ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 40, Number 5, 2010

# APPROXIMATING EULER PRODUCTS AND CLASS NUMBER COMPUTATION IN ALGEBRAIC FUNCTION FIELDS

RENATE SCHEIDLER AND ANDREAS STEIN

ABSTRACT. We provide a number of results that can be used to derive approximations for the Euler product representation of the zeta function of an arbitrary algebraic function field. Three such approximations are given here. Our results have two main applications. They lead to a computationally suitable algorithm for computing the class number of an arbitrary function field. The ideas underlying the class number algorithms in turn can be used to analyze the distribution of the zeros of its zeta function.

**1. Background and motivation.** The zeta function of an algebraic object incorporates a large amount of information about its associated object. For computational purposes, it is often necessary to compute a large but finite number of terms in the Euler product representation of the zeta function. Primarily, this idea has been used for regulator and class number computation of global fields, as well as in other applications.

Analytic class number formulas are a powerful number theoretic tool, since they relate the class number of a global field to its zeta function. In the 1970s and 80s, a number of algorithms for computing the class number and, where applicable, the regulator, of an algebraic number field by way of truncated Euler products were proposed. Quadratic number fields were investigated by Shanks [**47**] and Lenstra [**38**], and cubic extensions by Williams et al. [**4, 17, 57**]. Hafner and McCurley's seminal subexponential algorithm for imaginary quadratic fields [**22**] was subsequently generalized to arbitrary number fields by Buchmann et al. [**8, 9**] and has since undergone many improvements, especially for

2010 AMS *Mathematics subject classification.* Primary 11R58, 11Y16, Secondary 11M38, 11R65.
*Keywords and phrases.* Algebraic function field, zeta function, Euler product, class number, distribution.
Research supported by NSERC of Canada.
Received by the editors on September 24, 2007, and in revised form on April 16, 2008.

DOI:10.1216/RMJ-2010-40-5-1689 

quadratic number fields. Newer methods use Bach's improved method for approximating Euler products [**3**]. In addition, the analytic class number formula and truncated Euler products have been employed in numerous other applications by Buchmann, Williams, and others; these applications include proving regulator and class number computation NP-complete [**10**], testing whether a real quadratic field has class number one [**51**], investigating bounds on the regulator of a real quadratic field [**25**], finding polynomials with high prime value density and testing the Hardy-Littlewood Conjecture F [**28, 39**], as well as numerically verifying the Cohen-Lenstra heuristics [**53**] and the Ankeny-Artin-Chowla conjecture [**54, 55**].

The function field analog of the class number question is the problem of finding the divisor class number of an algebraic function field over a finite field, or equivalently, the number of rational points on the Jacobian of the absolutely irreducible nonsingular curve associated with this field. This is an interesting and in general computationally challenging problem in number theory and arithmetic geometry, especially if the underlying finite field has large characteristic. It also has applications to cryptography, since cryptographic systems based on elliptic and hyperelliptic curves of small genus have had considerable success due to their good security and efficiency properties. For these schemes, the class number must be known, and should be a prime or a small multiple of a prime of a size at least 160 bits.

There are two general approaches to solving the class number problem for function fields: general methods that place no restriction on the base field or the curve, and specific techniques that apply only to certain types of curves but tend to be much more efficient. For elliptic curves, the task amounts to counting points on the curve, and the two major algorithms, due to Schoof-Atkin-Elkies [**46**] and Satoh [**43**], respectively, have been extensively researched, improved, and implemented. Both approaches were generalized to other types of curves and Abelian varieties. Kedlaya's $p$-adic algorithm for hyperelliptic curves [**31, 32**] is particularly well-suited to fields of small characteristic and has since been extended to hyperelliptic curves of characteristic two [**15**], Artin-Schreier extensions [**13, 36, 37**], superelliptic curves [**18, 35**], $C_{ab}$ curves [**14**], and more general curves [**12, 19**]; see also the survey by Kedlaya [**33**]. Schoof's elliptic curve method was generalized to Abelian varieties by Pila [**40, 41**] and improved by Adleman and Huang [**1, 2**].

The Adleman-Huang algorithm computes the characteristic polynomial of the Frobenius endomorphism of an Abelian variety of dimension $d$ in projective $N$-space over a finite field $\mathbf{F}_q$ in time $O(\log(q)^{\delta})$, where $\delta$ depends polynomially on $d$ and $N$. For plane curves of degree $n$, a randomized algorithm with running time $O(\log(q)^{n^{O(1)}})$ was given by Huang and Ierardi [**24**].

None of the last five citations above provides an implementation or numerical data, so their practical effectiveness remains to be established. In fact, the method of [**2**] requires a semi-algebraic description of the Jacobian as an algebraic variety, and while the authors illustrate how to obtain such a description for hyperelliptic curves from the Mumford representations of reduced divisors, this task can be complicated for more general curves. Methods for special types of curves on the other hand have yielded impressive numerical results. The algorithm of [**20**] for genus 2 hyperelliptic curves for example produced class numbers of 39 decimal digits, and the improvements of [**21**] pushed this up to the cryptographically secure range of 50 decimal digits (164 bits). In 2002, a class number of 29 digits of a genus 3 hyperelliptic curve was computed in [**49**]. A method for Picard curves given in [**6**] generated prime class numbers of up to 39 decimal digits as well as a 55-digit class number with a 52-digit (173 bit) prime factor.

The idea of truncated Euler products was first employed in [**50**] to compute the regulator of a real quadratic function field. The algorithm subsequently produced class numbers in excess of $10^{28}$ (with computer technology dating from before 2002 [**49**]) and was extended to purely cubic function fields in [**45**]. Inspired by the number field methods discussed earlier as well as the success of these ideas when applied to quadratic and cubic function fields, we generalize the techniques of [**45**] to arbitrary function field extensions in this paper. We provide a number of bounds and identities relating to the Euler product representation of the zeta function of an arbitrary function field. The usefulness of our ideas is by no means limited to class number computation, although this topic is undoubtedly their foremost application. We describe how our results can be employed as the basis of a computationally suitable algorithm for finding the class number of an arbitrary algebraic function field via truncated Euler products and the analytic class number formula. We also explain how the ideas underlying our

class number algorithm are related to the distribution of class numbers and of zeros of the zeta function.

Our discussion begins with an overview of function fields and their zeta functions as well as a brief outline of our method for approximating the class number in Section 2. In Section 3, we derive bounds that dictate the quality of our class number approximations. Here, we also provide a geometric interpretation of our arithmetic results. Sections 4 and 5 discuss two major applications, namely, the actual computation of the class number and an approach for analyzing the distribution of the zeros of the zeta function. We conclude with some open problems in Section 6.

**2. The zeta function of an algebraic function field.** For an introduction to function fields and their zeta functions, we refer the reader to [**16, 42, 52**]. Let $K$ be an algebraic function field of genus $g$ over a finite field $\mathbf{F}_q$. Denote by $\mathcal{D}_K$ the group of divisors defined over $\mathbf{F}_q$, by $\mathcal{D}_K^0$ the subgroup of $\mathcal{D}_K$ of degree zero divisors of $K$ defined over $\mathbf{F}_q$, and by $\mathcal{P}_K$ the subgroup of principal divisors of $K$ defined over $\mathbf{F}_q$. Then the factor group $\mathrm{Pic}_K^0 = \mathcal{D}_K^0/\mathcal{P}_K$ is the (*degree zero*) *divisor class group* of $K/\mathbf{F}_q$. It is a finite Abelian group whose cardinality $h_K = |\mathrm{Pic}_K^0|$ is called the (*divisor*) *class number of* $K/\mathbf{F}_q$.

**2.1. Outline of the method.** Our ultimate goal is to find a good approximation $E$ of $h_K$ as well as an upper bound $U$ on the error $|h_K - E|$. This approximation is computed with two applications in mind. The first application is the actual computation of $h_K$, which can be achieved by searching the interval $[E-U, E+U]$, using standard techniques such as Shanks' baby step giant step or Pollard's kangaroo method, see Section 4 for details. The second application is an analysis of the mean values of $|h_K - E|/U$ when averaged over all function fields $K/\mathbf{F}_q$ for fixed $g$ and $q$. The limit of this mean value as $q$ tends to infinity relates to the distribution of zeros of the zeta functions of function fields of genus $g$, see Section 5.

Let $L_K(u) \in \mathbf{Z}[u]$ denote the *L-polynomial* of $K$. Then

$$L_K(u) = \prod_{j=1}^{2g} (1 - \omega_j u), \tag{2.1}$$

where the $\omega_j$ are algebraic integers with

$$|\omega_j| = \sqrt{q} \text{ for } j = 1, 2, \dots, 2g \tag{2.2}$$

by the Hasse-Weil theorem (see for example [**52**, Theorem V.2.1, page 169]). Furthermore, the $L$-polynomial satisfies the functional equation $L_K(u) = q^g u^{2g} L(1/qu)$. The analytic class number formula states that

$$h_K = L_K(1) = q^g L_K(1/q). \tag{2.3}$$

The first equality of (2.3) in conjunction with (2.1) and (2.2) yields the well-known Hasse-Weil interval for $h_K$:

$$(\sqrt{q} - 1)^{2g} \leq h_K \leq (\sqrt{q} + 1)^{2g}, \tag{2.4}$$

which implies that $h_K \approx q^g$. Thus, $h_K$ is very large even for function fields $K/\mathbf{F}_q$ of modest size.

The $L$-polynomial is closely related to the zeta function of $K$. More exactly, we have

$$L_K(u) = (1 - u)(1 - qu) Z_K(u), \tag{2.5}$$

where $Z_K(u) = \zeta_K(s)$ with $q^{-s} = u$, and $\zeta_K(s)$ is the *zeta function* of $K/\mathbf{F}_q$, i.e., the power series

$$\zeta_K(s) = \sum_{\mathfrak{A} \geq 0} \frac{1}{N(\mathfrak{A})^s} \quad (\Re(s) > 1).$$

Here, $N(\mathfrak{A}) = q^{\deg(\mathfrak{A})}$ is the *absolute norm* of a divisor $\mathfrak{A} \in \mathcal{D}_K$ of *degree* $\deg(\mathfrak{A})$, the summation is over all integral (i.e., effective) divisors $\mathfrak{A}$ of $K$, and $\Re(s)$ denotes the real part of the complex variable $s$. It is known that $\zeta_K(s)$ is periodic with period $2\pi i/\log q$ and analytic on the entire complex plane with the exception of simple poles at $s \equiv 0,\ 1 \pmod{2\pi i/\log q}$, corresponding to simple poles at $u = 1$ and $u = 1/q$ of $Z_K(u)$.

$Z_K(u)$ has an Euler product expansion that reads

$$Z_K(u) = \prod_{\mathfrak{P}} \frac{1}{1 - u^{\deg(\mathfrak{P})}} = \prod_{\nu=1}^{\infty} \prod_{\deg(\mathfrak{P})=\nu} \frac{1}{1 - u^{\nu}}, \tag{2.6}$$

where $\mathfrak{P}$ ranges over all prime divisors of $K$. One can use a truncated version of this Euler product representation of $Z_K(u)$, together with (2.3), to approximate $h_K$. Since $Z_K(u)$ has poles at $u = 1$ and $u = 1/q$, these poles need to be extracted from expansion (2.6) in order to make use of (2.3). This is accomplished in Theorems 2.1, 2.3 and 2.4 below. Results derived from Theorem 3.1 below then provide bounds that determine how closely $h_K$ can be approximated.

