Contributions to Discrete Mathematics

Volume 2, Number 2, Pages 107–132
ISSN 1715-0868

CLASS NUMBER APPROXIMATION IN CUBIC FUNCTION FIELDS

RENATE SCHEIDLER AND ANDREAS STEIN

Abstract. We develop explicitly computable bounds for the order of the Jacobian of a cubic function field. We use approximations via truncated Euler products and thus derive effective methods of computing the order of the Jacobian of a cubic function field. Also, a detailed discussion of the zeta function of a cubic function field extension is included.

1. Introduction and Motivation

A central problem in number theory and algebraic geometry is the determination of the size of the group of rational points on the Jacobian of an algebraic curve over a finite field. This question also has applications to cryptography, since cryptographic systems based on algebraic curves generally require a Jacobian of non-smooth order in order to foil certain types of attacks.

There a variety of methods for accomplishing this task; some are general, while others are only applicable to specific types of curves. In the interest of space, we forego citing most the large volume of literature on elliptic and hyperelliptic curves in detail, and mention only two sources. Kedlaya's p-adic algorithm for hyperelliptic curves [23, 24] is particularly well-suited to fields of small characteristic and has since been extended to Artin-Schreier extensions [14, 26, 27], superelliptic curves [17, 28], C_{ab} curves [15], and more general curves [18, 13]; see also the survey by Kelaya [25]. A very different approach was first given by Schoof for elliptic curves [37]; this method was generalized to Abelian varieties by Pila [30, 31] 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 $\mathbb{F}_q$ in time $O(\log(q)^\delta)$ where δ depends polynomially on d and N. For plane curves

Received by the editors June 21, 2007, and in revised form September 13, 2007.

1991 *Mathematics Subject Classification.* Primary 11R58, 11Y16. Secondary 11M38, 11R65,11R16.

Key words and phrases. cubic function field, class number, regulator, truncated Euler product.

Research of the first author supported by NSERC of Canada.

Research by the second author supported by NSF Grant DMS-0201337.

of degree n, a randomized algorithm with running time $O(\log(q)^{n^{O(1)}})$ was given by Hang and Ierardi [22].

We note that 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. On the other hand, methods for special types of curves have yielded impressive results. The algorithm of [19] for genus 2 hyperelliptic curves, for example, produced class numbers of 39 decimal digits, and the improvements of [20] pushed this up to the cryptographically secure range of 50 decimal digits (164 bits). In 2002, a class number of 29 digits for a genus 3 hyperelliptic curve was computed in [39]. The method for Picard curves given in [4] 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.

In this paper, we develop explicit bounds on the divisor class number h, i.e. the order of the Jacobian of a cubic extension K of a rational function field $\mathbb{F}_q(X)$ of finite characteristic different from 3. More exactly, we determine a good approximation E and an accuracy measure L such that $|h - E| < L^2$. In the case where the genus g of the extension is at most 2, the Hasse-Weil bound yields good choices for E and L. If $g \geq 3$, then we find better effective choices for E and L by making use of the Euler product representation of the L-polynomial of $K/\mathbb{F}_q(X)$. In essence, E is obtained by truncating this Euler product at some suitable point, and L is given by the tail of the truncated Euler product. Here, the cut-off point for the Euler product needs to be chosen in a way that minimizes the time required to find h in the open interval $]E - L^2, E + L^2[$.

Once E and L are determined, the actual value of h can subsequently be found by searching the open interval $]E - L^2, E + L^2[$ using Shanks' baby step-giant step method or Pollard's kangaroo method. The complexity of this search (in terms of multiplications and reductions on ideals in the maximal order of $K/\mathbb{F}_q(X)$) is determined by the square root of the length of the interval, i.e. $O(\sqrt{2L^2 - 1}) = O(L)$, so the overall complexity of the method is $O(\max\{T_E, L\})$, where T_E denotes the time for computing the approximation E. For small genus g, the Hasse-Weil bound yields running times of $O(q^{1/4})$ for $g = 1$ and $O(q^{3/4})$ for $g = 2$, while for $g \geq 3$, we obtain a running time of essentially $O(q^{(2g-1)/5})$ as q grows.

The above technique for finding E and L was first introduced in [41] where it was used to bound the class number of a hyperelliptic function field of odd characteristic and arbitrary genus. It was applied to generating class numbers of hyperelliptic curves using an optimized baby step-giant step search in [40] and a parallelized version of Pollard's kangaroo method in [39]; as mentioned earlier, the latter produced class numbers in excess of

10^{28} with computer technology dating from before 2002. Given the success in generating large numerical examples in the hyperelliptic scenario, the method seemed a promising candidate for generalization to cubic and other types of function fields. While the basic idea is the same for both the hyperelliptic and the cubic case, the actual realization of the bounds is significantly more complicated in the latter scenario. In fact, the method can be used for any function field extension $K/\mathbb{F}_q(X)$, but the derivation of explicit values for E and L becomes increasingly more complicated as the degree of the extension — and thus the number of possibilities for the splitting behavior in K of the places of $\mathbb{F}_q(X)$ — grows.

The emphasis and scope of this article is the development of precise formulae for the quantities E and L for a cubic extension $K/\mathbb{F}_q(X)$. In the case where the extension is purely cubic, i.e. $K = \mathbb{F}_q(X, Y)$ with $Y^3 \in \mathbb{F}_q[X]$ a cube-free polynomial, we also provide algorithms for explicitly calculating the relevant character that appears in these formulae. We defer the implementation and the actual computation of the divisor class number h, including the generation of numerical data, to a future paper.

We now proceed as follows. We begin by summarizing results on curves and (cubic) function fields in Section 2. Section 3 describes the idea of the algorithms. In Section 4, we develop results on the zeta function of a cubic function field and prove our main theorems. In Section 5, we apply these results to cubic function fields and discuss two choices for E and L, deriving explicit bounds for both choices as well. This section also includes a complexity analysis of our algorithms. In Section 6, we study the computation of the d^{th} power residue symbol that is needed in our algorithms. We finish our paper with open problems and future research topics.

2. Curves and Function Fields

2.1. **Notation and Definitions.** For a general overview of function fields, we refer to [32, 42]. Let K/k with $k = \mathbb{F}_q$ be an algebraic function field of genus g where q is a prime power, and let $X \in K$ be transcendental over k, so that $K/k(X)$ is a finite separable extension of degree m. We assume that $\gcd(q, m) = 1$. We can write $K = k(X, Y)$ with $F(X, Y) = 0$ where $F(X, Y)$ is an absolutely irreducible polynomial of degree m in Y with coefficients in $k[X]$, so $F(X, Y) = 0$ is an absolutely irreducible affine plane curve over k, and K is the function field of this curve over k.

We denote by $\mathcal{D}$ the group of divisors of K defined over k, by $\mathcal{D}^0$ the subgroup of $\mathcal{D}$ of divisors of degree 0 defined over k, and by $\mathcal{P}$ the subgroup of $\mathcal{D}^0$ of principal divisors defined over k. The factor group $\mathcal{D}^0/\mathcal{P}$ is called the *(degree* 0 *divisor) class group* of K and is isomorphic to the group $\mathcal{J}$ of k-rational points on the *Jacobian* of K. Its order $h = |\mathcal{J}|$ is said to be the *(degree 0 divisor) class number* of K.

Denote by ∞ the place at infinity of $k(X)$ (defined by the negative degree valuation), and let $S = \{\infty_1, \infty_2, \ldots, \infty_r\}$ be the set of places of K lying

above ∞. If ∞_i has degree f_i and ramification index e_i for $1 \leq i \leq r$, then $\sum_{i=1}^{r} e_i f_i = m$. Let $\mathcal{D}(S)$ be the group of divisors generated by the places in S, $\mathcal{D}^0(S) = \mathcal{D}^0 \cap \mathcal{D}(S)$, and $\mathcal{P}(S) = \mathcal{P} \cap \mathcal{D}(S)$.

The maximal order $\mathcal{O}_X$ of $K/k(X)$ is the integral closure of $k(X)$ in K. From Schmidt [36], we know that there is a one-to-one correspondence between the prime ideals in $\mathcal{O}_X$ and the finite places, also called *prime divisors*, of K/k, which extends naturally to a one-to-one correspondence between ideals of $\mathcal{O}_X$ and integral (i.e. effective) divisors of K defined over k. This correspondence preserves degrees, where the *degree* of a prime divisor $\mathfrak{P}$ of K/k is the field extension degree $\deg(\mathfrak{P}) = [\mathcal{O}_X/\mathfrak{P} : k]$, and this definition extends naturally to integral divisors of K/k via unique prime ideal/divisor factorization. The *absolute norm* of a divisor/ideal $\mathfrak{A}$ is $N(\mathfrak{A}) = q^{\deg(\mathfrak{A})}$, where $\deg(\mathfrak{A})$ is the degree of $\mathfrak{A}$.

The *($\mathcal{O}_X$)-ideal class group* $\mathrm{Cl}(\mathcal{O}_X)$ is the factor group of fractional $\mathcal{O}_X$-ideals modulo principal fractional $\mathcal{O}_X$-ideals. Its order, $h_X = |\mathrm{Cl}(\mathcal{O}_X)|$, is the *ideal class number* of $K/k(X)$. We have the following exact sequences (see Proposition 14.1, p. 243, of [32]):

$$(0) \;\to\; \mathbb{F}_q^* \;\to\; \mathcal{O}_X^* \;\to\; \mathcal{P}(S) \;\to\; (0), \tag{2.1}$$

$$(0) \;\to \mathcal{D}^0(S)/\mathcal{P}(S) \;\to\; \mathcal{J} \;\to\; \mathrm{Cl}(\mathcal{O}_X) \;\to\; \mathbb{Z}/f\mathbb{Z} \to\; (0), \tag{2.2}$$

where $\mathbb{F}_q^*$ is the multiplicative group of $\mathbb{F}_q$ and $\mathcal{O}_X^*$ is the group of units of $\mathcal{O}_X$. It follows from (2.1) that $\mathcal{O}_X^*$ is an Abelian group of rank $r-1$ (the *unit rank* of $K/k(X)$) whose torsion part is $\mathbb{F}_q^*$. The exact sequence (2.2) implies an important result originally due to Schmidt (see [36]):

$$f_X h = R_X h_X, \tag{2.3}$$

where $f_X = \gcd(f_1, f_2, \ldots, f_r)$ and $R_X = [\mathcal{D}^0(S) : \mathcal{P}(S)]$ is the *regulator* of $K/k(X)$.[1] If we can determine R_X and h_X, then (2.3) can be used to find h, the divisor class number of K. We can derive from the Hasse-Weil inequalities (Equation (4.3) in Section 4.1 below) that $h \sim q^g$, so h is exponential in the size of the field K.

