Explicit Bounds and Heuristics on Class Numbers in Hyperelliptic Function Fields

Andreas Stein, Edlyn Teske
Centre for Applied Cryptographic Research
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
{astein,eteske}@cacr.math.uwaterloo.ca

July 19, 1999

Abstract

In this paper, we provide sharp 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 with the help of new results. We thus obtain a faster method of computing regulators and class numbers. Furthermore, we provide heuristics on the distribution of the class number within the bounds on the class number. These heuristics suggest that, although the bounds are sharp, the approximation is in general far better.

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 employ 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 non-special 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 $h \in \,]E-L^2, E+L^2[$. Once 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 [ST99] 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 our following main theorem.

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. We have for all integers $n \geq 1$ that*

$$\sum_{\nu|n} \nu \sum_{\deg(P)=\nu} \chi(P)^{n/\nu} = 1 - r - (-1)^n r_2 - \sum_{i=1}^{2g} \omega_i^n \,, \tag{1.1}$$

where r is the number of infinite places of k, r_2 is the number of infinite places of degree 2, and the complex numbers ω_i $(i = 1, \dots, 2g)$ 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 sharper 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 results about the distribution of $|h-E|/L^2$ in the case of real quadratic function fields. Our conclusions and further discussions can be found in Section 7.

2 ζ-Functions 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 $Div_0(K)$ the group of divisors of degree 0. The group of principal divisors $P(K)$ is a subgroup of $Div_0(K)$ and the factor group $Cl_0(K) = Div_0(K)/P(K)$ is called the *divisor class group (of degree 0)* of K. Its order $h = |Cl_0(K)|$ 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 $s = 0$ and $1 + l \cdot 2\pi i/\log q$ $(l \in \mathbb{Z})$. More precisely, we have (see, for instance, [Sti93, Theorem V.1.15 and V.2.1]) that

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

where $|\omega_i| = \sqrt{q}$ for $i = 1, 2, \ldots, 2g$. 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 transcendent 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 $\infty_1, \ldots, \infty_r$ denote the infinite primes of K with respect to $\mathcal{O}(X)$ of degree $f_1, \ldots, f_r$, then we derive from [Sch31] (see also [MM80]) that

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

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

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

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 $k(X)$ ($i = 1, \ldots, r$), then $n = \sum_{i=1}^{r} e_i f_i$.

3 ζ-Functions in Hyperelliptic Function Fields

In this section, let K be a hyperelliptic function field over the 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 that $\mathcal{O}(X) = k[X][\sqrt{D}]$. 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]). In the first case, there are two distinct conjugated 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 (1.1) in Theorem 1.1 reads

$$\sum_{\nu | n} \nu\, S_\nu \left(\frac{n}{\nu}\right) = 1 - r - (-1)^n r_2 - \sum_{i=1}^{2g} \omega_i^n \quad (n \in \mathbb{N}) . \tag{3.3}$$

Proof. *(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

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

This gives the desired result. □

With the help of this theorem, we are able to provide sharp 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

$$S_1(1)=\sum_{\deg(P)=1}\chi(P)=-\sum_{i=1}^{2g}\omega_i+1-r+r_2\ . \tag{3.4}$$

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

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

where

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

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

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

From Theorem 1.1, we derive that

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

By special Möbius inversion [1], we see that

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

The assertion then follows from the fact that

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

$\square$

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

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

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

$$nS_n(1) = -\sum_{i=1}^{2g} \omega_i^n + 1 - r - r_2 - \sum_{\nu \mid \frac{n}{2}} \nu\, S_\nu(2)\ .$$

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

4 New Sharp 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 $E = \mathrm{Ne}(E')$, where $\mathrm{Ne}(y)$ denotes the nearest integer to y. [2] Thus,

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

and

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

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 sharp estimate 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 sharp 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 sharp 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

$$h = q^g L(1/q, K) = \frac{q^{g+r-1+r_2}}{(q-1)^{r-1}(q+1)^{r_2}} \prod_P \frac{1}{1 - \chi(P) q^{-\deg(P)}} \ .$$

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

As in the proof of Theorem 1.1, it follows that

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

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

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

and

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

Then $E_1(\lambda, D) := \mathrm{Ne}(E_1'(\lambda, D))$ is an approximation of h and $B_1(\lambda, D) = \log h - \log E_1'(\lambda, D)$ is to estimate the error in this approximation. Below, we will show that