Let $x \in K$ be a transcendental element such that $K/\mathbf{F}_q(x)$ is a finite separable extension of degree $[K : \mathbf{F}_q(x)] = m$. If $\mathfrak{P}_\infty$ is the infinite place of $\mathbf{F}_q(x)$, then its co-norm with respect to $K/\mathbf{F}_q(x)$ is

$$\mathrm{Con}_{K/\mathbf{F}_q(x)}(\mathfrak{P}_\infty) = e_1\mathfrak{P}_{\infty_1} + e_2\mathfrak{P}_{\infty_2} + \cdots + e_r\mathfrak{P}_{\infty_r},$$

where the set $S = \{\mathfrak{P}_{\infty_1}, \ldots, \mathfrak{P}_{\infty_r}\}$ consists of all the infinite places of $K$ with respect to $x$, and $e_j$ is the ramification index of $\mathfrak{P}_{\infty_j}$ in $K$. Setting $f_j = \deg(\mathfrak{P}_{\infty_j})$, we have $\sum_{j=1}^{r} e_j f_j = m$.

If $\mathcal{O}_x$ denotes the integral closure of $\mathbf{F}_q[x]$ in $K$, then the finite prime divisors of $K/\mathbf{F}_q(x)$ are in one-to-one correspondence with the prime ideals in $\mathcal{O}_x$. By (2.6), $Z_K(u)$ can thus be split up as

$$Z_K(u) = Z_K^{\infty}(u) \cdot Z_K^{x}(u), \tag{2.7}$$

where

$$Z_K^{\infty}(u) = \prod_{j=1}^{r} \frac{1}{1 - u^{f_j}} \tag{2.8}$$

represents the contribution of the infinite places to $Z_K(u)$ and

$$Z_K^{x}(u) = \prod_{\mathfrak{p}} \frac{1}{1 - u^{\deg(\mathfrak{p})}} = \prod_{P} \prod_{\mathfrak{p}|P} \frac{1}{1 - u^{\deg(\mathfrak{p})}} \tag{2.9}$$

represents the contribution of the $\mathcal{O}_x$-prime ideals. In the first product in (2.9), $\mathfrak{p}$ runs through all $\mathcal{O}_x$-prime ideals of $K$, and in the second double product, $P$ runs through all the monic prime polynomials in $\mathbf{F}_q(x)$ and $\mathfrak{p}$ through the $\mathcal{O}_x$-prime ideals lying over $P$. Note that the factorization of $Z_K(u)$ given in (2.7) is dependent on the defining equation, i.e., the minimal polynomial of the extension $K/\mathbf{F}_q(x)$.

We now develop explicit formulas for $Z_K^\infty(u)$ and for $Z_K^x(u)$. In particular, we prove in Theorems 2.1 and 2.4 that the poles of $Z_K(u)$ at $u = 1$ and $u = 1/q$ occur in (2.8) and (2.9), respectively. Then we combine these identities with (2.5) and (2.3) to derive bounds that can be used to approximate $h_K$.

**2.2. Results on $Z_K^\infty(u)$.** The product representation of $Z_K^\infty(u)$ contains only finitely many terms and is thus potentially explicitly computable. We begin by recalling some useful results on roots of unity. Let $f \in \mathbf{N}$, and let $\zeta_f \in \mathbf{C}$ denote a primitive $f$th root of unity, i.e., $\zeta_f \neq 1$ and $\zeta_f^f = 1$. Consider the polynomial

$$C_f(u) = \frac{u^f - 1}{u - 1} = \sum_{j=0}^{f-1} u^j = \prod_{j=1}^{f-1} (u - \zeta_f^j) \in \mathbf{Z}[u] \tag{2.10}$$

of degree $f - 1$, and let $n \in \mathbf{N}$. If $f \mid n$, then $\zeta_f^n = 1$, so the second expression for $C_f(u)$ in (2.10) yields $C_f(\zeta_f^n) = f$, whereas if $f \nmid n$, then $\zeta_f^n \neq 1$ and $\zeta_f^{fn} = 1$, so $C_f(\zeta_f^n) = 0$ from the first expression for $C_f(u)$ in (2.10). We thus obtain

$$\sum_{j=1}^{f-1} \zeta_f^{jn} = C_f(\zeta_f^n) - 1 = \begin{cases} -1 & \text{if } f \nmid n, \\ f - 1 & \text{if } f \mid n. \end{cases} \tag{2.11}$$

We use (2.10) to obtain the following representation of $Z_K^\infty(u)$.

**Theorem 2.1.** *Let $K/\mathbf{F}_q$ be an algebraic function field of genus $g$, $x \in K$ transcendental over $\mathbf{F}_q$, and $[K : \mathbf{F}_q(x)] = m$. Then*

$$Z_K^\infty(u) = \frac{1}{1-u} \cdot \frac{1}{1 + \sum_{j=1}^{m-1} s_j u^j} = \frac{1}{1-u} \prod_{j=1}^{m-1} \frac{1}{1 - x_j u},$$

*where for $m \geq 2$ $s_j \in \mathbf{Z}$ and $x_j = 0$ or $x_j^d = 1$ for some $d \leq m$.*

*Proof.* The proof simply applies our above observations on roots of unity to $Z_K^\infty(u)$. By (2.8) and (2.10), we have

$$Z_K^\infty(u) = \frac{1}{(1-u)^r} \cdot \prod_{j=1}^{r} \frac{1-u}{1-u^{f_j}} = \frac{1}{1-u} \cdot \frac{1}{P(u)},$$

where

$$P(u) = (1-u)^{r-1} \prod_{j=1}^{r} \frac{1-u^{f_j}}{1-u} = (1-u)^{r-1} \prod_{j=1}^{r} C_{f_j}(u), \tag{2.12}$$

and $C_{f_j}(u)$ is given as in (2.10) with $f = f_j$. It follows that $P(u) \in \mathbf{Z}[u]$, $P(0) = 1$ and

$$\deg P(u) = r - 1 + \sum_{j=1}^{r} (f_j - 1) = \sum_{j=1}^{r} f_j - 1 \le \sum_{j=1}^{r} e_j f_j - 1 = m - 1.$$

Thus, $P(u) = 1 + \sum_{j=1}^{m-1} s_j u^j$ with $s_j \in \mathbf{Z}$ for $j = 1, \dots, m-1$. Furthermore, (2.12) and (2.10) imply that the roots of $P(u)$ are 1 and the $f_j$th primitive roots of unity for $1 \le j \le r$. Since the nonzero $x_j$ are the reciprocals of these roots, the result follows. □

By (2.12), $r-1$ of the $x_i$ are equal to 1, and the remaining $x_i$ are of the form $\zeta_{f_j}^{-k}$ with $1 \le k \le f_j - 1$ and $1 \le j \le r$. For any $n \in \mathbf{N}$, we now set $d_{jn} = 1$ if $f_j \mid n$ and $d_{jn} = 0$ otherwise. Since $C_f(\zeta_f^{-n}) = C_f(\zeta_f^n)$ for all $f, n \in \mathbf{N}$ by (2.11), we obtain

$$\sum_{k=1}^{f_j - 1} \zeta_{f_j}^{-kn} = \sum_{k=1}^{f_j - 1} \zeta_{f_j}^{kn} = d_{jn} f_j - 1.$$

It follows that

$$\begin{aligned} \sum_{j=1}^{m-1} x_j^n &= \sum_{j=1}^{r-1} 1^{-n} + \sum_{j=1}^{r} \sum_{k=1}^{f_j - 1} \zeta_{f_j}^{-kn} \\ &= r - 1 + \sum_{j=1}^{r} (d_{jn} f_j - 1) \\ &= \sum_{j=1}^{r} d_{jn} f_j - 1, \end{aligned}$$

for all $n \in \mathbf{N}$. In particular, the expression $\sum_{j=1}^{m-1} x_j^n$ is always an integer. Since we have $|x_j^n| \le 1$ for all $n \in \mathbf{N}$ and $j \in \{1, \dots, m-1\}$, we obtain the general bound

$$\left| \sum_{j=1}^{m-1} x_j^n \right| \le m - 1, \quad n \in \mathbf{N}. \tag{2.13}$$

Since $d_{jn} \leq 1 \leq e_j$, this bound is attained if and only if $e_j = 1$ and $d_{jn} = 1$, i.e., $f_j \mid n$ for all $j \in \{1, \dots, r\}$ as only in this case,

$$\sum_{j=1}^{m-1} x_j^n = \sum_{j=1}^{r} f_j - 1 = \sum_{j=1}^{r} e_j f_j - 1 = m - 1.$$

For our purposes, the bound in (2.13) will be sufficiently tight. However, it can potentially be sharpened in specific situations. For example for $n = 1$ we have $d_{jn} = 1$ if $f_j = 1$ and $d_{jn} = 0$ otherwise, so

$$\sum_{j=1}^{m-1} x_j = \sum_{j=1}^{m-1} d_{j1} f_j - 1 = \#\{\mathfrak{P}_{\infty_j} \mid f_j = 1\} - 1 \begin{cases} \geq -1, \\ \leq r - 1. \end{cases}$$

We investigate a few specific splitting situations below to show that, while the bound in (2.13) is met in some instances, there are other cases where the bound is far from being achieved and the sum in (2.13) can in fact vanish. The examples below also illustrate that our results represent a generalization of the situations of [**45, 48, 49, 50**].

**Example 2.2.** Let $K/\mathbf{F}_q(x)$ be an extension of degree $m > 1$.

(1) Totally ramified case: if $\mathrm{Con}_{K/\mathbf{F}_q(x)}(\mathfrak{P}_\infty) = m\mathfrak{P}_{\infty_1}$, then $r = 1$, $f_1 = 1$, $e_1 = m$, and thus

$$Z_K^\infty(u) = \prod_{j=1}^{r} \frac{1}{1 - u^{f_j}} = \frac{1}{1 - u}.$$

It follows that $x_j = 0$ for $j = 1, \dots, m-1$, and thus $\sum_{j=1}^{m-1} x_j^n = 0$ for any $n \in \mathbf{N}$.

(2) Totally inert case: if $\mathrm{Con}_{K/\mathbf{F}_q(x)}(\mathfrak{P}_\infty) = \mathfrak{P}_{\infty_1}$, then $r = 1$, $f_1 = m$, $e_1 = 1$, and thus

$$Z_K^\infty(u) = \prod_{j=1}^{r} \frac{1}{1 - u^m} = \frac{1}{1 - u} \cdot \frac{1}{C_m(u)}.$$

It follows that $x_j = \zeta_m^j$ for $j = 1, \dots, m-1$, and thus by (2.11) for any $n \in \mathbf{N}$:

$$\sum_{j=1}^{m-1} x_j^n = \begin{cases} -1 & \text{if } m \nmid n, \\ m - 1 & \text{if } m \mid n. \end{cases}$$

(3) Totally split case: if $\mathrm{Con}_{K/\mathbf{F}_q(x)}(\mathfrak{P}_\infty) = \mathfrak{P}_{\infty_1} + \mathfrak{P}_{\infty_2} + \cdots + \mathfrak{P}_{\infty_m}$, then $r = m$, $f_j = e_j = 1$ for $j = 1, \ldots, m$. Thus

$$Z_K^\infty(u) = \prod_{j=1}^{m} \frac{1}{1-u} = \frac{1}{1-u} \cdot \frac{1}{(1-u)^{m-1}}.$$

It follows that $x_j = 1$ for $j = 1, \ldots, m-1$, and thus $\sum_{j=1}^{m-1} x_j^n = m-1$ for any $n \in \mathbf{N}$.