2.2. **Cubic Function Fields.** Arbitrary cubic extensions were first studied in [34], while the arithmetic of purely cubic function fields was investigated in detail in [3],[35], [33], and [29]. Consider a (possibly singular) curve of the form $Y^3 - A(X)Y + B(X) = 0$ where $A, B \in \mathbb{F}_q[X], B \neq 0$; we may assume, without loss of generality, that for no polynomial $Q \in \mathbb{F}_q[X]$ can Q^2 divide A and Q^3 divide B. Here, we assume that $\mathbb{F}_q$ does not have characteristic 3. Then $K = \mathbb{F}_q(X, Y)$ is a cubic function field, and if $A = 0$, then $K/\mathbb{F}_q(X)$ is said to be *purely cubic*.

We first restrict ourselves to the purely cubic scenario. Since $B(X)$ is cube-free by our assumption, we generally write $-B(X) = D(X) =$

[1] We use Schmidt's definition of the regulator which is slightly different from Rosen's, see Lemma 14.3, p. 245, of [32], for the connection between the two quantities.

$G(X)H(X)^2$ with G, H square-free and coprime. Our curve then becomes $Y^3 - D(X) = 0$, which is singular if and only if H is non-constant, in which case the singular points are exactly the points $(a, 0)$ with $H(a) = 0$.

The splitting of the place at infinity of $\mathbb{F}_q(X)$ in K is determined by $q \pmod 3$ as well as the degree $\deg(D)$ and the leading coefficient $\operatorname{sgn}(D)$ of D (see Theorem 2.1 of [35]). If $\deg(D)$ is not a multiple of 3, then ∞ is totally ramified in K, so $r = f_X = 1$. It follows from (2.1) and (2.2) that $\mathcal{O}_X^* = \mathbb{F}_q^*$, $\mathrm{Cl}(\mathcal{O}_X) \cong \mathcal{J}$, $R_X = 1$, and $h = h_X$. We also note that the genus g of K is $g = \deg(GH) - 1$ in this case. If, on the other hand, $\deg(D)$ is divisible by 3, then the genus is $g = \deg(GH) - 2$, and we need to distinguish according to the congruence class of $q \pmod 3$ as follows. If $q \equiv -1 \pmod 3$, then ∞ splits into two places ∞_1 and ∞_2 of respective degrees 1 and 2, so $r = f_X = 1$ and $h = R_X h_X$. Here, $\mathcal{O}_X^* \cong \mathbb{F}_q^* \times \mathbb{Z}$, and the regulator R_X is usually nontrivial; in fact, $R = |v_2(\epsilon)| = |v_1(\epsilon)|/2$, where v_1 and v_2 are the two additive discrete valuations corresponding to ∞_1 and ∞_2, respectively, and ϵ is a *fundamental unit* of $K/k(X)$, i.e. a generator of $\mathcal{O}_X^*/\mathbb{F}_q^*$. Here, h_X is generally very small, while R_X tends to be very large.

Finally, if $\deg(D) \equiv 0 \pmod 3$ and $q \equiv 1 \pmod 3$, then $\mathbb{F}_q$ contains a nontrivial cube root of unity, so by Kummer theory, $K/\mathbb{F}_q(X)$ is a normal extension with Galois group $\mathbb{Z}/3\mathbb{Z}$. Here, we distinguish two more subcases. If $\operatorname{sgn}(D)$ is not a cube in $\mathbb{F}_q$, then ∞ is inert in K, so $\mathcal{O}_X^* = \mathbb{F}_q^*$, $R_X = 1$, $\mathcal{J}$ has index 3 in $\mathrm{Cl}(\mathcal{O}_X)$, and $h = h_X/3$. If, however, $\operatorname{sgn}(D)$ is a cube in $\mathbb{F}_q$, then ∞ splits completely in K, so $\mathcal{O}_X^*/\mathbb{F}_q^* \cong \mathbb{Z}^2$ and $h = R_X h_X$. If ϵ_1, ϵ_2 is a pair of fundamental units, i.e. $\mathcal{O}_X^* = \mathbb{F}_q^* \times \langle \epsilon_1, \epsilon_2 \rangle$, and v_1, v_2 are discrete valuations corresponding to any two of the three places at infinity of K, then

$$R_X = \left| \det \begin{pmatrix} v_1(\epsilon_1) & v_1(\epsilon_2) \\ v_2(\epsilon_1) & v_2(\epsilon_2) \end{pmatrix} \right|.$$

We point out that whenever ∞ is ramified in K, it is totally ramified. However, partial ramification (where ∞ splits into two places with respective ramification indices 1 and 2) does occur in arbitrary cubic extensions of $\mathbb{F}_q(X)$. We now return to the arbitrary setting.

Let $K = \mathbb{F}_q(X, Y)$ where $Y^3 - AY + B = 0$. If $\mathbb{F}_q$ has characteristic at least 5, then the splitting at infinity is described in [34] as follows. Set $D = 4A^3 - 27B^2$. If $\deg(D) \neq 2\deg(B)$ — this is exactly the case if either $3\deg(A) > 2\deg(B)$ or $3\deg(A) = 2\deg(B)$ and $4\operatorname{sgn}(A)^3 = 27\operatorname{sgn}(B)^2$ — then the place at infinity splits into a place of degree 1 and a second divisor $\mathfrak{A}$ whose splitting behavior is determined by the hyperelliptic extension $\mathbb{F}_q(X, Z)/\mathbb{F}_q(X)$ where $Z^2 - D(X) = 0$. That is, $\mathfrak{A}$ splits into two degree 1 places if $\deg(D)$ is even and $\operatorname{sgn}(D)$ is a square in $\mathbb{F}_q$, $\mathfrak{A}$ is prime of degree 2 if $\deg(D)$ is even and $\operatorname{sgn}(D)$ is a non-square in $\mathbb{F}_q$, and $\mathfrak{A}$ is the square of a prime divisor if $\deg(D)$ is odd. If on the other hand $\deg(D) = 2\deg(B)$, then there are two cases: if $3\deg(A) < 2\deg(B)$, then the place at infinity of $K/\mathbb{F}_q(X)$ splits exactly as it would in the purely cubic extension

$\mathbb{F}_q(X,U)/\mathbb{F}_q(X)$, where $U^3 - D(X) = 0$. If $3\deg(A) = 2\deg(B)$ and $4\,\mathrm{sgn}(A)^3 \neq 27\,\mathrm{sgn}(B)^2$, then $K/\mathbb{F}_q(X)$ is unramified, and the degrees f_i of the places at infinity of $K/\mathbb{F}_q(X)$ are the degrees (with respect to the indeterminate t) of the irreducible factors of the equation $t^3 - \mathrm{sgn}(A)\,t + \mathrm{sgn}(B) = 0$ over $\mathbb{F}_q$.

3. The Idea of the Algorithm

3.1. **Approximation Method.** The general idea of the approximation method is very simple. It is based on the following algorithm for a generic finite Abelian group G. Suppose we want to compute the group order h of G, and we are in possession of a method that determines an approximation of h, along with the accuracy of this approximation. Furthermore, we are able to perform arithmetic in G. Then our method for determining h can be described as follows:

1. Compute an approximation E of h and an integer L such that $|h - E| < L^2$. Thus, h lies in the open interval $]E - L^2, E + L^2[$.
2. Use all computable extra information such as information on h mod r for small primes r, or information on the distribution of h in the interval $]E - L^2, E + L^2[$.
3. Find h in the interval $]E - L^2, E + L^2[$ by Shanks' *baby step giant step* method or *Pollard's Kangaroo* method in $O(\sqrt{2L^2 - 1}) = O(L)$ operations.

The complexity of this method is $O(\max\{T_E, L\})$, where T_E is the time required for computing E. Our aim is therefore to find a very good approximation E of h and a sharp bound L^2 on $|h - E|$ such that $T_E \sim L$.

Now let K be a a finite algebraic extension of a rational function field $k(X)$ of finite characteristic with r places at infinity. If $r \leq 2$, then we expect that steps 2 and 3 of the method will work very similarly to the hyperelliptic scenario as described in [41] and [39]. In fact, for cubic fields, the explicit divisor and ideal arithmetic of [3] and [35] together with the infrastructure analysis of [33] will guarantee this.[2] As stated in Section 1, we limit our discussion here to step 1; a detailed treatment of steps 2 and 3 as well as numerical computations will be presented in a subsequent paper. We also mention that the above technique has never been applied to any fields with $r \geq 3$, including cubic extensions; clearly, this is a subject for future research.

