak{p}} = q^2$. In this case, $\mathfrak{p}$ is inert.

Case 3. $P(X)$ does not divide $h(X)$ and (7.1) is solvable. Then $\chi(P) = 1$, since if $B(X) \pmod{P(X)}$ is a solution, then $-B(X) - h(X) \not\equiv B(X) \pmod{P(X)}$ is the other solution. Furthermore, $\varphi(X,Y) \equiv (Y - B(X))(Y + B(X) + h(X)) \pmod{P(X)}$. Thus, $P(X)\mathcal{O}(X) = \mathfrak{p}\,\overline{\mathfrak{p}}$ for prime ideals $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ of degree $f_\mathfrak{p} = 1 = f_{\overline{\mathfrak{p}}}$, and $|N(\mathfrak{p})| = |N(\overline{\mathfrak{p}})| = q$.

By following the lines of [Art24, pp. 208-209], we immediately derive (3.1) for the even characteristic case.

It remains to show how to evaluate $\chi(P)$ for a monic, prime polynomial $P(X)$ of degree ν. If $P(X)$ divides $h(X)$, then we surely know that $\chi(P) = 0$. Suppose that $P(X)$ does not divide $h(X)$. We only need to decide whether (7.1) is solvable or not. In case that it is solvable, we do not need to compute the explicit solutions. Since $h(X) \not\equiv 0 \pmod{P(X)}$, (7.1) is solvable if and only if

$$Y^2 + Y - a = 0 \tag{7.3}$$

is solvable in $\mathbb{F}_{2^{\nu t}}$, where a denotes the element $f(X) \cdot h(X)^{-2} \pmod{P(X)}$ in $\mathbb{F}_{2^{\nu t}}$. By [LN83, Theorem 2.25] we know that (7.3) has a solution if and only if $\mathrm{Tr}_{\mathbb{F}_{2^{\nu t}}/\mathbb{F}_2}(a) = \sum_{i=0}^{\nu t-1} a^{2^i} = 0$.

A method for computing $\chi(P)$ is then given as follows. If $P(X)$ divides $h(X)$, then $\chi(P) = 0$. Otherwise, determine $h(X)^{-1} \pmod{P(X)}$ and put $A(X) = f(X) \cdot h(X)^{-2} \pmod{P(X)}$. Finally, compute $\mathrm{Tr}_{\mathbb{F}_{2^{\nu t}}/\mathbb{F}_2}(A(X)) = \sum_{i=0}^{\nu t-1} (A(X))^{2^i}$, which is either 0 or 1. If it is 0, then $\chi(P) = 1$, and if it is 1, then $\chi(P) = -1$.

7.3. **Minimally better bounds.** We remark here that some of the bounds in Section 4 can be minimally improved. We also could have used the *Serre bound* or the asymptotic *Drinfeld-Vladut bound* to estimate $\sum_{i=1}^{2g} \omega_i^\nu$ for $\nu \in \mathbb{N}$ (see [Ser83, Sti93]). For our algorithmic applications of the bounds it is completely sufficient to use $|\sum_{i=1}^{2g} \omega_i^\nu| \leq 2gq^{\nu/2}$. The Serre bound yields $|\sum_{i=1}^{2g} \omega_i^\nu| \leq g\lfloor 2q^{\nu/2} \rfloor$, which gives a negligible improvement in our context. The Drinfeld-Vladut bound is effective only for very large genus and we cannot apply this bound, since we are mainly interested in hyperelliptic function fields of small genus.

7.4. **Real or imaginary?** We have seen in Section 5 that any hyperelliptic function field K can be represented as a real quadratic function field. If one uses a baby step–giant step strategy to search for a multiple of the regulator, then one should definitely use the arithmetic in real quadratic function fields. One obtains a considerable speed-up by making use of the comparably inexpensive baby steps and a convenient parameter choice. This is of particular interest if one has to deal with space restrictions. For a discussion of the optimal choice of the parameters, we refer to [STa].

7.5. **Generalizations.** We extended the previous methods of Stein and Williams to any hyperelliptic function field in a way that can be generalized to arbitrary algebraic function fields. Once we are given an equation as in (3.1), we can combine it with (2.5) to obtain an expression similar to (3.2). Of course, the exponents of $(1-u)$ and $(1+u)$ in (3.2) have to be adjusted. With slight modifications we are then able to proceed as in Section 3 and 4.