(4) Two-fold split with one degree one place: if $\mathrm{Con}_{K/\mathbf{F}_q(x)}(\mathfrak{P}_\infty) = e_1\mathfrak{P}_{\infty_1} + e_2\mathfrak{P}_{\infty_2}$, where $r = 2$ and $f_1 = 1$, then

$$Z_K^\infty(u) = \frac{1}{1-u} \cdot \frac{1}{1-u^{f_2}} = \frac{1}{1-u}\left(\frac{1}{C_{f_2}(u)} \cdot \frac{1}{1-u}\right).$$

It follows that $x_j = \zeta_{f_2}^j$ for $j = 1, \ldots, f_2 - 1$, $x_{f_2} = 1$, and $x_j = 0$ for $f_2 + 1 \le j \le m-1$. Thus, by (2.10) for any $n \in \mathbf{N}$:

$$\sum_{j=1}^{m-1} x_j^n = \sum_{j=1}^{f_2-1} \zeta_{f_2}^{jn} + 1 = \sum_{j=0}^{f_2-1} \zeta_{f_2}^{jn} = C_{f_2}(\zeta_{f_2}^n) = \begin{cases} 0 & \text{if } f_2 \nmid n, \\ f_2 & \text{if } f_2 \mid n. \end{cases}$$

**2.3. Results on $Z_K^x(u)$.** We now derive similar results for $Z_K^x(u)$ as we did for $Z_K^\infty(u)$ based on (2.10). We simply state these results; the proofs are completely analogous to those given in subsection 2.2. Recall from (2.9) that we can write $Z_K^x(u)$ as

$$Z_K^x(u) = \prod_{\mathfrak{p}} \frac{1}{1-u^{\deg(\mathfrak{p})}} = \prod_{P} \prod_{\mathfrak{p}|P} \frac{1}{1-u^{\deg(\mathfrak{p})}},$$

where $P$ runs through all monic prime polynomials $P \in \mathbf{F}_q[x]$. Therefore, it is useful to investigate $\prod_{\mathfrak{p}|P}(1-u^{\deg(\mathfrak{p})})^{-1}$ for an arbitrary but fixed prime polynomial $P \in \mathbf{F}_q[x]$. Note that, in this context, we are interested in the splitting behavior of the principal ideal $(P)$ generated by $P$ in $\mathcal{O}_x$.

**Theorem 2.3.** *Let $K/\mathbf{F}_q$ be an algebraic function field of genus $g$, $x \in K$ transcendental over $\mathbf{F}_q$, $[K : \mathbf{F}_q(x)] = m$, and $P \in \mathbf{F}_q[x]$ a monic prime polynomial of degree $\nu = \deg(P)$. Then*

$$\prod_{\mathfrak{p}|P} \frac{1}{1-u^{\deg(\mathfrak{p})}} = \frac{1}{1-u^{\nu}} \cdot \frac{1}{1+\sum_{j=1}^{m-1} a_j(P)u^{\nu}}$$
$$= \frac{1}{1-u^{\nu}} \prod_{j=1}^{m-1} \frac{1}{1-z_j(P)u^{\nu}},$$

*where for* $m \geq 2$, $a_j(P) \in \mathbf{Z}$ *and* $z_j(P) = 0$ *or* $z_j(P)^d = 1$ *for some* $d \leq m$.

Thus, we can easily determine $z_1(P), z_2(P), \ldots, z_{m-1}(P)$ and $a_1(P)$, $a_2(P), \ldots, a_{m-1}(P)$, once we know how the principal ideal $(P)$ splits in $\mathcal{O}_x$. As before, we have

$$\left| \sum_{j=1}^{m-1} z_j(P)^n \right| \leq m-1, n \in \mathbf{N}, \tag{2.14}$$

and the sum above is always an integer. By using the well-known identity

$$\prod_{P} \frac{1}{1-u^{\deg(P)}} = \prod_{\nu=1}^{\infty} \prod_{\deg(P)=\nu} \frac{1}{1-u^{\nu}} = \frac{1}{1-qu},$$

we obtain the following theorem.

**Theorem 2.4.** *Let* $K/\mathbf{F}_q$ *be an algebraic function field of genus* $g$, $x \in K$ *transcendental over* $\mathbf{F}_q$, *and* $[K : \mathbf{F}_q(x)] = m$. *Then*

$$Z_K^x(u) = \frac{1}{1-qu} \prod_{\nu=1}^{\infty} \prod_{\deg(P)=\nu} \prod_{j=1}^{m-1} \frac{1}{1-z_j(P)u^{\nu}},$$

*where the second product ranges over all monic prime polynomials* $P \in \mathbf{F}_q[x]$ *of degree* $\nu$.

*Proof.* By (2.9) and Theorem 2.3, we then have

$$\begin{aligned} Z_K^x(u) &= \prod_{\nu=1}^{\infty} \prod_{\deg(P)=\nu} \prod_{\mathfrak{p}|P} \frac{1}{1-u^{\deg(\mathfrak{p})}} \\ &= \prod_{\nu=1}^{\infty} \prod_{\deg(P)=\nu} \frac{1}{1-u^{\nu}} \prod_{j=1}^{m-1} \frac{1}{1-z_j(P)u^{\nu}} \\ &= \frac{1}{1-qu} \prod_{\nu=1}^{\infty} \prod_{\deg(P)=\nu} \prod_{j=1}^{m-1} \frac{1}{1-z_j(P)u^{\nu}}. \end{aligned}$$

□

**3. Bounds on the logarithm of the Euler product.** As before, let $K/\mathbf{F}_q$ be an algebraic function field of genus $g$ over a finite field $\mathbf{F}_q$, $x \in K$ a transcendental element over $\mathbf{F}_q$, and $[K : \mathbf{F}_q(x)] = m$. From the second equality of (2.3), (2.5), (2.7), as well as Theorems 2.1 and 2.4, we obtain

$$\begin{aligned} h_K &= q^g L_K(1/q) \\ &= q^g \prod_{j=1}^{m-1} \frac{1}{1-(x_j/q)} \prod_{\nu=1}^{\infty} \prod_{\deg(P)=\nu} \prod_{j=1}^{m-1} \frac{1}{1-(z_j(P)/q^{\nu})}. \end{aligned} \tag{3.1}$$

We can take the logarithm of (3.1), using the identity

$$-\log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n} \text{ for } |z| < 1. \tag{3.2}$$

Note that by Theorem 2.3, $|z_j(P)| \le 1 < q^{\nu}$ for $\nu \in \mathbf{N}$, so the corresponding power series converges. We obtain

$$\log(h_K) = A(K) + \sum_{n=1}^{\infty} \frac{1}{nq^n} \sum_{\nu|n} \nu \sum_{\deg(P)=\nu} \sum_{j=1}^{m-1} z_j(P)^{n/\nu}, \tag{3.3}$$

where $\nu$ runs through all positive divisors of $n$ and

$$A(K) = g\log q - \sum_{j=1}^{m-1} \log\left(1-\frac{x_j}{q}\right) = g\log q - \log\left(1+\sum_{j=1}^{m-1}\frac{s_j}{q}\right), \tag{3.4}$$

with $s_1, \dots, s_{m-1} \in \mathbf{Z}$ as in Theorem 2.1. Note that $A(K)$ can be computed from the splitting behavior of the place at infinity $\mathfrak{P}_\infty$ of $\mathbf{F}_q(x)$ in $K$. We now derive bounds relating to the infinite nested sum in (3.3) which will eventually lead to close approximations of $h_K$.

We proceed similarly to our derivation of (3.3). Identities (2.1), (2.5) and (2.7), together with Theorems 2.1 and 2.4 yield

$$\prod_{\nu=1}^{\infty} \prod_{\deg(P)=\nu} \prod_{j=1}^{m-1} \frac{1}{1 - z_j(P)u^\nu} = \prod_{j=1}^{m-1} (1 - x_j u) \prod_{j=1}^{2g} (1 - \omega_j u). \tag{3.5}$$

This time, we take formal logarithms, using (3.2) as a formal identity, to obtain

$$\sum_{n=1}^{\infty} \frac{u^n}{n} \sum_{\nu|n} \nu \sum_{\deg(P)=\nu} \sum_{j=1}^{m-1} z_j(P)^{n/\nu} = \sum_{n=1}^{\infty} \frac{u^n}{n} \Bigg( - \sum_{j=1}^{m-1} x_j^n - \sum_{j=1}^{2g} \omega_j^n \Bigg),$$

where $\nu$ again runs through all positive divisors of $n$. Comparing coefficients at $u^n$ for any $n \in \mathbf{N}$ implies the following theorem.

**Theorem 3.1.** *Let $K/\mathbf{F}_q$ be an algebraic function field of genus $g$, $x \in K$ transcendental over $\mathbf{F}_q$, and $[K : \mathbf{F}_q(x)] = m$. Let $x_1, \dots, x_{m-1}$ be as described in Theorem 2.3 and for any monic prime polynomial $P \in \mathbf{F}_q[x]$ let $z_1(P), \dots, z_{m-1}(P)$ be the quantities as described in Theorem 2.3. Then we have for all $n \in \mathbf{N}$:*

$$\sum_{\nu|n} \nu \sum_{\deg(P)=\nu} \sum_{j=1}^{m-1} z_j(P)^{n/\nu} = - \sum_{j=1}^{m-1} x_j^n - \sum_{j=1}^{2g} \omega_j^n,$$

*where $\nu$ runs through all positive divisors of $n$.*

For convenience, we put

$$S_\nu(i) = \sum_{\deg(P)=\nu} \sum_{j=1}^{m-1} z_j(P)^i, \quad \nu, i \in \mathbf{N}, \tag{3.6}$$

so Theorem 3.1 can be rewritten as

$$\sum_{\nu|n} \nu \, S_\nu\left(\frac{n}{\nu}\right) = - \sum_{j=1}^{m-1} x_j^n - \sum_{j=1}^{2g} \omega_j^n, \quad n \in \mathbf{N}, \tag{3.7}$$

and (3.3) reads

$$\log(h_K) = A(K) + \sum_{n=1}^{\infty} \frac{1}{nq^n} \sum_{\nu|n} \nu S_\nu\left(\frac{n}{\nu}\right). \tag{3.8}$$

In order to derive approximations for $h_K$, we need to estimate the infinite sum in (3.8). It is thus apparent that the quantities $\nu S_\nu(n/\nu)$ play an important role, especially $nS_n(1)$, i.e., the case $n = \nu$. We immediately obtain the following result from Theorem 3.1, (2.2) and (2.13).

**Corollary 3.2.** *For all* $n \in \mathbf{N}$:

$$\left|\sum_{\nu|n} \nu S_\nu\left(\frac{n}{\nu}\right)\right| \le \left|\sum_{j=1}^{m-1} x_j^n\right| + 2gq^{n/2} \le (m-1) + 2gq^{n/2}.$$

Clearly, the second expression above yields a more accurate bound than the third, but requires that $x_1, \dots, x_{m-1}$ be known. Corollary 3.2 is the basis for the first choice of approximation for $h_K$ as described in subsection 4.2. For the second approximation of subsection 4.3, we need to find a bound on $nS_n(1)$. For $n = 1$, (3.7) yields

$$1 \cdot S_1(1) = \sum_{\deg(P)=1} \sum_{j=1}^{m-1} z_j(P) = -\sum_{j=1}^{m-1} x_j - \sum_{j=1}^{2g} \omega_j,$$

which implies the sharp bound

$$|S_1(1)| \le m - 1 + 2g\sqrt{q}.$$

Therefore, let $n \ge 2$ and $l$ the smallest prime divisor of $n$, i.e., $n/l$ is the largest divisor of $n$ that is not equal to $n$. Note that $l = 2$ for $n$ even and $l \ge 3$ for $n$ odd. By (3.6) and (3.7), we easily see that

$$nS_n(1) = -\sum_{j=1}^{m-1} x_j^n - \sum_{j=1}^{2g} \omega_j^n - \sum_{\substack{\nu|n \\ \nu \ne n}} \nu S_\nu\left(\frac{n}{\nu}\right) \tag{3.9}$$

$$= -\sum_{j=1}^{m-1} x_j^n - \sum_{j=1}^{2g} \omega_j^n - \frac{n}{l} S_{n/l}(l) - \sum_{\substack{\nu|n \\ \nu \le n/l-1}} \nu S_\nu\left(\frac{n}{\nu}\right) \tag{3.10}$$

for $n \geq 2$. In order to bound $n|S_n(1)|$, we let $I_\nu$ denote the number of monic prime polynomials of degree $\nu$ in $\mathbf{F}_q[x]$ and recall that $\sum_{\nu|n} \nu I_\nu = q^n$. Hence, $nI_n \leq q^n$, and thus

$$(3.11)\quad |S_\nu(i)| \leq (m-1) \sum_{\deg(P)=\nu} 1 = (m-1)I_\nu \leq \frac{m-1}{\nu}\, q^\nu, \quad \nu, i \in \mathbf{N}$$

by (2.14). It follows from (2.13) and (3.11) that for large values of $q$ only the third term $(n/l)S_{n/l}(l)$ in (3.10) has a chance of contributing significantly to $nS_n(1)$ besides the second term $\sum_{j=1}^{2g} \omega_j^n$, and this only happens if $n$ is even, i.e., $l = 2$.