3.2. **Truncated Euler Products.** As explained in the previous section, we want to find integers E and L such that $|h - E| < L^2$, i.e. $h \in]E - L^2, E + L^2[$. Since the size of this interval is $2L^2 - 1$, it is important that L be small. Suppose that h is given in the "truncated Euler product form," namely

$$h = E' \cdot e^B$$

[2]The sources cited here only consider purely cubic fields, but the ideas can be extended to arbitrary cubic extensions through the work of [34].

for some real numbers E' and B. Notice that $B = \log h - \log E'$. The real goal is to determine a sharp upper bound $\psi \in \mathbb{R}$ on $|B|$. We now assume that ψ is small, i.e. noticeably smaller than one.[3] Then $|e^B - 1| < e^\psi - 1$ and we put[4]

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

It follows that

$$|h - E| \le |h - E'| + |E' - E| \le E'|e^B - 1| + \tfrac{1}{2} \le E'(e^\psi - 1) + \tfrac{1}{2} \le L^2.$$

4. The Zeta Function

4.1. **Arbitrary Function Fields.** For a discussion of the following results, we refer to [32, 36, 42]. Let K/k be an algebraic function field of genus g over the finite field $k = \mathbb{F}_q$, and let $X \in K$ be transcendental over k, so that $K/k(X)$ is a finite separable extension of degree m. 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 and $\Re(s)$ denotes the real part of the complex variable s. It is customary to put $u = q^{-s}$ and define $\zeta(s, K) = Z(u, K)$. For instance, the rational function field $k(X)$ has the zeta function $Z(u, k(X)) = (1 - u)^{-1}(1 - qu)^{-1}$. Naturally, there exists an Euler product formula for $Z(u, K)$:

$$Z(u, K) = \prod_{\mathfrak{P}} \frac{1}{1 - u^{\deg(\mathfrak{P})}} = \prod_{\nu=1}^{\infty} (1 - u^\nu)^{-B_\nu},$$

where $\mathfrak{P}$ ranges over all prime divisors of K and B_ν denotes the number of prime divisors of K of degree ν. It is well-known that the zeta function of K has an analytic continuation to all of $\mathbb{C}$. In fact, $Z(u, K)$ is a rational function in u:

$$Z(u, K) = \frac{\prod_{i=1}^{2g} (1 - \alpha_i u)}{(1 - u)\,(1 - qu)} = Z(u, k(X))L(u, K), \tag{4.1}$$

where the L-polynomial $L(u, K) = \prod_{i=1}^{2g}(1 - \alpha_i u)$ satisfies the functional equation $L(u, K) = q^g u^{2g} L(1/qu, K)$. A key fact is that $h = L(1, K)$, and

[3] This is guaranteed in our application to cubic function fields over finite fields of large characteristic.

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

thus

$$h = L(1, K) = \prod_{i=1}^{2g} (1 - \alpha_i) = q^g L(1/q, K). \tag{4.2}$$

The Theorem of Hasse-Weil (see for example Theorem V.2.1, p. 169, of [42]) implies that $|\alpha_i| = \sqrt{q}$ for $i = 1, 2, \ldots, 2g$, and we obtain the bounds

$$\left(\sqrt{q} - 1\right)^{2g} \leq h \leq \left(\sqrt{q} + 1\right)^{2g}. \tag{4.3}$$

We let N_ν denote the number of prime divisors of degree one in the constant field extension $K_\nu := K\mathbb{F}_{q^\nu}$.[5] Then

$$N_\nu = \sum_{d|\nu} dB_\nu = q^\nu + 1 - \sum_{\nu=1}^{2g} \alpha_i^\nu,$$

and the zeta function is given by the exponential sum

$$Z(u, K) = \exp\left(\sum_{\nu=1}^{\infty} N_\nu \frac{u^\nu}{\nu}\right).$$

Due to the one-to-one correspondence between finite prime divisors (places) of K and prime ideals in $\mathcal{O}_X$, we can split up the zeta function into an infinite part and a finite part as follows.

$$Z(u, K) = Z_\infty(u, K) \cdot Z_X(u, K), \tag{4.4}$$

where[6]

$$Z_\infty(u, K) = \prod_{i=1}^{r} \frac{1}{(1 - u^{f_i})} \tag{4.5}$$

and

$$Z_X(u, K) = \prod_{\mathfrak{p}} \frac{1}{(1 - u^{\deg(\mathfrak{p})})} = \prod_{P} \prod_{\mathfrak{p}|P} \frac{1}{(1 - u^{\deg(\mathfrak{p})})}. \tag{4.6}$$

In the first product of (4.6), $\mathfrak{p}$ ranges over all prime ideals of K with respect to $\mathcal{O}_X$. In the second product, P runs through all monic irreducible polynomials in $k[X]$ and $\mathfrak{p}$ runs through all prime ideals lying over the principal ideal (P) in $\mathcal{O}_X$.

4.2. **Cubic Function Fields.** Let K be a cubic function field of genus g over the finite field $k = \mathbb{F}_q$ of characteristic not equal to 3. This means $[K : k(X)] = 3$, $\sum_{i=1}^{r} e_i f_i = 3$, and we have $r \leq 3$ infinite places.

[5] In geometric terms, let C denote the absolutely irreducible, non-singular curve defined over $\mathbb{F}_q$ associated to K. Then $N_\nu = \#C(\mathbb{F}_{q^\nu})$, i.e.the number of $\mathbb{F}_{q^\nu}$-rational points on C.

[6] Recall that the infinite place ∞ of $k(X)$ splits as $\infty = \infty_1^{e_1} \cdots \infty_r^{e_r}$ and ∞_i has degree f_i.

4.2.1. *Infinite Part.* We first investigate $Z_\infty(u,K)$ for any cubic function field and then discuss the special case of purely cubic function fields. In particular, we want to show that $Z_\infty(u,K)$ contains the factor $1/(1-u)$. Let ω_3 denote a fixed primitive complex cube root of unity, i.e. $\omega_3^2+\omega_3+1=0$.

Theorem 4.1. *Let $K/\mathbb{F}_q$ be a cubic function field. Then there exist $x_1,x_2 \in \{0,1,-1,\omega_3,\omega_3^2\}$ and $s_1,s_2 \in \{0,1,-1,-2\}$ such that the infinite part of the zeta function satisfies*

$$Z_\infty(u,K)=\frac{1}{(1-u)}\frac{1}{(1-x_1u)}\frac{1}{(1-x_2u)}=\frac{1}{(1-u)}\frac{1}{(1+s_1u+s_2u^2)}.$$

In particular,

$$(x_1,x_2,s_1,s_2)=\begin{cases}(0,0,0,0) & \text{if } \infty=\infty_1^3,\\ (\omega_3,\omega_3^2,1,1) & \text{if } \infty=\infty_1,\\ (1,-1,0,-1) & \text{if } \infty=\infty_1\infty_2,\\ (1,0,-1,0) & \text{if } \infty=\infty_1\infty_2^2,\\ (1,1,-2,1) & \text{if } \infty=\infty_1\infty_2\infty_3.\end{cases}$$

Proof. It is clear that the 5 cases listed above represent all possible splittings of ∞. Applying (4.5) in each case yields the desired result. □

Note that x_1+x_2+1 is exactly the number of degree one places of K lying above ∞. Since $\omega_3^2+\omega_3+1=0$, we have, for arbitrary $n\in\mathbb{N}$, that $\omega_3^n+\omega_3^{2n}=2$, if $3\mid n$, and $\omega_3^n+\omega_3^{2n}=-1$ otherwise. We therefore obtain

Corollary 4.2. *In the situation of Theorem 4.1, we have for $n\in\mathbb{N}$:*

$$x_1^n+x_2^n=\begin{cases}-1 & \text{if } \infty=\infty_1 \text{ and } 3\nmid n,\\ 0 & \text{if } \infty=\infty_1^3 \text{ or if } \infty=\infty_1\infty_2 \text{ and } n \text{ odd},\\ 1 & \text{if } \infty=\infty_1\infty_2^2,\\ 2 & \text{otherwise.}\end{cases}$$

In particular, it follows that $|x_1^n+x_2^n|\le 2$ for all $n\in\mathbb{N}$.

As an example, we demonstrate how to compute these quantities in the special case of purely cubic function fields. Let $K=\mathbb{F}_q(X,Y)$ be a purely cubic function field of characteristic not equal to 3 where $Y^3=D=GH^2$ with $G,H\in\mathbb{F}_q[X]$ square-free and coprime. Using the results of Section 2.2 and [35], we derive the algorithm below that determines the splitting in K of the infinite place of $\mathbb{F}_q(X)$ and outputs x_1 and x_2 as given in Theorem 4.1. Optionally, it could also output s_1 and s_2.

Algorithm. ($Z_\infty(u,K)$ in purely cubic function fields)
Input: $q=p^l$ where $p\neq 3$ prime, and $D\in\mathbb{F}_q[X]$ cube-free such that $K=\mathbb{F}_q(X)(\sqrt[3]{D})$.
Output: (x_1,x_2) with $x_1,x_2\in\{0,1,-1,\omega_3,\omega_3^2\}$ as in Theorem 4.1.

1) If $3\nmid \deg(D)$, then $\infty=\infty_1^3$, return $(x_1,x_2)=(0,0)$.
2) If $3\mid \deg(D)$, then

(a) If $q \equiv -1 \pmod 3$, then $\infty = \infty_1\infty_2$, return $(x_1, x_2) = (1, -1)$.
(b) If $q \equiv 1 \pmod 3$, then
  (i) If $\operatorname{sgn}(D)$ is not a cube in $\mathbb{F}_q$, then $\infty = \infty_1$, return $(x_1, x_2) = (\omega_3, \omega_3^2)$.
  (ii) If $\operatorname{sgn}(D)$ is a cube in $\mathbb{F}_q$, then $\infty = \infty_1\infty_2\infty_3$, return $(x_1, x_2) = (1, 1)$.

The correctness of this algorithm follows from Section 2.2, and the most expensive step is to determine whether $\operatorname{sgn}(D)$ is a cube or not. This can be accomplished by evaluating the cubic power residue symbol $(\operatorname{sgn}(D)/q)_3$ which equals 1 if and only if $\operatorname{sgn}(D)$ is a cube in $\mathbb{F}_q$.

Using the results summarized at the end of Section 2.2, the algorithm can easily be extended to arbitrary cubic function fields $K = \mathbb{F}_q(X, Y)$ with $Y^3 - AY + B = 0$ of characteristic at least 5. This requires the evaluation of either the cubic or the quadratic power residue symbol of $\operatorname{sgn}(D)$ where $D = 4A^3 - 27B^2$, or possibly determining the number of roots in $\mathbb{F}_q$ of the equation $t^3 - \operatorname{sgn}(A)\, t + \operatorname{sgn}(B) = 0$.