7.6. **Choice of the approximation.** In Section 4, we presented two possible approximations $E_1(\lambda, D)$ and $E_2(\lambda, D)$ for the divisor class number h. The bound on $|B_1(\lambda, D)|$ and thus the bound on $|h - E_1(\lambda, D)|$ is smaller than the bound on $|B_2(\lambda, D)|$, if the genus of the hyperelliptic function field is odd. But, numerical experiments showed that the second approximation is more accurate. This is at first sight surprising. However, it follows from (4.2) and (4.4) that the second approximation contains more information about the hyperelliptic function field than the first one. Therefore, the result seems to be natural. For our purposes, we used $E_2(\lambda, D)$ and $L_2(\lambda, D)$. Still, there might be applications in which $E_1(\lambda, D)$ and $L_1(\lambda, D)$ are more useful.

7.7. **Applying Bach's method?** Bach's method [Bac95] of weighted averages of truncated Euler products in the number field case seems not to apply *ad hoc* in the function field situation. This method was investigated by Jacobson, Lukes, and Williams [JLW95] for the computation of class numbers and regulators of quadratic number fields and turned out to be a huge improvement over the truncated product method of Lenstra [Len82]. Unfortunately, the method is based on the fact that the size of the prime numbers constitutes an ordering of them. Instead of computing all Euler product terms for primes between 0 and an upper bound Q, one computes the terms for primes between 0 and $2Q$, where one multiplies the terms between Q and $2Q$ with a certain weight. In the function field case, the monic prime polynomials

are ordered with respect to their degree. An ordering of prime polynomials of equal degree seems to be difficult. For instance, let $g = 3$ and thus $\lambda = 1$. Then the analogue of Bach's method would imply to consider all monic prime polynomials of degree 1 and in addition the ones of degree 2. For the $q(q-1)/2$ monic prime polynomials P of degree 2, one then evaluates the character values $\chi(P)$ and multiplies the Euler product terms of degree 2 with certain weights. But, this means that one has to perform at least $q(q-1)/2 = O(q^2)$ operations. Since the complexity of the algorithm described in Section 5 for hyperelliptic function fields of genus 3 is only $O(q)$ polynomial operations, the weighted average of truncated Euler products would worsen the complexity of the algorithm.

Acknowledgments

We would like to thank Professor Alf van der Poorten for inviting us to his Centre for Number Theory Research at the Macquarie University, Sydney, Australia, in the Canadian Winter 98/99, where we did most of this work. We are most grateful to Professor J.-P. Serre for very helpful comments on Section 6. We also wish to thank Professor Eric Bach for pointing out the reference [KS99b]. We are indebted to the Centre for Applied Cryptographic Research at the University of Waterloo; we especially wish to thank Professor Alfred Menezes for his continuous support. Finally, we would like to thank an anonymous referee for useful comments.

References

[ADH94] L. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. In *Algorithmic Number Theory Seminar ANTS-I*, volume 877 of *Lecture Notes in Computer Science*, pages 28–40. Springer, 1994. MR **96b:**11078

[Art24] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen I, II. *Math. Zeitschr.*, 19:153–206, 1924.

[Bac95] E. Bach. Improved approximations for euler products. In *Proc. CNTA-4 (Canadian Math. Soc. Conference)*, volume 15, pages 13–28, 1995. MR **96i:**11124

[Bir68] B. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968. MR **37:**6242

[BT00] S. R. Blackburn and E. Teske. Baby-step giant-step algorithms for non-uniform distributions. In *Algorithmic Number Theory Seminar ANTS-IV*, volume 1838 of *Lecture Notes in Computer Science*, pages 153–168. Springer-Verlag, 2000.

[CF96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Series*. Cambridge University Press, 1996. MR **97i:**11071

[Deu73] M. Deuring. *Lectures on the Theory of Algebraic Functions of One Variable*. Number 314 in Lect. Notes in Math. Springer-Verlag, Berlin, 1973. MR **49:**8970

[DW85] G. Dueck and H. C. Williams. Computation of the class number and class group of a complex cubic field. *Mathematics of Computation*, 45(171):223–231, 1985. MR **86m:**11078

[JLW95] Michael J. Jacobson, Richard F. Lukes, and Hugh C. Williams. An investigation of bounds for the regulator of quadratic fields. *Experimental Mathematics*, 4(3):211–225, 1995. MR **97d:**11173

[Kob88] N. Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1:139–150, 1988. MR **90k:**11165

[KS99a] N. M. Katz and P. Sarnak. *Random matrices, Frobenius eigenvalues and monodromy*, volume 45 of *AMS Colloquium Publications*. AMS, Providence, Rhode Island, 1999. MR **2000b:**11070