The following estimate will prove useful.

**Lemma 3.3.** *For all $n, \beta \in \mathbf{N}$ with $n \geq 2$ and $\beta < n$:*

$$\Big| \sum_{\substack{\nu|n \\ \beta \leq \nu < n}} \nu S_\nu\Big(\frac{n}{\nu}\Big) \Big| \leq (m-1)(q^{n/l} - 1)\frac{q}{q-1},$$

*where $l$ denotes the smallest prime divisor of $n$.*

*Proof.* Note that, if $\beta > n/l$, then

$$\sum_{\substack{\nu|n \\ \beta \leq \nu < n}} \nu S_\nu\Big(\frac{n}{\nu}\Big) = 0.$$

If $\beta \leq n/l$, then we derive from (3.11) that

$$\begin{aligned} \Big| \sum_{\substack{\nu|n \\ \beta \leq \nu < n}} \nu\, S_\nu\Big(\frac{n}{\nu}\Big) \Big| &\leq (m-1) \sum_{\substack{\nu|n \\ \beta \leq \nu < n}} q^\nu \\ &\leq (m-1) \sum_{\nu=1}^{n/l} q^\nu \\ &= (m-1)(q^{n/l} - 1)\frac{q}{q-1}. \end{aligned}$$

□

We are now able to provide a bound on $nS_n(1)$ for $n \geq 2$.

**Theorem 3.4.** *For all $n \in \mathbf{N}$ with $n \geq 2$:*

$$|nS_n(1)| \leq (m-1) + 2gq^{n/2} + (m-1)(q^{n/l} - 1)\frac{q}{q-1},$$

*where $l$ denotes the smallest prime divisor of $n$.*

*Proof.* This follows from (2.2), (2.13), (3.9), and Lemma 3.3 with $\beta = 1$. □

We remark that this bound will be reasonably sharp for larger values of $q$. In specific situations, for example, if $x_1, x_2, \ldots, x_{m-1}$ are known, we can find a better estimate for the sum $\sum_{j=1}^{m-1} x_j^n$ than (2.13) and thus reduce the first term of $m-1$ in Theorem 3.4. However, since the contribution of this term is generally negligible compared to the other terms, the given bound is sufficient. The following less sharp bound is also useful.

**Corollary 3.5.** *For all $n \in \mathbf{N}$ with $n \geq 2$:*

$$n\,|S_n(1)| < 2gq^{n/2} + (m-1)\frac{q}{q-1}q^{n/l} \leq (2g+m-1)\frac{q}{q-1}\,q^{n/2}.$$

*Proof.* This follows from Theorem 3.4 since $1 - q/(q-1) < 0$. For the last inequality, we use in addition that $l \geq 2$. □

**Corollary 3.6.** *For all $n, \lambda \in \mathbf{N}$ with $n \geq 2$ and $\lambda < n$:*

$$\left|\sum_{\substack{\nu \mid n \\ \nu > \lambda}} \nu S_\nu\left(\frac{n}{\nu}\right)\right| < 2gq^{n/2} + 2(m-1)\frac{q}{q-1}q^{n/l} < 2(g+m-1)\frac{q}{(q-1)}\,q^{n/2}.$$

*Proof.* The last inequality is again clear since $q/(q-1) > 1$ and $l \geq 2$. For the first inequality, we use Corollary 3.5 and Lemma 3.3

with $\beta = \lambda + 1$ to estimate

$$\begin{aligned}\left|\sum_{\substack{\nu|n\\ \nu>\lambda}} \nu S_\nu\left(\frac{n}{\nu}\right)\right| &\le n\,|S_n(1)| + \left|\sum_{\substack{\nu|n\\ \lambda<\nu<n}} \nu\, S_\nu\left(\frac{n}{\nu}\right)\right| \\ &< 2gq^{n/2} + 2(m-1)\frac{q}{q-1}q^{n/l},\end{aligned}$$

as claimed. □

The following corollary will be used in the second approximation for $h_K$ described in subsection 4.3. It is essential for accurate bounds.

**Corollary 3.7.** *For $\mu, \lambda \in \mathbf{N}$ with $\mu > \lambda$:*

$$\begin{aligned}\left|\sum_{n=\mu}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n\\ \nu>\lambda}} \nu S_\nu\left(\frac{n}{\nu}\right)\right| &< \frac{2g}{\mu}\,\frac{\sqrt{q}}{\sqrt{q}-1}\,q^{-\mu/2} \\ &\quad + \frac{2(m-1)}{\mu}\,\frac{q}{q-1}\,\frac{q^{1-(1/l)}}{q^{1-(1/l)}-1}\,q^{-(1-(1/l))\mu}.\end{aligned}$$

*Proof.* By Corollary 3.6, we have

$$\begin{aligned}\left|\sum_{n=\mu}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n\\ \nu>\lambda}} \nu S_\nu\left(\frac{n}{\nu}\right)\right| &< \sum_{n=\mu}^{\infty} \frac{1}{nq^n}\left(2gq^{n/2} + 2(m-1)\frac{q}{q-1}q^{n/l}\right) \\ &\le \frac{2g}{\mu}\sum_{n=\mu}^{\infty} q^{-n/2} \\ &\quad + \frac{2(m-1)}{\mu}\frac{q}{q-1}\sum_{n=\mu}^{\infty} q^{-n(1-(1/l))}.\end{aligned}$$

The statement now follows from the formula

$$\sum_{n=\mu}^{\infty} q^{-\alpha n} = \frac{q^\alpha}{q^\alpha - 1}\cdot q^{-\alpha\mu}, \quad \alpha \in \mathbf{R}_{>0}. \qquad \square$$

If $n$ is odd and $q$ is large, then the second term in the bound of Corollary 3.7 does not contribute significantly. However, if $n$ is even, i.e., $l = 2$, then we could also use the somewhat simpler good estimate

$$\left| \sum_{n=\mu}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu \mid n \\ \nu > \lambda}} \nu S_\nu \left( \frac{n}{\nu} \right) \right| < \frac{2(g+m-1)}{\mu} \frac{q}{q-1} \frac{\sqrt{q}}{\sqrt{q}-1} q^{-n/2}.$$

**3.1. Geometric interpretation.** Before we provide applications of the above results, a geometric interpretation is in order. Let $C$ denote the absolutely irreducible nonsingular curve over $\mathbf{F}_q$ that has $K$ as its function field. For any $n \in \mathbf{N}$, let $k_n = \mathbf{F}_{q^n}$ and $K_n = Kk_n$. Then $K_n/k_n$ is an unramified extension of $K/\mathbf{F}_q$ with the same associated curve $C$ and hence the same genus. If $N_n$ denotes the number of $k_n$-rational points on $C$ (including those at infinity), or equivalently, the number of degree one places of the function field $K_n/k_n$, then

$$N_n = q^n + 1 - \sum_{j=1}^{2g} \omega_j^n. \tag{3.12}$$

Let $x \in K$ be transcendental over $\mathbf{F}_q$ and $[K : \mathbf{F}_q(x)] = m$. If $x_1, x_2, \ldots, x_{m-1}$ are defined as in Theorem 2.1, then the quantity

$$N_n^\infty = \sum_{j=1}^{m-1} x_j^n + 1$$

is exactly the number of degree one places of $K_n/k_n$ lying above the place at infinity of $k_n(x)$. Then the number of finite degree one places of $K_n/k_n$, or equivalently, the number of points on $C$ with coordinates in $k_n$, is

$$N_n^x = N_n - N_n^\infty = q^n - \sum_{j=1}^{2g} \omega_j^n - \sum_{j=1}^{m-1} x_j^n. \tag{3.13}$$

Let $\nu \in \mathbf{N}$, and let $N'_\nu$ denote the number of points on $C$ with coordinates in $k_\nu$ but in no subfield of $k_\nu$. Since the subfields of $k_n$ are exactly the fields $k_\nu$ with $\nu \mid n$, we have

$$\sum_{\nu \mid n} N'_\nu = N_n^x.$$

Recall that $I_\nu$ is the number of monic prime polynomials of degree $\nu$ in $\mathbf{F}_q[x]$. Then $\nu I_\nu$ is the number of elements in $k_\nu$ that do not lie in any subfield of $k_\nu$. If $S_\nu(i)$ is defined as in (3.6), then we have

$$\nu S_\nu\left(\frac{n}{\nu}\right) = N'_\nu - \nu I_\nu.$$

Using (3.13) and the fact that $\sum_{\nu|n} \nu I_\nu = q^n$, it follows that

$$\sum_{\nu|n} \nu S_\nu\left(\frac{n}{\nu}\right) = N_n^x - q^n = -\sum_{j=1}^{2g} \omega_j^n - \sum_{j=1}^{m-1} x_j^n,$$

which is exactly (3.7), i.e., the result of Theorem 3.1. By (2.2), (3.12) implies the well known Hasse-Weil bound

$$|N_n - (q^n + 1)| \le 2gq^{n/2}. \tag{3.14}$$

It follows from (3.13) that

$$\begin{aligned}\left|\sum_{\nu|n} \nu S_\nu\left(\frac{n}{\nu}\right)\right| &= |N_n - N_n^\infty - q^n| \\ &= \left|N_n - q^n - 1 - \sum_{j=1}^{m-1} x_j^n\right| \\ &\le 2gq^{n/2} + \left|\sum_{j=1}^{m-1} x_j^n\right| \le 2gq^{n/2} + (m-1),\end{aligned}$$

which is the result of Corollary 3.2. So Corollary 3.2 can be interpreted as the Hasse-Weil bound with the information about the infinite places incorporated.

We now provide two applications of the results of Section 3, namely computing the class number $h_K$ of $K/\mathbf{F}_q$ and analyzing the distribution of the zeros of $\zeta_K(s)$.

**4. Application 1: A class number algorithm for algebraic function fields.** In this section, we provide a context where the multiple nested sums of Section 3 occur and how they can be used

to estimate the divisor class number of a function field. We continue to let $K/\mathbf{F}_q$ be an algebraic function field of genus $g$ over a finite field $\mathbf{F}_q$, $x \in K$ a transcendental element over $\mathbf{F}_q$, and $[K : \mathbf{F}_q(x)] = m$. We begin by explaining how a good approximation of the class number $h_K$ of $K$ can be used to actually find $h_K$. Then we provide three approaches for obtaining such an approximation.

**4.1. The idea of the algorithm.** Here is a general outline of the algorithm for computing $h_K$.

(1) Evaluate sufficiently many terms in (3.1) or (3.8) to obtain an approximation $E$ of $h_K$ and a bound $U$ such that $|h_K - E| \leq U$. It follows that $h_K \in [E - U, E + U]$.

(2) Use Shanks' *baby step giant step* or *Pollard's kangaroo* method to search through the interval $[E-U, E+U]$ of size $2U+1$ to determine $h_K$. Assuming that efficient arithmetic in the ideal or divisor class group of $K$ is available, the methods in [**48, 49**] should be easily generalizable.