4.2.2. *Finite Part.* We now investigate the finite part $Z_X(u, K)$ of the zeta function of a cubic function field K over the finite field $k = \mathbb{F}_q$, where q is not a power of 3. For any monic irreducible polynomial $P \in \mathbb{F}_q[X]$, we wish to determine how the principal ideal (P) in $\mathbb{F}_q[X]$ splits in $\mathcal{O}_X$ and show that $Z_X(u, K)$ contains the factor $1/(1 - qu)$. Once again, there are 5 distinct splitting possibilities of (P) in $\mathcal{O}_X$, so using (4.6) in each case, we can derive the following results.

Theorem 4.4. *Let $K/\mathbb{F}_q$ be a cubic function field. For any monic irreducible polynomial $P \in \mathbb{F}_q[X]$ there exist $z_1(P), z_2(P) \in \{0, 1, -1, \omega_3, \omega_3^2\}$ and $a_1(P)$, $a_2(P) \in \{0, 1, -1, -2\}$ such that*

$$\prod_{\mathfrak{p}|P} \frac{1}{(1 - u^{\deg(\mathfrak{p})})} = \frac{1}{(1 - u^{\deg(P)})} \frac{1}{(1 - z_1(P)u^{\deg(P)})} \frac{1}{(1 - z_2(P)u^{\deg(P)})}$$
$$= \frac{1}{(1 - u^{\deg(P)})} \frac{1}{(1 + a_1(P)u^{\deg(P)} + a_2(P)u^{2\deg(P)})}.$$

In particular,

$$(z_1(P), z_2(P), a_1(P), a_2(P)) = \begin{cases} (0, 0, 0, 0) & \text{if } (P) = \mathfrak{p}_1^3, \\ (\omega_3, \omega_3^2, 1, 1) & \text{if } (P) = \mathfrak{p}_1, \\ (1, -1, 0, -1) & \text{if } (P) = \mathfrak{p}_1\mathfrak{p}_2, \\ (1, 0, -1, 0) & \text{if } (P) = \mathfrak{p}_1\mathfrak{p}_2^2, \\ (1, 1, -2, 1) & \text{if } (P) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3. \end{cases}$$

Note again that $z_1(P) + z_2(P) + 1$ is exactly the number of degree one places of K lying above P.

Corollary 4.5. *In the situation of Theorem 4.4, we have for $n \in \mathbb{N}$:*

$$z_1(P)^n + z_2(P)^n = \begin{cases} -1 & \text{if } (P) = \mathfrak{p}_1 \text{ and } 3 \nmid n, \\ 0 & \text{if } (P) = \mathfrak{p}_1^3 \text{ or if } (P) = \mathfrak{p}_1\mathfrak{p}_2 \text{ and } n \text{ odd}, \\ 1 & \text{if } (P) = \mathfrak{p}_1\mathfrak{p}_2^2, \\ 2 & \text{otherwise.} \end{cases}$$

In particular, it follows that $|z_1(P)^n + z_2(P)^n| \leq 2$ for all $n \in \mathbb{N}$.

Putting

$$f(P,u) = \frac{1}{(1 - z_1(P)u^{\deg(P)})} \frac{1}{(1 - z_2(P)u^{\deg(P)})} \tag{4.7}$$

and using the well-known formula

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

we obtain the following important corollary.

Corollary 4.6. *In the situation of Theorem 4.4, we have*

$$Z_X(u,K) = \frac{1}{(1-qu)} \prod_P f(P,u) = \frac{1}{(1-qu)} \prod_{\nu=1}^{\infty} \prod_{\deg(P)=\nu} f(P,u).$$

As an example, we provide an algorithm for finding $z_1(P)$ and $z_2(P)$ (and optionally, $a_1(P)$ and $a_2(P)$) for any monic irreducible polynomial $P \in \mathbb{F}_q[X]$ in the case where $K/\mathbb{F}_q(X)$ is a purely cubic extension of characteristic different from 3. It uses the cubic power residue symbol $[D/P]_3$ as defined in Section 6.

Algorithm. (Splitting of primes in purely cubic function fields)
Input: $q = p^l$ where $p \neq 3$ prime, $D \in \mathbb{F}_q[X]$ cube-free such that $K = \mathbb{F}_q(X)(\sqrt[3]{D})$, and a monic irreducible polynomial $P \in \mathbb{F}_q[X]$.
Output: $(z_1(P), z_2(P))$ with $z_1(P), z_2(P) \in \{0, 1, -1, \omega_3, \omega_3^2\}$ as in Theorem 4.4.

1) If $q^{\deg(P)} \equiv -1 \pmod 3$, then
   (a) If $P \mid GH$, then $(P) = \mathfrak{p}_1^3$, return $(z_1(P), z_2(P)) = (0,0)$.
   (b) If $P \nmid GH$, then $(P) = \mathfrak{p}_1\mathfrak{p}_2$, return $(z_1(P), z_2(P)) = (1,-1)$.
2) If $q^{\deg(P)} \equiv 1 \pmod 3$, then compute

$$\chi(P) = \left[\frac{D}{P}\right]_3.$$

If $[D/P]_3 = 1$, return $(z_1(P), z_2(P)) = (1,1)$,
else return $(z_1(P), z_2(P)) = (\omega_3, \omega_3^2)$.

Note that the case $(P) = \mathfrak{p}_1\mathfrak{p}_2^2$ does not occur for purely cubic function fields with $q \neq 3^l$. The correctness of the above algorithm follows from Theorem 3.1 of [33], and the complexity is dominated by the computation

of $\gcd(D, P)$ in the case where $q^{\deg(P)} \equiv -1 \pmod 3$ and the evaluation of $[D/P]_3$ in the case where $q^{\deg(P)} \equiv 1 \pmod 3$. Algorithm 6.2 in Section 6 shows that both scenarios yield essentially the same running time.

4.3. **Main Theorems in Cubic Function Fields.** We now establish connections between the quantities $x_1, x_2, z_1(P), z_2(P)$, and develop estimates that will eventually lead to a good approximation of the class number of a cubic function field. Let K be a cubic function fields of genus g over the finite field $k = \mathbb{F}_q$ where q is not a power of 3. By (4.1), (4.4), and the results of Theorem 4.1 and Corollary 4.6, we have

$$\prod_{i=1}^{2g}(1-\alpha_i u) = \frac{Z(u,K)}{Z(u,k(X))} = \frac{1}{(1-x_1u)}\frac{1}{(1-x_2u)}\prod_P f(P,u), \tag{4.8}$$

or, equivalently,

$$(1-x_1u)(1-x_2u)\prod_{i=1}^{2g}(1-\alpha_i u) = \prod_{\nu=1}^{\infty}\prod_{\deg(P)=\nu}\frac{1}{(1-z_1(P)u^\nu)}\frac{1}{(1-z_2(P)u^\nu)}. \tag{4.9}$$

Theorem 4.8. *Let K be a cubic function field of genus g over the finite field $k = \mathbb{F}_q$ of characteristic not equal to 3. Furthermore, let x_1, x_2, be as in Theorem 4.1, and let $z_1(P)$, and $z_2(P)$ be as in Theorem 4.4 for any monic irreducible polynomial $P \in \mathbb{F}_q[X]$. Then we have for all $n \in \mathbb{N}$:*

$$\sum_{\nu|n}\nu\sum_{\deg(P)=\nu}(z_1(P)^{n/\nu} + z_2(P)^{n/\nu}) = -(x_1^n + x_2^n) - \sum_{i=1}^{2g}\alpha_i^n,$$

where $\alpha_1, \ldots, \alpha_{2g}$ denote the reciprocals of the roots of $Z(u, K)$.

Proof. By taking formal logarithms on both sides of (4.9) and using the formal identity $-\log(1-z) = \sum_{n=1}^{\infty} z^n/n$, we obtain

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{u^n}{n}\left(-x_1^n - x_2^n - \sum_{i=1}^{2g}\alpha_i^n\right) &= \sum_{\nu=1}^{\infty}\sum_{\deg(P)=\nu}\sum_{n=1}^{\infty}(z_1(P)^n + z_2(P)^n)\frac{u^{n\nu}}{n} \\ &= \sum_{n=1}^{\infty}\frac{u^n}{n}\sum_{\nu|n}\nu\sum_{\deg(P)=\nu}(z_1(P)^{n/\nu} + z_2(P)^{n/\nu}),\end{aligned}$$

where ν runs through all positive divisors of n. Comparing the coefficients of u^n for any $n \geq 1$ yields

$$-x_1^n - x_2^n - \sum_{i=1}^{2g}\alpha_i^n = \sum_{\nu|n}\nu\sum_{\deg(P)=\nu}(z_1(P)^{n/\nu} + z_2(P)^{n/\nu}),$$

and the statement follows. □

We now put

$$S_\nu(j) = \sum_{\deg(P)=\nu} (z_1(P)^j + z_2(P)^j) \quad (\nu, j \in \mathbb{N}).$$

Then Theorem 4.8 reads[7]

$$\sum_{\nu|n} \nu\, S_\nu\,(n/\nu) = -(x_1^n + x_2^n) - \sum_{i=1}^{2g} \alpha_i^n \quad (n \in \mathbb{N}). \tag{4.10}$$

For instance, if the infinite place ∞ of $k(X)$ totally ramifies in K, i.e. $\infty = \infty_1^3$, then by Corollary 4.2,

$$\sum_{\nu|n} \nu\, S_\nu\,(n/\nu) = -\sum_{i=1}^{2g} \alpha_i^n \quad (n \in \mathbb{N}).$$

Corollary 4.9. *For all $n \in \mathbb{N}$:*

$$\Big| \sum_{\nu|n} \nu\, S_\nu\,(n/\nu) \Big| \le |x_1^n + x_2^n| + 2gq^{n/2} \le 2 + 2gq^{n/2}.$$

Proof. This follows from Theorem 4.8 by using $|\alpha_i| = \sqrt{q}$ for $i = 1, 2, \ldots, 2g$. The second inequality can be obtained from the bound in Corollary 4.2. □

It will be essential to find good bounds on $nS_n(1)$. We will use the following.

Corollary 4.10. *For all $n \in \mathbb{N}$:*

$$n\, S_n\,(1) = -(x_1^n + x_2^n) - \sum_{i=1}^{2g} \alpha_i^n - \sum_{\substack{\nu|n \\ \nu \ne n}} \nu\, S_\nu\,(n/\nu)\,.$$

For example, consider purely cubic function fields. If $q \equiv -1 \pmod 3$ and n is odd, we know much more.