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

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

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

or, equivalently,

$$E_2'(\lambda, D) = \frac{q^{g+r-1+r_2}}{(q-1)^{r-1}(q+1)^{r_2}} \prod_{\substack{P \\ \deg(P) \le \lambda}} \frac{1}{1 - \chi(P) q^{-\deg(P)}}$$

and

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

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

Then $E_2(\lambda, D) := \mathrm{Ne}(E_2'(\lambda, D))$ is an approximation of h and $B_2(\lambda, D) = \log h - \log E_2'(\lambda, D)$ is the logarithm of the tail of the truncated Euler product. 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 sharper 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 $\lambda \geq 1$. 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 sharp bounds for $|B_1(\lambda, D)|$, we make use of Theorem 1.1 and find that

$$\begin{aligned} \Big| \sum_{\nu | n} \nu\, S_\nu \left(\frac{n}{\nu}\right) \Big| &\leq |1 - r - (-1)^n r_2| + \Big| \sum_{i=1}^{2g} \omega_i^n \Big| \\ &\leq 2gq^{\frac{n}{2}} + 1 , \end{aligned} \tag{4.6}$$

since $|\omega_i| = \sqrt{q}$ and $|1 - r - (-1)^n r_2| \leq 1$ by definition of r and r_2. 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,

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

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

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

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

Proof. From (4.6), it follows that

$$\Big|\sum_{n=1}^{\lambda} \frac{1}{nq^n} \sum_{\nu | n} \nu\, S_\nu\left(\frac{n}{\nu}\right)\Big| \leq \sum_{n=1}^{\lambda} \frac{2gq^{\frac{n}{2}} + 1}{nq^n} < 2g \sum_{n=1}^{\infty} \frac{1}{nq^{\frac{n}{2}}} + \sum_{n=1}^{\infty} \frac{1}{nq^n}$$
$$= 2g\log\Big(\frac{\sqrt{q}}{\sqrt{q}-1}\Big) + \log\Big(\frac{q}{q-1}\Big) .$$

Thus, by (4.2),

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

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

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

In this case, we have that $E_1'(\lambda, D) \leq e(3/2)^r \cdot q^g$. 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 that

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

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

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

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 $S_\nu(2)$ only differ by the number of prime factors of D of degree ν, i.e.,

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

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

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

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

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

where $|\rho(n)| \leq 1$. 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

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

Summarizing, we obtain

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

□

Note that the bound in the above lemma can be minimally sharpened by only considering 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 that*

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

Proof. First, we see that

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

Then we make use of Lemma 4.1 to find that

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

Thus,

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

Summing up we can conclude that

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

□

Lemma 4.1 and 4.2 provide us with sharp 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

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

We proved the following

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

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

If it happens that $\omega_i = -\sqrt{q}$ for $i = 1, \dots, 2g$, i.e. K is a *maximal function field* (see [Sti93, p.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 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 $\lambda \geq 1$, we have*

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

Proof. By (4.4), we have that

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

If we use that

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

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

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

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 that $h_X = 2h$. 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 $q > 5$. 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 sharp estimate. For $g \geq 3$, we put $E' = E_2'(\lambda, D)$, $E = \mathrm{Ne}(E_2'(\lambda, D))$, 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 [ST99]). 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

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

which yields a total running time of

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

[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.

where

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

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 $E = \mathrm{Ne}(E')$, $|B| < \psi$, 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 $\widetilde{h}$ of the ideal class number h_X. Second, we discuss how one might obtain such a divisor. Let $\widetilde{h}|h_X$, and let $h_X = \widetilde{h}\,H$ for some positive integer H, i.e. $h = \widetilde{h}\,HR_X$. We put

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

Then,

$$|HR_X - E''| = \frac{|h - E'|}{\widetilde{h}} < \frac{L^2}{\widetilde{h}} \leq (L'')^2$$

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 $\widetilde{h}$ smaller than the interval $]E - L^2, E + L^2[$. Note that if $R_X \geq 2(L'')^2$, then $H = \mathrm{Ne}(E''/R_X)$. Moreover, we put $\widetilde{H} = \mathrm{Ne}(E''/R_X)$ and $F = E''/R_X - \mathrm{Ne}(E''/R_X)$. If $\psi < \log((\widetilde{H} + 1)/(\widetilde{H} + |F|))$, then $H = \widetilde{H}$. 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 Heuristic Results

We now 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). 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 only consider the estimate for $|h - E_2|$ in Theorem 4.3. This estimate is almost sharp. 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 heuristic 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 value and the standard deviation