Note that the search could be shortened by undertaking precomputations or using other information where possible. For instance, one could determine $h_K \pmod{l}$ for small primes $l$ or exploit knowledge about the distribution of $h_K$ in the interval $[E - U, E + U]$.

The complexity of the above algorithm is $O(\max\{t_a, t_s\})$, where $t_a$ is the time required for computing the approximation $E$ of $h_K$, and $t_s$ is the time it takes to search through the interval $[E - U, E + U]$. Necessarily, the total running time will be exponential in $q$ and will be optimized if $t_a \approx t_s$. The number of arithmetic operations in the divisor class group of $K$ required to find $h_K$ is on the order of the square root of the length of the search interval, i.e., $\sqrt{2U+1}$. It follows that $t_s = O(\sqrt{U})$, where the $O(\cdot)$ notation refers to fixed $g$ and $q \to \infty$.

If (3.8) is used in the approximation step, then the computation of $e^{A(K)}$ with $A(K)$ as given in (3.4) takes negligible running time. For a parameter $\lambda \in \mathbf{N}$, the main contributing part for $t_a$ is the evaluation of either the summands $S_\nu(n/\nu)$ in (3.8) with $\nu \leq \lambda$, or the product in (3.1) of all the Euler factors $\prod_{j=1}^{m-1}(1 - z_j(P)/q^\nu)^{-1}$, where $P$ runs through all the monic prime polynomials in $\mathbf{F}_q[x]$ of degree up to $\lambda$. Note that there are $O(q^\lambda/\lambda)$ such polynomials. So, in either case, the computation takes $O(S \cdot q^\lambda)$ operations, where $S$ is the running

time to determine the splitting behavior of the principal ideal $(P)$ in the maximal order $\mathcal{O}_x$ of $K/\mathbf{F}_q(x)$ for a monic prime polynomial $P$ of degree $\deg(P) \leq \lambda$. Ignoring the running time $S$ and the complexity of one arithmetic operation, we see that this algorithm is optimized when $q^\lambda \sim \sqrt{U}$.

In the following sections, we generalize ideas from the quadratic and cubic cases; see [**49**] for $m = 2$ and [**45**] for $m = 3$. We compute an approximation depending on a parameter $\lambda \in \mathbf{N}$ which will be chosen later for optimal complexity. First, we state the most obvious choice of $E$ and $U$, namely, to simply truncate the sum in (3.8); this choice generalizes the approximations in [**49**, Theorem 4.1] and [**45**, Theorem 5.1]. The idea is to represent $h_K$ as $h_K = Ee^B$ and find a sharp bound $\psi$ on $|B|$. Then $E$ will be our approximation to $h_K$, and $\psi$ is a bound on the absolute value of the logarithm of the tail of the Euler product representation of $h_K$.

**4.2. The first approximation.**

**Theorem 4.1.** *Let $\lambda \in \mathbf{N}$ and $A(K)$ be as defined in* (3.4). *If we put*

$$\begin{aligned}
\log E_1(\lambda) &= A(K) + \sum_{n=1}^{\lambda} \frac{1}{nq^n} \sum_{\nu|n} \nu\, S_\nu\left(\frac{n}{\nu}\right),\\
B_1(\lambda) &= \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \sum_{\nu|n} \nu\, S_\nu\left(\frac{n}{\nu}\right),\\
\psi_1(\lambda) &= 2g \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^{n/2}} + (m-1) \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n},\\
U_1(\lambda) &= E_1(\lambda)(e^{\psi_1(\lambda)} - 1),
\end{aligned}$$

*then we have $|B_1(\lambda)| \leq \psi_1(\lambda)$ and $|h_K - E_1(\lambda)| \leq U_1(\lambda)$.*

*Proof.* From the definition of $E_1(\lambda)$, $B_1(\lambda)$ and (3.8), it follows immediately that

$$h_K = E_1(\lambda)\ e^{B_1(\lambda)}.$$

From Corollary 3.2, we estimate

$$|B_1(\lambda)| \le \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \left| \sum_{\nu|n} \nu\, S_\nu\left(\frac{n}{\nu}\right) \right| \le \sum_{n=\lambda+1}^{\infty} \frac{m-1+2gq^{n/2}}{nq^n} = \psi_1(\lambda).$$

Since $\psi_1(\lambda)$ is much smaller than 1 for $q$ large, we obtain

$$|h_K - E_1(\lambda)| = E_1(\lambda)|e^{B_1(\lambda)} - 1| \le E_1(\lambda)(e^{\psi_1(\lambda)} - 1) = U_1(\lambda). \qquad \square$$

We remark that $\psi_1(\lambda)$ can be evaluated using (3.2) with $z = q^{-1/2}$, which yields

$$\psi_1(\lambda) = 2g\left( \log\left(\frac{\sqrt{q}}{\sqrt{q}-1}\right) - \sum_{n=1}^{\lambda} \frac{1}{nq^{n/2}} \right) + (m-1)\left( \log\left(\frac{q}{q-1}\right) - \sum_{n=1}^{\lambda} \frac{1}{nq^n} \right).$$

It is also worth noting that, as in [**49**], we could use the following upper bound on $\psi_1(\lambda)$ instead of $\psi_1(\lambda)$ itself:

$$\begin{aligned} \psi_1(\lambda) &< \frac{2g}{\lambda+1}\, q^{-(\lambda+1)/2} + \frac{2g}{\lambda+2} \sum_{n=\lambda+2}^{\infty} q^{-n/2} + \frac{m-1}{\lambda+1} \sum_{n=\lambda+1}^{\infty} q^{-n} \\ &= \frac{2g}{\lambda+1}\, q^{-(\lambda+1)/2} + \frac{2g}{\lambda+2}\, \frac{\sqrt{q}}{\sqrt{q}-1}\, q^{-(\lambda+2)/2} \\ &\quad + \frac{m-1}{\lambda+1}\, \frac{q}{q-1}\, q^{-\lambda+1} \ . \end{aligned}$$

Using (3.2) and Corollary 3.2, it is also easy to see that

$$E_1(\lambda) < e^{A(K)} \left(\frac{\sqrt{q}}{\sqrt{q}-1}\right)^{2g} \left(\frac{q}{q-1}\right)^{m-1}. \tag{4.1}$$

Thus. for fixed $g$ and $q \to \infty$ it follows that $E_1(\lambda) = O(e^{A(K)}) = O(q^g)$ as expected from (2.4). Since $\psi_1(\lambda) < 1$, we can also estimate $e^{\psi_1(\lambda)} \sim 1 + \psi_1(\lambda)$ which yields that $U_1(\lambda) = O(q^{g-(\lambda+1)/2})$.

Computations in [**49**] showed that this approximation was significantly less effective in the hyperelliptic case than the suggested choice of $E_2$ in subsection 4.3. The reason will become clear from the definition of $E_2$; see the discussion in subsection 4.5.

### 4.3. The second approximation.

**Theorem 4.2.** *Let $\lambda \in \mathbf{N}$ and $A(K)$ be as defined in* (3.4). *Also, let $l'$ be the smallest prime divisor of $\lambda+1$. If we put*

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

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

$$\begin{aligned}\psi_2(\lambda) = {} & \frac{2g}{\lambda+1}\, q^{-(\lambda+1)/2} + \frac{m-1}{\lambda+1}\,\frac{q}{q-1}\,\frac{\left(q^{(\lambda+1)/l'}-1\right)}{q^{\lambda+1}} \\ & + \frac{m-1}{\lambda+1}\, q^{-(\lambda+1)} + \frac{2g}{\lambda+2}\,\frac{\sqrt{q}}{\sqrt{q}-1}\, q^{-(\lambda+2)/2} \\ & + \frac{2(m-1)}{\lambda+2}\,\frac{q}{q-1}\,\frac{q^{(1-(1/l'))}}{q^{(1-(1/l'))}-1}\, q^{-(1-(1/l'))(\lambda+2)},\end{aligned}$$

$$U_2(\lambda) = E_2(\lambda)(e^{\psi_2(\lambda)}-1),$$

*then we have $|B_2(\lambda)| < \psi_2(\lambda)$ and $|h_K - E_2(\lambda)| < U_2(\lambda)$.*

*Proof.* Note that by (3.1) and (3.4), the definition of $E_2(\lambda)$ is equivalent to

$$E_2(\lambda) = e^{A(K)} \prod_{\nu=1}^{\lambda} \prod_{\deg(P)=\nu} \prod_{j=1}^{m-1} \frac{1}{1-(z_j(P)/q^\nu)},$$

so $E_2(\lambda)$ is in fact computable. It then follows from the definition of $B_2(\lambda)$ that

$$h_K = E_2(\lambda)\ e^{B_2(\lambda)}.$$

This yields the representation as required in subsection 4.1. We now use Theorem 3.4 and Corollary 3.7 to bound $|B_2(\lambda)|$.

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

As in the proof of Theorem 4.1, we then obtain that $|h_K - E_2(\lambda)| < U_2(\lambda)$. □

Analogous to the proof of (4.1), we derive that

$$E_2(\lambda) < e^{A(K)}\left(\frac{\sqrt{q}}{\sqrt{q}-1}\right)^{2g}\left(\frac{q}{q-1}\right)^{m-1} e^{\psi_2(\lambda)}. \tag{4.2}$$

Thus, for fixed $g$ and $q \to \infty$, we again have $\psi_2(\lambda) < 1$. It follows that $E_2(\lambda) = O(q^g)$ and $U_2(\lambda) = O(q^{g-(\lambda+1)/2})$.

**4.4. The third approximation.** We now discuss a third choice for the approximation. It is based on the second choice plus the following observations. Let $\lambda \in \mathbf{N}$. In order to compute $E_2(\lambda)$ as defined in Theorem 4.2, we need to compute $z_1(P), \dots, z_{m-1}(P)$ for all monic prime polynomials $P$ with $\deg(P) \le \lambda$. Once we know $z_j(P)$ for all $j = 1, \dots, m-1$, it is easy to evaluate the powers $z_j(P)^i$ for arbitrary $i \in \mathbf{N}$. In particular, we can easily compute $S_\nu(i)$ for $1 \le \nu \le \lambda$ and any $i \in \mathbf{N}$. Therefore, we may assume that we know $\nu S_\nu((\lambda+1)/\nu)$

for all $\nu$ with $l' \le \nu < \lambda+1$ and $\nu \mid \lambda+1$, where as before, $l'$ denotes the smallest prime divisor of $\lambda+1$. Furthermore, we assume that we have computed $x_1, \dots, x_{m-1}$ and thus know their $(\lambda+1)$st powers. We then obtain from (3.9) that

$$(\lambda+1)S_{\lambda+1}(1) = -\sum_{j=1}^{m-1} x_j^{\lambda+1} - \sum_{j=1}^{2g} \omega_j^{\lambda+1} - \sum_{\substack{\nu \mid \lambda+1 \\ \nu \neq \lambda+1}} \nu S_\nu\left(\frac{\lambda+1}{\nu}\right),$$

where only the second term on the righthand side is unknown. The following bound is then immediate.

$$\begin{aligned}(\lambda+1)|S_{\lambda+1}(1)| \le{}& \left|\sum_{j=1}^{m-1} x_j^{\lambda+1}\right| + 2gq^{(\lambda+1)/2} \\ &+ \left|\sum_{\substack{\nu \mid \lambda+1 \\ \nu \neq \lambda+1}} \nu S_\nu\left(\frac{\lambda+1}{\nu}\right)\right|.\end{aligned} \tag{4.3}$$

**Theorem 4.3.** *Let $\lambda \in \mathbf{N}$ and $A(K)$ be as defined in* (3.4)*. Also, let $l'$ be the smallest prime divisor of $\lambda+1$. If we put*

$$\begin{aligned}\log E_3(\lambda) &= A(K) + \sum_{n=1}^{\lambda} \frac{1}{nq^n} \sum_{\nu \mid n} \nu\, S_\nu\left(\frac{n}{\nu}\right) \\ &\quad + \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu \mid n \\ \nu \le \lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right) \\ &= \log E_2(\lambda),\end{aligned}$$

$$B_3(\lambda) = \sum_{n=\lambda+1}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu \mid n \\ \nu > \lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right) = B_2(\lambda),$$

$$\begin{aligned}\psi_3(\lambda) &= \frac{2g}{\lambda+1}\, q^{-(\lambda+1)/2} \\ &\quad + \frac{1}{(\lambda+1)q^{\lambda+1}}\left(\left|\sum_{j=1}^{m-1} x_j^{\lambda+1}\right| + \left|\sum_{\substack{\nu\mid\lambda+1\\ \nu\neq\lambda+1}} \nu S_\nu\left(\frac{\lambda+1}{\nu}\right)\right|\right) \\ &\quad + \frac{2g}{\lambda+2}\,\frac{\sqrt{q}}{\sqrt{q}-1}\, q^{-(\lambda+2)/2} \\ &\quad + \frac{2(m-1)}{\lambda+2}\,\frac{q}{q-1}\,\frac{q^{(1-(1/l'))}}{q^{(1-(1/l'))}-1}\, q^{-(1-(1/l'))(\lambda+2)},\end{aligned}$$

$$U_3(\lambda) = E_3(\lambda)(e^{\psi_3(\lambda)} - 1),$$

*then we have* $|B_3(\lambda)| < \psi_3(\lambda)$ *and* $|h_K - E_3(\lambda)| < U_3(\lambda)$.