Corollary 4.11. *Let K be a purely cubic function field of genus g over the finite field $k = \mathbb{F}_q$ of characteristic not equal to 3. If $q \equiv -1 \pmod 3$ and n is odd, then $S_\nu\,(n/\nu) = 0$ for all divisors ν of n, and*

$$\sum_{i=1}^{2g} \alpha_i^n = -(x_1^n + x_2^n).$$

In particular, we have $N_n = q^n + 1 + x_1^n + x_2^n$.

[7] In geometric terms, if C again denotes the absolutely irreducible, non-singular curve over $\mathbb{F}_q$ associated to K, then the quantity $\nu S_\nu(n/\nu)$ is the difference between the number of points on C defined over $\mathbb{F}_{q^\nu}$ but contained in no subfield thereof and the number of elements in $\mathbb{F}_{q^\nu}$ but contained in no subfield thereof. Thus, we have $\sum_{\nu|n} \nu S_\nu(n/\nu) = N_n - (x_1^n + x_2^n + 1) - q^n$, where N_n is the number of $\mathbb{F}_{q^n}$-rational points on C and $x_1^n + x_2^n + 1$ is the number of points at infinity on C over $\mathbb{F}_{q^n}$. Then Corollary 4.9 is simply the Hasse-Weil bound with the information about the infinite places incorporated.

Proof. Let ν be a divisor of n. Since n is odd, ν and n/ν are odd. Let $P \in \mathbb{F}_q[X]$ be any monic irreducible polynomial of degree $\deg(P) = \nu$. From Algorithm 4.7, we see that there are only two possible cases. If $P \mid GH$, then $z_1(P) = z_2(P) = 0$. If $P \nmid GH$, then $z_1(P) = 1 = -z_2(P)$. In both cases, we have

$$z_1(P)^{n/\nu} + z_2(P)^{n/\nu} = 0.$$

Since P was arbitrary, $S_\nu(n/\nu) = 0$ and therefore

$$\sum_{\nu \mid n} \nu\, S_\nu(n/\nu) = 0.$$

The result now follows from (4.10). □

Similarly, we derive results on the class number h. By (4.2), (4.7) (4.8) and (4.9), the analog of the analytic class number formula for cubic function fields reads

$$h = L(1,K) = q^g L(1/q,K) = \frac{q^{g+2}}{(q-x_1)(q-x_2)} \prod_P f(P,1/q) \tag{4.11}$$

$$= \frac{q^{g+2}}{(q-x_1)(q-x_2)} \prod_{\nu=1}^{\infty} \prod_{\deg(P)=\nu} \frac{q^{2\nu}}{(q^\nu - z_1(P))(q^\nu - z_2(P))}. \tag{4.12}$$

In order to proceed similarly to Theorem 4.8, we have to ascertain that the power series expansion of the logarithm of (4.12) is defined.[8]This is easily seen since for any monic irreducible polynomial P of degree ν and $i = 1, 2$, we have

$$\log\left(\frac{q^\nu}{q^\nu - z_i(P)}\right) = -\log(1 - z_i(P)q^{-\nu}),$$

and obviously $|z_i(P)q^{-\nu}| < 1$.

Theorem 4.12. *Let K be a cubic function field of genus g over the finite field $k = \mathbb{F}_q$ of characteristic not equal to 3. Then we have for all $n \in \mathbb{N}$:*

$$\log(h) = A(K) + \sum_{n=1}^{\infty} \frac{1}{nq^n} \sum_{\nu \mid n} \nu\, S_\nu(n/\nu),$$

where $A(K) = (g+2)\log q - \log(q^2 + s_1 q + s_2)$ with s_1, s_2 as in Theorem 4.1.

Proof. Let $z_1(P)$, and $z_2(P)$ be as in Theorem 4.4 for any monic irreducible polynomial $P \in \mathbb{F}_q[X]$. We apply the power series expansion of the logarithm

[8]In the proof of Theorem 4.8, we used the formal logarithm and applied the formal identity $-\log(1-z) = \sum_{n=1}^{\infty} z^n/n$. Here, we require $|z| < 1$.

to (4.12). As in the proof of Theorem 4.8, we obtain

$$\begin{aligned}\log(h) &= \log\left(\frac{q^{g+2}}{(q-x_1)(q-x_2)}\right) + \sum_{\nu=1}^{\infty}\sum_{\deg(P)=\nu}\sum_{n=1}^{\infty}(z_1(P)^n + z_2(P)^n)\frac{1}{nq^{n\nu}}\\ &= A(K) + \sum_{n=1}^{\infty}\frac{1}{nq^n}\sum_{\nu|n}\nu\sum_{\deg(P)=\nu}(z_1(P)^{n/\nu} + z_2(P)^{n/\nu})\\ &= A(K) + \sum_{n=1}^{\infty}\frac{1}{nq^n}\sum_{\nu|n}\nu\, S_\nu(n/\nu),\end{aligned}$$

by definition of $S_\nu(n/\nu)$. Note that $(q-x_1)(q-x_2) = q^2 + s_1 q + s_2$. □

5. Explicit Bounds for Cubic Function Fields

We follow the main idea of Section 3.2. For $g = 1$ and 2, it turns out that the Hasse-Weil bounds (4.3) are best. Therefore, we focus on cubic function fields of genus $g \geq 3$.

5.1. **A First Estimate.** The first approximation is an immediate consequence of Theorem 4.12 and Corollary 4.9. It corresponds to the first choice of approximation in [38, Theorem 4.1] and to similar non-computational expositions in [21]. It is easier to analyze than the bound given in Section 5.2 below, but yields a slightly worse approximation.

For any $\lambda \in \mathbb{N}$, we simply put

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

$$B_1(\lambda, K) := \sum_{n=\lambda+1}^{\infty}\frac{1}{nq^n}\sum_{\nu|n}\nu\, S_\nu(n/\nu).$$

By Theorem 4.12, we have $\log h = B_1(\lambda, K) + \log E_1'(\lambda, K)$, or, equivalently,

$$h = E_1'(\lambda, K)\; e^{B_1(\lambda,K)},$$

as required in Section 3.2. A bound on $|B_1(\lambda, K)|$ is given by Corollary 4.9:

$$\begin{aligned}|B_1(\lambda, K)| &\leq \sum_{n=\lambda+1}^{\infty}\frac{1}{nq^n}\Big|\sum_{\nu|n}\nu\, S_\nu(n/\nu)\Big|\\ &\leq 2g\sum_{n=\lambda+1}^{\infty}\frac{1}{nq^{\frac{n}{2}}} + 2\sum_{n=\lambda+1}^{\infty}\frac{1}{nq^n} =: \psi_1(\lambda, K).\end{aligned}$$

First, note that $\psi_1(\lambda, K)$ can be computed by

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

Furthermore, we estimate

$$\psi_1(\lambda,K) \le \frac{2g}{\lambda+1}q^{-\frac{(\lambda+1)}{2}} + \frac{2g}{\lambda+2}\sum_{n=\lambda+2}^{\infty}\frac{1}{q^{\frac{n}{2}}} + \frac{2}{\lambda+1}\sum_{n=\lambda+1}^{\infty}\frac{1}{q^n}$$
$$= \frac{2g}{\lambda+1}q^{-\frac{(\lambda+1)}{2}} + O\left(\frac{g}{\lambda}q^{-\frac{(\lambda+2)}{2}}\right).$$

Finally, we let $E_1(\lambda,K) := \operatorname{round}(E_1'(\lambda,K))$ and

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

Then we have proved the following theorem.

Theorem 5.1. *For any $\lambda \in \mathbb{N}$, we have $|h - E_1(\lambda,K)| < L_1^2(\lambda,K)$.*

For the overall complexity of finding the class number h, we need to know the size of E_1.

Theorem 5.2. *For any $\lambda \in \mathbb{N}$, we have*

$$E_1'(\lambda,K) < \left(\frac{q^{g+2}}{q^2+s_1q+s_2}\right)\left(\frac{\sqrt{q}}{\sqrt{q}-1}\right)^{2g}\left(\frac{q}{q-1}\right)^2.$$

Proof. Proceeding as above, we use the definition of E_1' and Corollary 4.9 to obtain

$$\log E_1'(\lambda,K) \le A(K) + 2g\sum_{n=1}^{\lambda}\frac{1}{nq^{\frac{n}{2}}} + 2\sum_{n=1}^{\lambda}\frac{1}{nq^n}$$
$$< A(K) + 2g\log\left(\frac{\sqrt{q}}{\sqrt{q}-1}\right) + 2\log\left(\frac{q}{q-1}\right).$$

This is the assertion since $A(K) = (g+2)\log q - \log(q^2+s_1q+s_2)$. □

If g is sufficiently small and $q \to \infty$, it follows that $E_1(\lambda,K) = O(q^g)$. In particular, if $\psi_1(\lambda,K) < 1$, then $e^{\psi_1(\lambda,K)} - 1 \sim \psi_1(\lambda,K)$, and thus $L_1(\lambda,K) = O(q^{g/2-(\lambda+1)/4})$.