[KS99b] N. M. Katz and P. Sarnak. Zeroes of zeta functions and symmetry. *Bulletin of the AMS*, 36(1):1–26, January 1999. MR **2000f:**11114

[Len82] H. W. Lenstra. On the calculation of regulators and class numbers of quadratic fields. *London. Math. Soc. Lec. Note Ser.*, 56:123–150, 1982. MR **86g:**11080

[LN83] R. Lidl and H. Niederreiter. *Finite Fields*. Addison-Wesley, Reading, MA, 1983. MR **86c:**11106

[Lor96] D. Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. AMS, Providence, Rhode Island, 1996. MR **97e:**14035

[MM80] M. L. Madan and D. J. Madden. On the theory of congruence function fields. *Communications in Algebra*, 8(17):1687–1697, 1980. MR **82b:**12011

[MST99] V. Müller, A. Stein, and C. Thiel. Computing discrete logarithms in real quadratic congruence function fields of large genus. *Mathematics of Computation*, 68:807–822, 1999. MR **99i:**11119

[Poo96] B. Poonen. Computational aspects of curves of genus at least 2. In *Algorithmic Number Theory Seminar ANTS-II*, volume 1122 of *Lecture Notes in Computer Science*, pages 283–306. Springer, 1996. MR **98c:**11059

[PR99] S. Paulus and H.-G. Rück. Real and imaginary quadratic representations of hyperelliptic function fields. *Mathematics of Computation*, 68:1233–1241, 1999. MR **99i:**11107

[Sch31] F. K. Schmidt. Analytische Zahlentheorie in Körpern der Charakteristik p. *Mathematische Zeitschrift*, 33:1–32, 1931.

[Ser83] J. P. Serre. Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini. *C. R. Acad. Sci. Paris*, 296:397–401, 1983. MR **85b:**14027

[Ser99] J. P. Serre, 1999. Personal communications, Aug. 27, Aug. 28, Sept. 7, Sept. 11.

[SSW96] R. Scheidler, A. Stein, and H. C. Williams. Key-exchange in real quadratic congruence function fields. *Designs, Codes and Cryptography*, 7:153–174, 1996. MR **97d:**94009

[STa] A. Stein and E. Teske. Optimized baby step–giant step methods and applications to hyperelliptic function fields. Unpublished manuscript.

[STb] A. Stein and E. Teske. The parallelized Pollard kangaroo method in real quadratic function fields. Math. Comp., posted on October 4, 2001, PII 50025-5718(01)01343-6 (to appear in print).

[Sti93] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer, Berlin, 1993. MR **94k:**14016

[SW98] A. Stein and H. C. Williams. An improved method of computing the regulator of a real quadratic function field. In *Algorithmic Number Theory Seminar ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 607–620. Springer, 1998. MR **2000j:**11201

[SW99] A. Stein and H. C. Williams. Some methods for evaluating the regulator of a real quadratic function field. *Experimental Mathematics*, 8(2):119–133, 1999. MR **2000f:**11152

[Tat65] J. Tate. Algebraic cycles and poles of zeta functions. In O. F. G. Schilling, editor, *Arithmetical Algebraic Geometry*, pages 93–110, New York, 1965. Harper & Row. MR **37:**1371

[Wey68] H. Weyl. *Gesammelte Abhandlungen*, volume II. Springer-Verlag, Berlin, Heidelberg, New York, 1968. MR **37:**6157

[WZ91] B. Weis and H. G. Zimmer. Artin's Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen. *Mitt. Math. Ges. Hamburg, Sond.*, XII(2), 1991. MR **93e:**11141

[Yos73] H. Yoshida. On an analogue of the Sato conjecture. *Inventiones mathematicae*, 19:261–277, 1973. MR **49:**2746

[Zha87] X. Zhang. Ambiguous classes and 2-rank of class groups of quadratic function fields. *J. of China University of Science and Technology*, 17(4):425–431, 1987. MR **89j:**11115

[Zuc97] R. Zuccherato. The continued fraction algorithm and regulator for quadratic function fields of characteristic 2. *Journal of Algebra*, 190:563–587, 1997. MR **98a:**11156

University of Illinois at Urbana-Champaign, Department of Mathematics, 1409 West Green Street. Urbana, Illinois 61801

E-mail address: andreas@math.uiuc.edu

University of Waterloo, Department of Combinatorics and Optimization, Waterloo, Ontario, Canada N2L 3G1

E-mail address: eteske@math.uwaterloo.ca