*Proof.* As in the proof of Theorem 4.2, we have $E_3(\lambda)\ e^{B_3(\lambda)} = E_2(\lambda)\ e^{B_3(\lambda)} = h_K$. Since

$$B_3(\lambda) = \frac{S_{\lambda+1}(1)}{q^{\lambda+1}} + \sum_{n=\lambda+2}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu\mid n\\ \nu>\lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right),$$

we use (4.3) to estimate

$$\begin{aligned}|B_3(\lambda)| &\le \frac{(\lambda+1)|S_{\lambda+1}(1)|}{(\lambda+1)q^{\lambda+1}} + \left|\sum_{n=\lambda+2}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu\mid n\\ \nu>\lambda}} \nu\, S_\nu\left(\frac{n}{\nu}\right)\right| \\ &< \frac{2g}{\lambda+1}\, q^{-(\lambda+1)/2} \\ &\quad + \frac{1}{(\lambda+1)q^{\lambda+1}}\left(\left|\sum_{j=1}^{m-1} x_j^{\lambda+1}\right| + \left|\sum_{\substack{\nu\mid\lambda+1\\ \nu\neq\lambda+1}} \nu S_\nu\left(\frac{\lambda+1}{\nu}\right)\right|\right) \\ &\quad + \frac{2g}{\lambda+2}\,\frac{\sqrt{q}}{\sqrt{q}-1}\, q^{-(\lambda+2)/2} \\ &\quad + \frac{2(m-1)}{\lambda+2}\,\frac{q}{q-1}\,\frac{q^{(1-(1/l'))}}{q^{(1-(1/l'))}-1}\, q^{-(1-(1/l'))(\lambda+2)} \\ &= \psi_3(\lambda).\end{aligned}$$

As in the proofs of Theorems 4.1 and 4.2, it is clear that $|h_K - E_3(\lambda)| < U_3(\lambda)$. □

Since $E_3(\lambda) = E_2(\lambda)$ and $B_3(\lambda) = B_2(\lambda)$, we see that

$$E_3(\lambda) < e^{A(K)} \left( \frac{\sqrt{q}}{\sqrt{q}-1} \right)^{2g} \left( \frac{q}{q-1} \right)^{m-1} e^{\psi_3(\lambda)}. \tag{4.4}$$

Again, we have $\psi_3(\lambda) < 1$, $E_3(\lambda) = O(q^g)$ and $U_3(\lambda) = O(q^{g-(\lambda+1)/2})$.

**4.5. Complexity.** We need to determine how to select a value of $\lambda$ that optimizes the algorithm and which of the approximations given in the previous three sections to choose. Each of the three approximations for $h_K$ given above was given in terms of quantities $E(\lambda)$ and $U(\lambda)$ such that $|h_K - E(\lambda)| \le U(\lambda)$, so $h_K$ lies in the interval $[E(\lambda) - U(\lambda), E(\lambda) + U(\lambda)]$ of length $2U(\lambda) + 1$. Our most important application is when $q$ is large, yielding in each case that $E(\lambda) = O(q^g)$ and $U(\lambda) = O(q^{g-(\lambda+1)/2})$. As pointed out in subsection 4.1, the total running time of the class number algorithm will be exponential in $q$ and is optimal when

$$q^\lambda \sim \sqrt{U(\lambda)} = q^{(2g-(\lambda+1))/4},$$

yielding an optimal choice of $\lambda \approx (2g-1)/5$. Since $\lambda$ must be an integer, we obtain

$$\lambda = \begin{cases} \lfloor (2g-1)/5 \rfloor & \text{if } g \equiv 2 \pmod 5, \\ \text{round}\,((2g-1)/5) & \text{otherwise.} \end{cases} \tag{4.5}$$

This yields a total expected running time of

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

where

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

Note that for $g \leq 2$ (4.5) would yield the meaningless choice $\lambda = 0$. Here, we can obtain running times of $O(q^{1/4})$ for $g = 1$ and $O(q^{3/4})$ for $g = 2$ using for example (2.4). However, we point out that there are better methods for these genera, as outlined in Section 1.

Finally, a comment on which choice of approximation might be optimal. The first approximation in Theorem 4.1 has a clean and sharp error term, whereas the approximations in Theorems 4.2 and 4.3 use all of the computable information about the Euler factors. The difference between $E_1(\lambda)$ and $E_2(\lambda) = E_3(\lambda)$ is precisely the term

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

which is not contained in $E_1(\lambda)$. In the hyperelliptic case, see [**48, 49, 50**], the second choice of the approximation turned out to be better than the first choice; the third approximation was not included in the discussion there. In view of the better error term, one might expect that the third approximation is yet more accurate than the second choice, as $U_3(\lambda)$ might be a better bound on $|h_K - E_2(\lambda)|$ than $U_2(\lambda)$, resulting in a shorter search interval. However, it needs to be seen in any given situation which approximation works best. One possibility is to use the intersection of all three intervals when searching for $h_K$, but it is unclear whether this intersection will on average coincide with one specific interval.

We remark that the computational effort is essentially the same for all three approximations. For each approximation, we basically need to compute $z_1(P), \ldots, z_{m-1}(P)$ for all monic prime polynomials $P$ with $\deg(P) \leq \lambda$. As pointed out at the beginning of subsection 4.4, the additional running time for computing $z_j(P)^i$ is then negligible. This yields the quantities $S_\nu(i)$ for $1 \leq \nu \leq \lambda$ and for any $\in \mathbf{N}$ without too much additional effort. Thus, all three approximations, error terms and intervals should be computable in roughly the same running time.

**5. Application 2: Distribution of the zeroes of the zeta function.** The second application of our bounds in Section 3 is a generalization of ideas in [**48**] and relates the results of the previous sections to the distribution of zeros of the zeta function of an algebraic

function field of genus $g$. Note that by (2.1) and (2.5), the function $Z_K(u)$ has zeros $\omega_j$, $1 \le j \le 2g$. If we write $\omega_j = \sqrt{q}e^{i\varphi_j}$ according to (2.2), where $i$ is a fixed square root of $-1$ and $\varphi_j \in [0, 2\pi[$, then this is essentially asking the question of how the values $\varphi_j$ are distributed as we range over all function fields of genus $g$.

In Section 4, we used the ideas of Section 2 to find an approximation $E(\lambda)$ and a real number $U(\lambda)$ such that $|h_K - E(\lambda)| \le U(\lambda)$. In all three cases, we represented $h_K$ as $h_K = E(\lambda)\, e^{B(\lambda)}$ and found a sharp upper bound $\psi(\lambda)$ on $|B(\lambda)|$. Furthermore, $U(\lambda)$ was defined as $U(\lambda) = E(\lambda)(e^{\psi(\lambda)} - 1)$. Our considerations in this section are again mainly of interest for the case that $g$ is fixed and $q \to \infty$, in which case we have $\psi(\lambda) < 1$. The power series expansion of the exponential function then implies $e^{\psi(\lambda)} \approx 1 + \psi(\lambda)$. Thus, we expect that for large $q$,

$$U(\lambda) = E(\lambda)(e^{\psi(\lambda)} - 1) \approx E(\lambda)\psi(\lambda).$$

Similarly, we expect that

$$|h_K - E(\lambda)| = E(\lambda)|e^{B(\lambda)} - 1| \approx E(\lambda)|B(\lambda)|,$$

and hence

$$\frac{|h_K - E(\lambda)|}{U(\lambda)} \approx \frac{|B(\lambda)|}{\psi(\lambda)}. \tag{5.1}$$

Let $\alpha(g,q)$ be the average value of $|h_K - E(\lambda)|/U(\lambda)$ over all function fields $K/\mathbf{F}_q$ of genus $g$ for fixed values of $g$ and $q$. The quantity $\alpha(g,q)$ measures how closely $U(\lambda)$ bounds the "error" $|h_K - E(\lambda)|$ in general, i.e., how the values of $h_K$ cluster around the center point of the interval $[E(\lambda) - U(\lambda), E(\lambda) + U(\lambda)]$. We therefore wish to determine $\alpha(g) = \lim_{q\to\infty} \alpha(g,q)$, at least heuristically. The interpretation here is that for fixed $g$, the bound $U(\lambda)$ on $|h_K - E(\lambda)|$ is on average by a factor of $\alpha(g)^{-1}$ too large. From (5.1), we expect that for large $q$,

$$\alpha(g,q) \approx \text{Mean}\left(\frac{|B(\lambda)|}{\psi(\lambda)}\right). \tag{5.2}$$

In order to obtain an expression for $\alpha(g,q)$, the goal is to analyze the quotient $|B(\lambda)|/\psi(\lambda)$ of (5.1) for each of the three approximations of

Section 4. Letting $q \to \infty$, we can then obtain an approximate value for $\alpha(g)$.

As before, we put $\omega_j = \sqrt{q}e^{i\varphi_j}$ with $\varphi_j \in [0, 2\pi[$ for $1 \le j \le 2g$. We know that the $\omega_j$ satisfy $\omega_{j+g} = \overline{\omega}_j$, the complex conjugate of $\omega_j$, for $1 \le j \le g$ and that the $\varphi_j$ are periodic, i.e., $\varphi_{j+g} \equiv -\varphi_j \pmod{2\pi}$ for $1 \le j \le g$. Therefore, we can enumerate the $\varphi_j$ such that $0 \le \varphi_j \le \pi$ and $\varphi_{j+g} \equiv -\varphi_j \pmod{2\pi}$ for $1 \le j \le g$.