5.2. **A Second Estimate.** The second possibility is to proceed as in [41, 38]. For any $\lambda \in \mathbb{N}$, we define $E_2' = E_2'(\lambda,K)$ and $B_2 = B_2(\lambda,K)$ by

$$E_2'(\lambda,K) := \frac{q^{g+2}}{(q-x_1)(q-x_2)}\prod_{\substack{P\\ \deg(P)=\nu\le\lambda}}\frac{q^{2\nu}}{(q^\nu - z_1(P))(q^\nu - z_2(P))}, \tag{5.1}$$

$$B_2(\lambda,K) := \log\prod_{\substack{P\\ \deg(P)=\nu>\lambda}}\frac{q^{2\nu}}{(q^\nu - z_1(P))(q^\nu - z_2(P))}$$

$$= \sum_{n=\lambda+1}^{\infty}\frac{1}{nq^n}\sum_{\substack{\nu\mid n\\ \nu>\lambda}}\nu\, S_\nu(n/\nu). \tag{5.2}$$

Note that $E_2'(\lambda, K)$ contains more information about h than $E_1'(\lambda, K)$, since all computable information for polynomials up to degree λ is included in $E_2'(\lambda, K)$. For hyperelliptic curves, this estimate yielded faster computational results than the first estimate. We have

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

and by (4.11) and Theorem 4.12, we have

$$h = E_2'(\lambda, K)\ e^{B_2(\lambda,K)}.$$

If we put $E_2(\lambda, K) := \mathrm{round}(E_2'(\lambda, K))$, then $E_2(\lambda, K)$ is an approximation of h. As pointed out in Section 3.2, we need to find a sharp upper bound on $|B_2(\lambda, K)|$. From (5.2), we see that

$$B_2(\lambda, K) = \frac{S_{\lambda+1}(1)}{q^{\lambda+1}} + \sum_{n=\lambda+2}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu\, S_\nu(n/\nu). \tag{5.3}$$

The dominant term of $B_2(\lambda, K)$ is $S_{\lambda+1}(1)/q^{\lambda+1}$. In order to find sharp upper bounds on $|B_2(\lambda, K)|$, we need to investigate $S_\nu(j)$, particularly $S_\nu(1)$.

We denote by I_ν the number of monic prime polynomials of degree ν. Then νI_ν is the number of elements in $\mathbb{F}_{q^\nu}$ but contained in no subfield thereof, and it is well-known that $\sum_{\nu|n} \nu I_\nu = q^n$ for all $n \in \mathbb{N}$. Also, Möbius inversion[9] implies that

$$nI_n = \sum_{\nu|n} \mu(n/\nu) q^\nu = q^n + \sum_{\substack{\nu|n \\ \nu\ne n}} \mu(n/\nu) q^\nu \quad (n \in \mathbb{N})\ . \tag{5.4}$$

Lemma 5.3. *For $\nu, j, l \in \mathbb{N}$, we have*

a) $S_\nu(j + 6l) = S_\nu(j)$.

b) *If $3 \nmid j$, then* $S_\nu(j) = \begin{cases} S_\nu(1) & \text{if } j \text{ odd}, \\ S_\nu(2) & \text{if } j \text{ even}. \end{cases}$

c) $|S_\nu(j)| \le 2I_\nu$.

Proof. It is easy to see that $z_i(P)^{j+6l} = z_1(P)$ for $i = 1, 2$, and if $3 \nmid j$, then $z_1(P)^j + z_2(P)^j = z_1(P) + z_2(P)$ if j is odd, and $z_1(P)^j + z_2(P)^j = z_1(P)^2 + z_2(P)^2$ if j is even. Parts a) and b) now follow from the definition of $S_\nu(j)$. Furthermore, $|z_1(P)^j + z_2(P)^j| \le 2$ by Corollary 4.5, so $S_\nu(j) \le \sum_{\deg(P)=\nu} 2 = 2I_\nu$. □

Since $z_1(P)^6 = z_2(P)^6 = 1$ if the ideal (P) is unramified, it is clear that $S_\nu(6)$ and $2I_\nu$ agree except for the irreducible polynomials for which the

[9] If f is an arithmetic function and $F(n) = \sum_{\nu|n} f(\nu)$ for $n \in \mathbb{N}$, then $f(n) = \sum_{\nu|n} \mu(n/\nu) F(\nu)$ where μ denotes the Möbius function.

ideal (P) ramifies. Next, we want to bound $nS_n(1)$. By Corollary 4.10, we need to bound $\sum_{\substack{\nu|n \\ \nu\neq n}} \nu\, S_\nu\,(n/\nu)$.

Lemma 5.4. *For $n \in \mathbb{N}$,*

$$n|S_n(1)| \le 2gq^{\frac{n}{2}} + 2 + \frac{2q}{(q-1)} \begin{cases} (q^{\frac{n}{2}}-1) & \text{if } n \text{ even} \\ (q^{\frac{n}{3}}-1) & \text{if } n \text{ odd} \end{cases} < (2g+2)q^{\frac{n}{2}} \frac{q}{(q-1)}.$$

Proof. Lemma 5.3 c) and (5.4) yield

$$\begin{aligned} \Big|\sum_{\substack{\nu|n \\ \nu\neq n}} \nu\, S_\nu\,(n/\nu)\Big| \;&\le\; \sum_{\substack{\nu|n \\ \nu\neq n}} \nu|\, S_\nu\,(n/\nu)\,| \;\le\; 2\sum_{\substack{\nu|n \\ \nu\neq n}} \nu I_\nu = 2\Big(\sum_{\nu|n} \nu I_\nu - nI_n\Big) \\ &= 2(q^n - nI_n) = -2\sum_{\substack{\nu|n \\ \nu\neq n}} \mu(n/\nu) q^\nu \le 2\sum_{\substack{\nu|n \\ \nu\neq n}} q^\nu \\ &\le \begin{cases} 2\sum_{\nu=1}^{n/2} q^\nu \le 2(q^{\frac{n}{2}}-1)q/(q-1) & \text{if } n \text{ even}, \\ 2\sum_{\nu=1}^{\lfloor n/3 \rfloor} q^\nu \le 2(q^{\frac{n}{3}}-1)q/(q-1) & \text{if } n \text{ odd}. \end{cases} \end{aligned}$$

By Corollary 4.10, we get

$$n|S_n(1)| \le |x_1^n + x_2^n| + 2gq^{\frac{n}{2}} + \Big|\sum_{\substack{\nu|n \\ \nu\neq n}} \nu\, S_\nu\,(n/\nu)\Big|$$

since $|\alpha_i| = \sqrt{q}$ for $i = 1, 2, \ldots, 2g$. The first estimate then follows from the above and Corollary 4.2. For the second inequality, we note that

$$2 + 2gq^{\frac{n}{2}} + 2\frac{(q^{\frac{n}{2}}-1)q}{(q-1)} < 2 + (2g+2)q^{\frac{n}{2}}\frac{q}{(q-1)} - \frac{2q}{(q-1)} \;\;.$$

□

We will use the first bound of the lemma in implementations and the second bound for estimating the tail of the truncated Euler product. Also notice that another (in general less sharp) bound would be $n|S_n(1)| < (2g+4)q^{\frac{n}{2}}$.

Example 5.5. *For small genus, the bound in Lemma 5.4 is relatively sharp. For instance, let K be a purely cubic function field $K = \mathbb{F}_q(X,Y)$ of characteristic different from 3 where $Y^3 = D$, and $D \in \mathbb{F}_q[X]$ is irreducible with $\deg(D) > 1$. Then there are no ramified prime polynomials in $\mathbb{F}_q[x]$ of degree 1. Furthermore, if we assume that $q \equiv 1 \pmod 3$, then all monic prime polynomials $P \in \mathbb{F}_q[x]$ of degree 1 are either inert or totally split (because $K/\mathbb{F}_q(x)$ is a Galois extension), so $z_1(P)^3 = z_2(P)^3 = 1$, and hence*

$S_1(3) = 2I_1 = 2q$. *By Corollary 4.10,*

$$3S_3(1) = -x_1^3 - x_2^3 - \sum_{i=1}^{2g} \alpha_i^3 - S_1(3) = -2 - \sum_{i=1}^{2g} \alpha_i^3 - 2q \ .$$

On the other hand, the bound of Lemma 5.4 yields

$$3|S_3(1)| \leq 2 + 2gq^{\frac{3}{2}} + |S_1(3)| \leq 2 + 2gq^{\frac{3}{2}} + 2q.$$

In this situation, this is the best possible bound, unless we have more information about $|\sum_{i=1}^{2g} \alpha_i^3|$.

Lemma 5.6. *For* $\lambda, n \in \mathbb{N}$ *with* $\lambda < n$, *we have*

$$\Big| \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu \, S_\nu(n/\nu) \Big| < (2g+4) \frac{q}{(q-1)} q^{\frac{n}{2}}.$$

Proof. Note that

$$\sum_{\substack{\nu|n \\ \nu>\lambda}} \nu \, S_\nu(n/\nu) = nS_n(1) + \sum_{\substack{\nu|n \\ \lambda<\nu<n}} \nu \, S_\nu(n/\nu).$$

We can use the result of Lemma 5.4 and proceed as in the proof of that Lemma to obtain

$$\Big| \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu \, S_\nu(n/\nu) \Big| \leq 2 + 2gq^{\frac{n}{2}} + 4\frac{(q^{\frac{n}{2}}-1)q}{(q-1)} < (2g+4)q^{\frac{n}{2}} \frac{q}{(q-1)} \ .$$

□

We use the previous lemma to bound the second summand in (5.3).