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	10^5
199	3	0.141	0.74	0.16e-3	0.584	22.2	42.3	73.8	0.12	0.33	0.44	10^3
991	3	0.161	0.72	0.55e-3	0.608	18.9	36	67.1	0.14	0.38	0.49	10^3
10009	3	0.157	0.76	0.2e-4	0.733	20.6	38.3	67.4	0.13	0.39	0.5	10^3
10009	3	0.161	0.73	0.312e-5	0.862	18.8	37.1	67.4	0.14	0.38	0.49	10^5
100003	3	0.16	0.72	0.12e-3	0.741	17.8	36.2	67.3	0.14	0.37	0.5	10^3
1000003	3	0.165	0.72	0.32e-3	0.602	18	35.6	66.3	0.14	0.39	0.5	10^3
37	4	0.116	0.73	0.9e-4	0.395	27.2	51.4	82.2	0.1	0.28	0.35	10^3
97	4	0.136	0.76	0.1e-3	0.566	23	45.6	76.9	0.12	0.33	0.45	10^3
199	4	0.147	0.74	0.47e-3	0.59	21.4	40.6	71.3	0.13	0.35	0.45	10^3
991	4	0.116	0.77	0.14e-3	0.584	26.8	52.3	83	0.1	0.29	0.39	10^3
37	5	0.094	0.76	0.4e-4	0.391	32.6	59.4	90.8	0.8e-1	0.23	0.3	10^3
97	5	0.107	0.75	0.26e-3	0.445	27.9	54.5	86	0.9e-1	0.26	0.34	10^3
199	5	0.119	0.75	0.5e-4	0.544	24.4	50.9	82.7	0.1	0.29	0.39	10^3
991	5	0.133	0.75	0.266e-5	0.6	22.3	45	77.9	0.11	0.34	0.43	10^3
37	6	0.081	0.75	0.9e-4	0.328	37.5	69.4	94.6	0.7e-1	0.2	0.26	10^3
97	6	0.096	0.76	0.7e-4	0.44	31.2	58.2	90.4	0.8e-1	0.23	0.32	10^3
199	6	0.1	0.75	0.13e-3	0.36	31	57.4	88.2	0.8e-1	0.25	0.31	10^3
37	7	0.074	0.74	0.3e-4	0.298	39.6	71.7	97.1	0.6e-1	0.18	0.23	10^3
97	7	0.089	0.71	0.24e-3	0.371	33.1	62.4	93.8	0.8e-1	0.21	0.27	10^3
17	8	0.052	0.73	0.7e-4	0.199	54.1	88.6	100	0.5e-1	0.13	0.16	10^3
17	9	0.055	0.73	0.9e-4	0.244	52.4	84.9	99.7	0.5e-1	0.13	0.16	10^3

Table 1: On the distribution of $|h - E_2|/L_2^2$

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 or equal than 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.

Moreover, if we look at the average values μ more closely, we notice that they are very close to $1/(2g)$. That is, the bound L_2^2 is, *on average*, by a factor of $2g$ too large. We discuss these observations, and go back to Theorem 4.3 where we derived the bound $\psi_2(\lambda, D)$ on $|B_2(\lambda, D)| = |h - E_2|$. 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 to large. For most of our examples, however, we have that $\psi_2(\lambda, D) < 0.05$ 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 $\omega_j = q^{1/2}e^{i\varphi_j}$, $\varphi_j \in [0, 2\pi[$, $j = 1, \ldots, 2g$,

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

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

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

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

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

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 observation $\mu \approx 1/(2g)$ reads as

$$\mu\Big(|S_{\lambda+1}(1)|/q^{\frac{\lambda+1}{2}}\Big) \approx \frac{1}{2g}\frac{2g+\epsilon(\lambda)}{\lambda+1} = \frac{1+\frac{\epsilon(\lambda)}{2g}}{\lambda+1}\ , \tag{6.2}$$

where $\mu(Y)$ stands for the average value of Y. For odd λ this is equivalent to saying that

$$\mu\Big(\Big|1 + \sum_{j=1}^{2g} e^{i(\lambda+1)\varphi_j}\Big|\Big) \approx 1 + \frac{1}{2g}\ ,$$

while for even λ this reads as

$$\mu\Big(\Big|\sum_{j=1}^{2g} e^{i(\lambda+1)\varphi_j}\Big|\Big) \approx 1 \ .$$

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]).

Notice that, clearly, the φ_j cannot be viewed as random numbers in the interval $[0, 2\pi[$: First, we have that the ω_j occur as pairs (ω_j, ω_{j+g}) $(j = 1, \dots, g)$, where $\omega_{j+g} = \overline{\omega_j}$, i.e., $\varphi_{j+g} = -\varphi_j$. But, even stronger, there exist relations among the ω_j, since (1.1) implies that

$$\sum_{j=1}^{2g} \omega_j^n \in \mathbb{Z} \ , \qquad n \in \mathbb{N} \ .$$

Indeed, if we let the $\varphi_1, \dots, \varphi_j$ to be randomly chosen from $[0, 2\pi[$ and we put $\varphi_{j+g} = -\varphi_j$ for $j = 1, \dots, g$, we find that, numerically, the expected value of the term in (6.1) grows with $\sqrt{g}$ rather than staying close to one, just as we expect from results on random walks.