For $\lambda \in \mathbf{N}$ as in (4.5), we now define

$$G_\lambda(\varphi_1, \dots, \varphi_g) = \sum_{j=1}^{2g} e^{i(\lambda+1)\varphi_j} = 2\sum_{j=1}^{g} \cos((\lambda+1)\varphi_j). \tag{5.3}$$

For brevity, we also set

$$\varepsilon(\lambda, m, q) = \frac{\lambda+1}{l'} S_{(\lambda+1)/l'}(l')\, q^{-(\lambda+1)/2}, \tag{5.4}$$

where as before, $l'$ is the smallest prime divisor of $\lambda+1$. The idea is to relate $\alpha(g)$ to the average of $|G_\lambda|$, or of $|F_\lambda|$ where $F_\lambda = G_\lambda + \varepsilon(\lambda, m)$ and $\varepsilon(\lambda, m)$ is the contribution of the average of $\varepsilon(\lambda, m, q)$, taken over all function fields of degree $m$ and genus $g$, and for $q \to \infty$. Note that for $\lambda$ even, $l' > 2$, and hence $\varepsilon(\lambda, m, q)$ tends to zero as $q \to \infty$ by (3.11). The same holds true in many cases when the extension degree $m = [K : \mathbf{F}_q(x)] \ge 3$; for example, obviously whenever $S_{(\lambda+1)/l'}(l') = 0$. However, $\varepsilon(\lambda, m)$ does not always vanish. For example, we know from [**48**] that $\varepsilon(\lambda, 2) = 1$ for $\lambda$ odd.

For quadratic function fields, i.e., $m = 2$, the connection between Mean $(|F_\lambda|)$ and $\alpha(g)$ was established in [**48**]. For this case, results by Katz and Sarnak [**29, 30**] lead to a close numerical approximation of Mean $(|F_\lambda|)$, which in turn yielded good approximate values of $\alpha(g)$ for several genera $g$. Unfortunately, finding the exact value of Mean $(|F_\lambda|)$ appears to be difficult in general.

The argument of [**48**] could potentially be turned around as follows. With a fast class number algorithm, it would be possible to compute the quotients $|h_K - E(\lambda)|/U(\lambda)$ for a large number of function fields $K/\mathbf{F}_q$ for fixed $q$ and $g$. Taking the numerical average of all these quotients could give an idea of the value of $\alpha(g, q)$. Repeating this process for

many large prime powers $q$ might ultimately shed light on the value of the limit $\alpha(g)$.

We now investigate the quotient $|B(\lambda)|/\psi(\lambda)$ for all three approximations given in Section 4, thereby obtaining an approximate value for $\alpha(g,q)$, and ultimately for $\alpha(g)$ in all three cases.

**5.1. Heuristics for the first approximation.** By the definition of $B_1(\lambda)$ in Theorem 4.1 and (3.7), we have

$$\begin{aligned} B_1(\lambda) &= \frac{1}{(\lambda+1)q^{\lambda+1}} \sum_{\nu|(\lambda+1)} \nu\, S_\nu\Big(\frac{\lambda+1}{\nu}\Big) \\ &\quad + \sum_{n=\lambda+2}^{\infty} \frac{1}{nq^n} \sum_{\nu|n} \nu\, S_\nu\Big(\frac{n}{\nu}\Big) \\ &= \frac{1}{(\lambda+1)q^{\lambda+1}}\Big( -\sum_{j=1}^{m-1} x_j^{\lambda+1} - \sum_{j=1}^{2g} \omega_j^{\lambda+1}\Big) \\ &\quad + \sum_{n=\lambda+2}^{\infty} \frac{1}{nq^n}\Big( -\sum_{j=1}^{m-1} x_j^{n} - \sum_{j=1}^{2g} \omega_j^{n}\Big). \end{aligned}$$

Since $\omega_j^{\lambda+1} = q^{(\lambda+1)/2} e^{(\lambda+1)i\varphi_j}$, it follows by (5.3) that

$$\begin{aligned} B_1(\lambda) &= \frac{1}{(\lambda+1)q^{\lambda+1}} \Big| \sum_{j=1}^{2g} \omega_j^{\lambda+1} \Big| + O(q^{-(\lambda+2)/2}) \\ &= \frac{|G_\lambda|}{(\lambda+1)q^{(\lambda+1)/2}} + O(q^{-(\lambda+2)/2}), \end{aligned} \tag{5.5}$$

where we recall that the $O(\cdot)$ notation refers to $g$ fixed and $q \to \infty$. From Theorem 4.1 and the comments afterwards, we know that

$$\psi_1(\lambda) = \frac{2g}{(\lambda+1)q^{(\lambda+1)/2}} + O(q^{-(\lambda+2)/2}),$$

so (5.2) yields $\alpha(g,q) \approx |G_\lambda|/2g$ for large $q$. One would thus expect that

$$\alpha(g) \approx \frac{1}{2g}\,\mathrm{Mean}\,(|G_\lambda|). \tag{5.6}$$

Thus, if we know how to evaluate Mean $(|G_\lambda|)$, then we are able to determine $\alpha(g)$.

**5.2. Heuristics for the second approximation.** From Theorem 4.2, we have

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

where as before, we assume $g$ fixed and $q \to \infty$. By (3.10) and (3.11), we see that

$$(\lambda+1)|S_{\lambda+1}(1)| = \left| \sum_{j=1}^{2g} \omega_j^{\lambda+1} + \frac{\lambda+1}{l'} S_{(\lambda+1)/l'}(l') \right| + O(q^{(\lambda+1/l')-1}),$$

where $l'$ is again the smallest prime divisor of $\lambda+1$. When dividing $|S_{\lambda+1}(1)|$ by $q^{\lambda+1}$, the error term becomes $O(q^{-(\lambda+1)(1-(1/l'))-1})$, which is negligible compared to the term $O(q^{-(\lambda+2)/2})$ in $|B_2(\lambda)|$. So we obtain by (5.3) and (5.4) that

$$\begin{aligned}
|B_2(\lambda)| &= \frac{1}{(\lambda+1)q^{\lambda+1}} \left| \sum_{j=1}^{2g} \omega_j^{\lambda+1} + \frac{\lambda+1}{l'} S_{(\lambda+1)/l'}(l') \right| + O(q^{(\lambda+2)/2}) \\
&= \frac{1}{(\lambda+1)q^{(\lambda+1)/2}} \left| \sum_{j=1}^{2g} e^{i(\lambda+1)\varphi_j} + \frac{\lambda+1}{l'} S_{(\lambda+1)/l'}(l') q^{-(\lambda+1)/2} \right| \\
&\quad + O(q^{-(\lambda+2)/2}) \\
&= \frac{1}{(\lambda+1)q^{(\lambda+1)/2}} |G_\lambda + \varepsilon(\lambda, m, q)| + O(q^{-(\lambda+2)/2}).
\end{aligned}$$

Similarly, from Theorem 4.2,

$$\begin{aligned}
\psi_2(\lambda) &= \frac{2g}{\lambda+1} q^{-(\lambda+1)/2} + \frac{m-1}{\lambda+1} q^{-(\lambda+1)(1-(1/l'))} + O(q^{-(\lambda+2)/2}) \\
&= \frac{1}{(\lambda+1)q^{(\lambda+1)/2}} \left( 2g + (m-1)q^{-(\lambda+1)(1/2-1/l')} \right) \\
&\quad + O(q^{-(\lambda+2)/2}).
\end{aligned}$$

It follows from (5.2) that for large $q$

$$\alpha(g,q) \approx \frac{|G_\lambda + \varepsilon(\lambda,m,q)|}{2g + (m-1)q^{-(\lambda+1)(1/2-1/l')}}. \tag{5.7}$$

Note that for $\lambda$ odd we have $l' = 2$, so the second term in the denominator of the righthand side of (5.7) is equal to $(m-1)q^0 = m-1$, whereas for $\lambda$ even, the term tends to zero as $q \to \infty$. Therefore, altogether, this term tends to $(m-1)\cdot \text{parity}\,(\lambda)$. Recalling that we defined $F_\lambda = G_\lambda + \varepsilon(\lambda,m)$ where $\varepsilon(\lambda,m)$ is the contribution of $\varepsilon(\lambda,m,q)$ as $q \to \infty$, we expect

$$\alpha(g) \approx \frac{\text{Mean}\,(|F_\lambda|)}{2g + (m-1)\cdot \text{parity}\,(\lambda)}. \tag{5.8}$$

Thus, again, if we can compute $\text{Mean}\,(|F_\lambda|)$, then we are able to determine $\alpha(g)$. Recall that $\text{parity}\,(\lambda) = 0$ and $F_\lambda = G_\lambda$ for $\lambda$ even. In this case, (5.8) reduces to (5.6). However, if $\lambda$ is odd, then (5.8) reads $\alpha(g) = \text{Mean}\,(|F_\lambda|)/(2g+m-1)$, which is different from (5.6).

**5.3. Heuristics for the third approximation.** Theorem 4.3 and (3.11) imply that $B_3(\lambda) = B_2(\lambda)$ and

$$\begin{aligned}\psi_3(\lambda) &= \frac{2g}{\lambda+1}\, q^{-(\lambda+1)/2} + \frac{\lambda+1}{l'}\frac{|S_{(\lambda+1)/l'}(l')|}{(\lambda+1)q^{\lambda+1}} + O(q^{-(\lambda+2)/2}) \\ &= \frac{1}{(\lambda+1)q^{(\lambda+1)/2}}\,(2g + \varepsilon(\lambda,m,q)) + O(q^{-(\lambda+2)/2}),\end{aligned}$$

so that we expect by (5.2) that for large $q$

$$\alpha(g,q) \approx \frac{|G_\lambda + \varepsilon(\lambda,m,q)|}{2g + \varepsilon(\lambda,q,m)}.$$

Thus, one would expect that

$$\alpha(g) \approx \frac{\text{Mean}\,(|F_\lambda|)}{2g + \varepsilon(\lambda,m)}. \tag{5.9}$$

Note that for $\varepsilon(\lambda,m) = 0$, (5.9) is once again equivalent to (5.6), but for $\lambda$ odd it yields a different result.

**5.4. Evaluation of Mean $(|F_\lambda|)$ and Mean $(|G_\lambda|)$.** It remains to investigate how to evaluate Mean $(|F_\lambda|)$ and Mean $(|G_\lambda|)$. Since similar arguments hold true for Mean $(|G_\lambda|)$, it is sufficient to describe the evaluation of Mean $(|F_\lambda|)$. Finding the exact value of Mean $(|F_\lambda|)$ appears to be difficult. However, if we are able to determine a good numerical approximation of Mean $(|F_\lambda|)$, then we are able to derive a good numerical approximation of $\alpha(g)$. In [**48**], results by Katz and Sarnak [**29, 30**] led to an approximation of $\alpha(g)$ for quadratic extensions ($m = 2$). These results verified numerical data obtained in [**48**] about the average value of $|h_K - E(\lambda)|/U(\lambda)$ explicitly.

We now explain how to generalize these ideas. In order to compute or approximate Mean $(|F_\lambda|)$, the idea is to express this mean as

$$\begin{aligned} \text{Mean}\,(|F_\lambda|) &= \int_A |F_\lambda|\, d\,\text{Haar} \\ &= \int_{[0,\pi]^g} |F_\lambda(\varphi_1, \dots, \varphi_g)|\, \mu_g(d\varphi_1, \dots, d\varphi_g), \end{aligned} \tag{5.10}$$

where "Haar" in the first integral denotes the Haar measure of a subgroup of the symplectic group $\mathrm{Sp}\,(2g)$ and $\mu_g$ denotes the appropriate measure. Obviously, the main difficulty is to determine $\mu_g$ for a given class of curves. Once we know $\mu_g$, we are simply faced with computing a Riemann integral. There are various numerical methods for accomplishing this task. If none of them applies, we might approximate the Riemann integral in (5.10) by Riemann sums.