Lemma 5.7. *For* $\lambda \in \mathbb{N}$, *we have*

$$\Big| \sum_{n=\lambda+2}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu \, S_\nu(n/\nu) \Big| < \frac{(2g+4)}{(\lambda+2)} \frac{\sqrt{q}}{(\sqrt{q}-1)} \frac{q}{(q-1)} q^{-\frac{\lambda+2}{2}}.$$

Proof. We use Lemma 5.6 to obtain

$$\begin{aligned} \Big| \sum_{n=\lambda+2}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu|n \\ \nu>\lambda}} \nu \, S_\nu(n/\nu) \Big| &\leq (2g+4) \frac{q}{(q-1)} \sum_{n=\lambda+2}^{\infty} \frac{1}{nq^{\frac{n}{2}}} \\ &< \frac{(2g+4)}{(\lambda+2)} \frac{q}{(q-1)} \sum_{n=\lambda+2}^{\infty} \frac{1}{q^{\frac{n}{2}}} \\ &\leq \frac{(2g+4)}{(\lambda+2)} \frac{q}{(q-1)} \frac{\sqrt{q}}{(\sqrt{q}-1)} q^{-\frac{\lambda+2}{2}} \ . \end{aligned}$$

□

We are now able to define an upper bound on $B_2(\lambda, K)$. For $\lambda \in \mathbb{N}$, we define

$$\psi_2(\lambda,K) = \frac{2g}{\lambda+1}q^{-\frac{\lambda+1}{2}} + \frac{(2g+4)}{(\lambda+2)}\frac{\sqrt{q}}{(\sqrt{q}-1)}\frac{q}{(q-1)}q^{-\frac{\lambda+2}{2}} + \frac{2}{\lambda+1}q^{-(\lambda+1)} + \frac{2}{(\lambda+1)}\frac{q}{(q-1)}q^{-(\lambda+1)}\begin{cases}(q^{\frac{\lambda+1}{2}}-1) & \text{if } \lambda \text{ odd},\\ (q^{\frac{\lambda+1}{3}}-1) & \text{if } \lambda \text{ even}.\end{cases}$$

By the previous lemmas and (5.3), we derive that $|B_2(\lambda, K)| < \psi_2(\lambda, K)$. Thus, $\psi_2(\lambda, K)$ is the required bound on $|B_2(\lambda, K)|$. Again, we put

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

Theorem 5.8. *For any $\lambda \in \mathbb{N}$, we have $|h - E_2(\lambda, K)| < L_2^2(\lambda, K)$.*

Theorem 5.9. *For any $\lambda \in \mathbb{N}$, we have*

$$E_2'(\lambda,K) \le \left(\frac{q^{g+2}}{q^2+s_1q+s_2}\right)\left(\frac{\sqrt{q}}{\sqrt{q}-1}\right)^{2g}\left(\frac{q}{q-1}\right)^2 e^{\psi_2(\lambda,K)}.$$

Proof. By (5.1), we have

$$\log E_2'(\lambda,K) = A(K) + \sum_{n=1}^{\infty}\frac{1}{nq^n}\sum_{\nu|n}\nu\, S_\nu(n/\nu) - B_2(\lambda,K).$$

From the proof of Theorem 5.2, it follows that

$$|\log E_2'(\lambda,K)| \le A(K) + 2g\log\left(\frac{\sqrt{q}}{\sqrt{q}-1}\right) + 2\log\left(\frac{q}{q-1}\right) + \psi_2(\lambda,K).$$

This is the statement. □

For small g and large q, we conclude that $E_2(\lambda, K) = O(q^g)$. If $\psi_2(\lambda, K) < 1$, then we have $L_2(\lambda, K) = O(q^{g/2-(\lambda+1)/4})$ as $q \to \infty$.

5.3. **Complexity Analysis and Optimization.** The complexity analysis is analogous to the one in Section 5.1 of [38]. We follow the idea of Sections 3.1 and 3.2. If $g \le 2$, the Hasse-Weil bound (4.3) is best. More precisely, if $g = 1$ or 2 then the total running time for computing an approximation of h, and subsequently finding h, is $O(q^{1/4})$ and $O(q^{3/4})$, respectively. For $g \ge 3$, we put $E = E_2'(\lambda, K)$ and $L = L_2(\lambda, K)$. Since determining E requires the computation of $O(q^\lambda)$ values $z_1(P), z_2(P)$, the estimate on L yields a complexity of $\max\{O(q^\lambda), O(q^{g/2-(\lambda+1)/4})\}$ for finding h. Thus, the optimal choice for λ is

$$\lambda = \begin{cases}\lfloor (2g-1)/5 \rfloor & \text{if } g \equiv 2 \pmod 5,\\ \operatorname{round}((2g-1)/5) & \text{otherwise.}\end{cases} \tag{5.5}$$

This gives a total (expected) running time of

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

where

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

6. The d^{TH} Power Residue Symbol

We saw in the previous sections that in order to obtain explicit formulae for $\zeta_X(s)$ as well as E and L, it is necessary to compute the relevant character of $K/\mathbb{F}_q$. We now explain how to do this in the case where this character is the d^{th} power residue symbol for any $d \in \mathbb{N}$ coprime to q. For $d = 3$, we obtain the scenario of purely cubic function fields. We begin by reviewing the d^{th} power residue symbol in finite fields since it plays an important role here.

Henceforth, let q be a prime power and d a divisor of $q-1$; note that $\mathbb{F}_q$ contains the d^{th} roots of unity. Let $a \in \mathbb{F}_q^*$. Since $a^{q-1} = 1$, $a^{(q-1)/d}$ is a d^{th} root of unity in $\mathbb{F}_q$. Recall that the d^{th} power residue symbol (in $\mathbb{F}_q$) of a is defined to be

$$\left(\frac{a}{q}\right)_d = a^{(q-1)/d}.$$

We also set $(0/q)_d = 0$. Note that for any integer n and any $a \in \mathbb{F}_q$, $(a/q)_d^n = (a/q)_d^{n_d}$ where $n_d \equiv n \pmod d$, so in order to evaluate a power of a residue symbol, one needs to compute no powers higher than $d-1$.

We now extend this notion to polynomials. As usual, write $|F| = q^{\deg(F)}$ for any non-zero polynomial $F \in \mathbb{F}_q[X]$; we note that $|F| - 1$ is always divisible by d. Let $P \in \mathbb{F}_q[X]$ be an irreducible polynomial with coefficients in $\mathbb{F}_q$. Then $L = \mathbb{F}_q[X]/(P)$ is a field with $|P|$ elements, so for any $F \in \mathbb{F}_q[X]$ that is not a multiple of P, $F^{|P|-1} \equiv 1 \pmod P$, and therefore $|F|^{(|P|-1)/d} \equiv \zeta_d \pmod P$ where $\zeta_d \in \mathbb{F}_q$ is a d^{th} root of unity. The *d^{th} power residue symbol* $[F/P]_d$ is defined to be ζ_d if P does not divide F and 0 otherwise; in other words,

$$\left[\frac{F}{P}\right]_d = \zeta_d \ \text{ where } \ F^{\frac{|P|-1}{d}} \equiv \zeta_d \pmod P$$

for any $P, F \in \mathbb{F}_q[X]$ with P irreducible. We see that $[F/P]_d = 0$ if and only if P divides F; otherwise $[F/P]_d$ is a d^{th} root of unity. In particular, $[F/P]_d = 1$ if and only if F is a non-zero d^{th} power modulo P.

In the usual fashion, we now define $[F/PQ]_d = [F/P]_d[F/Q]_d$ for $F, P, Q \in \mathbb{F}_q[X]$ with P, Q irreducible (and not necessarily distinct). This defines the d^{th} power residue symbol $[F/G]_d$ for any polynomials $F, G \in \mathbb{F}_q[X]$. We

summarize some properties that can be found in Propositions 3.2 and 3.4 as well as Theorem 3.5, pp. 24-27, of [32].

Lemma 6.1. *Let $F, F_1, F_2, G \in \mathbb{F}_q[X]$ and $a \in \mathbb{F}_q$. Set $f \equiv \deg(F) \pmod d$ and $g \equiv \deg(G) \pmod d$. Then the following properties hold:*

1. *If $F_1 \equiv F_2 \pmod G$, then $\left[\frac{F_1}{G}\right]_d = \left[\frac{F_2}{G}\right]_d$.*
2. $\left[\frac{F_1F_2}{G}\right]_d = \left[\frac{F_1}{G}\right]_d \left[\frac{F_2}{G}\right]_d$.
3. $\left[\frac{F}{G_1G_2}\right]_d = \left[\frac{F}{G_1}\right]_d \left[\frac{F}{G_2}\right]_d$.
4. $\left[\frac{F}{G}\right]_d = 0$ *if and only if F and G are not coprime.*
5. $\left[\frac{a}{G}\right]_d = \left(\frac{a}{q}\right)_d^g$.
6. $\left[\frac{F}{G}\right]_d = \left(\frac{-1}{q}\right)_d^{fg} \left(\frac{\operatorname{sgn}(F)}{q}\right)_d^g \left(\frac{\operatorname{sgn}(G)}{q}\right)_d^{-f} \left[\frac{G}{F}\right]_d$ *if F and G are coprime.*

Property 6 is known as the *reciprocity law*, and property 5 is sometimes referred to as the *complementary*. Properties 1, 4, 5, and 6 above give rise to the following fast algorithm for evaluating d^{th} power residue symbols when q is even or $(q-1)/d$ is even:

Algorithm. (The d^{th} Power Residue Symbol)
Input: $F, G \in \mathbb{F}_q[X]$, $d \in \mathbb{N}$ with $\gcd(d, q) = 1$.
Output: $e = \left[\frac{F}{G}\right]_d$.

1) If $\gcd(F, G) \neq 1$, then return $e = 0$ and STOP.
2) Set $e = 1$.
3) While $F \notin \mathbb{F}_q^*$ do
   (a) Replace F by $F \pmod G$.
   (b) Set $f \equiv \deg(F) \pmod d$, $g \equiv \deg(G) \pmod d$.
   (c) Multiply e by $\left(\frac{-1}{q}\right)_d^{fg} \left(\frac{\operatorname{sgn}(F)}{q}\right)_d^g \left(\frac{\operatorname{sgn}(G)}{q}\right)_d^{-f}$.
   (d) Swap F and G.
4) Multiply e by $(F/q)_d^g$ where $g \equiv \deg(G) \pmod d$.
5) Return e.

We note that if q and d are both odd (e.g. $d = 3$), then $(-1/q)_d = 1$, in which case the factor $(-1/q)_d^{fg}$ in step 3 (c) can be omitted.

Proposition 6.3. *Algorithm 6.2 is correct and will compute $[F/G]_d$ in $O(\deg(G))$ loop iterations; specifically, its asymptotic running time is the same as the running time for computing $\gcd(F, G)$.*

Proof. Step 1 certainly returns the correct result by property 4. So suppose that F and G are coprime. Steps (a) and (d) of the while loop in step 3 constitute simply the Euclidean Algorithm for computing $\gcd(F, G)$, starting with dividing F by G. So the while loop is executed $O(\deg(G))$ times and terminates with a remainder F that is a constant, since $\gcd(F, G) = 1$.