For odd λ the expected value of $|S_{\lambda+1}(1)|$ does not only depend on the zeroes of $Z(u, K)$. Thus, the observation that the bound on L_2^2 is, on average, by a factor of $2g$ too large appears to be a property of the absolute value of the character sum $S_{\lambda+1}(1) = \sum_{\deg(P)=\lambda+1} \chi(P)$.

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 (3.4) and Corollary 3.1 that

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

and

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

q	g	$\frac{\mu(\lvert\sum\omega_j\rvert)}{\sqrt{q}}$	$\frac{\mu(\lvert S_1(1)\rvert)}{\sqrt{q}}$	$\frac{\mu(\lvert\sum\omega_j^2\rvert)}{q}$	$\frac{\mu(\lvert S_2(1)\rvert)}{q}$	$\frac{\mu(S_1(1))}{\sqrt{q}}$	$\frac{\mu(S_2(1))}{q}$
97	3	0.773	0.770	0.138e1	0.572	0.305e-3	-0.110e-1
97	4	0.795	0.792	0.142e1	0.575	-0.166e-1	0.137e-2
97	5	0.790	0.784	0.138e1	0.559	0.260e-1	-0.539e-2
97	6	0.824	0.821	0.139e1	0.586	-0.124e-1	-0.449e-1
97	7	0.779	0.776	0.138e1	0.547	-0.457e-2	0.235e-1
97	8	0.806	0.802	0.145e1	0.566	-0.873e-2	0.190e-1
97	9	0.789	0.787	0.137e1	0.572	-0.196e-1	-0.328e-1
199	3	0.801	0.806			-0.902e-1	
199	4	0.792	0.793			-0.335e-1	
199	7	0.797	0.794			0.194e-1	
991	3	0.802	0.801			0.560e-1	
991	4	0.790	0.791			-0.424e-1	
991	7	0.800	0.801			-0.154e-1	
10009	3	0.853	0.853	0.148e1	0.549	-0.406e-1	0.916e-1
10009	4	0.778	0.778			-0.163e-1	
10009	7	0.806	0.806			-0.246e-1	
100003	3	0.773	0.773			-0.527e-1	
100003	4	0.759	0.759			-0.223e-1	
100003	7	0.810	0.810			0.566e-1	

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

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 computations, with the exception of $g = 3$ and $q = 10009$, where only 100 distinct monic, squarefree polynomials D have been considered. That all average values seem to be essentially independent of g fully matches our observation from Table 1 that $\mu \approx 1/(2g)$. 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 $\lambda \geq 1$; thus, we consider $S_n(1)$ for $n \geq 2$.

To conclude, note that our heuristics have another very practical application: we can exploit them to optimize the choice of parameters in algorithms to compute the regulator and the class number. See [ST].

7 Discussion, Outlook, Conclusion

7.1 Optimized baby step-giant step methods

The improved bounds and the heuristics can be used to optimize baby step-giant step algorithms (see [ST]). In particular, we can use the expected value of $|h - E|/L^2$ which we conjecture to be $1/2g$.

7.2 The factor $1/2g$

The results in Table 1 seem to imply that the average value of $|h - E_2|/L_2^2$ is $1/2g$ or a value close to $1/2g$. We discussed this phenomenon in Section 6. It is unclear whether it is a property of the roots of the zeta-function $Z(u, K)$ in $u = q^{-s}$, more precisely of $|\sum_{i=1}^{2g} \omega_i^\nu|$, or a property of the character sums $|\sum_{\deg(P)=\nu} \chi(P)|$ for $\nu \in \mathbb{N}$.

7.3 Minimally better bounds

We remark here that some of the bounds in Section 4 can be minimally sharpened as mentioned at the corresponding places. 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 $|\sum_{i=1}^{2g} \omega_i^\nu| \leq g\mathrm{Ne}(2q^{\nu/2})$, which gives a negligible improvement in our context. The Drinfeld-Vladut bound is only effective for very large genus and we can not 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 comparable 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 [ST].

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 sharper 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 the $E_2(\lambda, D)$ 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 average 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 Prof. 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 also indebted to the Centre for Applied Cryptographic Research at the University of Waterloo. We especially wish to thank Prof. Alfred Menezes for his continuous support.

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.

[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.

[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.

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

[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.

[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.

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

[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.

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

[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.

[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.

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

[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*, 297:397–401, 1983.

[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.

[ST] A. Stein and E. Teske. Optimized baby step-giant step methods. Unpublished manuscript.

[ST99] A. Stein and E. Teske. Catching kangaroos in function fields. In *Proc. of The Mathematics of Public Key Cryptography*, Toronto, June 1999.

[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.

[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.

[Sti93] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer, Berlin, 1993.

[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.

[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.