In the elliptic case, i.e., $m = 2$ and $g = 1$, Birch [**7**] showed that the correct choice is

$$\mu_1(d\varphi_1) = \frac{2}{\pi} \sin^2(\varphi_1)\, d\varphi_1.$$

In the hyperelliptic case, i.e., $m = 2$ and $g > 1$, Katz and Sarnak [**29**, Theorem 10.8.2, page 321] showed that $\mu_g$ is basically the Haar measure of a maximal compact subgroup of the symplectic group $\mathrm{Sp}\,(2g)$. It then follows from Weyl [**56**, page 591] that the correct choice is

$$\begin{aligned} &\mu_g(d\varphi_1, \dots, d\varphi_g) \\ &\qquad = \frac{1}{g!} \prod_{j=1}^{g} \frac{2}{\pi} \sin^2(\varphi_j) \prod_{i<j} 4\,(\cos(\varphi_i) - \cos(\varphi_j))^2\, d\varphi_1 \cdots d\varphi_g. \end{aligned}$$

In the general case of an arbitrary function field, where $m \geq 3$ and $g \geq 3$, it is not necessarily true that $\mu_g$ is the Haar measure of a maximal compact subgroup of the symplectic group $\mathrm{Sp}\,(2g)$. It would be very interesting to find $\mu_g$ for a given class of nonhyperelliptic curves and then apply the above construction to find $\alpha(g)$ or a good numerical approximation of $\alpha(g)$. Conversely, using the method of Section 4, one could compute the quotients $|h_K - E(\lambda)|/U(\lambda)$ for a large number of function fields $K/\mathbf{F}_q$ of genus $g$, and for a large number of values of $q$. The numerical average of all these quotients could produce approximate values for $\alpha(g,q)$ and might give a clue as to the value of $\alpha(g)$, at least for certain genera $g$.

**6. Conclusion and open problems.** In this paper, we provided a number of results that can be used to bound the Euler product representation of the zeta function of an arbitrary algebraic function field. These results lead to a computationally suitable algorithm for determining the class number and can also be used to analyze the distribution of the zeros of the zeta function.

Our methods require that the quantities $x_1, \ldots, x_{m-1}$ as given in Theorem 2.1 and $z_1(P), \ldots z_{m-1}(P)$ as given in Theorem 2.3 for monic prime polynomials $P \in \mathbf{F}_q[x]$ be known up to a certain degree bound. In other words, it is necessary to determine the splitting behavior in $K$ of a large number of places of $\mathbf{F}_q(x)$, including the place at infinity. While this can be done very efficiently for certain types of function fields, including quadratic and cubic extensions, this task is more difficult in general.

Our second application dealt with the distribution of class numbers. By our construction, this question is ultimately linked to equidistribution of the zeros of $\zeta_K(s)$ relative to a measure $\mu_g$. In the elliptic and the hyperelliptic case, it is known that $\mu_g$ corresponds to the Haar measure of a maximal compact subgroup of the symplectic group $\mathrm{Sp}\,(2g)$. In the general case of an arbitrary function field, it would be most interesting to find the correct value of $\mu_g$. It would even be of interest to classify certain curves where $\mu_g$ is known and apply this knowledge to approximating $\alpha(g)$. Alternatively, one could use the class number algorithm of Section 4 to compute numerical averages to approximate the relevant mean value as explained just prior to subsection 5.1.

In subsection 4.1, we outlined only the most basic framework of our class number algorithm. It would be interesting to use additional information in the search phase, such as the values $h_K \pmod{l}$ for small primes $l$, or information on where $h_K$ is expected to lie relative to $E(\lambda)$ in the interval $[E(\lambda) - U(\lambda), E(\lambda) + U(\lambda)]$, to speed up this method. This latter question of where in the search interval the class number is expected to be found relates back to the quality of the error bound $U(\lambda)$ and hence to the issues discussed in Section 5. It remains to be seen how this information can be computed effectively for large values of $q$ and genera $g \geq 3$.

Finally, we point out that in step (2) of the class number algorithm (the search), very efficient ideal or divisor arithmetic is needed. There are highly suitable algorithms for the case of hyperelliptic [**11, 26, 27**] and purely cubic [**5, 44**] function fields. Arithmetic for the general case was given in [**23**], and a more geometric approach was taken in [**34**], but it is unclear how well these methods perform in actual implementations on very large function fields. Clearly, this is a subject of much needed future research.

## REFERENCES

**1.** L.M. Adleman and M.-D. Huang, *Counting rational points on curves and Abelian varieties over finite fields*, Lect. Notes Comp. Sci. **1122** (1996), 1–16.

**2.** ———, *Counting points on curves and Abelian varieties over finite fields*, J. Symbolic Comp. **32** (2001), 171–189.

**3.** E. Bach, *Improved approximations for Euler products*, Proc. Canad. Number Theory Assoc. **15** (1995), 13–28.

**4.** P. Barrucand, H.C. Williams and L. Baniuk, *A computational technique for determining the class number of a pure cubic field*, Math. Comp. **30** (1976), 312–323.

**5.** M.L. Bauer, *The arithmetic of certain cubic function fields*, Math. Comp. **73** (2004), 387–413.

**6.** M.L. Bauer, E. Teske and A. Weng, *Point counting on Picard curves in large characteristic*, Math. Comp. **74** (2005), 1983–2005.

**7.** B. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43** (1968), 57–60.

**8.** J.A. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Sem. Theor. Nombres Paris **1** (1990), 27–41.

**9.** J.A. Buchmann and H.C. Williams, *On the computation of the class number of an algebraic number field*, Math. Comp. **53** (1989), 679–688.

**10.** J.A. Buchmann and H.C. Williams, *On the existence of a short proof for the value of the class number and regulator of a real quadratic field*, Kluwer Academic Publishers, Dordrecht, 1989.

**11.** D.G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), 95–101.

**12.** W. Castryck, J. Denef and F. Vercauteren, *Computing zeta functions of nondegenerate curves*, Internat. Math. Research Papers Article ID 72017 (2006), 1–57.

**13.** J. Denef and F. Vercauteren, *An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic* 2, Lect. Notes Comp. Sci. **2369** (2002), 308–323.

**14.** ———, *Counting points on $C_{ab}$ curves using Monsky-Washnitzer cohomology*, Finite Fields Appl. **12** (2006), 78–102.

**15.** ———, *An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic* 2, J. Cryptology **19** (2006), 1–25.

**16.** M. Deuring, *Lectures on the theory of algebraic functions of one variable*, Lect. Notes Math. **314**, Springer-Verlag, Berlin, 1973.

**17.** G. Dueck and H.C. Williams, *Computation of the class number and class group of a complex cubic field*, Math. Comp. **45** (1985), 223–231.

**18.** P. Gaudry and M. Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Lect. Notes Comp. Sci. **2248** (2001), 480–494.

**19.** ———, *Counting points in medium characteristic using Kedlaya's algorithm*, Exp. Math. **12** (2003), 395–402.

**20.** P. Gaudry and R. Harley, *Counting points on hyperelliptic curves over finite fields*, Lect. Notes Comp. Sci. **1838** (2000), 313–332.

**21.** P. Gaudry and É. Schost, *Construction of secure random curves of genus* 2 *over prime fields*, Lect. Notes Comp. Sci. **3027** (2004), 239–256.

**22.** J. Hafner and K. McCurley, *A rigorous subexponential algorithm for computation of class groups*, J. Amer. Math. Soc. **2** (1989), 837–850.

**23.** F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symb. Comp. **33** (2002), 425–445.

**24.** M.-D.A. Huang and D. Ierardi, *Counting points on curves over finite fields*, J. Symb. Comp. **25** (1998), 1–21.

**25.** M.J. Jacobson, Jr., R.F. Lukes and H.C. Williams, *An investigation of bounds for the regulator of quadratic fields*, Exper. Math. **4** (1995), 211–225.

**26.** M.J. Jacobson, Jr., A.J. Menezes and A. Stein, *Hyperelliptic curves and cryptography*, Amer. Math. Soc., Fields Institute Communications Series **41** (2004), 255–282.

**27.** M.J. Jacobson, Jr., R. Scheidler and A. Stein, *Fast arithmetic on hyperelliptic curves via continued fraction expansions*, in *Advances in coding theory and cryptology*, D. Joyner, T. Shaska, W.C. Huffman and V. Ustimenko, eds., World Scientific Publishing Co., Hackensack, NJ, 2007.

**28.** M.J. Jacobson, Jr. and H.C. Williams, *New quadratic polynomials with high densities of prime values*, Math. Comp. **72** (2003), 499–519.

**29.** N.M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues and monodromy*, AMS Colloquium Publ. **45**, American Mathematical Society, Providence, Rhode Island, 1999.

**30.** ———, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. **36** (1999), 1–26.

**31.** K.S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 323–338.

**32.** ———, *Errata for "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology"*, J. Ramanujan Math. Soc. **18** (2003), 417–418.

**33.** ———, *Computing zeta functions via p-adic cohomology*, Lect. Notes Comp. Sci. **3076** (2004), 1–17.

**34.** K. Khuri-Makdisi, *Linear algebra algorithms for divisors on an algebraic curve*, Math. Comp. **73** (2004), 333–357.

**35.** A.G.B. Lauder, *Computing zeta functions of Kummer curves via multiplicative characters*, Found. Comp. Math. **3** (2003), 273–295.

**36.** A.G.B. Lauder and D. Wan, *Computing zeta functions of Artin-Schreier curves over finite fields*, LMS J. Comp. Math. **5** (2002), 34–55.

**37.** ———, *Computing zeta functions of Artin-Schreier curves over finite fields* II, J. Complexity **20** (2004), 331–349.

**38.** H.W. Lenstra, *On the calculation of regulators and class numbers of quadratic fields*, London Math. Soc. Lect. Notes Ser. **56** (1982), 123–150.

**39.** R.F. Lukes, C.D. Patterson and H.C. Williams, *Numerical sieving devices: Their history and some applications*, Nieuw Arch. Wisk. **13** (1995), 113–139.

**40.** J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), 745–763.

**41.** ———, *Counting points on curves over families in polynomial time*, Eprint arXiv:math/0504570, 2005.

**42.** M. Rosen, *Number theory in function fields*, Springer-Verlag, Berlin, 2002.

**43.** T. Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, J. Ramanujan Math. Soc. **15** (2000), 247–270.

**44.** R. Scheidler, *Ideal arithmetic and infrastructure in purely cubic function fields*, J. Theorie Nombres Bordeaux **13** (2001), 609–631.

**45.** R. Scheidler and A. Stein, *Class number approximation in cubic function fields*, Contr. Disc. Math. **2** (2007), 107–132.

**46.** R.J. Schoof, *Counting points on elliptic curves over finite fields*, J. Theor. Nombres Bordeaux **7** (1995), 219–254.

**47.** D. Shanks, *Class number, a theory of factorization, and genera*, Amer. Math. Soc. **20** (1971), 415–440, Providence, RI, 1971.

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

**49.** ———, *The parallelized Pollard kangaroo method in real quadratic function fields*, Math. Comp. **71** (2002), 793–814.

**50.** A. Stein and H.C. Williams, *Some methods for evaluating the regulator of a real quadratic function field*, Exper. Math. **8** (1999), 119–133.

**51.** A.J. Stephens and H.C. Williams, *Computation of real quadratic fields with class number one*, Math. Comp. **51** (1988), 809–824.

**52.** H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993.

**53.** H.J.J. te Riele and H.C. Williams, *New computations concerning the Cohen-Lenstra heuristics*, Exper. Math. **12** (2003), 99–113.

**54.** A.J. van der Poorten, H.J.J. te Riele and H.C. Williams, *Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than* 100 000 000 000, Math. Comp. **70** (2001), 1311–1328.

**55.** ———, *Corrigenda and addition to "Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than* 100000000000*"*, Math. Comp. **72** (2002), 521–523.

**56.** H. Weyl, *Gesammelte Abhandlungen*, vol. II. Springer-Verlag, Berlin, 1968.

**57.** H.C. Williams, G.W. Dueck and B.K. Schmidt, *A rapid method for evaluating the regulator and class number of a pure cubic field*, Math. Comp. **41** (1983), 235–286.

Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada
**Email address: rscheidl@ucalgary.ca**

Institut für Mathematik, Carl von Ossietzky Universität Oldenburg, D-26111 Oldenburg, Germany
**Email address: andreas.stein1@uni-oldenburg.de**