Now step 3 (a) does not change the value of $[F/G]_d$ by property 1. The reciprocity law (property 6) shows that the value of e is correctly modified in each iteration of the while loop. After the loop, $F \in \mathbb{F}_q^*$, so by property 5, $[F/G]_d$ is obtained by multiplying the current value of e by $[F/G]_d = (F/q)_d^g$ with $g \equiv \deg(G) \pmod{d}$. □

7. Open Problems and Future Research

7.1. **Cubic Function Fields.** The formulae for E and L given in Section 5 are still valid when there are more than two places at infinity. However, in this setting, it is not obvious how to use the baby step giant step or Pollard kangaroo methods to search for h in the interval $]E - L^2, E + L^2[$. The case where there is only one place at infinity, i.e. $\mathcal{O}_X^* = \mathbb{F}_q^*$, simply requires searching in a group; that is, searching on reduced (distinguished) representatives in the ideal class group of $K/k(X)$. When there are two infinite places, i.e. $K/k(X)$ has unit rank 1, the infrastructure as described in [33] can be utilized for the search. But for higher unit rank, it is as yet unclear how to extend these techniques; this question definitely warrants further study.

The analysis of purely cubic function fields of characteristic different from 3 seems to carry over with few changes to the case of arbitrary cubic function fields; an initial investigation was already done in [34] and includes an explicit description of the splitting at infinity. The next step is to find a simple characterization of the splitting of the finite places (work in progress), and to extend the arithmetic and the investigation of the infrastructure given in [33] as well as the algorithms given in this paper from the purely cubic case to the general setting.

We also mention that cubic function fields of characteristic 3 have not been researched at all. Their behavior is very different from that of their counterparts of characteristic different from 3. Examples of such differences include the possibility of wild ramification, and of course there is no analog to the purely cubic scenario; instead, certain cubic curves give rise to Artin-Schreier extensions in this case.

7.2. **Function Fields of Higher Degree.** Contrary to the situation of algebraic number fields, it is possible to construct function field extensions of a given unit rank and arbitrary degree, since there is much more flexibility for the splitting at infinity. Number fields have $e_i f_i = 1$ for real embeddings and $e_i f_i = 2$ for complex embeddings, whilst there is no such restriction on the value of $e_i f_i$ in a function field. For example, the only number fields of unit rank 0 are imaginary quadratic fields, whereas any function field with

only one (totally inert or ramified) place at infinity has unit rank 0; the family of *superelliptic* function fields $K = \mathbb{F}_q(X, Y)$ with $Y^n = D(X)$ and $\gcd(q, n) = \gcd(\deg(D), n) = 1$ studied in [16] represent such examples.

There is a wealth of open problems pertaining to the arithmetic of ideals in both algebraic number fields and algebraic function fields. Two approaches to this topic are prevalent. General purpose methods are applicable to any extension, but they tend to be inefficient. In order to obtain efficiency, one may need to sacrifice generality and focus instead on special purpose techniques. This has already shown to be very successful in the quadratic and cubic scenarios of both number fields and function fields. No other number fields have been studied in any detail, with the exception of quartic fields which were investigated in a series of papers by Buchmann et al. [5, 6, 10, 12, 8, 7, 9]. In addition, a more general treatment of number fields of unit rank 1 (which always exhibit an infrastructure) can be found in [11]. It is worthwhile to explore these ideas for their applicability to function fields. A description of how the analytic class number can be used to find the ideal class number of any number field was given in [11] and has inspired some of the ideas in this article.

8. Acknowledgements

The authors wish to thank an anonymous referee for carefully proofreading the paper and making valuable suggestions. Furthermore, our thanks go to Eric Landquist for suggesting improvements and useful changes to Section 4.

References

1. L. M. Adleman and M.-D. Huang, *Counting rational points on curves and Abelian varieties over finite fields*, Algorithmic Number Theory ANTS-II (Berlin (Germany)), Lect. Notes Comput. Sci., vol. 1122, Springer-Verlag, 1996, pp. 1–16.
2. ———, *Counting points on curves and Abelian varieties over finite fields*, J. Symbolic Comput. **32** (2001), 171–189.
3. M. Bauer, *The arithmetic of certain cubic function fields*, Math. Comp. **73** (2004), 387–413.
4. M. Bauer, E. Teske, and A. Weng, *Point counting on Picard curves in large characteristic*, Math. Comp. **74** (2005), 1983–2005.
5. J. A. Buchmann, *The computation of the fundamental unit of totally complex quartic orders*, Math. Comp. **48** (1987), 39–54.
6. ———, *On the computation of units and class numbers by a generalization of Lagrange's algorithm*, J. Number Theory **26** (1987), 8–30.
7. J. A. Buchmann, D. Ford, and M. Pohst, *Enumeration of quartic fields of small discriminant*, Math. Comp. **61** (1993), 873–879.
8. J. A. Buchmann, M. Pohst, and J. Graf von Schmettow, *On the computation of unit groups and class groups of totally real quartic fields*, Math. Comp. **53** (1989), 387–397.
9. ———, *On unit groups and class groups of quartic fields of signature* $(2, 1)$, Math. Comp. **62** (1994), 387–390.
10. J. A. Buchmann and H. C. Williams, *On principal ideal testing in totally complex quartic fields and the determination of certain cyclotomic constants*, Math. Comp. **48** (1987), 55–66.

11. ———, *On the computation of the class number of an algebraic number field*, Math. Comp. **53** (1988), 679–688.
12. ———, *On the infrastructure of the principal ideal class of an algebraic number field of unit rank one*, Math. Comp. **50** (1988), 569–579.
13. W. Castryck, J. Denef, and F. Vercauteren, *Computing zeta functions of nondegenerate curves*, Internat. Math. Research Papers **Article ID 72017** (2006), 1–57.
14. J. Denef and F. Vercauteren, *An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2*, Algorithmic Number Theory ANTS-V (Berlin (Germany)), Lect. Notes Comput. Sci., vol. 2369, Springer-Verlag, 2002, pp. 308–323.
15. ———, *Counting points on C_{ab} curves using Monsky-Washnitzer cohomology*, Finite Fields Appl. **12** (2006), 78–102.
16. S. D. Galbraith, S. Paulus, and N. P. Smart, *Arithmetic on superelliptic curves*, Math. Comp. **71** (2002), 393–405.
17. P. Gaudry and M. Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in Cryptology – ASIACRYPT 2001 (Berlin (Germany)), Lect. Notes Comput. Sci., vol. 2248, Springer-Verlag, 2001, pp. 480–494.
18. ———, *Counting points in medium characteristic using Kedlaya's algorithm*, Exp. Math. **12** (2003), 395–402.
19. P. Gaudry and R. Harley, *Counting points on hyperelliptic curves over finite fields*, Algorithmic Number Theory ANTS-IV (Berlin (Germany)), Lect. Notes Comput. Sci., vol. 1838, Springer-Verlag, 2000, pp. 313–332.
20. P. Gaudry and É. Schost, *Construction of secure random curves of genus 2 over prime fields*, Advances in Cryptology – Eurocrypt 2004 (Berlin (Germany)), Lect. Notes Comput. Sci., vol. 3027, Springer-Verlag, 2004, pp. 239–256.
21. F. Hess, *Zur divisorklassengruppenberechnung in globalen funktionenkörpern*, Ph.D. thesis, Technische Universität Berlin, Berlin (Germany), 1999.
22. M.-D. Huang and D. Ierardi, *Counting points on curves over finite fields*, J. Symb. Comput. **25** (1998), 1–21.
23. K. S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 323–338.
24. ———, *Errata for "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology"*, J. Ramanujan Math. Soc. **18** (2003), 417–418.
25. ———, *Computing zeta functions via p-adic cohomology*, Algorithmic Number Theory ANTS-VI (Berlin (Germany)), Lect. Notes Comput. Sci., vol. 3076, Springer-Verlag, 2004, pp. 1–17.
26. A. G. B. Lauder and D. Wan, *Computing zeta functions of Artin-Schreier curves over finite fields.*, LMS J. Comput. Math. **5** (2002), 34–55.
27. ———, *Computing zeta functions of Artin-Schreier curves over finite fields. ii*, J. Complexity **20** (2004), 331–349.
28. A. G. B. Lauer, *Computing zeta functions of Kummer curves via multiplicative characters*, Found. Comput. Math. **3** (2003), 273–295.
29. Y. Lee, R. Scheidler, and C. Yarrish, *Computation of the fundamental units and the regulator of a cyclic cubic function field*, Exp. Math. **12** (2003), 211–225.
30. J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), 745–763.
31. ———, *Counting points on curves over families in polynomial time*, eprint arXiv:math/0504570 (2005).
32. M. Rosen, *Number theory in function fields*, Springer-Verlag, Berlin (Germany), 2002.
33. R. Scheidler, *Ideal arithmetic and infrastructure in purely cubic function fields*, J. Théor. Nombr. Bordeaux **13** (2001), 609–631.
34. ———, *Algorithmic aspects of cubic function fields*, Algorithmic Number Theory ANTS-VI (Berlin (Germany)), Lect. Notes Comp. Sci., vol. 3976, Springer-Verlag, 2004, pp. 395–410.

35. R. Scheidler and A. Stein, *Voronoi's algorithm in purely cubic congruence function fields of unit rank 1*, Math. Comp. **69** (2000), 1245–1266.
36. F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math. Zeitschr. **33** (1931), 1–32.
37. R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux **7** (1995), 219–254.
38. A. Stein and E. Teske, *Explicit bounds and heuristics on class numbers in hyperelliptic function fields*, Math. Comp. **71** (2002), 837–861.
39. ———, *The parallelized Pollard kangaroo method in real quadratic function fields*, Math. Comp. **71** (2002), 793–814.
40. ———, *Optimized baby step-giant step methods*, J. Ramanujan Math. Soc. **20** (2005), 27–58.
41. A. Stein and H. C. Williams, *Some methods for evaluating the regulator of a real quadratic function field*, Exper. Math. **8** (1999), 119–133.
42. H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin (Germany), 1993.

Department of Mathematics and Statistics, University of Calgary,
2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada
E-mail address: rscheidl@math.ucalgary.ca

Department of Mathematics, University of Wyoming,
P.O. Box 3036, 1000 E. University Avenue, Laramie, Wyoming 82071-3036, USA
E-mail address: andreas@math.uiuc.edu